



Informatica®
10.5

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, le logo Informatica, Informatica Cloud, PowerCenter et PowerExchange 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.

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: 2021-05-12

Sommaire

Préface.....	11
Ressources Informatica.	11
Informatica Network.	11
Base de connaissances Informatica.	11
Documentation Informatica.	12
Matrices de disponibilité des produits Informatica.	12
Informatica Velocity.	12
Informatica Marketplace.	12
Support client international Informatica.	12
 Chapitre 1: Introduction à la sécurité Informatica.....	 13
Présentation de la sécurité Informatica.	13
Sécurité de l'infrastructure.	14
Authentification.	14
Communication sécurisée du domaine.	15
Stockage de données sécurisé.	16
Sécurité opérationnelle.	16
Référentiel de configuration du domaine.	17
Domaine de sécurité.	17
 Chapitre 2: Authentification utilisateur.....	 19
Présentation de l'authentification utilisateur.	19
Authentification utilisateur native.	20
Authentification utilisateur LDAP.	20
Authentification Kerberos.	21
Authentification SAML pour les applications Web Informatica.	22
 Chapitre 3: Authentification LDAP.....	 23
Présentation.	23
Domaines de sécurité LDAP.	24
Synchronisation des comptes utilisateurs.	24
Services d'annuaire LDAP.	24
Azure Active Directory pour l'authentification LDAP sécurisée.	25
Création d'une configuration LDAP.	26
Créer la configuration LDAP et configurer la connexion au serveur LDAP.	27
Configurer le domaine de sécurité.	28
Configurer le calendrier de synchronisation.	30
Utilisation de groupes imbriqués dans le service d'annuaire LDAP.	31
Utilisation d'un certificat SSL auto-signé.	31
Suppression d'une configuration LDAP.	31

Chapitre 4: Authentification Kerberos.....	33
Présentation de Kerberos.	33
Fonctionnement de Kerberos dans un domaine Informatica.	34
Authentification Kerberos inter-domaines.	36
Conversion d'un domaine de l'authentification Kerberos à domaine unique en authentification Kerberos inter-domaines.	36
Préparation de l'activation de l'authentification Kerberos.	37
Déterminer le niveau de principal du service Kerberos.	37
Configurer le fichier de configuration Kerberos.	38
Création de comptes de principaux Kerberos dans Active Directory.	41
Générer les formats de nom de principal de service et de fichier Keytab.	42
Générer les fichiers Keytab.	48
Activer la délégation pour les comptes utilisateurs de principaux Kerberos dans Active Directory.	52
Activation de l'authentification Kerberos.	53
Activer l'authentification Kerberos dans le domaine.	54
Mise à jour des nœuds dans le domaine.	56
Activation de Kerberos sur les nœuds Informatica.	58
Copier les fichiers Keytab sur les nœuds Informatica.	59
Activer l'authentification Kerberos pour les clients Informatica.	59
Activation des comptes utilisateurs pour utiliser l'authentification Kerberos.	60
Importer des comptes utilisateurs d'Active Directory dans des domaines de sécurité LDAP. . .	60
Migrer les privilèges et autorisations des utilisateurs natifs vers le domaine de sécurité Kerberos.	63
 Chapitre 5: Authentification SAML pour les applications Web Informatica. . .	 66
Présentation de l'authentification SAML.	66
Répertoire du keystore et du truststore par défaut.	67
Fournisseurs d'identité pris en charge.	67
Processus d'authentification SAML.	68
Activer l'authentification SAML dans un domaine.	69
Créer une configuration LDAP pour le fournisseur d'identité ou le magasin LDAP.	69
Exporter le certificat de signature d'assertion.	69
Importer le certificat dans le fichier truststore utilisé pour l'authentification SAML.	70
Configurer le fournisseur d'identité.	70
Ajouter des URL de l'application Web Informatica au fournisseur d'identité.	70
Configurer l'authentification SAML dans le domaine.	70
Activer l'authentification SAML sur les nœuds de passerelle.	71
Sécurité de l'authentification améliorée.	71
Signature de demande.	72
Réponse signée.	73
Assertion chiffrée.	74

Configurer les applications Web pour utiliser des fournisseurs d'identité différents.	74
Préparer l'utilisation d'un fournisseur d'identité.	75
Configurer Informatica Administrator pour utiliser un fournisseur d'identité.	75
Configurer une application Web Informatica.	77

Chapitre 6: Sécurité de domaine..... 79

Présentation de la sécurité de domaine.	79
Communication sécurisée à l'intérieur du domaine.	80
Communication sécurisée pour les services et le gestionnaire de service.	81
Base de données de référentiel de configuration du domaine sécurisée.	88
Base de données de référentiel PowerCenter sécurisée.	90
Base de données du référentiel modèle sécurisée.	91
Communication sécurisée pour les flux de travail et les sessions.	92
Connexions sécurisées à un service d'application Web.	93
Exigences pour les connexions sécurisées aux services d'application Web.	93
Activation des connexions sécurisées sur l'outil Administrator.	94
Services d'applications Web Informatica.	94
Suites de chiffres du domaine Informatica.	97
Créer des listes de suites de chiffres.	97
Configurer le domaine Informatica à l'aide d'une nouvelle liste effective de suites de chiffres.	99
Sources et cibles sécurisées.	100
Sources et cibles du service d'intégration de données.	100
Sources et cibles PowerCenter.	101
Stockage de données sécurisé.	102
Répertoire sécurisé sous UNIX.	102
Modification de la clé de cryptage à partir de la ligne de commande.	103
Services et ports d'application.	106

Chapitre 7: Gestion de la sécurité dans Informatica Administrator..... 109

Présentation de l'utilisation d'Informatica Administrator.	109
Sécurité utilisateur.	110
Cryptage.	110
Authentification.	111
Autorisation.	111
Onglet Sécurité.	112
Utilisation de la section Rechercher.	112
Utilisation du navigateur de sécurité.	113
Groupes.	113
Utilisateurs.	114
Rôles.	114
Profils de système d'exploitation.	115
Configuration LDAP.	115
Gestion des comptes.	115

Rapports d'audit.	116
Gestion du mot de passe.	116
Modification de votre mot de passe.	117
Gestion de la sécurité de domaine.	117
Gestion de la sécurité des utilisateurs.	118

Chapitre 8: Utilisateurs et groupes. 119

Présentation des utilisateurs et des groupes.	119
Groupes par défaut.	120
Groupe d'administration.	120
Groupe Tout le monde.	120
Groupe d'opérateurs.	121
Comprendre les comptes utilisateurs.	121
Administrateur par défaut.	121
Administrateur de domaine.	121
Administrateur de client d'application.	122
Utilisateur.	123
Gestion des utilisateurs.	123
Création d'utilisateurs natifs.	123
Modification des propriétés générales d'utilisateurs natifs.	124
Assignation des utilisateurs natifs aux groupes natifs.	124
Assignation des utilisateurs LDAP aux groupes natifs.	125
Activation et désactivation des comptes utilisateurs.	125
Suppression d'utilisateurs natifs.	125
Utilisateurs LDAP.	126
Déverrouillage d'un compte utilisateur.	126
Augmentation de la mémoire système pour un grand nombre d'utilisateurs.	127
Affichage de l'activité utilisateur.	128
Gestion des groupes.	132
Ajout d'un groupe natif.	132
Modification des propriétés d'un groupe natif.	132
Déplacement d'un groupe natif vers un autre groupe natif.	133
Suppression d'un groupe natif.	133
Groupes LDAP.	133
Gestion des profils de systèmes d'exploitation.	133
Propriétés du profil de système d'exploitation du service d'intégration PowerCenter.	134
Propriétés du profil de système d'exploitation du service d'intégration de données.	136
Propriétés du profil de système d'exploitation du service d'accès aux métadonnées.	138
Création d'un profil de système d'exploitation.	138
Modification d'un profil de système d'exploitation.	140
Attribution d'un profil de système d'exploitation par défaut à un utilisateur ou à un groupe.	140
Suppression d'un profil de système d'exploitation.	141
Utilisation des profils du système d'exploitation dans un domaine sécurisé.	141

Utilisation des profils du système d'exploitation dans un domaine avec l'authentification Kerberos.	142
Verrouillage de compte.	143
Configuration du verrouillage de compte.	143
Règles et directives de verrouillage de compte.	144

Chapitre 9: Privilèges et rôles. 145

Privilèges.	145
Groupes de privilèges.	146
Rôles.	147
Privilèges du domaine.	147
Groupe de privilèges Administration de la sécurité.	147
Groupe de privilèges Administration de domaine.	148
Groupe de privilèges Surveillance.	153
Groupe de privilèges Outils.	154
Groupe de privilèges d'administration Cloud.	155
Privilèges du service Analyst.	155
Privilèges du service de gestion de contenu.	156
Privilèges du service d'intégration de données.	157
Privilège du service d'ingestion de masse.	157
Privilèges du Metadata Manager Service.	158
Groupe de privilèges Catalogue.	158
Groupe de privilèges Chargement.	159
Groupe de privilèges du modèle.	161
Groupe de privilèges Sécurité.	161
Privilèges du service de référentiel modèle.	161
Privilèges du PowerCenter Repository Service.	163
Groupe de privilèges Outils.	163
Groupe de privilèges Dossiers.	164
Groupe de privilèges Objets de conception.	166
Groupe de privilèges Sources et cibles.	168
Groupe de privilèges Objets d'exécution.	170
Groupe de privilèges des objets globaux.	174
Privilèges du service d'écoute PowerExchange.	177
Privilèges du service de journalisation PowerExchange.	177
Privilèges du service de planificateur.	178
Privilèges du service Test Data Manager.	179
Groupe de privilèges Administration.	179
Groupe de privilèges Connexions.	180
Groupe de privilèges Domaines de données.	180
Groupe de privilèges Masquage des données.	181
Groupe de privilèges Sous-ensemble de données.	181
Groupe de privilèges Stratégies.	181

Groupe de privilèges Projets.	182
Groupe de privilèges Règles.	182
Groupe de privilèges Génération de données.	182
Gestion des rôles.	183
Rôles définis par le système.	183
Rôles personnalisés.	184
Attribution de privilèges et de rôles aux utilisateurs et aux groupes.	186
Privilèges hérités.	186
Assignation de privilèges et de rôles à un utilisateur ou un groupe par navigation.	187
Affichage des utilisateurs avec des privilèges pour un service.	188
Dépannage des problèmes de privilèges et de rôles.	188
Chapitre 10: Autorisations.	191
Présentation des autorisations.	191
Types d'autorisations.	192
Filtres de recherche des autorisations.	193
Autorisations d'objets de domaines.	193
Autorisations par objet de domaine.	194
Autorisations par utilisateur ou groupe.	195
Autorisations du profil de système d'exploitation.	196
Autorisations de connexion.	197
Types d'autorisations de connexion.	198
Autorisations de connexion par défaut.	198
Attribution d'autorisations à une connexion.	199
Affichage des détails des autorisations pour une connexion.	199
Modification des autorisations sur une connexion.	199
Autorisations de configuration de grappe.	200
Autorisations d'applications et d'objets d'applications.	200
Types d'autorisations sur les applications et les objets d'application.	201
Attribution d'autorisations sur une application ou un objet d'application.	201
Affichage des détails des autorisations sur une application ou un objet d'application.	201
Modification des autorisations sur une application ou un objet d'application.	202
Refus d'autorisations sur une application ou un objet d'application.	202
Autorisations du service de données SQL.	203
Types d'autorisations de service de données SQL.	203
Attribuer des autorisations pour un service de données SQL.	204
Affichage des détails des autorisations pour un service de données SQL.	204
Modification des autorisations pour un service de données SQL.	205
Refus d'autorisations pour un service de données SQL.	205
Sécurité au niveau des colonnes.	206
Autorisations du service web.	207
Types d'autorisations de service Web.	207
Attribution des autorisations pour un service Web.	208

Affichage des détails des autorisations pour un service Web.	209
Modification des autorisations dans un service Web.	209
Chapitre 11: Rapports d'audit.	211
Présentation des rapports d'audit.	211
Informations personnelles de l'utilisateur.	212
Association de groupes d'utilisateurs.	213
Privilèges.	214
Association de rôles.	214
Autorisation d'objet de domaine.	215
Sélection d'utilisateurs pour un rapport d'audit.	215
Sélection des groupes pour un rapport d'audit	216
Sélection des rôles pour un rapport d'audit.	217
Annexe A: Privilèges et autorisations de ligne de commande.	218
Commandes infacmd as.	218
commandes infacmd cluster.	219
Commandes infacmd dis	220
Commandes infacmd dp.	222
commandes infacmd es.	222
Commandes infacmd ipc.	222
Commandes infacmd isp.	223
Commandes infacmd mas.	233
Commandes infacmd mi.	233
Commandes infacmd mrs.	233
Commandes infacmd ms.	236
Commandes infacmd tools.	236
Commandes infacmd ps.	236
Commandes infacmd pwx.	237
Commandes infacmd rms.	238
Commandes infacmd rtm.	239
Commandes infacmd sch.	239
Commandes infacmd sql.	240
Commandes infacmd wfs.	241
Commandes pmcmd.	241
Commandes pmrep.	244
Annexe B: Rôles personnalisés.	249
Rôle personnalisé du service Analyst.	249
Rôles personnalisés du service Metadata Manager.	250
Rôle personnalisé de l'opérateur.	251
Rôles personnalisés du service de référentiel PowerCenter.	252
Rôles personnalisés du Test Data Manager.	254

Index..... 257

Préface

Utilisez le *Guide de sécurité d'Informatica* pour apprendre à activer la sécurité dans un domaine Informatica. Familiarisez-vous avec la configuration et la gestion des différents protocoles d'authentification, dont le protocole LDAP (Lightweight Directory Access Protocol), Kerberos et le langage SAML (Security Assertion Markup Language). Apprenez à gérer les utilisateurs et les groupes et comment utiliser des autorisations, des privilèges et des rôles pour gérer la sécurité utilisateur.

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 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 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.

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 le réseau Informatica.

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

CHAPITRE 1

Introduction à la sécurité Informatica

Ce chapitre comprend les rubriques suivantes :

- [Présentation de la sécurité Informatica, 13](#)
- [Sécurité de l'infrastructure, 14](#)
- [Sécurité opérationnelle, 16](#)
- [Référentiel de configuration du domaine, 17](#)
- [Domaine de sécurité, 17](#)

Présentation de la sécurité Informatica

Vous pouvez sécuriser le domaine Informatica pour le protéger contre les menaces à l'intérieur et à l'extérieur du réseau sur lequel il s'exécute.

La sécurité du domaine Informatica comprend les types de sécurité suivants :

Sécurité de l'infrastructure

La sécurité de l'infrastructure protège le domaine Informatica contre les accès non autorisés ou la modification des services et des ressources dans le domaine Informatica. La sécurité de l'infrastructure comprend les aspects suivants :

- Protection des données transmises et stockées dans le domaine Informatica
- Authentification des utilisateurs et des services se connectant au domaine Informatica
- Sécurité des connexions pour les composants externes, y compris les applications client et les bases de données relationnelles pour les référentiels, les sources et les cibles.

Sécurité opérationnelle

La sécurité opérationnelle contrôle l'accès aux données et aux services dans le domaine Informatica. La sécurité opérationnelle comprend les aspects suivants :

- Définition de restrictions d'accès aux données et aux métadonnées en fonction du rôle de l'utilisateur dans l'organisation
- Définition de restrictions en matière d'exécution d'opérations dans le domaine Informatica en fonction du rôle de l'utilisateur dans l'organisation

Informatica stocke les informations de configuration du domaine et la liste des utilisateurs autorisés à accéder au domaine dans le référentiel de configuration du domaine. Le référentiel de configuration du

domaine contient également les groupes, les rôles, les privilèges et les autorisations qui sont attribués à chaque utilisateur dans le domaine Informatica.

Informatica organise la liste des utilisateurs par domaine de sécurité. Un domaine de sécurité contient un ensemble de comptes utilisateur. Un domaine peut comporter plusieurs domaines de sécurité.

Sécurité de l'infrastructure

La sécurité de l'infrastructure comprend l'authentification des utilisateurs et des services, la communication sécurisée dans le domaine et le stockage sécurisé des données.

Authentification

Le gestionnaire de service authentifie les services exécutés dans le domaine et les utilisateurs qui se connectent aux outils clients Informatica.

Vous pouvez configurer le domaine Informatica pour utiliser les types d'authentification suivants :

Authentification native

L'authentification native est un mode d'authentification disponible uniquement pour les comptes utilisateur du domaine Informatica. Lorsque le domaine Informatica utilise l'authentification native, le gestionnaire de service stocke les justificatifs d'identité et les privilèges des utilisateurs dans le référentiel de configuration du domaine et effectue l'authentification des utilisateurs dans le domaine Informatica.

Si le domaine Informatica utilise l'authentification native, par défaut, le domaine possède un domaine de sécurité natif et tous les comptes d'utilisateur appartenant au domaine de sécurité natif.

Informatica utilise le nom d'utilisateur et les mots de passe pour authentifier les utilisateurs et les services dans le domaine Informatica.

Authentification Lightweight Directory Access Protocol (LDAP)

LDAP est un protocole logiciel pour l'accès aux utilisateurs et aux ressources sur un réseau. Si le domaine Informatica utilise l'authentification LDAP, les comptes et les justificatifs d'identité des utilisateurs sont stockés dans le service d'annuaire LDAP. Les privilèges et les autorisations des utilisateurs sont stockés dans le référentiel de configuration du domaine. Vous devez synchroniser périodiquement les comptes utilisateur du référentiel de configuration du domaine avec les ceux du service d'annuaire LDAP.

Informatica utilise le nom d'utilisateur et les mots de passe pour authentifier les utilisateurs d'Informatica et les services dans le domaine Informatica.

Authentification Kerberos

Kerberos est un protocole d'authentification réseau qui utilise des tickets pour l'authentification des utilisateurs et des services dans un réseau. Lorsque le domaine Informatica utilise l'authentification Kerberos, les comptes utilisateur et les justificatifs d'identité sont stockés dans la base de données de principaux Kerberos, qui peut être un service d'annuaire LDAP. Les privilèges et les autorisations des utilisateurs sont stockés dans le référentiel de configuration du domaine. Vous devez synchroniser périodiquement les comptes utilisateur du référentiel de configuration du domaine avec les ceux de la base de données de principaux Kerberos.

Informatica utilise les tickets Kerberos pour authentifier les utilisateurs d'Informatica et les services dans le domaine Informatica.

Authentification unique basée sur SAML

Le langage SAML (Security Assertion Markup Language) est un format de données XML utilisé pour échanger les informations d'authentification et d'autorisation entre un fournisseur de service et un fournisseur d'identité. Vous pouvez configurer l'authentification unique basée sur SAML pour les applications Web des outils Administrator tool, Analyst tool et Monitoring tool.

Dans un domaine Informatica, l'application Web Informatica est le fournisseur de service, et Microsoft Active Directory Federation Services (AD FS) est le fournisseur d'identité. Les comptes et les justificatifs d'identité pour les utilisateurs des applications Web Informatica sont stockés dans Microsoft Active Directory. Importez des comptes d'Active Directory vers un domaine de sécurité au sein du domaine Informatica. Vous devez synchroniser régulièrement les comptes utilisateur dans le domaine de sécurité avec ceux du service d'annuaire Active Directory.

Notez que vous ne pouvez pas activer l'authentification unique basée sur SAML dans un domaine Informatica configuré pour utiliser l'authentification Kerberos.

Communication sécurisée du domaine

Le domaine Informatica dispose de plusieurs options pour sécuriser les données et les métadonnées qui sont transmises entre le gestionnaire de service et les services du domaine et des applications clientes. Informatica utilise les protocoles TCP/IP et HTTP pour communiquer entre les composants du domaine et utilise les certificats SSL pour sécuriser la communication entre les services et le gestionnaire de service du domaine.

Le protocole SSL/TLS utilise la cryptographie de clé publique pour crypter et décrypter le trafic réseau. La clé publique utilisée pour crypter et décrypter le trafic est stockée dans un certificat SSL qui peut être auto-signé ou signé. Un certificat auto-signé est signé par son créateur. L'identité du signataire n'étant pas vérifiée, un certificat auto-signé est moins sécurisé qu'un certificat signé. Un certificat signé est un certificat SSL pour lequel l'identité de la personne ayant demandé le certificat est vérifiée par une autorité de certification. Informatica recommande l'utilisation de certificats signés par une autorité de certification afin d'obtenir un niveau de sécurité supérieur.

Un keystore contient des clés privées et des certificats. Il est utilisé pour fournir un justificatif d'identité. Un truststore contient le certificat de serveurs SSL/TLS de confiance. Il est utilisé pour vérifier un justificatif d'identité.

Pour sécuriser des connexions dans le domaine, Informatica requiert des keystores et des truststores au format PEM et JKS. Vous pouvez utiliser les programmes suivants pour créer les fichiers requis :

keytool

Vous pouvez utiliser l'utilitaire de gestion des clés et des certificats Java keytool pour créer un certificat SSL ou une demande de signature de certificat (CSR) ainsi que des fichiers keystore et truststore au format JKS.

L'utilitaire keytool est disponible dans le répertoire suivant sur les nœuds de domaine :

```
<Informatica installation directory>\java\bin
```

Si ces derniers s'exécutent sur AIX, vous pouvez utiliser l'utilitaire keytool fourni avec IBM JDK pour créer un certificat SSL ou une demande de signature de certificat (CSR) ainsi que des fichiers keystore et truststore.

OpenSSL

Vous pouvez utiliser OpenSSL pour créer un certificat SSL ou CSR, ainsi que pour convertir un keystore du format JKS au format PEM.

Pour plus d'informations sur OpenSSL, consultez sa documentation sur le site Web suivant :

<https://www.openssl.org/docs/>

Le type de connexion que vous sécurisez détermine les fichiers requis.

Stockage de données sécurisé

Informatica crypte les données sensibles telles que les mots de passe et les paramètres de connexion sécurisée avant de stocker les données dans le référentiel de configuration du domaine. Informatica enregistre également les fichiers sensibles, comme les fichiers de configuration, dans un répertoire sécurisé.

Sécurité opérationnelle

Vous pouvez attribuer des privilèges, des rôles et des autorisations aux utilisateurs ou aux groupes d'utilisateurs pour gérer le niveau d'accès dont peuvent disposer les utilisateurs et les groupes et la portée des actions que les utilisateurs et les groupes peuvent effectuer dans le domaine.

Vous pouvez utiliser les méthodes suivantes pour gérer l'accès des utilisateurs et des groupes dans le domaine :

Privilèges

Les privilèges déterminent les actions que les utilisateurs peuvent effectuer dans les outils clients Informatica. Vous pouvez attribuer un ensemble de privilèges à un utilisateur pour restreindre l'accès aux services disponibles dans le domaine. Vous pouvez également attribuer des privilèges à un groupe d'utilisateurs pour accorder à tous ses membres le même accès aux services.

Rôles

Un rôle est un ensemble de privilèges que vous pouvez attribuer à des utilisateurs ou à des groupes. Vous pouvez utiliser des rôles pour simplifier la gestion des attributions de privilèges aux utilisateurs. Vous pouvez créer un rôle avec des privilèges limités et l'attribuer aux utilisateurs et aux groupes qui ont un accès restreint aux services du domaine. Vous pouvez également créer des rôles avec des privilèges similaires à attribuer aux utilisateurs et aux groupes qui nécessitent le même niveau d'accès.

Autorisations

Les autorisations définissent le niveau d'accès des utilisateurs à un objet. Un utilisateur ayant le privilège d'effectuer une action spécifique devra en outre disposer de l'autorisation correspondant à un objet particulier pour pouvoir effectuer cette action sur celui-ci. Par exemple, pour gérer un service d'application, un utilisateur doit disposer du privilège de gestion des services et d'une autorisation sur le service d'application spécifique.

Groupe d'administrateurs par défaut

Le domaine Informatica dispose d'un groupe d'administrateurs défini par le système qui comprend l'ensemble des privilèges et autorisations relatifs à un service. Un compte d'utilisateur que vous ajoutez au groupe d'administrateurs possède des privilèges et des autorisations sur tous les services et objets dans le domaine. Lorsque vous installez les services Informatica, le programme d'installation crée un compte d'utilisateur qui appartient au groupe d'administrateurs. Vous pouvez utiliser le compte de l'administrateur par défaut pour vous connecter la première fois à l'outil Administrator.

Référentiel de configuration du domaine

Le référentiel de configuration du domaine contient des informations sur la configuration du domaine et les privilèges et autorisations de l'utilisateur.

Si le domaine Informatica utilise l'authentification utilisateur native, le référentiel de configuration du domaine contient également les justificatifs d'identité de l'utilisateur. Si le domaine utilise l'authentification LDAP ou Kerberos, le référentiel de configuration du domaine ne contient pas les justificatifs d'identité de l'utilisateur. Tous les justificatifs d'identité de l'utilisateur LDAP et Kerberos sont stockés en dehors du domaine Informatica, dans le service d'annuaire LDAP ou la base de données de principaux Kerberos.

Lorsque vous créez le domaine Informatica durant l'installation, le programme d'installation crée un référentiel de configuration du domaine dans une base de données relationnelle. Vous devez spécifier la base de données dans laquelle créer le référentiel de configuration du domaine. Vous pouvez créer le référentiel sur une base de données sécurisée avec le protocole SSL.

Domaine de sécurité

Un domaine de sécurité regroupe des comptes et des groupes d'utilisateurs dans un domaine Informatica.

Le domaine Informatica peut posséder les types suivants de domaines de sécurité :

Domaine de sécurité natif

Le domaine de sécurité natif contient les utilisateurs et les groupes créés et gérés dans l'outil Administrator. Informatica stocke tous les justificatifs d'identité pour des comptes utilisateur dans le domaine de sécurité natif dans le référentiel de configuration du domaine. Par défaut, le domaine de sécurité natif est créé lors de l'installation. Après l'installation, vous ne pouvez pas créer des domaines de sécurité natifs supplémentaires ou supprimer le domaine de sécurité natif.

Si le domaine Informatica utilise l'authentification Kerberos, il n'utilise pas le domaine de sécurité natif.

Domaine de sécurité LDAP

Un domaine de sécurité LDAP contient les utilisateurs et les groupes importés d'un service d'annuaire LDAP. Si le domaine Informatica utilise l'authentification LDAP ou Kerberos, vous pouvez créer un domaine de sécurité LDAP et ajouter des utilisateurs et des groupes que vous importez du service d'annuaire LDAP.

Lorsque vous installez les services Informatica et créez un domaine qui utilise l'authentification native ou LDAP, le programme d'installation crée le domaine de sécurité natif, mais pas de domaine de sécurité LDAP. Vous pouvez créer des domaines de sécurité LDAP après l'installation.

Lorsque vous installez les services Informatica et créez un domaine qui utilise l'authentification Kerberos, le programme d'installation crée les domaines de sécurité LDAP suivants :

- **Domaine de sécurité interne** : Le programme d'installation crée un domaine de sécurité LDAP avec le nom *_infalInternalNamespace*. Le domaine de sécurité *_infalInternalNamespace* contient le compte d'administrateur par défaut que vous créez lors de l'installation. Après l'installation, vous ne pouvez pas ajouter d'utilisateurs au domaine de sécurité *_infalInternalNamespace* ni supprimer le domaine de sécurité.

- **Domaine de sécurité de la zone de l'utilisateur.** Le programme d'installation crée un domaine de sécurité LDAP vide en lui donnant le même nom que la zone de l'utilisateur Kerberos que vous indiquez lors de l'installation. Après l'installation, vous pouvez importer des utilisateurs de la base de données de principaux Kerberos dans le domaine de sécurité de la zone de l'utilisateur. Vous ne pouvez pas supprimer le domaine de sécurité de la zone de l'utilisateur.
Lorsque vous exécutez les programmes de ligne de commande dans un domaine qui utilise l'authentification Kerberos, l'option de domaine de sécurité sera par défaut celle du domaine de sécurité de la zone de l'utilisateur créé lors de l'installation.

Vous pouvez créer et gérer les domaines de sécurité LDAP de la même manière, que le domaine Informatica utilise l'authentification LDAP ou l'authentification Kerberos.

CHAPITRE 2

Authentification utilisateur

Ce chapitre comprend les rubriques suivantes :

- [Présentation de l'authentification utilisateur, 19](#)
- [Authentification utilisateur native, 20](#)
- [Authentification utilisateur LDAP, 20](#)
- [Authentification Kerberos, 21](#)
- [Authentification SAML pour les applications Web Informatica, 22](#)

Présentation de l'authentification utilisateur

L'authentification utilisateur dans le domaine Informatica dépend du type d'authentification que vous configurez lorsque vous installez les services Informatica.

Le domaine Informatica peut utiliser les types d'authentification suivants pour authentifier les utilisateurs :

- Authentification utilisateur native
- Authentification utilisateur LDAP
- Authentification réseau Kerberos
- Authentification unique basée sur SAML (Security Assertion Markup Language)

Les comptes d'utilisateurs natifs sont stockés dans le domaine Informatica et peuvent uniquement être utilisés dans ce domaine.

Les comptes LDAP, Kerberos et d'utilisateurs sont stockés dans un service d'annuaire LDAP et sont partagés par des applications de l'entreprise.

L'authentification unique basée sur SAML authentifie les utilisateurs à l'aide de justificatifs d'identité de compte stockés dans Microsoft Active Directory. Les comptes sont importés à partir d'Active Directory vers un domaine de sécurité au sein du domaine Informatica.

Vous pouvez sélectionner le type d'authentification à utiliser dans le domaine Informatica lors de l'installation. Si vous activez l'authentification Kerberos pendant l'installation, vous devez configurer le domaine Informatica afin qu'il travaille avec le centre de distribution de clés (KDC) Kerberos. Vous devez créer les noms des principaux du service (SPN) requis par le domaine Informatica dans la base de données des principaux Kerberos. La base de données de principaux Kerberos peut être un service d'annuaire LDAP. Vous devez également créer les fichiers keytab pour les SPN et les stocker dans le répertoire Informatica, comme requis par le domaine Informatica.

Si vous n'activez pas l'authentification Kerberos lors de l'installation, le programme d'installation configure le domaine Informatica pour utiliser l'authentification native. Après l'installation, vous pouvez configurer une

connexion à un serveur LDAP et configurer le domaine Informatica pour utiliser l'authentification LDAP en plus de l'authentification native.

Vous pouvez utiliser à la fois l'authentification native et l'authentification LDAP dans le domaine Informatica. Le gestionnaire de service authentifie les utilisateurs en fonction du domaine de sécurité. Si un utilisateur appartient au domaine de sécurité natif, le gestionnaire de service l'authentifie dans le référentiel de configuration du domaine. Si l'utilisateur appartient à un domaine de sécurité LDAP, le gestionnaire de service transmet son nom et son mot de passe au serveur LDAP pour authentification.

Vous ne pouvez pas utiliser l'authentification native avec l'authentification Kerberos. Si le domaine Informatica utilise l'authentification Kerberos, tous les comptes utilisateur doivent se trouver dans des domaines de sécurité LDAP. Le serveur Kerberos authentifie un compte d'utilisateur lorsque l'utilisateur se connecte au réseau. Les applications clientes Informatica utilisent les justificatifs d'identité de la connexion réseau pour authentifier les utilisateurs dans le domaine Informatica. Les groupes et les rôles natifs sont toujours pris en charge.

Vous pouvez activer l'authentification unique basée sur SAML pour les applications Web Informatica pendant ou après l'installation. Néanmoins, vous devez compléter toutes les tâches de configuration requises avant d'activer l'authentification unique basée sur SAML. Vous ne pouvez pas activer l'authentification unique basée sur SAML dans un domaine Informatica configuré pour utiliser l'authentification Kerberos.

Vous pouvez chiffrer le jeton d'informations d'identification de l'utilisateur avec la clé de site unique. Pour chiffrer le jeton d'informations d'identification de l'utilisateur, définissez la variable d'environnement `infaEnableAdvancedEncryptionSchemeForCredential` sur `True`. En cas d'authentification utilisateur native et LDAP, après une authentification utilisateur réussie, le jeton d'informations d'identification chiffré est utilisé à la place du mot de passe utilisateur.

Authentification utilisateur native

Si le domaine Informatica utilise l'authentification native, le gestionnaire de service stocke toutes les informations du compte utilisateur et effectue toutes les authentifications utilisateur dans le domaine Informatica. Lorsqu'un utilisateur se connecte, le gestionnaire de service utilise le domaine de sécurité natif pour authentifier le nom et le mot de passe de l'utilisateur.

Si vous ne configurez pas le domaine Informatica de manière qu'il utilise l'authentification réseau Kerberos, ce domaine contient un domaine de sécurité natif par défaut. Le domaine de sécurité natif est créé au moment de l'installation et ne peut pas être supprimé. Un domaine Informatica ne peut posséder qu'un seul domaine de sécurité natif. Vous créez et gérez les comptes utilisateur du domaine de sécurité natif dans l'outil Administrator. Le gestionnaire de service stocke les informations concernant les comptes utilisateur, y compris les justificatifs d'identité et les privilèges, dans le référentiel de configuration du domaine.

Authentification utilisateur LDAP

Vous pouvez configurer un domaine Informatica pour permettre aux utilisateurs figurant dans un service d'annuaire LDAP de se connecter aux applications clientes Informatica. Vous pouvez créer plusieurs configurations LDAP pour un domaine, chacune se connectant à un serveur LDAP différent. Un domaine peut utiliser l'authentification utilisateur LDAP en plus de l'authentification utilisateur native.

Pour permettre au domaine Informatica d'utiliser l'authentification utilisateur LDAP, vous devez configurer une connexion à un serveur LDAP et indiquer les utilisateurs et les groupes du service d'annuaire LDAP qui

peuvent accéder au domaine Informatica. Vous pouvez utiliser l'outil Administrator pour définir la connexion au serveur LDAP.

Lorsque vous synchronisez les domaines de sécurité LDAP avec le service d'annuaire LDAP, le gestionnaire de service importe la liste des comptes d'utilisateur LDAP avec accès au domaine Informatica dans les domaines de sécurité LDAP. Lorsque vous attribuez des privilèges et des autorisations aux utilisateurs dans les domaines de sécurité LDAP, le gestionnaire de service stocke les informations dans le référentiel de configuration du domaine. Le gestionnaire de service ne stocke pas les justificatifs d'identité de l'utilisateur dans le référentiel de configuration du domaine.

Lorsqu'un utilisateur se connecte, le gestionnaire de service transmet son nom et son mot de passe au serveur LDAP pour authentification.

Remarque: Le gestionnaire de service requiert que les utilisateurs LDAP se connectent à une application client à l'aide d'un mot de passe, même si un service d'annuaire LDAP permet éventuellement de laisser le mot de passe vide pour le mode de connexion anonyme.

Authentification Kerberos

Vous pouvez configurer le domaine Informatica pour qu'il utilise l'authentification réseau Kerberos afin d'authentifier les utilisateurs et les services d'un réseau.

Kerberos est un protocole d'authentification réseau qui utilise des tickets afin d'authentifier l'accès aux services et aux nœuds dans un réseau. Kerberos utilise un centre de distribution de clés (KDC) pour valider les identités des utilisateurs et des services et pour accorder des tickets aux comptes utilisateur et de service authentifiés. Dans le protocole Kerberos, les utilisateurs et les services sont appelés « principaux ». Le KDC dispose d'une base de données de principaux et de leurs clés secrètes associées, utilisées comme preuve de leur identité. Kerberos peut utiliser un service d'annuaire LDAP en tant que base de données de principaux.

Pour utiliser l'authentification Kerberos, vous devez installer et exécuter le domaine Informatica sur un réseau qui utilise l'authentification réseau Kerberos. Informatica peut s'exécuter sur un réseau qui utilise l'authentification Kerberos avec le service Microsoft Active Directory en tant que base de données de principaux.

Vous pouvez configurer un domaine Informatica pour utiliser l'authentification Kerberos inter-domaines. Ce type d'authentification permet aux clients Informatica, qui appartiennent à un domaine Kerberos, de s'authentifier auprès des nœuds et des services d'application qui appartiennent à un autre domaine Kerberos.

Le domaine Informatica requiert des fichiers Keytab pour authentifier les nœuds et les services du domaine sans transmettre de mots de passe sur le réseau. Les fichiers Keytab contiennent les noms de principaux de service (SPN) et les clés cryptées associées. Créez les fichiers Keytab avant de créer des nœuds et des services dans le domaine Informatica.

Authentification SAML pour les applications Web Informatica

Vous pouvez configurer un domaine Informatica pour permettre aux utilisateurs de se connecter aux applications Web des outils Administrator tool, Analyst tool, Ingestion de masse, Metadata Manager et Surveillance à l'aide de l'authentification SAML (Security Assertion Markup Language).

Le langage SAML (Security Assertion Markup Language) est un format de données XML utilisé pour échanger les informations d'authentification et d'autorisation entre un fournisseur de service et un fournisseur d'identité. Dans un domaine Informatica, l'application Web Informatica est le fournisseur de service. Microsoft Active Directory Federation Services (AD FS) est le fournisseur d'identité, qui authentifie les utilisateurs d'applications Web auprès du magasin d'identités Active Directory de votre organisation.

Pour activer le domaine Informatica pour l'utilisation de l'authentification unique basée sur SAML, vous devez créer un domaine de sécurité LDAP pour les comptes d'utilisateurs d'application Web Informatica, puis importer les utilisateurs dans le domaine à partir d'Active Directory. Vous pouvez utiliser l'outil Administrator tool pour configurer la connexion au serveur Active Directory, puis importer les utilisateurs dans le domaine de sécurité.

Lorsqu'un utilisateur se connecte à une application Web Informatica, l'application envoie une demande d'authentification SAML à AD FS. AD FS authentifie les justificatifs d'identité de l'utilisateur par rapport aux informations du compte d'utilisateur dans Active Directory, puis renvoie à l'application Web un jeton d'assertion SAML contenant des informations de sécurité de l'utilisation.

Configurez AD FS pour qu'il envoie les jetons SAML utilisés pour authentifier les utilisateurs d'applications Web Informatica. Vous devez également exporter le certificat de signature d'assertion du fournisseur d'identité à partir d'AD FS, puis importer le certificat dans le fichier truststore Informatica par défaut sur chacun des nœuds de passerelle dans le domaine.

CHAPITRE 3

Authentification LDAP

Ce chapitre comprend les rubriques suivantes :

- [Présentation, 23](#)
- [Domaines de sécurité LDAP, 24](#)
- [Synchronisation des comptes utilisateurs, 24](#)
- [Services d'annuaire LDAP, 24](#)
- [Azure Active Directory pour l'authentification LDAP sécurisée, 25](#)
- [Création d'une configuration LDAP, 26](#)
- [Suppression d'une configuration LDAP, 31](#)

Présentation

Vous pouvez configurer un domaine Informatica pour permettre aux utilisateurs importés d'un ou de plusieurs services d'annuaire LDAP de se connecter aux nœuds, services et clients d'application Informatica tels qu'Informatica Developer et Informatica Analyst.

Un service d'annuaire LDAP stocke les noms d'utilisateur et les mots de passe des comptes. L'utilisation de l'authentification LDAP vous permet de consolider les informations d'identification de tous vos utilisateurs Informatica dans un seul magasin d'identité, ce qui simplifie la tâche de création et de mise à jour des informations d'identification de compte.

Vous pouvez utiliser à la fois l'authentification native et l'authentification LDAP dans un domaine Informatica. Le gestionnaire de service qui s'exécute sur le nœud de passerelle principal du domaine authentifie les utilisateurs en fonction du domaine de sécurité auquel ils appartiennent. Si un utilisateur appartient au domaine de sécurité natif par défaut, le gestionnaire de service l'authentifie en fonction des informations de compte dans le référentiel de configuration du domaine. Si l'utilisateur appartient à un domaine de sécurité LDAP, le gestionnaire de service transmet ses informations d'identification au serveur LDAP pour authentification.

Domaines de sécurité LDAP

Un domaine de sécurité LDAP contient les utilisateurs et les groupes importés d'un service d'annuaire LDAP. Vous pouvez définir plusieurs domaines de sécurité LDAP au sein d'un domaine Informatica. Vous pouvez ensuite importer des comptes depuis les services d'annuaire LDAP dans les domaines de sécurité.

Vous devez créer un domaine de sécurité LDAP si vous configurez un domaine Informatica pour utiliser l'authentification Kerberos. Lorsque vous installez les services Informatica et activez l'authentification Kerberos, le programme d'installation Informatica crée un domaine de sécurité LDAP avec le nom de la zone Kerberos que vous indiquez lors de l'installation.

Lorsque vous créez un domaine de sécurité LDAP, vous configurez des bases de recherche et des filtres qui définissent l'ensemble des comptes utilisateurs et des groupes LDAP à inclure dans le domaine de sécurité. Le gestionnaire de service utilise la configuration du domaine de sécurité pour importer ou synchroniser des utilisateurs et des groupes du domaine de sécurité avec des utilisateurs et des groupes du service d'annuaire LDAP.

Le gestionnaire de service utilise les critères suivants lorsqu'il importe ou synchronise des utilisateurs et des groupes au sein d'un domaine de sécurité LDAP :

- Le gestionnaire de service utilise les bases de recherche d'utilisateurs et les filtres pour importer les comptes utilisateurs.
- Le gestionnaire de service utilise les bases de recherche et les filtres de groupes pour importer des groupes.
- Le gestionnaire de service importe les groupes inclus dans le filtre de groupes et les comptes d'utilisateurs inclus dans le filtre d'utilisateurs.

Synchronisation des comptes utilisateurs

Le gestionnaire de service met à jour le domaine de sécurité avec les utilisateurs et les groupes d'un service d'annuaire LDAP. Vous pouvez configurer la planification de la synchronisation lorsque vous configurez l'authentification LDAP.

Le gestionnaire de service effectue les étapes suivantes lors de la synchronisation :

- Récupère une liste mise à jour d'utilisateurs et de groupes du service d'annuaire LDAP, en fonction de la base de recherche et des filtres que vous avez configurés pour le domaine de sécurité.
- Met à jour la liste des utilisateurs et des groupes LDAP du domaine de sécurité. Si un utilisateur LDAP du domaine de sécurité a été supprimé du service d'annuaire LDAP, le gestionnaire de service transfère la propriété des objets de l'utilisateur au compte d'administrateur du domaine.

Services d'annuaire LDAP

Vous pouvez importer des comptes utilisateur depuis des services d'annuaire LDAP dans des domaines de sécurité Informatica.

Vous pouvez importer des utilisateurs à partir des services d'annuaire LDAP suivants :

- IBM Tivoli Directory Server

- Microsoft Active Directory
- Microsoft Azure Active Directory
- Novell eDirectory
- OpenLDAP
- Oracle Directory Server (ODSEE)
- Oracle Unified Directory (OUD)
- Sun Java System Directory Server

Remarque: Si vous utilisez l'authentification Kerberos, vous pouvez importer des utilisateurs uniquement à partir de Microsoft Active Directory.

Le gestionnaire de service exige un ID unique (UID) spécifique pour identifier les utilisateurs dans chaque service d'annuaire LDAP. Le tableau suivant indique l'UID par défaut pour chaque service d'annuaire LDAP :

Service d'annuaire LDAP	UID
IBM Tivoli Directory Server	uid
Microsoft Active Directory	sAMAccountName
Microsoft Azure Active Directory	UserPrincipalName
Novell eDirectory	uid
OpenLDAP	uid
Oracle Directory Server (ODSEE)	uid
Oracle Unified Directory (OUD)	uid
Sun Java System Directory Server	uid

Azure Active Directory pour l'authentification LDAP sécurisée

Vous pouvez importer des utilisateurs depuis Azure Active Directory (Azure AD) dans un domaine de sécurité LDAP.

Azure Active Directory Domain Services fournit une adresse IP publique LDAP sécurisée que vous utilisez pour importer les comptes utilisateurs d'Azure Active Directory dans un domaine de sécurité LDAP. Les utilisateurs que vous importez peuvent utiliser leurs identifiants LDAP pour se connecter aux nœuds, services et applications Informatica exécutés sur des machines virtuelles dans un domaine géré par Azure Active Directory.

Vous devez activer l'authentification Secure Lightweight Directory Access Protocol (LDAP sécurisé) dans Azure Active Directory Domain Services pour authentifier les utilisateurs Informatica.

Effectuez les étapes suivantes pour préparer l'importation des comptes utilisateurs d'Azure Active Directory dans un domaine Informatica :

1. Vérifiez que le port 636, qui est le port LDAP sécurisé d'Azure Active Directory, est accessible à travers votre pare-feu.
2. Activez l'authentification LDAP sécurisée dans Azure Active Directory Domain Services.
Utilisez le portail Azure pour activer le protocole LDAP sécurisé dans Azure Active Directory Domain Services. Pour plus d'informations sur la configuration du protocole LDAP sécurisé dans Azure Active Directory Domain Services, consultez le lien suivant :
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-configure-secure-ldap>
3. Lorsque vous configurez le certificat LDAP sécurisé dans Azure Active Directory Domain Services, assurez-vous que le nom du sujet sur le certificat est le nom de domaine complètement qualifié (FQDN) d'Azure Active Directory.
4. Convertissez le certificat LDAP sécurisé du format PFX au format PEM. Java nécessite que le certificat soit au format PEM.
5. Importez les certificats utilisés par tous les nœuds de domaine dans le fichier truststore `cacerts` Java dans le répertoire suivant sur un nœud de passerelle unique du domaine :
`<répertoire d'installation Informatica>/java/jre/lib/security/`
6. Copiez le fichier `cacerts` qui contient les certificats importés dans le même répertoire sur chaque autre nœud de passerelle du domaine.
7. Ajoutez l'adresse IP publique Azure Active Directory et le nom de domaine complètement qualifié (FQDN) d'Azure Active Directory au fichier `/etc/hosts` sur chaque nœud de passerelle du domaine. Utilisez le format suivant :
`<Adresse IP de l'hôte Azure Active Directory> ldaps.<FQDN d'Azure Active Directory>`

Création d'une configuration LDAP

Vous pouvez créer une ou plusieurs configurations LDAP pour permettre l'authentification des comptes utilisateur et des groupes d'utilisateurs importés depuis les services d'annuaire LDAP avec un domaine Informatica.

Créez et gérez les utilisateurs et les groupes LDAP dans le service d'annuaire LDAP. Vous configurez une connexion au serveur d'annuaire LDAP et utilisez les filtres de recherche pour spécifier les utilisateurs et les groupes dont vous souhaitez l'accès au domaine Informatica. Vous importez ensuite les comptes utilisateur dans un domaine de sécurité LDAP. Si le serveur LDAP utilise le protocole SSL, vous devez également spécifier l'emplacement du certificat SSL.

Lorsque vous importez des utilisateurs dans un domaine de sécurité LDAP, vous pouvez leur attribuer des rôles, des privilèges et des autorisations. Vous pouvez attribuer des comptes utilisateur LDAP aux groupes natifs pour les organiser en fonction de leurs rôles dans le domaine Informatica.

Vous ne pouvez pas utiliser l'outil Administrator tool pour créer, modifier ou supprimer des utilisateurs et groupes dans un domaine de sécurité LDAP. Vous devez apporter les modifications aux utilisateurs et groupes LDAP dans le service d'annuaire LDAP, puis synchroniser le domaine de sécurité LDAP avec le service d'annuaire LDAP.

Utilisez la boîte de dialogue Configuration LDAP pour définir la connexion au service d'annuaire LDAP et créer le domaine de sécurité LDAP dans lequel importer les comptes utilisateur. Vous pouvez également utiliser la boîte de dialogue Configuration LDAP pour configurer une planification de synchronisation.

Pour créer une configuration LDAP, effectuez les étapes suivantes :

1. Configurez la connexion au serveur LDAP contenant le service d'annuaire à partir duquel vous voulez importer les comptes utilisateur et les groupes.
2. Créez un domaine de sécurité LDAP pour chaque ensemble de comptes utilisateur et de groupes à importer à partir du service d'annuaire LDAP.
3. Configurez une planification pour le gestionnaire de service afin de mettre à jour les domaines de sécurité LDAP avec des utilisateurs et des groupes nouveaux ou modifiés dans le service d'annuaire LDAP.

Créer la configuration LDAP et configurer la connexion au serveur LDAP

Créez la configuration LDAP et configurez la connexion au serveur LDAP contenant le service d'annuaire à partir duquel vous voulez importer les comptes utilisateur.

Lorsque vous configurez la connexion au serveur LDAP, indiquez que le gestionnaire de service ne doit pas tenir compte de la casse des attributs de nom unique des comptes utilisateur LDAP lorsqu'il affecte des utilisateurs aux groupes dans le domaine Informatica. Si le gestionnaire de service tient compte de la casse, il risque de ne pas affecter tous les utilisateurs qui appartiennent à un groupe.

Si le serveur LDAP utilise SSL, vous devez importer le certificat utilisé par chaque nœud de domaine dans le fichier truststore `cacerts` sur un domaine de nœud de passerelle. Vous copiez ensuite le fichier `cacerts` qui contient les certificats importés dans le même répertoire sur chaque nœud du domaine. Pour plus d'informations, voir ["Utilisation d'un certificat SSL auto-signé" à la page 31](#)

Pour configurer une connexion au service d'annuaire LDAP, procédez comme suit :

1. Dans l'outil Administrator, cliquez sur l'onglet **Sécurité**.
2. Cliquez sur l'onglet **Configuration LDAP**.
3. Cliquez sur le menu **Actions**, puis sélectionnez **Créer une configuration LDAP**.
4. Dans la boîte de dialogue **Créer une configuration LDAP**, cliquez sur l'onglet **Connectivité LDAP**.
5. Configurez les propriétés de la connexion pour le serveur LDAP.

Vous devrez peut-être consulter l'administrateur LDAP pour obtenir les informations nécessaires à la connexion au serveur LDAP.

Le tableau suivant décrit les propriétés de configuration du serveur LDAP :

Propriété	Description
Nom de la configuration LDAP	Nom de la configuration LDAP.
Nom du serveur	Nom d'hôte ou adresse IP de la machine qui héberge le service d'annuaire LDAP.
Port	Port d'écoute du serveur LDAP. Numéro de port permettant de communiquer avec le service d'annuaire LDAP. Généralement, le numéro de port du serveur LDAP est 389. Si le serveur LDAP utilise SSL, le numéro de port du serveur LDAP est 636. Le numéro de port maximum est 65535.

Propriété	Description
Service d'annuaire LDAP	Type de service d'annuaire LDAP. Remarque: Si vous utilisez l'authentification Kerberos, vous devez sélectionner le service Microsoft Active Directory.
Nom	Nom unique (DN) de l'utilisateur principal. Le nom d'utilisateur est souvent composé d'un nom commun (CN), d'une organisation (O) et d'un pays (C). Le nom d'utilisateur principal est un utilisateur administratif avec accès à l'annuaire. Indiquez un utilisateur qui est autorisé à lire d'autres entrées utilisateurs dans le service d'annuaire LDAP. Pour vous connecter à Azure Active Directory, spécifiez le nom d'utilisateur principal (UPN) de l'utilisateur principal.
Mot de passe	Mot de passe de l'utilisateur principal. Laissez le champ vide pour vous connecter anonymement.
Utiliser le certificat SSL	Indique que le serveur LDAP utilise le protocole SSL (Secure Socket Layer).
Certificat LDAP d'approbation	Détermine si le gestionnaire de service peut se fier au certificat SSL du serveur LDAP. Si cette option est sélectionnée, le gestionnaire de service se connecte au serveur LDAP sans vérifier le certificat SSL. Sinon, le gestionnaire de service vérifie que le certificat SSL est signé par une autorité de certification avant de se connecter au serveur LDAP.
Non sensible à la casse	Indique que le gestionnaire de service ne doit pas tenir compte de la sensibilité à la casse pour les attributs de noms uniques lors de l'assignation d'utilisateurs aux groupes.
Attribut d'appartenance à un groupe	Nom de l'attribut qui contient les informations d'appartenance au groupe d'un utilisateur. Attribut de l'objet de groupe LDAP qui contient les DN des utilisateurs et des groupes membres d'un groupe. Par exemple, <i>member</i> ou <i>memberof</i> .
Taille maximale	Nombre maximal de comptes utilisateurs à importer dans un domaine de sécurité. Par exemple, si la valeur est définie sur 100, vous pouvez importer un maximum de 100 comptes utilisateurs dans le domaine de sécurité. Si le nombre d'utilisateurs à importer dépasse la valeur de cette propriété, le gestionnaire de service génère un message d'erreur et n'importe pas d'utilisateurs. Définissez une valeur plus importante pour cette propriété si vous avez de nombreux utilisateurs à importer. La valeur par défaut est 1000.

6. Cliquez sur **Tester la connexion** pour vérifier que la connexion au serveur LDAP est valide.
7. Cliquez sur **OK** pour enregistrer la configuration LDAP.

Configurer le domaine de sécurité

Créez un domaine de sécurité LDAP pour chaque ensemble de comptes utilisateur et de groupes à importer à partir du service d'annuaire LDAP. Configurez les bases et filtres de la recherche pour définir l'ensemble des comptes d'utilisateurs et groupes à inclure dans un domaine de sécurité.

Les noms d'utilisateurs et de groupes à importer depuis le service d'annuaire LDAP doivent être conformes aux mêmes règles que les noms des utilisateurs et groupes natifs. Le gestionnaire de service n'importe pas les utilisateurs ou groupes LDAP si les noms ne sont pas conformes aux règles des noms d'utilisateurs et de groupes natifs. Notez que contrairement aux noms d'utilisateur natifs, les noms d'utilisateur LDAP peuvent être sensibles à la casse.

Le gestionnaire de service utilise les bases et filtres de la recherche des utilisateurs pour importer les comptes d'utilisateurs ainsi que les bases et filtres de la recherche des groupes pour importer des groupes. Le gestionnaire de service utilise les filtres pour importer les groupes et la liste des utilisateurs appartenant à chaque groupe.

Si vous modifiez les propriétés de la connexion LDAP pour vous connecter à un serveur LDAP différent, le gestionnaire de service ne supprime pas les domaines de sécurité existants. Vous devez vous assurer que les domaines de sécurité LDAP sont corrects pour le nouveau serveur LDAP. Modifiez les filtres d'utilisateurs et de groupes dans les domaines de sécurité ou créez des domaines de sécurité supplémentaires pour que le gestionnaire de service importe correctement les utilisateurs et les groupes à utiliser dans le domaine Informatica.

Pour configurer un domaine de sécurité LDAP, procédez comme suit :

1. Dans l'outil Administrator, cliquez sur l'onglet **Sécurité**.
2. Cliquez sur le menu **Actions**, puis sélectionnez **Configuration LDAP**.
3. Dans la boîte de dialogue **Configuration LDAP**, cliquez sur l'onglet **Domaines de sécurité**.
4. Cliquez sur **Ajouter**.

Le tableau suivant décrit les propriétés de filtre que vous pouvez définir pour un domaine de sécurité :

Propriété	Description
Domaine de sécurité	Nom du domaine de sécurité LDAP. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. La chaîne ne peut pas dépasser 128 caractères ni contenir les caractères spéciaux suivants : , + / < > @ ; \ % ? Le nom peut inclure des espaces ASCII, sauf en première et en dernière position. Tous les autres caractères d'espacement sont interdits.
Base de recherche des utilisateurs	Le nom unique (DN) de l'entrée sert de point de départ pour rechercher les noms d'utilisateurs dans le service d'annuaire LDAP. La recherche s'effectue sur un objet dans l'annuaire selon le chemin d'accès dans le nom unique de l'objet. Par exemple, dans Microsoft Active Directory, le nom unique d'un objet utilisateur peut être cn=UserName,ou=OrganizationalUnit,dc=DomainName, où la série des noms uniques relatifs indiqués par dc=DomainName identifie le domaine DNS de l'objet.
Filtre d'utilisateurs	Une chaîne de requête LDAP qui spécifie les critères de recherche pour les utilisateurs dans le service d'annuaire. Le filtre peut indiquer les types d'attributs, les valeurs d'assertion et les critères de correspondance. Par exemple : (objectclass=*) recherche tous les objets. ((&(objectClass=user)(!(cn=susan))) recherche tous les objets utilisateurs sauf « susan ». Pour plus d'informations sur les filtres de recherche, consultez la documentation du service d'annuaire LDAP.
Base de recherche des groupes	Le nom unique (DN) de l'entrée sert de point de départ pour rechercher les noms de groupes dans le service d'annuaire LDAP.
Filtre de groupes	Chaîne de requête LDAP qui spécifie les critères de recherche pour les groupes dans le service d'annuaire.

5. Cliquez sur **Aperçu** pour afficher un sous-ensemble de la liste d'utilisateurs et de groupes qui relèvent des paramètres de filtre.

Si l'aperçu n'affiche pas l'ensemble d'utilisateurs et de groupes, modifiez les filtres d'utilisateurs et de groupes et les bases de la recherche pour obtenir les utilisateurs et groupes corrects.

6. Pour synchroniser immédiatement les utilisateurs et les groupes des domaines de sécurité avec ceux du service d'annuaire LDAP, cliquez sur **Synchroniser maintenant**.

Le gestionnaire de service synchronise les utilisateurs de tous les domaines de sécurité LDAP avec ceux du service d'annuaire LDAP. La durée de la synchronisation dépend du nombre d'utilisateurs et de groupes à importer.

7. Cliquez sur **OK** pour enregistrer le domaine de sécurité.

Configurer le calendrier de synchronisation

Vous pouvez configurer une planification quotidienne pour le gestionnaire de service afin de mettre à jour les domaines de sécurité LDAP avec des utilisateurs et des groupes nouveaux ou modifiés dans le service d'annuaire LDAP.

Lorsque le gestionnaire de service synchronise les domaines de sécurité LDAP avec le service d'annuaire LDAP, il importe tous les utilisateurs correspondant aux paramètres de filtrage d'utilisateurs du service d'annuaire LDAP dans le domaine de sécurité. Le gestionnaire de service importe ensuite tous les groupes correspondant aux paramètres de filtre de groupes et associe les utilisateurs aux groupes correspondants. Le gestionnaire de service supprime également tout utilisateur ou groupe non trouvé dans le service d'annuaire LDAP du domaine de sécurité.

Par défaut, aucune heure n'est planifiée dans le gestionnaire de service pour une synchronisation avec le service d'annuaire LDAP. Pour vous assurer que la liste des utilisateurs et des groupes des domaines de sécurité LDAP est exacte, planifiez le moment où le gestionnaire de service synchronise les domaines de sécurité LDAP avec le service d'annuaire LDAP. Le gestionnaire de service synchronise les domaines de sécurité LDAP avec le service d'annuaire LDAP tous les jours aux heures que vous définissez.

Pour vous assurer que la synchronisation réussit, prenez en compte les recommandations suivantes avant de configurer la planification de la synchronisation :

Vérifiez que le fichier `/etc/hosts` contient une entrée pour le serveur LDAP.

Vérifiez que le fichier `/etc/hosts` sur chaque passerelle de nœud du domaine contient une entrée avec le nom d'hôte et l'adresse IP du serveur LDAP. Si le gestionnaire de service ne peut pas résoudre le nom d'hôte pour le serveur LDAP, la synchronisation peut échouer.

Activez la pagination dans LDAP si vous synchronisez plus de 100 utilisateurs ou groupes.

Activez la pagination sur le service d'annuaire LDAP avant de synchroniser plus de 100 utilisateurs ou groupes. Si vous n'activez pas la pagination dans le service d'annuaire LDAP, la synchronisation peut échouer.

Synchronisez les domaines de sécurité lorsque la plupart des utilisateurs ne sont pas connectés aux applications Informatica.

Pendant la synchronisation, le gestionnaire de service verrouille chaque compte d'utilisateur qu'il synchronise. Les utilisateurs peuvent ne pas être en mesure de se connecter aux clients d'applications Informatica lors de la synchronisation. Les utilisateurs connectés à un client d'application au démarrage de la synchronisation risquent de ne pas pouvoir effectuer certaines tâches.

Pour configurer une planification qui synchronise les domaines de sécurité LDAP avec le service d'annuaire LDAP, procédez comme suit :

1. Dans l'outil Administrator, cliquez sur l'onglet **Sécurité**.
2. Cliquez sur le menu **Actions** et sélectionnez **Configuration LDAP**.
3. Dans la boîte de dialogue **Configuration LDAP**, cliquez sur l'onglet **Planifier**.
4. Cliquez sur le bouton **Ajouter (+)** pour ajouter une heure.

La planification de la synchronisation utilise un format 24 heures standard.

5. Pour synchroniser immédiatement les utilisateurs et les groupes des domaines de sécurité LDAP avec ceux du service d'annuaire LDAP, cliquez sur **Synchroniser maintenant**.
6. Cliquez sur **OK** pour enregistrer la planification de la synchronisation.

Remarque: Attendez que le gestionnaire de service se synchronise avec le service d'annuaire LDAP avant de redémarrer le domaine Informatica afin d'éviter de perdre les temps de synchronisation que vous avez définis dans le calendrier.

Utilisation de groupes imbriqués dans le service d'annuaire LDAP

Un domaine de sécurité LDAP peut contenir des groupes LDAP imbriqués. Le gestionnaire de service peut importer des groupes imbriqués créés de la manière suivante :

- Créez les groupes sous les mêmes unités d'organisation (OU).
- Définissez les relations entre les groupes.

Par exemple, vous voulez créer un regroupement où GroupB est membre de GroupA et GroupD est membre de GroupC.

1. Créez GroupA, GroupB, GroupC et GroupD dans la même OU.
2. Modifiez GroupA, et ajoutez GroupB comme membre.
3. Modifiez GroupC, et ajoutez GroupD comme membre.

Vous ne pouvez pas importer dans un domaine de sécurité des groupes LDAP imbriqués créés d'une manière différente.

Utilisation d'un certificat SSL auto-signé

Vous pouvez vous connecter à un serveur LDAP qui utilise un certificat SSL signé par une autorité de certification (CA). Par défaut, le gestionnaire de service ne se connecte pas à un serveur LDAP qui utilise un certificat auto-signé.

Pour vous connecter à un serveur LDAP qui utilise un certificat SSL, utilisez l'utilitaire de gestion des clés et certificats keytool Java afin d'importer les certificats utilisés par tous les nœuds de domaine dans le fichier truststore `cacerts` sur un nœud de passerelle unique du domaine. Vous copiez ensuite le fichier keystore `cacerts` qui contient les certificats importés dans les autres nœuds du domaine.

Le fichier truststore `cacerts` se trouve dans le répertoire suivant sur chaque nœud :

```
<répertoire d'installation Informatica>\java\jre\lib\security
```

L'utilitaire keytool est disponible dans le répertoire suivant sur chaque nœud :

```
<Informatica installation directory>\java\bin
```

Redémarrez le nœud après avoir importé le certificat.

Suppression d'une configuration LDAP

Vous pouvez supprimer une configuration LDAP et les domaines de sécurité associés afin d'interdire définitivement aux utilisateurs d'accéder au domaine.

Lorsque vous supprimez une configuration LDAP, vous devez d'abord supprimer les domaines de sécurité qui lui sont associés. Le gestionnaire de service supprime tous les comptes utilisateur et les groupes dans chaque domaine de sécurité LDAP de la base de données de configuration des domaines.

1. Dans l'outil Administrator, cliquez sur l'onglet **Sécurité**.
2. Cliquez sur l'onglet **Configuration LDAP**.
3. Cliquez sur l'onglet **Domaines de sécurité**, puis cliquez sur le bouton **Modifier**.
4. Sélectionnez un domaine de sécurité dans la boîte de dialogue **Modifier la configuration LDAP**, puis cliquez sur **Supprimer**.
5. Sélectionnez la configuration LDAP à supprimer dans le navigateur de configuration LDAP.
6. Cliquez sur le menu **Actions**, puis sélectionnez **Supprimer la configuration LDAP**.
7. Cliquez sur **OK** pour confirmer que vous voulez supprimer la configuration LDAP.

CHAPITRE 4

Authentification Kerberos

Ce chapitre comprend les rubriques suivantes :

- [Présentation de Kerberos, 33](#)
- [Fonctionnement de Kerberos dans un domaine Informatica, 34](#)
- [Authentification Kerberos inter-domaines, 36](#)
- [Préparation de l'activation de l'authentification Kerberos, 37](#)
- [Activation de l'authentification Kerberos, 53](#)
- [Activation de Kerberos sur les nœuds Informatica, 58](#)
- [Activation des comptes utilisateurs pour utiliser l'authentification Kerberos, 60](#)

Présentation de Kerberos

Kerberos est un protocole d'authentification de réseau informatique qui permet aux clients, nœuds et services Informatica de communiquer sur un réseau pour se connecter les uns aux autres d'une manière sécurisée.

L'authentification Kerberos élimine les comptes natifs d'Informatica et supprime la nécessité pour le domaine de transmettre les informations d'identification de l'utilisateur à un serveur LDAP. Une fois que l'authentification Kerberos est activée dans un domaine, les clients Informatica utilisent les tickets Kerberos créés pendant le processus d'authentification Windows pour se connecter aux services Informatica exécutés dans le domaine.

Vous pouvez activer l'authentification Kerberos dans un domaine qui s'exécute sur un réseau Windows. Le réseau doit utiliser les services de domaine Microsoft Active Directory (AD DS) comme base de données de principaux Kerberos.

Pour activer l'authentification Kerberos dans un domaine Informatica, effectuez les opérations suivantes :

Préparez-vous à activer l'authentification Kerberos.

Vous devez effectuer plusieurs tâches avant d'activer l'authentification Kerberos. Les tâches que vous devez effectuer incluent les tâches suivantes :

- Créez le fichier de configuration Kerberos.
- Créez des comptes pour les utilisateurs de principaux Kerberos dans Active Directory.
- Générez les formats de SPN (nom de principal du service) et Keytab.
- Créez les fichiers Keytab utilisés pour authentifier les utilisateurs et les services dans le réseau.

Activez l'authentification Kerberos dans le domaine Informatica.

Vous pouvez activer l'authentification Kerberos dans un domaine Informatica lorsque vous installez les services Informatica ou après leur installation. Si vous n'activez pas l'authentification Kerberos lors de l'installation, vous pouvez utiliser les programmes de ligne de commande Informatica pour configurer le domaine de manière à utiliser l'authentification Kerberos.

Activez l'authentification Kerberos sur les nœuds Informatica et les hôtes du client.

Après avoir activé Kerberos dans le domaine, copiez le fichier de configuration Kerberos sur chaque nœud du domaine et sur chaque hôte du client Informatica. Vous pouvez également configurer des navigateurs Web pour accéder aux applications Web d'Informatica.

Autorisez les utilisateurs d'Informatica à utiliser l'authentification Kerberos.

Après avoir activé l'authentification Kerberos, importez les utilisateurs d'Informatica depuis Active Directory dans un domaine de sécurité LDAP qui contient les comptes utilisateurs Kerberos. Vous devez également migrer les groupes, rôles, privilèges et autorisations des comptes utilisateurs natifs vers les comptes utilisateurs du domaine de sécurité LDAP.

Fonctionnement de Kerberos dans un domaine Informatica

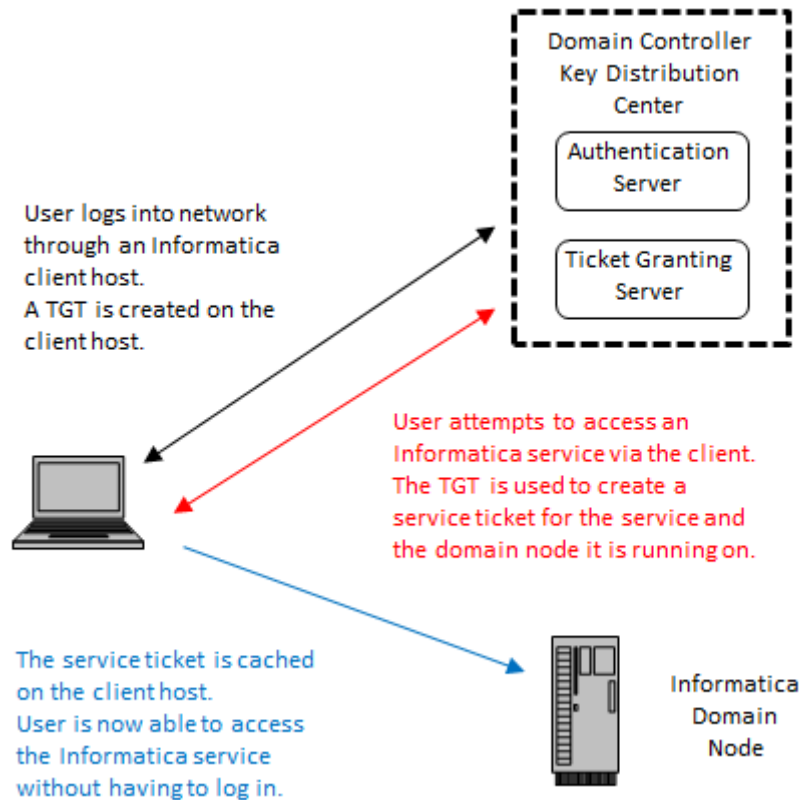
Dans un domaine configuré pour utiliser l'authentification Kerberos, les clients d'Informatica s'authentifient auprès des nœuds et des services d'application dans le domaine, sans mot de passe requis.

Dans un domaine qui utilise l'authentification Kerberos, les services qui s'exécutent dans le domaine, y compris les processus de nœud, les processus d'application Web et les services d'application Informatica, sont les *principaux* Kerberos. La base de données de principaux Active Directory que le domaine Kerberos utilise contient un compte utilisateur pour chaque principal.

Le protocole d'authentification Kerberos utilise les *keytabs* pour authentifier les clients Informatica avec les services qui s'exécutent dans le domaine. Le keytab d'un principal est stocké sur le nœud sur lequel le service s'exécute. Le keytab contient le *nom de principal du service (SPN)* qui identifie le service dans le domaine Kerberos, et la clé attribuée au SPN dans Active Directory.

Lorsque le KDC donne un ticket de service à un client, il chiffre le ticket à l'aide de la clé attribuée au SPN. Le service demandé utilise la clé pour déchiffrer le ticket de service.

L'image suivante montre le flux d'authentification Kerberos de base :



La structure suivante décrit le flux d'authentification Kerberos de base :

1. Un utilisateur de client Informatica se connecte à un ordinateur réseau hébergeant un client Informatica.
2. La demande de connexion est dirigée vers le *serveur d'authentification*, un composant du *centre de distribution de clés (KDC) Kerberos*. Le KDC est un service réseau avec accès aux informations de compte utilisateur qui s'exécute sur chaque contrôleur de domaine dans le domaine Active Directory.
3. Le serveur d'authentification vérifie que l'utilisateur existe dans la base de données de principaux, puis crée un jeton Kerberos appelé *ticket TGT (ticket-granting-ticket)* sur l'ordinateur de l'utilisateur.
4. L'utilisateur tente d'accéder à un processus ou à un service dans le domaine Informatica via un client Informatica.
5. Informatica et les bibliothèques Kerberos utilisent le ticket TGT afin de demander un *ticket de service* et une *clé de session* du serveur demandé depuis le *serveur d'émission de tickets*, qui s'exécute également dans le KDC.

Par exemple, si l'utilisateur accède à un service de référentiel modèle à partir du client Informatica Developer, le TGT demande un ticket de service pour le nœud sur lequel s'exécute le service demandé. Il demande également un ticket de service pour le service de référentiel modèle.

6. Kerberos utilise le ticket de service pour authentifier le client avec le service demandé. Le ticket de service est mis en cache sur l'ordinateur qui héberge le client Informatica, ce qui permet au client d'utiliser le ticket pendant toute la durée de sa validité. Si l'utilisateur arrête, puis redémarre le client Informatica, le client réutilise le même ticket pour accéder aux processus et aux services dans le domaine Informatica.

Authentification Kerberos inter-domaines

Vous pouvez configurer un domaine Informatica pour utiliser l'authentification Kerberos inter-domaines. Ce type d'authentification permet aux clients Informatica, qui appartiennent à un domaine Kerberos, de s'authentifier auprès des nœuds et des services d'application qui appartiennent à un autre domaine Kerberos.

Lorsque vous configurez un domaine afin d'utiliser l'authentification Kerberos inter-domaines, vous ajoutez des propriétés de chaque domaine Kerberos au fichier de configuration Kerberos. Vous incluez également le nom de chaque domaine lorsque vous exécutez des commandes infasetup pour activer l'authentification Kerberos dans le domaine et dans les nœuds de celui-ci.

Les serveurs Active Directory, que le domaine utilise pour l'authentification Kerberos inter-domaines, doivent appartenir à la même forêt Active Directory. Ce type de forêt est un groupe de domaines Active Directory qui partagent un catalogue global commun, un schéma d'annuaire, une structure logique et une configuration d'annuaire. Vous vous connectez au catalogue global afin d'importer des utilisateurs de serveurs Active Directory dans des domaines de sécurité LDAP.

Pour utiliser l'authentification Kerberos inter-domaines, l'approbation bidirectionnelle doit être activée entre les serveurs Active Directory de la forêt.

Conversion d'un domaine de l'authentification Kerberos à domaine unique en authentification Kerberos inter-domaines

Vous pouvez convertir un domaine Informatica qui utilise un domaine Kerberos unique afin d'authentifier les utilisateurs pour utiliser l'authentification Kerberos inter-domaines.

Vous devez mettre à niveau le domaine vers la version 10.2 HotFix 2 avant de convertir le domaine afin d'utiliser l'authentification Kerberos inter-domaines.

Vous devez également importer des comptes utilisateurs et de groupes du catalogue global Active Directory dans un domaine de sécurité LDAP. Lorsque vous importez des comptes, ceux du domaine de sécurité LDAP, qui utilisent l'attribut de nom samAccount, sont supprimés et remplacés par de nouveaux comptes qui utilisent l'attribut de nom de principal de l'utilisateur.

Les utilisateurs se connectent aux clients Informatica à l'aide du nom de principal de l'utilisateur complet, qui est au format suivant :

```
<user name>@<KERBEROS REALM NAME>
```

Après avoir importé les comptes utilisateurs et de groupes, attribuez des privilèges, des rôles et des autorisations aux comptes.

1. Mettez à niveau le domaine vers la version 10.2 HotFix 2.
2. Ajoutez les propriétés requises de chaque domaine Kerberos au fichier de configuration Kerberos.

Définissez les propriétés de chaque domaine dans le fichier de configuration `krb5.conf` sur chaque nœud du domaine. Redémarrez le domaine après avoir mis à jour le fichier sur tous les nœuds du domaine.

Pour plus d'informations sur le paramétrage du fichier de configuration `krb5.conf` pour l'authentification Kerberos inter-domaines, consultez la section ["Configurer le fichier de configuration Kerberos" à la page 38](#).

3. Copiez le fichier `krb5.conf` mis à jour dans le répertoire suivant de chaque ordinateur qui héberge un client Informatica :

```
<Informatica installation directory>\clients\shared\security
```

4. Exécutez les commandes `infasetup UpdateGatewayNode` et `infasetup UpdateWorkerNode` sur les nœuds de domaine.
Spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs en tant que valeurs pour les options `-srn` et `-urn`, séparées par une virgule.
Pour plus d'informations sur l'exécution des commandes `infasetup`, consultez la « Référence des commandes `infasetup` » du *Guide de référence des commandes d'Informatica 10.2 HotFix 2*.
5. Exécutez la commande `UpdateKerberosConfig` sur un nœud de passerelle dans le domaine.
Spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs en tant que valeurs pour les options `-srn` et `-urn`, séparées par une virgule.
6. Exécutez la commande `UpdateKerberosAdminUser` sur un nœud de passerelle dans le domaine.
Spécifiez le nom de principal de l'utilisateur complet du compte utilisateur de l'administrateur du domaine.
7. Importez les comptes utilisateurs et de groupes dans les domaines de sécurité LDAP.
Connectez-vous au catalogue global Active Directory. Lors de la connexion au catalogue global, vous importez des utilisateurs du serveur Active Directory utilisé par chaque domaine Kerberos.
Pour plus d'informations sur la connexion au catalogue global et l'importation de comptes, consultez la section ["Importer des comptes utilisateurs d'Active Directory dans des domaines de sécurité LDAP" à la page 60](#).
8. Attribuez des privilèges, des rôles et des autorisations aux comptes utilisateurs et de groupes que vous avez importés dans un domaine de sécurité LDAP.
Pour plus d'informations sur l'attribution de privilèges et de rôles, consultez la section [Chapitre 9, "Privilèges et rôles" à la page 145](#).
Pour plus d'informations sur l'attribution d'autorisations, consultez la section [Chapitre 10, "Autorisations" à la page 191](#).

Préparation de l'activation de l'authentification Kerberos

Vous devez effectuer plusieurs tâches pour vous préparer à activer l'authentification Kerberos dans un domaine Informatica. Les procédures à suivre pour chaque tâche dépendent du niveau de principal du service sur lequel vous activez Kerberos.

Remarque: Vous ne pouvez pas désactiver l'authentification Kerberos dans un domaine après l'avoir activé. Vous ne pouvez pas non plus basculer le niveau de principal du service entre le niveau du nœud et le niveau du processus.

Déterminer le niveau de principal du service Kerberos

Lorsque vous vous préparez à activer l'authentification Kerberos, vous devez déterminer le niveau de principal du service requis. Le niveau de principal du service requis détermine les procédures à suivre pour vous préparer à activer l'authentification Kerberos dans le domaine.

Vous pouvez activer l'authentification Kerberos sur l'un des niveaux suivants :

Niveau nœud

Si vous utilisez le domaine à des fins de test ou de développement, et que le domaine ne requiert pas un niveau élevé de sécurité, vous pouvez activer Kerberos au niveau du nœud. Vous pouvez utiliser un nom de principal du service unique et un seul fichier Keytab pour le nœud et pour tous les processus et services qui s'exécutent sur le nœud. Vous devez également créer un SPN et un fichier Keytab pour les processus HTTP qui s'exécutent sur le nœud.

Niveau processus

Si vous utilisez le domaine à des fins de production et qu'il requiert un niveau de sécurité élevé, vous pouvez définir le principal du service au niveau du processus. Créez un SPN et un fichier Keytab uniques pour chaque nœud et chacun de ses processus. Vous devez également créer un SPN et un fichier Keytab pour les processus HTTP qui s'exécutent sur le nœud.

L'authentification Kerberos activée au niveau du processus fournit le plus haut niveau de sécurité, mais peut être difficile à gérer dans un domaine Informatica qui contient de nombreux nœuds ou de nombreux services. Dans ce cas, vous souhaitez peut-être activer Kerberos au niveau du nœud.

Configurer le fichier de configuration Kerberos

Définissez les propriétés requises par Informatica dans le fichier de configuration Kerberos, puis copiez le fichier dans chaque nœud du domaine Informatica.

Kerberos stocke les informations de configuration dans un fichier nommé *krb5.conf*. Vous devez définir les propriétés dans le fichier de configuration *krb5.conf*, puis copier le fichier dans chaque nœud du domaine Informatica.

Si le domaine utilise l'authentification Kerberos inter-domaines, entrez les propriétés requises de chaque domaine Kerberos.

1. Configurez les propriétés suivantes de la bibliothèque Kerberos dans la section *libdefaults* du fichier.
Le tableau suivant décrit les propriétés à entrer :

Propriété	Description
default_realm	Nom du domaine Kerberos auquel les services du domaine Informatica appartiennent. Le nom du domaine doit être en majuscules. Si un domaine Kerberos unique est utilisé pour l'authentification, le nom du domaine de service et le nom du domaine de l'utilisateur doivent être identiques.
forwardable	Permet à un service de déléguer les informations d'identification d'un l'utilisateur client à un autre service. Le domaine Informatica requiert que les services d'application authentifient les informations d'identification de l'utilisateur client avec d'autres services. Définissez la propriété sur True.

Propriété	Description
default_tkt_enctypes	Types de chiffrement de la clé de session inclus dans les tickets TGT. Définissez cette propriété uniquement si les clés de session doivent utiliser des types de chiffrement spécifiques. Assurez-vous que le centre de distribution de clés Kerberos (KDC) prend en charge le type de chiffrement que vous spécifiez. Ne définissez pas cette propriété pour permettre au protocole Kerberos de sélectionner le type de chiffrement à utiliser. Si les hôtes du nœud ou du client Informatica utilisent le chiffrement 256 bits, installez les fichiers de stratégie JCE (Java Cryptography Extension) à accès illimité sur tous les hôtes du nœud et du client Informatica pour éviter les problèmes d'authentification.
rdns	Détermine si la recherche de nom inversée est utilisée en complément de la recherche de nom avancée pour la mise en forme canonique des noms d'hôte à utiliser dans les noms principaux de service. Définissez cette valeur sur False.
renew_lifetime	Durée de vie renouvelable par défaut pour les demandes de ticket initiales.
ticket_lifetime	Durée de vie par défaut pour les demandes de ticket initiales.
udp_preference_limit	Détermine le protocole utilisé par Kerberos lors de l'envoi d'un message au KDC. Définissez sur 1 pour utiliser le protocole TCP si le domaine connaît des échecs d'authentification Kerberos intermittents.
dns_lookup_kdc	Indique si le client Kerberos utilise des enregistrements DNS SRV pour localiser les KDC et autres serveurs d'un domaine, s'ils ne sont pas répertoriés dans les informations du domaine. DNS utilise des enregistrements SRV pour identifier des ordinateurs qui hébergent des services spécifiques. Requis lorsque le domaine est compatible Kerberos. Exige que vous définissiez la propriété de domaine admin_server. Définissez la propriété sur True.
dns_lookup_realm	Indique si le client Kerberos utilise des enregistrements DNS TXT pour déterminer le domaine Kerberos d'un hôte. DNS utilise des enregistrements de texte ou TXT pour associer le texte arbitraire à un hôte ou à un autre nom, par exemple des informations contrôlables de visu sur un serveur, un réseau, un centre de données ou d'autres informations de compte. Requis lorsque le domaine est compatible Kerberos. Définissez la propriété sur True.

2. Définissez chaque domaine Kerberos dans la section *realms* du fichier.

L'exemple suivant montre l'entrée d'un domaine Kerberos nommé COMPANY.COM :

```
[realms]
COMPANY.COM = {...}
```

3. Entrez les propriétés suivantes du domaine entre crochets pour chaque domaine Kerberos dans la section *realms* du fichier.

Le tableau suivant décrit les propriétés à entrer :

Propriété	Description
admin_server	Nom ou adresse IP de l'hôte du serveur d'administration Kerberos. Vous pouvez inclure un numéro de port facultatif, séparé du nom d'hôte par deux points. La valeur par défaut est 749. Requis si vous configurez dns_lookup_kdc dans la section <i>libdefaults</i> .
kdc	Nom ou adresse IP d'un hôte exécutant le centre de distribution de clés (KDC) du domaine. Vous pouvez inclure un numéro de port facultatif, séparé du nom d'hôte par deux points. La valeur par défaut est 88.

L'exemple suivant montre les entrées de chaque domaine Kerberos dans une configuration Kerberos inter-domaines :

```
[realms]
COMPANY.COM = {
  admin_server = KDC01.COMPANY.COM:749
  kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
  kdc = 10.75.141.193
  admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
  kdc = 10.78.140.111
  admin_server = 10.78.140.111
}
```

4. Dans la section *domain_realms*, mappez le nom du domaine ou le nom d'hôte à un nom de domaine Kerberos. Le nom de domaine est préfixé par un point (.).

L'exemple suivant montre les paramètres du *domain_realm* Hadoop si le domaine Informatica n'utilise pas l'authentification Kerberos :

```
[domain_realm]
.hadoop_realm.com = HADOOP-REALM
hadoop_realm.com = HADOOP-REALM
```

L'exemple suivant montre les paramètres du *domain_realm* Hadoop si le domaine Informatica utilise l'authentification Kerberos :

```
[domain_realm]
.infa_ad_realm.com = INFA-AD-REALM
infa_ad_realm.com = INFA-AD-REALM
.hadoop_realm.com = HADOOP-REALM
hadoop_realm.com = HADOOP-REALM
```

5. Copiez le fichier *krb5.conf* vers les emplacements suivants de la machine qui héberge le service d'intégration de données :

- <Informatica installation directory>/services/shared/security/
- <Informatica installation directory>/java/jre/lib/security

L'exemple suivant montre le contenu d'un fichier de configuration Kerberos avec les propriétés requises d'une configuration de domaine Kerberos unique :

```
[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
```



```

dns_lookup_realm = true

[realms]
COMPANY.COM = {
  admin_server = KDC01.COMPANY.COM:749
  kdc = KDC01.COMPANY.COM:88
}

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM

```

L'exemple suivant montre le contenu d'un fichier de configuration Kerberos avec les propriétés requises d'une configuration Kerberos inter-domaines :

```

[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realm = true

[realms]
COMPANY.COM = {
  admin_server = KDC01.COMPANY.COM:749
  kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
  kdc = 10.75.141.193
  admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
  kdc = 10.78.140.111
  admin_server = 10.78.140.111
}

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
.east.company.com = EAST.COMPANY.COM
east.company.com = EAST.COMPANY.COM
.west.company.com = WEST.COMPANY.COM
west.company.com = WEST.COMPANY.COM

```

Pour plus d'informations sur le fichier de configuration Kerberos, consultez la documentation relative à l'authentification réseau Kerberos.

Création de comptes de principaux Kerberos dans Active Directory

Créez des comptes utilisateurs LDAP pour les principaux Kerberos dans Active Directory. Un principal Kerberos est un processus, un service ou un utilisateur du domaine Kerberos.

Si vous définissez la propriété `default_tkt_enctypes` dans le fichier de configuration `krb5.conf` sur des types de chiffrement AES 128 bits ou 256 bits, configurez chaque compte pour qu'il utilise le type de chiffrement correspondant dans Active Directory.

Les comptes que vous créez dépendent de l'activation de Kerberos au niveau du nœud ou du processus.

Remarque: Les noms de comptes ne doivent pas dépasser 20 caractères.

Comptes requis au niveau du nœud

Créez les comptes utilisateurs LDAP requis pour activer l'authentification Kerberos au niveau du nœud dans Active Directory.

Créez les comptes principaux Kerberos suivants dans Active Directory si vous activez Kerberos au niveau du nœud :

Processus de nœud

Créez un compte pour chaque nœud qui s'exécute dans le domaine.

Processus HTTP

Créez un compte pour les applications Web Informatica qui s'exécutent sur un nœud dans le domaine. Les applications Web qui s'exécutent sur un nœud peuvent inclure l'outil Administrator tool, Informatica Analyst et Catalog Administrator. Créez un compte unique partagé par toutes les applications Web qui s'exécutent sur le nœud.

Nom unique (NU) de l'utilisateur de liaison

Créez un compte utilisateur de liaison LDAP afin de synchroniser le domaine de sécurité LDAP contenant des comptes utilisateurs Kerberos avec Active Directory.

Comptes requis au niveau du processus

Créez les comptes utilisateurs LDAP requis pour activer l'authentification Kerberos au niveau du processus dans Active Directory.

Créez les comptes principaux Kerberos suivants dans Active Directory si vous activez Kerberos au niveau du processus :

Processus de nœud

Créez un compte pour chaque nœud qui s'exécute dans le domaine.

Processus HTTP

Créez un compte pour les applications Web Informatica qui s'exécutent sur un nœud dans le domaine. Les applications Web qui s'exécutent sur un nœud peuvent inclure Informatica Analyst et Catalog Administrator. Créez un compte unique partagé par toutes les applications Web qui s'exécutent sur le nœud.

Service Informatica Administrator

Créez un compte pour l'outil Administrator tool sur chaque nœud de passerelle du domaine.

Services d'application Informatica

Créez un compte pour chaque service d'application Informatica qui s'exécute sur chaque nœud du domaine.

Nom unique (NU) de l'utilisateur de liaison

Créez un compte utilisateur LDAP afin de synchroniser le domaine de sécurité LDAP qui contient des comptes utilisateurs Kerberos avec Active Directory.

Générer les formats de nom de principal de service et de fichier Keytab

Utilisez l'utilitaire SPN Format Generator Kerberos d'Informatica pour générer les formats de nom de principal de service (SPN) et de fichier Keytab requis pour utiliser l'authentification Kerberos. L'utilitaire SPN Format

Generator Kerberos génère un fichier texte nommé SPNKeytabFormat qui contient le format correct pour les noms de fichiers SPN et Keytab.

Les formats de nom de SPN et de fichier Keytab que vous générez varient selon que l'activation de Kerberos se fait au niveau du nœud ou au niveau du processus.

Générer les formats de nom de principal de service et de fichier Keytab au niveau du nœud

Générez les formats de nom de SPN et de fichier Keytab requis pour activer l'authentification Kerberos au niveau du nœud.

Le domaine Informatica requiert des SPN et des fichiers Keytab pour les processus suivants lorsque vous activez l'authentification Kerberos au niveau du nœud :

Processus de nœud

Informatica requiert un SPN et un fichier Keytab pour chaque nœud du domaine. Kerberos utilise le même nom de principal de service et de fichier Keytab pour authentifier les services d'application Informatica qui s'exécutent sur le nœud.

Processus HTTP

Informatica requiert un SPN et un fichier Keytab pour les applications Web qui s'exécutent sur chaque nœud du domaine. Les applications Web qui s'exécutent sur un nœud peuvent inclure l'outil Administrator tool, Informatica Analyst et Catalog Administrator. Kerberos utilise le même nom de principal de service pour authentifier les applications Web qui s'exécutent sur le nœud.

1. Sur un hôte du nœud Windows Informatica, accédez au répertoire qui contient le fichier de commandes SPNFormatGenerator.bat :

```
<Informatica installation directory>\tools\Kerberos
```

Sur un hôte de nœud Informatica UNIX, accédez au répertoire qui contient le fichier shell SPNFormatGenerator.sh :

```
<Informatica installation directory>/tools/Kerberos
```

2. Exécutez SPNFormatGenerator.bat ou SPNFormatGenerator.sh.
3. Cliquez sur **Suivant**.
4. Sélectionnez **Niveau du nœud**.
5. Cliquez sur **Suivant**.
6. Entrez les propriétés requises pour générer les formats de SPN et de fichier Keytab.

Le tableau suivant décrit les propriétés :

Invite	Description
Nom du domaine	Nom du domaine Informatica. Le nom ne doit pas dépasser 128 caractères et doit être en ASCII 7 bits. Il ne peut pas contenir d'espaces ni les caractères spéciaux suivants : ` % * + ; " ? , < > \ /
Nom du domaine du service	Nom du domaine Kerberos. Le nom du domaine doit être en majuscules.

Invite	Description
Nom du nœud	Nom du nœud Informatica.
Nom d'hôte du nœud	Nom complet de l'hôte du nœud. Le nom d'hôte du nœud ne peut pas contenir le caractère de soulignement (_). Remarque: N'utilisez pas <i>localhost</i> . Le nom d'hôte doit explicitement identifier l'hôte.

- Pour générer le format SPN pour un autre nœud, cliquez sur **+Nœud** et spécifiez le nom de nœud et le nom d'hôte.

L'image suivante montre les entrées de plusieurs nœuds dans le domaine InfaDomain dans l'utilitaire SPN Format Generator :

- Cliquez sur **Suivant**.

L'utilitaire SPN Format Generator affiche le chemin et le nom du fichier qui contient la liste des noms de principaux du service et de fichiers keytab.

- Cliquez sur **Terminé** pour quitter l'utilitaire SPN Format Generator.

Générer les formats de nom de principal de service et de fichier Keytab au niveau du processus

Générez les formats de nom de SPN et de fichier Keytab requis pour activer l'authentification Kerberos au niveau du processus.

Le domaine Informatica requiert des SPN et des fichiers Keytab pour les processus et les services suivants lorsque vous activez l'authentification Kerberos au niveau du processus :

Processus de nœud

Informatica requiert un SPN et un fichier Keytab pour chaque nœud du domaine.

Informatica Administrator

Informatica requiert un SPN et un fichier Keytab pour l'outil Administrator tool pour chaque nœud de passerelle du domaine.

Processus HTTP

Informatica requiert un SPN et un fichier Keytab pour les applications Web qui s'exécutent sur un nœud du domaine. Les applications Web qui s'exécutent sur un nœud peuvent inclure Informatica Analyst et Catalog Administrator.

Processus de service d'application Informatica

Informatica requiert un SPN et un fichier Keytab pour chaque service d'application Informatica qui s'exécute sur un nœud du domaine.

1. Sur un hôte du nœud Windows Informatica, accédez au répertoire qui contient le fichier de commandes SPNFormatGenerator.bat :

```
<Informatica installation directory>\tools\Kerberos
```

Sur un hôte de nœud Informatica UNIX, accédez au répertoire qui contient le fichier shell SPNFormatGenerator.sh :

```
<Informatica installation directory>/tools/Kerberos
```

2. Exécutez SPNFormatGenerator.bat ou SPNFormatGenerator.sh.
3. Cliquez sur **Suivant**.
4. Sélectionnez **Niveau du processus**.
5. Cliquez sur **Suivant**.
6. Entrez les propriétés requises pour générer les formats de SPN et de fichier Keytab.

Le tableau suivant décrit les propriétés :

Invite	Description
Nom du domaine	Nom du domaine Informatica. Le nom ne doit pas dépasser 128 caractères et doit être en ASCII 7 bits. Il ne peut pas contenir d'espaces ni les caractères spéciaux suivants : ` % * + ; " ? , < > \ /
Nom du domaine du service	Nom du domaine Kerberos. Le nom du domaine doit être en majuscules.
Nom du nœud	Nom du nœud Informatica.
Nom d'hôte du nœud	Nom complet ou adresse IP de l'hôte du nœud. Le nom d'hôte du nœud ne peut pas contenir le caractère de soulignement (_). Remarque: N'utilisez pas <i>localhost</i> . Le nom d'hôte doit explicitement identifier l'hôte.

7. Pour générer le format SPN pour un service d'application Informatica qui s'exécute sur un nœud, cliquez sur **Service** après avoir entré les détails du nœud.

Entrez le nom du service d'application Informatica comme indiqué dans l'outil Administrator tool. Complétez cette étape pour chaque service d'application Informatica qui s'exécute sur chaque nœud du domaine.

8. Pour générer le format SPN pour un autre nœud, cliquez sur **+Nœud** et spécifiez le nom de nœud et le nom d'hôte.

L'image suivante montre les entrées de plusieurs nœuds et services d'application qui s'exécutent dans le domaine InfaDomain dans l'utilitaire SPN Format Generator :

Informatica Kerberos SPN Format Generator

Authentication Parameters - Kerberos Authentication - Step 3 of 4

Specify the domain and Kerberos authentication parameters.

Domain name: InfaDomain

Service realm name: COMPANY.COM

Node name: node01

Node host name: JS001DEV

Service on node: MRS_dev

Service on node: DIS_dev

Node name: node02

Node host name: JS005DEV

Service on node: CMS_dev

+Node +Service -Node

< Previous Next > Cancel

9. Cliquez sur **Suivant**.

L'utilitaire SPN Format Generator affiche le chemin et le nom du fichier qui contient la liste des noms de principaux du service et de fichiers keytab.

10. Cliquez sur **Terminé** pour quitter l'utilitaire SPN Format Generator.

Vérifier le fichier texte du format du nom de principal du service et de fichier Keytab

Après avoir généré le fichier SPNKeytabFormat.txt, vous pouvez le vérifier.

Utilisez les informations du fichier pour générer les fichiers Keytab et associer chaque SPN au compte utilisateur de principal correspondant dans Active Directory.

Le fichier SPNKeytabFormat.txt contient les informations suivantes :

Nom de l'entité

Identifie le nœud ou le service associé au processus.

Nom de principal du service

Format du SPN. Le SPN est sensible à la casse.

Remarque: Si vous entrez une chaîne contenant plusieurs noms de domaine Kerberos, ou que vous ajoutez un astérisque avant un suffixe de domaine pour inclure tous les domaines qui incluent le suffixe, le format de SPN n'inclut pas le nom du domaine.

Le tableau suivant décrit les formats SPN :

Type de Keytab	Format SPN
NODE_SPN	isp/<nom de nœud>/<nom de domaine>@<REALM NAME>
NODE_AC_SPN	_AdminConsole/<nom de nœud>/<nom de domaine>@<REALM NAME>
NODE_HTTP_SPN	HTTP/<nom d'hôte du nœud>@<REALM NAME> Remarque: Kerberos SPN Format Generator valide le nom d'hôte du nœud. Si le nom d'hôte du nœud n'est pas valide, l'utilitaire ne génère pas de SPN. Il affiche le message suivant : Impossible de résoudre le nom d'hôte.
SERVICE_PROCESS_SPN	<nom du service d'application>/<nom du nœud>/<nom du domaine>@<REALM NAME>

Nom du fichier Keytab

Format du nom du fichier Keytab à créer pour le SPN associé. Le nom de fichier Keytab est sensible à la casse.

Le tableau suivant décrit les formats de nom de fichier Keytab :

Type de Keytab	Nom du fichier Keytab
NODE_SPN	<nom du nœud>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<nom du service d'application>.keytab

Principaux du service au niveau nœud

L'image suivante montre le contenu du fichier SPNKeytabFormat.txt généré pour les principaux du service au niveau nœud :

ENTITY_NAME	SPN	KEY_TAB_NAME	KEY_TAB_TYPE
node01	isp/node01/Infadomain@COMPANY.COM	node01.keytab	NODE_SPN
node01	HTTP/US001DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
node02	isp/node02/Infadomain@COMPANY.COM	node02.keytab	NODE_SPN
node02	HTTP/US005DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN

Principaux du service au niveau processus

L'image suivante montre le contenu du fichier SPNKeytabFormat.txt généré pour les principaux du service au niveau du nœud :

ENTITY_NAME	SPN	KEY_TAB_NAME	KEY_TAB_TYPE
node01	isp/node01/Infadomain@COMPANY.COM	node01.keytab	NODE_SPN
node01	_AdminConsole/node01/Infadomain@COMPANY.COM	_AdminConsole.keytab	NODE_AC_SPN
node01	HTTP/US001DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
node02	isp/node02/Infadomain@COMPANY.COM	node02.keytab	NODE_SPN
node02	_AdminConsole/node02/Infadomain@COMPANY.COM	_AdminConsole.keytab	NODE_AC_SPN
node02	HTTP/US005DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
MRS_dev:node01	MRS_dev/node01/Infadomain@COMPANY.COM	MRS_dev.keytab	SERVICE_PROCESS_SPN
DIS_dev:node01	DIS_dev/node01/Infadomain@COMPANY.COM	DIS_dev.keytab	SERVICE_PROCESS_SPN
CAT_dev:node02	CAT_dev/node02/Infadomain@COMPANY.COM	CAT_dev.keytab	SERVICE_PROCESS_SPN

Générer les fichiers Keytab

Générez les fichiers Keytab utilisés pour authentifier les utilisateurs et les services Informatica.

Utilisez l'utilitaire Ktpass de Microsoft Windows Server pour générer un fichier Keytab pour chaque compte utilisateur que vous avez créé dans Active Directory. Vous devez générer les fichiers Keytab sur un serveur membre ou sur un contrôleur de domaine dans le domaine Active Directory. Vous ne pouvez pas générer de fichier Keytab sur un système d'exploitation de poste de travail tel que Microsoft Windows 7.

Pour utiliser Ktpass pour générer un fichier Keytab, exécutez la commande suivante :

```
ktpass.exe -out <keytab filename> -princ <service principal name> -mapuser <user account> [-pass <user account password>] -crypto <key types> -ptype <principal type> [-target <realm name>]
```

Le tableau suivant décrit les options de commande :

Option	Description
-out	Nom du fichier Keytab Kerberos à générer comme indiqué dans la colonne <code>KEY_TAB_NAME</code> dans le fichier <code>SPNKeytabFormat.txt</code> .
-princ	Nom de principal du service affiché sous la colonne <code>SPN</code> dans le fichier <code>SPNKeytabFormat.txt</code> . Si le domaine utilise l'authentification Kerberos inter-domaines, le nom de principal du service doit être unique dans tous les domaines Kerberos.
-mapuser	Compte utilisateur Active Directory à associer au SPN. Le nom du compte ne doit pas dépasser 20 caractères.
-pass	Mot de passe défini dans Active Directory pour le compte utilisateur Active Directory, s'il y a lieu.
-crypto	Spécifie les types de clés générés dans le fichier Keytab. Définissez sur Tous pour utiliser tous les types de chiffrement pris en charge.
-ptype	Type de principal. Définissez sur <code>KRB5_NT_PRINCIPAL</code> .
-target	Nom du domaine auquel le serveur Active Directory appartient. Incluez cette option si l'erreur suivante se produit lorsque vous exécutez l'utilitaire : <code>DsCrackNames</code> a renvoyé 0x2 dans le nom

Les fichiers keytab que vous générez varient selon que l'activation de Kerberos se fait au niveau du nœud ou au niveau du processus.

Générer les fichiers Keytab au niveau du nœud

Lorsque vous exécutez Ktpass pour générer les fichiers Keytab au niveau du nœud, associez chaque compte utilisateur de principal Kerberos au SPN correspondant dans Active Directory.

Le tableau suivant montre l'association entre les comptes utilisateurs de principaux Kerberos et les SPN affichés dans l'exemple de fichier `SPNKeytabFormat` :

Compte utilisateur	Type de Keytab	Nom de principal du service
nodeuser01	NODE_SPN	isp/node01/Infadomain/COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM

Compte utilisateur	Type de Keytab	Nom de principal du service
nodeuser02	NODE_SPN	isp/node02/Infadomain/COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM

Créez également un fichier Keytab pour le compte utilisateur de liaison LDAP qui est utilisé pour accéder et rechercher dans Active Directory pendant la synchronisation LDAP.

1. Créez un fichier Keytab pour le compte utilisateur de principal Kerberos que vous avez créé pour chaque nœud dans Active Directory.

Copiez le nom du fichier Keytab depuis la colonne `KEY_TAB_NAME` dans le fichier `SPNKeytabFormat.txt`. Copiez le nom de principal du service de la colonne `SPN` dans le fichier `SPNKeytabFormat.txt`.

L'exemple suivant crée un fichier keytab pour un compte utilisateur de principal Kerberos nommé `nodeuser0` :

```
ktpass.exe -out node01.keytab -princ isp/node01/Infadomain/COMPANY.COM -mapuser nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

2. Créez un fichier keytab pour chaque compte utilisateur de principal Kerberos de processus HTTP que vous avez créé dans Active Directory.

Si le domaine utilise l'authentification Kerberos inter-domaines, le compte utilisateur du principal peut exister dans tout domaine Kerberos utilisé.

Copiez le nom du fichier keytab de la colonne `KEY_TAB_NAME` dans le fichier `SPNKeytabFormat.txt`. Copiez le nom de principal du service de la colonne `SPN` dans le fichier `SPNKeytabFormat.txt`.

L'exemple suivant crée un fichier keytab pour un compte utilisateur de principal Kerberos nommé `httpuser01` :

```
ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

3. Créez un fichier keytab pour le compte utilisateur de liaison LDAP qui est utilisé pour accéder et rechercher dans Active Directory pendant la synchronisation LDAP.

Structurez la valeur de l'option `-princ` en tant que `<principal name>@<KERBEROS REALM>`. Incluez le nom de la configuration LDAP pour le serveur Active Directory dans le nom de fichier keytab. Structurez celui-ci comme suit : `<Active Directory LDAP configuration_name>.keytab`.

L'exemple suivant crée un fichier Keytab pour un compte utilisateur de principal de service nommé `ldapuser` :

```
ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
```

Générer les fichiers Keytab au niveau du processus

Lorsque vous exécutez Ktpass pour générer les fichiers Keytab au niveau du processus, associez chaque compte utilisateur de principal Kerberos au SPN correspondant dans Active Directory.

Le tableau suivant montre l'association entre les comptes utilisateurs de principaux Kerberos et les SPN affichés dans l'exemple de fichier SPNKeytabFormat :

Compte utilisateur	Type de Keytab	Nom de principal du service
nodeuser01	NODE_SPN	isp/node01/Infadomain/COMPANY.COM
admintooluser01	NODE_AC_SPN	_AdminConsole/node01/Infadomain@COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
MRSdevuser01	SERVICE_PROCESS_SPN	MRS_dev/node01/Infadomain@COMPANY.COM
DISdevuser01	SERVICE_PROCESS_SPN	DIS_dev/node01/Infadomain@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/Infadomain/COMPANY.COM
admintooluser02	NODE_AC_SPN	_AdminConsole/node02/Infadomain@COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM
CATdevuser01	SERVICE_PROCESS_SPN	CAT_dev/node02/Infadomain@COMPANY.COM

Créez également un fichier Keytab pour le compte utilisateur de liaison LDAP qui est utilisé pour accéder et rechercher dans Active Directory pendant la synchronisation LDAP.

1. Créez un fichier Keytab pour le compte utilisateur de principal Kerberos que vous avez créé pour chaque nœud dans Active Directory.

Copiez le nom du fichier de la colonne `KEY_TAB_NAME` dans le fichier SPNKeytabFormat.txt. Copiez le nom de principal du service de la colonne `SPN` dans le fichier SPNKeytabFormat.txt.

L'exemple suivant crée un fichier keytab pour un compte utilisateur de principal Kerberos nommé nodeuser01 :

```
ktpass.exe -out node01.keytab -princ isp/node01/Infadomain/COMPANY.COM -mapuser nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

2. Créez un fichier keytab pour chaque compte utilisateur de principal Kerberos de processus HTTP que vous avez créé.

Si le domaine utilise l'authentification Kerberos inter-domaines, le compte utilisateur du principal peut exister dans tout domaine Kerberos utilisé.

Copiez le nom du fichier de la colonne `KEY_TAB_NAME` dans le fichier SPNKeytabFormat.txt. Copiez le nom de principal du service de la colonne `SPN` dans le fichier SPNKeytabFormat.txt.

L'exemple suivant crée un fichier keytab pour un compte utilisateur de principal Kerberos nommé httpuser01 :

```
ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

3. Créez un fichier keytab pour chaque compte utilisateur de principal Kerberos de l'outil Administrator tool que vous avez créé.

Copiez le nom du fichier de la colonne `KEY_TAB_NAME` dans le fichier `SPNKeytabFormat.txt`. Copiez le nom de principal du service de la colonne `SPN` dans le fichier `SPNKeytabFormat.txt`.

L'exemple suivant crée un fichier keytab pour un compte utilisateur de principal Kerberos nommé `admintooluser01` :

```
ktpass.exe -out _AdminConsole.keytab -princ _AdminConsole/node01/Infadomain@COMPANY.COM -mapuser admintooluser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

4. Créez un fichier keytab pour chaque compte utilisateur de principal Kerberos du service d'application d'Informatica que vous avez créé.

Copiez le nom du fichier de la colonne `KEY_TAB_NAME` dans le fichier `SPNKeytabFormat.txt`. Copiez le nom de principal du service de la colonne `SPN` dans le fichier `SPNKeytabFormat.txt`.

L'exemple suivant crée un fichier keytab pour un compte utilisateur de principal Kerberos de service nommé `MRSdevuser01` :

```
ktpass.exe -out MRS_dev.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser MRSdevuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

5. Créez un fichier keytab pour le compte utilisateur de liaison LDAP qui est utilisé pour accéder et rechercher dans Active Directory pendant la synchronisation LDAP.

Structurez la valeur de l'option `-princ` en tant que `<principal name>@<KERBEROS REALM>`. Incluez le nom de la configuration LDAP pour le serveur Active Directory dans le nom de fichier keytab. Structurez celui-ci comme suit : `<Active Directory LDAP configuration_name>.keytab`.

L'exemple suivant crée un fichier keytab pour un compte utilisateur de principal de service nommé `ldapuser` :

```
ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
```

Vérifier les noms de principaux du service et les fichiers Keytab

Vous pouvez employer les utilitaires Kerberos pour vérifier que les SPN et les fichiers Keytab sont valides. Vous pouvez également employer les utilitaires pour déterminer le statut du centre de distribution de clés (KDC) Kerberos.

Vous pouvez employer des utilitaires Kerberos tels que *kinit* et *klist* pour afficher et vérifier les SPN et les fichiers Keytab. Pour employer les utilitaires, vérifiez que la variable d'environnement `KRB5_CONFIG` contient le chemin et le nom du fichier de configuration Kerberos. Pour plus d'informations sur l'exécution des utilitaires Kerberos, consultez la documentation Kerberos.

Utilisez les utilitaires suivants pour vérifier les SPN et les fichiers Keytab :

kinit

Vous pouvez employer l'utilitaire *kinit* pour demander un ticket TGT à KDC et vérifier qu'un fichier Keytab peut être utilisé pour établir une connexion Kerberos. Si le fichier Keytab et le SPN spécifié sont valides, la commande obtient un ticket et le met en cache dans le cache spécifié.

L'utilitaire *kinit* est disponible dans le répertoire suivant sur un nœud Informatica :

```
<répertoire d'installation Informatica>\java\jre\bin
```

Pour demander un TGT pour un SPN, exécutez la commande suivante :

```
kinit -c <nom du cache> -k -t <nom du fichier keytab> <nom de principal du service>
```

L'exemple de sortie suivant montre le TGT créé dans le cache par défaut pour un fichier Keytab et un SPN spécifiés :

```
Cache: \temp\krb Using principal: isp/node01/Infadomain/COMPANY.COM Using keytab:
node01.keytab Authenticated to Kerberos v5
```

klist

Vous pouvez employer l'utilitaire *klist* pour répertorier les principaux et les clés Kerberos dans un fichier Keytab. Pour répertorier les clés dans le fichier Keytab et l'horodatage de l'entrée Keytab, exécutez la commande suivante :

```
klist -k -t <nom de fichier keytab>
```

L'exemple de sortie suivant montre les principaux dans un fichier Keytab :

```
Nom de Keytab : FILE:node01.keytab KVNO Timestamp Principal ----
----- 3 12/31/16 19:00:00 MRS_dev/
node01/Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/
Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/Infadomain@COMPANY.COM 3
12/31/16 19:00:00 MRS_dev/node01/Infadomain@COMPANY.COM
```

Activer la délégation pour les comptes utilisateurs de principaux Kerberos dans Active Directory

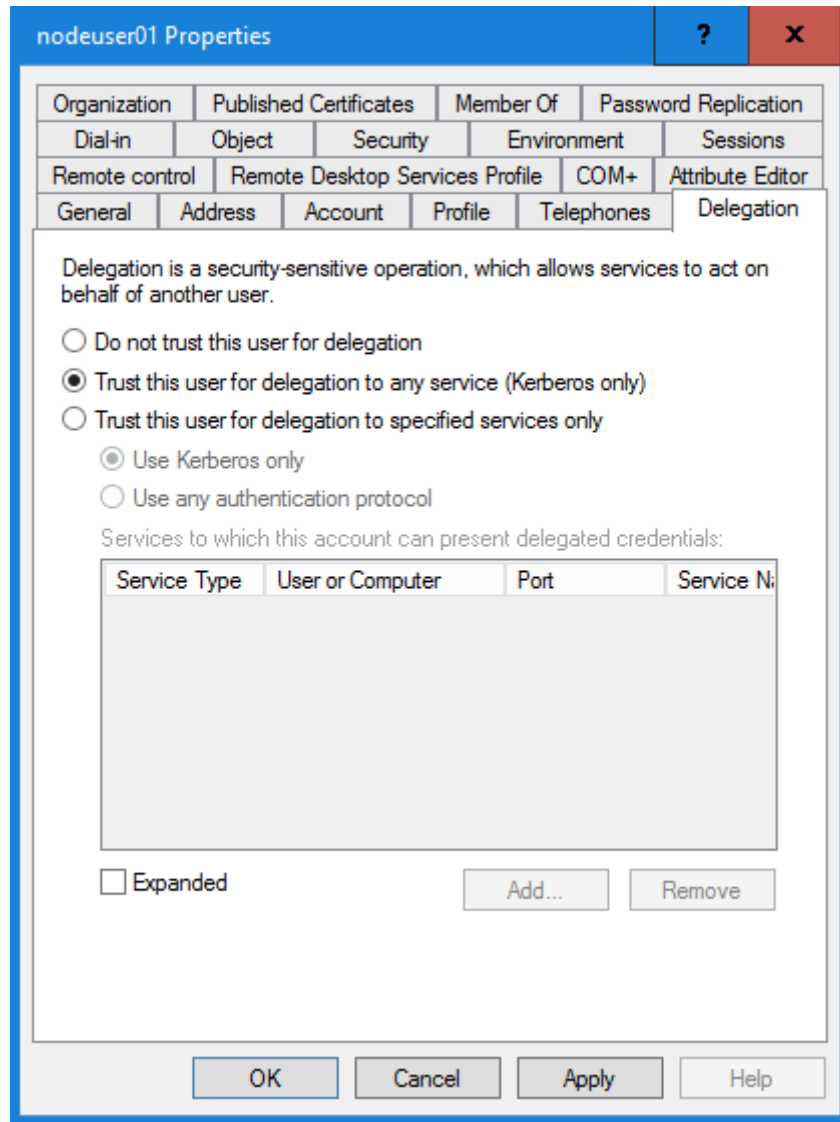
Activez la délégation pour chaque compte utilisateur de principal Kerberos que vous avez créé dans Active Directory.

L'authentification déléguée intervient quand un utilisateur est authentifié auprès d'un service et que ce service utilise les informations d'identification de l'utilisateur authentifié pour se connecter à un autre service. Du fait que les services du domaine Informatica doivent se connecter à d'autres services pour effectuer des opérations, le domaine Informatica exige que l'option de délégation soit activée dans Active Directory.

Vous devez activer la délégation pour tous les comptes que vous avez créés, à l'exception du compte utilisateur de liaison LDAP que vous utilisez pour accéder et rechercher dans Active Directory pendant la synchronisation LDAP. Définir la délégation sur **Approuver cet utilisateur pour la délégation à tous les services (Kerberos uniquement)** dans l'onglet Délégation de la boîte de dialogue de propriétés pour chaque compte utilisateur.

Remarque: L'onglet Délégation n'est pas disponible dans la boîte de dialogue Propriétés tant que vous n'exécutez pas Ktpass pour créer les fichiers Keytab.

L'image suivante montre l'onglet Délégation de la boîte de dialogue Propriétés du compte nodeuser01 :



Activation de l'authentification Kerberos

Vous pouvez activer l'authentification Kerberos dans un domaine Informatica lorsque vous installez les services Informatica ou après leur installation.

Pour plus d'informations sur l'activation de l'authentification Kerberos lors de l'installation des services Informatica, consultez le *Guide d'installation et de configuration d'Informatica 10.2 HotFix 2*.

Si vous n'activez pas l'authentification Kerberos pendant l'installation, suivez les étapes décrites dans cette section pour utiliser les programmes de ligne de commande Informatica afin d'activer l'authentification Kerberos après l'installation des services.

Activer l'authentification Kerberos dans le domaine

Activez Kerberos sur un nœud de passerelle dans le domaine.

Exécutez la commande `infasetup switchToKerberosMode` sur un nœud de passerelle dans le domaine pour passer l'authentification sur l'authentification réseau Kerberos.

1. Arrêtez le domaine et tous les services Informatica. Arrêtez les services dans l'ordre suivant :

- Service Metadata Manager
- Service d'intégration PowerCenter®
- Service de référentiel PowerCenter®
- Service de gestion de contenu
- service Analyst
- Service d'intégration de données
- Service de référentiel modèle

2. À l'invite de commandes sur un nœud de passerelle, basculez vers le répertoire où se trouve l'exécutable `infasetup` :

```
<Informatica installation directory>\isp\bin
```

3. Exécutez la commande suivante :

```
infasetup switchToKerberosMode -ad <administrator name> -srn <Kerberos realm names> -  
urn <Kerberos realm names> -spnSL <service principal level>
```

Le tableau suivant décrit les options et les arguments de la commande `infasetup switchToKerberosMode` :

Option	Argument	Description
-administratorName -ad	user_name	<p>Nom d'utilisateur du compte administrateur du domaine qui est créé lors de la configuration de l'authentification Kerberos. Spécifiez le nom d'un compte qui existe dans Active Directory.</p> <p>Après avoir configuré l'authentification Kerberos, cet utilisateur est inclus dans le domaine de sécurité <i>_infalInternalNamespace</i> que la commande crée.</p> <p>Si le domaine utilise un domaine Kerberos unique pour authentifier les utilisateurs, spécifiez le nom <code>samAccount</code> du compte à utiliser comme compte administrateur.</p> <p>Si votre domaine utilise l'authentification Kerberos inter-domaines, spécifiez le nom de principal de l'utilisateur complet du compte à utiliser comme compte administrateur, y compris le nom du domaine. Par exemple : <code>sysadmin@COMPANY.COM</code></p>
-ServiceRealmName -srn	Kerberos_realm_name	<p>Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules.</p> <p>Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : <code>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</code></p> <p>Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple : <code>*EAST.COMPANY.COM</code></p>

Option	Argument	Description
-UserRealmName -urn	Kerberos_realm_name	Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple : *EAST.COMPANY.COM
-SPNShareLevel -spnSL	NODE PROCESS	Niveau de principal du service pour le domaine. Définissez sur NODE pour activer Kerberos au niveau du nœud. Définissez sur PROCESS pour activer Kerberos au niveau du processus.

L'exemple suivant passe l'authentification du domaine sur Kerberos et définit le compte utilisateur sysadmin comme compte administrateur dans un domaine qui utilise un domaine Kerberos unique pour l'authentification des utilisateurs :

```
infasetup switchToKerberosMode -ad sysadmin -srn COMPANY.COM -urn COMPANY.COM -spnSL
NODE
```

L'exemple suivant passe l'authentification du domaine sur Kerberos et définit le compte utilisateur sysadmin comme compte administrateur dans un domaine qui utilise l'authentification Kerberos inter-domaines :

```
infasetup switchToKerberosMode -ad sysadmin@COMPANY.COM -srn
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -spnSL NODE
```

Mise à jour des nœuds dans le domaine

Mettez à jour tous les nœuds de passerelle et de travail avec les informations du serveur d'authentification Kerberos, à l'exception des nœuds de passerelle sur lesquels vous avez exécuté la commande `infasetup switchToKerberosMode`.

Utilisez les commandes suivantes pour mettre à jour les nœuds de passerelle et de travail :

infasetup UpdateGatewayNode

Utilisez la commande `UpdateGatewayNode` pour définir les paramètres d'authentification Kerberos sur un nœud de passerelle du domaine. Si le domaine comporte plusieurs nœuds de passerelle, exécutez la commande `UpdateGatewayNode` sur chaque nœud de passerelle.

infasetup UpdateWorkerNode

Utilisez la commande UpdateWorkerNode pour définir les paramètres d'authentification Kerberos sur un nœud de travail du domaine. Si le domaine comporte plusieurs nœuds de travail, exécutez la commande UpdateWorkerNode sur chaque nœud de travail.

1. À l'invite de commandes sur un nœud, basculez vers le répertoire où se trouve l'exécutable infasetup :

```
<Informatica installation directory>\isp\bin
```

2. Pour définir les paramètres d'authentification Kerberos sur un nœud de passerelle, exécutez la commande suivante :

```
infasetup UpdateGatewayNode -krb <true|false> -srn <Kerberos realm names> -urn  
<Kerberos realm names>
```

Pour définir les paramètres d'authentification Kerberos sur un nœud de travail, exécutez la commande suivante :

```
infasetup UpdateWorkerNode -krb <true|false> -srn <Kerberos realm names> -urn  
<Kerberos realm names>
```

Le tableau suivant décrit les options et les arguments requis pour activer l'authentification Kerberos sur un nœud :

Option	Argument	Description
-EnableKerberos -krb	True False	Configure le domaine Informatica pour utiliser l'authentification Kerberos. Définissez cette valeur sur True pour activer l'authentification Kerberos. La valeur par défaut est False.
-ServiceRealmName -srn	Kerberos_realm_name	Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple : *EAST.COMPANY.COM
-UserRealmName -urn	Kerberos_realm_name	Nom du domaine Kerberos utilisé pour l'authentification des utilisateurs. Le nom de domaine, sensible à la casse, doit être en majuscules. Pour configurer l'authentification Kerberos inter-domaines, spécifiez le nom de chaque domaine Kerberos utilisé pour l'authentification des utilisateurs, séparé par une virgule. Par exemple : COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Utilisez un astérisque comme caractère générique devant un nom de domaine pour inclure tous les domaines qui contiennent le nom. Par exemple : *EAST.COMPANY.COM

L'exemple suivant met à jour un nœud de travail pour utiliser l'authentification Kerberos :

```
infasetup updateWorkerNode -krb true -srn COMPANY.COM -urn COMPANY.COM
```

L'exemple suivant met à jour un nœud de travail pour utiliser l'authentification Kerberos inter-domaines :

```
infasetup updateWorkerNode -krb true -srn  
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn  
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM
```

Activation de Kerberos sur les nœuds Informatica

Après avoir activé Kerberos dans le domaine, vous devez copier le fichier de configuration Kerberos sur chaque nœud du domaine. Vous devez également configurer des navigateurs Web pour accéder aux applications Web d'Informatica.

Copiez les fichiers Keytab dans le répertoire suivant de chaque nœud :

```
<Informatica installation directory>\isp\config\keys
```

Les fichiers Keytab que vous copiez varient selon que vous activez l'authentification Kerberos au niveau du nœud ou au niveau du processus.

Fichiers Keytab au niveau du nœud

Copiez chaque fichier Keytab généré au niveau du nœud dans le nœud correspondant.

Le tableau suivant montre le nœud dans lequel copier chaque fichier Keytab :

Fichier Keytab	Emplacement sur le nœud
<nom du nœud>.keytab	Copiez chaque fichier dans le nœud correspondant.
webapp_http.keytab	Copiez chaque fichier dans le nœud de passerelle correspondant.
Idapuser.keytab	Copiez le fichier dans chaque nœud de passerelle.

Fichiers Keytab au niveau du processus

Copiez chaque fichier Keytab généré au niveau du processus dans le nœud correspondant.

Le tableau suivant montre le nœud dans lequel copier chaque fichier Keytab :

Fichier Keytab	Emplacement sur le nœud
<nom du nœud>.keytab	Copiez chaque fichier dans le nœud correspondant.
webapp_http.keytab	Copiez chaque fichier dans le nœud de passerelle correspondant.
_AdminConsole.keytab	Copiez chaque fichier dans le nœud de passerelle correspondant.
<nom du service d'application>.keytab	Copiez chaque fichier dans le nœud correspondant sur lequel s'exécute le service d'application d'Informatica.
Idapuser.keytab	Copiez le fichier dans chaque nœud de passerelle.

Configurez les navigateurs Web pour accéder aux applications Web d'Informatica.

Dans Microsoft Internet Explorer et Google Chrome, ajoutez l'URL des applications Web Informatica, telles que l'outil Analyst tool, à la liste des sites approuvés.

Si vous utilisez Chrome version 41 ou ultérieure, vous devez également définir les stratégies AuthServerWhitelist et AuthNegotiateDelegateWhitelist.

Copier les fichiers Keytab sur les nœuds Informatica

Après avoir créé les fichiers Keytab, copiez chacun d'eux dans le nœud correspondant.

Copiez les fichiers Keytab dans le répertoire suivant de chaque nœud :

```
<Informatica installation directory>\isp\config\keys
```

Les fichiers Keytab que vous copiez varient selon que vous activez l'authentification Kerberos au niveau du nœud ou au niveau du processus.

Fichiers Keytab au niveau du nœud

Copiez chaque fichier Keytab généré au niveau du nœud dans le nœud correspondant.

Le tableau suivant montre le nœud dans lequel copier chaque fichier Keytab :

Fichier Keytab	Emplacement sur le nœud
<nom du nœud>.keytab	Copiez chaque fichier dans le nœud correspondant.
webapp_http.keytab	Copiez chaque fichier dans le nœud correspondant.
Idapuser.keytab	Copiez le fichier dans chaque nœud de passerelle.

Fichiers Keytab au niveau du processus

Copiez chaque fichier Keytab généré au niveau du processus dans le nœud correspondant.

Le tableau suivant montre le nœud dans lequel copier chaque fichier Keytab :

Fichier Keytab	Emplacement sur le nœud
<nom du nœud>.keytab	Copiez chaque fichier dans le nœud correspondant.
webapp_http.keytab	Copiez chaque fichier dans le nœud correspondant.
_AdminConsole.keytab	Copiez chaque fichier dans le nœud correspondant.
<nom du service d'application>.keytab	Copiez chaque fichier dans le nœud correspondant sur lequel s'exécute le service d'application d'Informatica.
Idapuser.keytab	Copiez le fichier dans chaque nœud.

Activer l'authentification Kerberos pour les clients Informatica

Copiez le fichier de configuration Kerberos sur chaque ordinateur qui héberge un client Informatica, puis définissez une variable d'environnement pour qu'elle pointe vers le fichier de configuration. Vous devez également activer les navigateurs clients pour accéder aux applications Web d'Informatica.

Après avoir configuré le domaine Informatica pour qu'il s'exécute avec l'authentification Kerberos, effectuez les tâches suivantes sur les outils clients Informatica :

Copiez le fichier de configuration Kerberos sur chaque hôte client d'Informatica.

Copiez le fichier `krb5.conf` sur chaque ordinateur qui héberge un client Informatica, tel que le client PowerCenter ou Informatica Developer (outil Developer tool). Copiez le fichier dans le répertoire suivant sur chaque hôte :

```
<Informatica installation directory>\clients\shared\security
```

Définissez la variable d'environnement KRB5_CONFIG sur chaque hôte du client Informatica.

Définissez la variable d'environnement KRB5_CONFIG sur le chemin d'accès et le nom du fichier de configuration Kerberos sur chaque ordinateur qui héberge des clients Informatica, tels que le client PowerCenter et l'outil Developer tool.

Configurez les navigateurs Web pour accéder aux applications Web d'Informatica.

Dans Microsoft Internet Explorer et Google Chrome, ajoutez l'URL des applications Web Informatica, telles que l'outil Analyst tool, à la liste des sites approuvés.

Si vous utilisez Chrome version 41 ou ultérieure, vous devez également définir les stratégies `AuthServerWhitelist` et `AuthNegotiateDelegateWhitelist`.

Activation des comptes utilisateurs pour utiliser l'authentification Kerberos

Une fois que vous avez activé l'authentification Kerberos dans le domaine, importez les comptes utilisateurs Informatica à partir d'Active Directory dans le domaine de sécurité LDAP qui contient les comptes utilisateurs Kerberos. Vous devez également migrer les groupes, rôles, privilèges et autorisations du domaine de sécurité natif vers les comptes utilisateurs Active Directory correspondants dans le domaine de sécurité LDAP qui contient les comptes utilisateurs Kerberos.

Importer des comptes utilisateurs d'Active Directory dans des domaines de sécurité LDAP

Importez des comptes utilisateurs d'Active Directory dans des domaines de sécurité LDAP.

Lorsque vous activez l'authentification Kerberos dans le domaine, Informatica crée un domaine de sécurité LDAP vide du même nom que le domaine Kerberos. Vous pouvez importer des comptes utilisateurs d'Active Directory dans ce domaine de sécurité LDAP, ou vous pouvez importer les comptes utilisateurs dans un domaine de sécurité LDAP différent.

Utilisez l'outil Administrator tool pour importer les comptes utilisateurs qui utilisent l'authentification Kerberos à partir d'Active Directory dans un domaine de sécurité LDAP.

Pour configurer l'authentification Kerberos inter-domaines, connectez-vous au catalogue global Active Directory. Lors de la connexion au catalogue global, vous importez des utilisateurs du serveur Active Directory utilisé par chaque domaine Kerberos.

1. Démarrez le domaine et tous les services Informatica.
2. Connectez-vous à Windows avec le compte administrateur que vous avez spécifié lorsque vous avez activé l'authentification Kerberos dans le domaine.
3. Connexion à l'outil Administrator tool. Sélectionnez `_infalInternalNamespace` comme domaine de sécurité.

4. Dans l'outil Administrator, cliquez sur l'onglet **Sécurité**.
5. Cliquez sur le menu **Actions** et sélectionnez **Configuration LDAP**.
6. Dans la boîte de dialogue **Configuration LDAP**, cliquez sur l'onglet **Connectivité LDAP**.
7. Configurez les propriétés de la connexion du serveur Active Directory.

Vous devrez peut-être consulter l'administrateur LDAP pour obtenir les informations nécessaires à la connexion au serveur LDAP.

Le tableau suivant décrit les propriétés de configuration du serveur LDAP :

Propriété	Description
Nom du serveur	Nom d'hôte ou adresse IP du serveur Active Directory. Pour configurer l'authentification Kerberos inter-domaines, connectez-vous à l'hôte du catalogue global Active Directory. Spécifiez le nom d'hôte complet. Par exemple : host.company.local
Port	Port d'écoute du serveur Active Directory. La valeur par défaut est 389. Le port SSL par défaut est 636. Pour configurer l'authentification Kerberos inter-domaines, connectez-vous au port du catalogue global Active Directory. La valeur par défaut est 3268. Le port SSL par défaut est 3269.
Service d'annuaire LDAP	Sélectionnez Service Microsoft Active Directory .
Nom	Spécifiez le compte utilisateur de liaison que vous avez créé dans Active Directory pour synchroniser des comptes dans Active Directory avec le domaine de sécurité LDAP. Étant donné que l'authentification Kerberos est activée sur le domaine, vous n'avez pas la possibilité de fournir un mot de passe pour le compte. Si le domaine utilise l'authentification Kerberos inter-domaines, incluez le nom du domaine auquel la base de données du principal Active Directory appartient.
Utiliser le certificat SSL	Indique que le serveur LDAP utilise le protocole SSL (Secure Socket Layer).
Certificat LDAP d'approbation	Détermine si le gestionnaire de service peut se fier au certificat SSL du serveur LDAP. Si cette option est sélectionnée, le gestionnaire de service se connecte au serveur LDAP sans vérifier le certificat SSL. Sinon, le gestionnaire de service vérifie que le certificat SSL est signé par une autorité de certification avant de se connecter au serveur LDAP.
Non sensible à la casse	Indique que le gestionnaire de service ne doit pas tenir compte de la sensibilité à la casse pour les attributs de noms uniques lors de l'assignation d'utilisateurs aux groupes.

Propriété	Description
Attribut d'appartenance à un groupe	Nom de l'attribut qui contient les informations d'appartenance au groupe d'un utilisateur. Attribut de l'objet de groupe LDAP qui contient les DN des utilisateurs et des groupes membres d'un groupe. Par exemple, <i>member</i> ou <i>memberof</i> .
Taille maximale	<p>Nombre maximal de comptes utilisateurs à importer dans un domaine de sécurité. Par exemple, si la valeur est définie sur 100, vous pouvez importer un maximum de 100 comptes utilisateurs dans le domaine de sécurité.</p> <p>Si le nombre d'utilisateurs à importer dépasse la valeur de cette propriété, le gestionnaire de service génère un message d'erreur et n'importe pas d'utilisateurs. Définissez une valeur plus importante pour cette propriété si vous avez de nombreux utilisateurs à importer.</p> <p>La valeur par défaut est 1000.</p>

8. Dans la boîte de dialogue **Configuration LDAP**, cliquez sur l'onglet **Domaines de sécurité**.
9. Cliquez sur **Ajouter**.

Le tableau suivant décrit les propriétés de filtre que vous pouvez définir pour un domaine de sécurité :

Propriété	Description
Domaine de sécurité	Nom du domaine de sécurité LDAP dans lequel vous souhaitez importer des comptes utilisateurs à partir d'Active Directory.
Base de recherche des utilisateurs	<p>Nom unique (NU) de l'entrée qui sert de point de départ à la recherche des noms de groupes dans Active Directory. La recherche s'effectue sur un objet dans l'annuaire selon le chemin d'accès dans le nom unique de l'objet.</p> <p>Par exemple, pour rechercher le conteneur USERS contenant des comptes utilisateurs Informatica dans le domaine Windows example.com, spécifiez CN=USERS,DC=EXAMPLE,DC=COM.</p>
Filtre d'utilisateurs	<p>Une chaîne de requête LDAP qui spécifie les critères de recherche pour les utilisateurs dans le service d'annuaire. Le filtre peut indiquer les types d'attributs, les valeurs d'assertion et les critères de correspondance.</p> <p>Par exemple : <code>(objectclass=*)</code> recherche tous les objets. <code>(&(objectClass=user)(!(cn=susan)))</code> recherche tous les objets utilisateurs sauf « susan ». Pour plus d'informations sur les filtres de recherche, consultez la documentation du service d'annuaire LDAP.</p>

Propriété	Description
Base de recherche des groupes	Le nom unique (DN) de l'entrée sert de point de départ pour rechercher les noms de groupes dans le service d'annuaire LDAP.
Filtre de groupes	Chaîne de requête LDAP qui spécifie les critères de recherche pour les groupes dans le service d'annuaire.

L'image suivante montre les informations requises pour importer des utilisateurs LDAP depuis Active Directory dans le domaine de sécurité LDAP créé lorsque vous avez activé Kerberos dans le domaine :

The screenshot shows the 'LDAP Configuration' dialog box with the 'Security Domains' tab selected. The dialog has three tabs: 'LDAP Connectivity', 'Security Domains', and 'Schedule'. Below the tabs, there is a message: 'Fields marked with an asterisk (*) are required.' and 'You can specify multiple security domains for LDAP users and groups. Click Add to add a new security domain.' To the right of this message is a green plus icon and the text 'Add'. Below this is a section titled 'Add new Security Domain' with a dropdown arrow, a magnifying glass icon, and the text 'Preview' and 'Cancel'. The form contains the following fields: 'Security Domain *' with the value 'COMPANY.COM', 'User search base' with the value 'CN=USERS,DC=COMPANY,DC=COM', 'User filter' (empty), 'Group search base' (empty), and 'Group filter' (empty). At the bottom of the dialog are three buttons: 'Synchronize Now', 'OK', and 'Cancel'.

10. Cliquez sur **Synchroniser maintenant**.

Le gestionnaire de service synchronise les utilisateurs de tous les domaines de sécurité LDAP avec ceux du service d'annuaire LDAP. La durée de la synchronisation dépend du nombre d'utilisateurs et de groupes à importer.

11. Cliquez sur **OK** pour enregistrer le domaine de sécurité LDAP.

Migrer les privilèges et autorisations des utilisateurs natifs vers le domaine de sécurité Kerberos

Si le domaine Informatica comporte des comptes utilisateurs dans le domaine de sécurité natif, les comptes utilisateurs Active Directory correspondants du domaine de sécurité Kerberos doivent comporter les mêmes groupes, rôles, privilèges et autorisations. Migrez les groupes, rôles, privilèges et autorisations des

utilisateurs natifs vers les comptes utilisateurs correspondants dans le domaine de sécurité LDAP de Kerberos.

1. Vérifiez la liste des comptes utilisateurs natifs et déterminez les comptes à migrer vers un domaine de sécurité LDAP pour l'authentification Kerberos.

Pour répertorier les comptes utilisateurs du domaine Informatica, exécutez la commande suivante :

```
infacmd isp ListAllUsers
```

Chaque compte utilisateur natif à migrer vers le domaine de sécurité Kerberos doit avoir un compte correspondant dans le service Active Directory que vous utilisez pour l'authentification Kerberos.

2. Créez le fichier de migration d'utilisateur.

Le fichier de migration d'utilisateur est un fichier en texte brut qui contient la liste des utilisateurs natifs et des utilisateurs Kerberos correspondants qui requièrent les mêmes groupes, rôles, privilèges et autorisations.

Utilisez le format suivant pour répertorier les entrées du fichier de migration d'utilisateur :

```
Native/<source user name>,<LDAP security domain>/<target user name>
```

L'exemple suivant montre un fichier de migration d'utilisateur contenant la liste suivante des utilisateurs à migrer vers le domaine de sécurité COMPANY.COM :

```
Native/User1,COMPANY.COM/User1
Native/User2,COMPANY.COM/User2
Native/User3,COMPANY.COM/User3
```

3. Exécutez la commande `infacmd isp migrateUsers` pour migrer les privilèges et autorisations de compte dans le domaine de sécurité natif vers les comptes du domaine de sécurité Kerberos.

Pour migrer les groupes, rôles, privilèges et autorisations des utilisateurs, exécutez la commande suivante :

```
infacmd isp migrateUsers -dn <domain name> -un <administrator user name> -pd
<administrator password> -sdn <security domain> -umf <user migration file>
```

Le tableau suivant décrit les options de la commande

Option	Description
-DomainName -dn	Nom du domaine Informatica.
-UserName -un	Nom d'utilisateur pour se connecter au domaine. Spécifiez le nom d'utilisateur du compte administrateur que vous avez spécifié dans la commande <code>infasetup switchToKerberosMode</code> .
-Password -pd	Mot de passe du compte administrateur.
-SecurityDomain -sdn	Domaine de sécurité LDAP du compte administrateur utilisé pour se connecter au domaine. Spécifiez <code>_infaInternalNamespace</code> .
-UserMigrationFile -umf	Chemin et nom du fichier de migration d'utilisateur. La commande ignore les entrées comportant un nom d'utilisateur source ou cible en double.

L'exemple suivant migre les groupes, rôles, privilèges et autorisations des utilisateurs en fonction du fichier de migration de l'utilisateur `um_s.txt` :

```
infacmd isp migrateUsers -dn InfaDomain -un nodeuser01 -pd password -sdn
_infaInternalNamespace -umf C:\Infa\um_s.txt
```


La commande écrase les autorisations d'objet de connexion attribuées à l'utilisateur LDAP avec les autorisations d'objet de connexion de l'utilisateur natif. La commande fusionne les groupes, rôles, privilèges et autorisations d'objet de domaine des utilisateurs natifs et des utilisateurs LDAP correspondants.

La commande `migrateUsers` crée un fichier journal détaillé nommé `infacmd_umt_<date>_<time>.txt` dans le répertoire dans lequel vous exécutez la commande.

CHAPITRE 5

Authentification SAML pour les applications Web Informatica

Ce chapitre comprend les rubriques suivantes :

- [Présentation de l'authentification SAML, 66](#)
- [Processus d'authentification SAML, 68](#)
- [Activer l'authentification SAML dans un domaine, 69](#)
- [Sécurité de l'authentification améliorée, 71](#)
- [Configurer les applications Web pour utiliser des fournisseurs d'identité différents, 74](#)

Présentation de l'authentification SAML

Vous pouvez configurer l'authentification SAML (Security Assertion Markup Language) pour les applications Web Informatica.

Le langage SAML (Security Assertion Markup Language) est un format de données XML utilisé pour échanger les informations d'authentification entre un fournisseur de services et un fournisseur d'identité. Dans un domaine Informatica, l'application Web Informatica est le fournisseur de services.

Vous pouvez configurer les applications Web Informatica suivantes afin d'utiliser l'authentification SAML :

- Informatica Administrator
- Informatica Analyst
- Outil Ingestion de masse
- Metadata Manager
- Enterprise Data Catalog
- Enterprise Data Preparation
- Data Privacy Management

Remarque: L'authentification SAML ne peut pas être utilisée dans un domaine Informatica configuré pour utiliser l'authentification Kerberos.

Si vous activez un domaine pour utiliser l'authentification SAML, toutes les applications Web qui s'exécutent dans le domaine utilisent le fournisseur d'identité que vous configurez par défaut dans le domaine. En revanche, vous pouvez configurer des applications Web qui s'exécutent dans un domaine pour utiliser des fournisseurs d'identité différents. Par exemple, il est possible de configurer Informatica Administrator pour

utiliser AD FS comme fournisseur d'identité et de configurer Informatica Analyst pour utiliser PingFederate comme fournisseur d'identité.

Pour plus d'informations sur la configuration des applications Web permettant d'utiliser des fournisseurs d'identité différents, consultez la section ["Configurer les applications Web pour utiliser des fournisseurs d'identité différents" à la page 74.](#)

Répertoire du keystore et du truststore par défaut

Le déploiement d'Informatica inclut les fichiers keystore et truststore par défaut dans le répertoire

`<Informatica installation directory>\services\shared\security.`

Informatica vous recommande d'utiliser le keystore et le truststore par défaut uniquement pour la configuration et les cas d'utilisation de preuve de concept. Pour sécuriser un environnement de production, utilisez les directives suivantes :

- Configurez un keystore et un truststore personnalisés pour l'authentification SAML dans un emplacement autre que le répertoire par défaut :

`<Informatica installation directory>\services\shared\security`

- Vous ne pouvez pas utiliser le keystore et le truststore par défaut pour configurer d'autres services ou clients.

- Lorsque vous activez l'authentification SAML, vous importez des fichiers de certificats keystore ou truststore et des clés privées dans le répertoire par défaut :

`<Informatica installation directory>\services\shared\security`

- Lorsque vous attribuez un alias au keystore ou au truststore, n'utilisez pas « Informatica LLC », car Informatica utilise ce nom pour l'authentification par clé privée et la signature de certificats.
- La modification du keystore ou du truststore SAML par défaut est autorisée uniquement lorsque le répertoire par défaut est configuré en tant que répertoire de keystore et truststore SAML et que vous souhaitez importer des entrées de clé privée et de certificat dans le keystore ou le truststore par défaut.

Vous ne pouvez pas utiliser « Informatica LLC » comme alias pour les nouvelles entrées dans le keystore et le truststore par défaut. Vous pouvez utiliser « Informatica LLC » comme alias pour les entrées de keystore/truststore personnalisées.

Aucune autre opération n'est autorisée pour les fichiers keystore et truststore par défaut, y compris la suppression ou le remplacement des fichiers, la modification du mot de passe du keystore ou du truststore, ni la modification, la suppression ou le remplacement de la clé privée et du certificat de signature générés par Informatica.

Fournisseurs d'identité pris en charge

Utilisez un fournisseur d'identité pris en charge pour gérer l'authentification SAML sur le domaine pour les applications Web.

Informatica prend en charge les fournisseurs d'identité suivants. Cliquez sur le lien de l'article How-to Library (H2L) pour obtenir des instructions d'intégration entre chaque fournisseur d'identité et le domaine.

Fournisseur d'identité	Article How-to Library (H2L)
Microsoft Active Directory Federation Services (AD FS)	SAML Authentication with Active Directory Federation Services in Informatica 10.4.0
PingFederate	SAML Authentication with PingFederate in Informatica 10.4.0

Fournisseur d'identité	Article How-to Library (H2L)
F5 Big-IP	SAML Authentication with F5 Networks BIG-IP in Informatica 10.4.1
NetScaler	SAML Authentication with NetScaler for Web Applications
Oracle Access Manager (OAM)	Authentification SAML avec Oracle Access Manager pour les applications Web
Okta SSO	Authentification SAML avec Okta SSO pour les applications Web
Azure Active Directory	Authentification SAML avec Azure Active Directory pour les applications Web

Pour plus d'informations sur les versions prises en charge de ces fournisseurs d'identité, consultez la matrice de disponibilité des produits sur Informatica Network :

<https://network.informatica.com/community/informatica-network/product-availability-matrices>.

Processus d'authentification SAML

Applications Web Informatica et informations d'authentification pour l'échange du fournisseur d'identité permettant d'activer l'authentification SAML dans un domaine Informatica.

Les étapes suivantes décrivent le flux d'authentification SAML de base :

1. Un utilisateur accède à une application Web Informatica.
2. L'utilisateur sélectionne le domaine de sécurité contenant les comptes utilisateur LDAP pour l'authentification SAML sur la page de connexion à l'application, puis clique sur le bouton de connexion.
Si l'utilisateur sélectionne le domaine de sécurité natif, il fournit un nom d'utilisateur et un mot de passe et se connecte à l'application.
3. En fonction de la configuration du fournisseur d'identité, l'utilisateur est invité à fournir les informations d'identification requises pour la première authentification.
4. Le fournisseur d'identité valide les informations d'identification de l'utilisateur et crée une session pour l'utilisateur.
Le fournisseur d'identité valide également l'URL de l'application Web cible, puis redirige l'utilisateur vers l'application Web avec un jeton SAML contenant les informations d'identité de l'utilisateur.
5. L'application valide les informations du jeton SAML et de l'identité de l'utilisateur, crée une session utilisateur, puis termine le processus de connexion de l'utilisateur.

La session utilisateur existante dans le navigateur est utilisée pour l'authentification ultérieure. Pour sélectionner une autre application Web Informatica configurée pour utiliser l'authentification SAML, l'utilisateur sélectionne le domaine de sécurité LDAP sur la page de connexion à l'application. L'utilisateur n'a pas besoin d'indiquer de nom d'utilisateur ou de mot de passe.

L'utilisateur reste connecté à toutes les applications Web Informatica exécutées dans la même session de navigateur. Néanmoins, si l'utilisateur se déconnecte d'une application Web Informatica, il est également déconnecté des autres applications Web Informatica exécutées dans la même session du navigateur.

Activer l'authentification SAML dans un domaine

Configurez le fournisseur d'identité, le domaine Informatica et les nœuds de passerelle dans le domaine pour utiliser l'authentification SAML.

Pour configurer l'authentification SAML des applications Web Informatica prises en charge qui s'exécutent dans un domaine, effectuez les tâches suivantes :

1. Créez une configuration LDAP pour vous connecter au magasin d'identités LDAP qui contient les comptes utilisateur des applications Web Informatica. Vous créez également un domaine de sécurité LDAP, puis importez les comptes utilisateur dans le domaine de sécurité.
2. Exportez le certificat de signature d'assertion à partir du fournisseur d'identité.
3. Importez le certificat de signature d'assertion dans un fichier truststore sur chaque nœud de passerelle du domaine. Vous pouvez importer le certificat dans le fichier truststore Informatica par défaut ou dans un fichier truststore personnalisé.
4. Ajoutez un ou plusieurs tiers de confiance ou fournisseurs de services dans le fournisseur d'identité.
5. Ajoutez l'URL de chaque application Web Informatica au fournisseur d'identité.
6. Activez l'authentification SAML dans le domaine
7. Activez l'authentification SAML sur chaque nœud de passerelle dans le domaine.

Remarque: Pour plusieurs des fournisseurs d'identité SAML pris en charge par Informatica, vous pouvez suivre les étapes d'intégration détaillées dans un article How-To Library (H2L). Voir ["Fournisseurs d'identité pris en charge" à la page 67](#) pour obtenir des liens vers les articles.

Créer une configuration LDAP pour le fournisseur d'identité ou le magasin LDAP

Utilisez l'outil Administrator tool pour créer une configuration LDAP pour le fournisseur d'identité ou le magasin LDAP qui contient les comptes utilisateur de l'application Web qui utilisent l'authentification SAML.

Lorsque vous créez une configuration LDAP, vous créez un domaine de sécurité pour les comptes utilisateur, puis importez les comptes dans le domaine de sécurité. Après avoir importé les comptes dans le domaine de sécurité, attribuez les rôles, privilèges et autorisations de domaine Informatica appropriés aux comptes du domaine de sécurité.

Pour plus d'informations sur la création d'une configuration LDAP, consultez la section ["Création d'une configuration LDAP" à la page 26](#).

Exporter le certificat de signature d'assertion

Le fournisseur d'identité envoie des assertions d'authenticité aux fournisseurs de services sous la forme d'un certificat de signature d'assertion.

Une assertion signée contient une signature créée par le fournisseur d'identité à l'aide d'un algorithme choisi par l'administrateur du fournisseur d'identité. Informatica vérifie ensuite la signature à l'aide du certificat public correspondant que l'administrateur de domaine a importé dans le trustore SAML.

L'assertion signée est activée par défaut et ne peut pas être désactivée.

Toutes les demandes d'authentification SAML prises en charge par Informatica utilisent une assertion signée. Exportez le certificat de signature d'assertion à partir du fournisseur d'identité pour activer l'assertion signée.

Importer le certificat dans le fichier truststore utilisé pour l'authentification SAML

Importez le certificat de signature d'assertion utilisé par le fournisseur d'identité dans le fichier truststore utilisé pour l'authentification SAML sur chaque nœud de passerelle du domaine Informatica.

Vous pouvez importer le certificat dans le fichier truststore Informatica par défaut ou dans un fichier truststore personnalisé.

Configurer le fournisseur d'identité

Configurez le fournisseur d'identité pour qu'il envoie les jetons SAML aux applications Web Informatica.

Effectuez les tâches suivantes pour configurer le fournisseur d'identité :

- Ajoutez un tiers de confiance pour le domaine dans le fournisseur d'identité. La définition du tiers de confiance permet au fournisseur d'identité d'accepter les demandes d'authentification des applications Web Informatica exécutées dans le domaine.
- Modifiez la règle Envoyer les attributs LDAP comme revendications de sorte à mapper les attributs LDAP de votre magasin d'identités aux types correspondants utilisés dans les jetons SAML émis par le fournisseur d'identité.

Vous indiquez le nom du tiers de confiance lorsque vous activez l'authentification SAML dans un domaine. En fonction de vos exigences de sécurité, vous pouvez créer plusieurs tiers de confiance dans le fournisseur d'identité pour permettre aux domaines utilisés par différentes organisations de l'entreprise d'utiliser l'authentification SAML.

Informatica reconnaît « Informatica » comme nom de tiers de confiance par défaut. Si vous créez un tiers de confiance unique avec « Informatica » en tant que nom de tiers de confiance, vous n'avez pas besoin de fournir le nom de tiers de confiance lorsque vous activez l'authentification SAML dans un domaine.

Remarque: Toutes les chaînes sont sensibles à la casse dans le fournisseur d'identité, y compris les URL.

Ajouter des URL de l'application Web Informatica au fournisseur d'identité

Ajoutez l'URL de chaque application Web Informatica dans le fournisseur d'identité à l'aide de l'authentification SAML.

Fournissez l'URL d'une application Web Informatica pour permettre au fournisseur d'identité d'accepter les demandes d'authentification envoyées par l'application. L'URL fournie permet également au fournisseur d'identité d'envoyer le jeton SAML à l'application une fois l'utilisateur authentifié.

Configurer l'authentification SAML dans le domaine

Vous pouvez configurer l'authentification SAML dans un domaine Informatica existant ou l'activer lorsque vous créez un domaine.

Lorsque vous activez l'authentification SAML pour un domaine, toutes les applications Web qui s'exécutent dans ce domaine utilisent le fournisseur d'identité par défaut que vous spécifiez lorsque vous activez l'authentification SAML dans le domaine.

Sélectionnez l'une des options suivantes :

Activez l'authentification SAML lorsque vous exécutez le programme d'installation d'Informatica.

Vous pouvez activer l'authentification SAML et spécifier l'URL du fournisseur d'identité lorsque vous configurez le domaine dans le cadre de l'installation.

Activez l'authentification SAML dans un domaine existant.

Utilisez la commande `infasetup updateDomainSamlConfig` pour activer l'authentification SAML dans un domaine Informatica existant. Vous pouvez exécuter la commande sur n'importe quel nœud de passerelle au sein du domaine.

Activez l'authentification SAML lorsque vous créez un domaine.

Utilisez la commande `infasetup defineDomain` pour activer l'authentification SAML lorsque vous créez un domaine.

Pour obtenir des instructions sur l'utilisation des commandes, consultez le *Guide de référence des commandes d'Informatica*.

Activer l'authentification SAML sur les nœuds de passerelle

Vous devez configurer l'authentification SAML sur chaque nœud de passerelle dans le domaine Informatica.

Sélectionnez l'une des options suivantes pour configurer l'authentification SAML sur un nœud de passerelle :

Activez l'authentification SAML lorsque vous définissez un nœud de passerelle sur un ordinateur.

Utilisez la commande `infasetup DefineGatewayNode` pour activer l'authentification SAML sur le nœud de passerelle.

Activez l'authentification SAML lorsque vous configurez un nœud de passerelle pour joindre un domaine qui utilise l'authentification SAML.

Utilisez la commande `infasetup UpdateGatewayNode` pour activer l'authentification SAML sur le nœud de passerelle.

Activez l'authentification SAML lorsque vous convertissez un nœud de travail en nœud de passerelle.

Utilisez la commande `isp SwitchToGatewayNode` pour activer l'authentification SAML sur le nœud.

Pour obtenir des instructions sur l'utilisation des commandes, consultez le *Guide de référence des commandes d'Informatica*.

Sécurité de l'authentification améliorée

Vous pouvez activer la signature de demande, la réponse signée ou l'assertion chiffrée pour améliorer la sécurité de l'authentification :

Signature de demande

Une demande d'authentification signée contient une signature afin de vérifier l'authenticité de la demande elle-même. Informatica, agissant en tant que fournisseur de services, envoie une demande d'authentification au fournisseur d'identité. Pour maintenir l'intégrité de la demande, la demande d'authentification peut être signée.

Informatica signe une demande SAML à l'aide d'une clé privée et le fournisseur d'identité vérifie cette signature à l'aide du certificat public correspondant.

Informatica envoie des demandes d'authentification SAML via HTTP-Redirect. Les demandes utilisent le codage deflate, qui place la signature dans un paramètre d'URL.

Réponse signée

Le fournisseur d'identité répond aux demandes d'authentification d'un fournisseur de services. Une réponse signée contient une signature créée par le fournisseur d'identité à l'aide d'un algorithme choisi par l'administrateur du fournisseur d'identité. Informatica vérifie ensuite la signature à l'aide du certificat public correspondant que l'administrateur de domaine a importé dans le trustore SAML.

Assertion signée et assertion chiffrée

Le fournisseur d'identité envoie des assertions d'authenticité aux fournisseurs de services.

Une assertion signée contient une signature créée par le fournisseur d'identité à l'aide d'un algorithme choisi par l'administrateur du fournisseur d'identité. Informatica vérifie ensuite la signature à l'aide du certificat public correspondant que l'administrateur de domaine a importé dans le trustore SAML. L'assertion signée est activée par défaut et ne peut pas être désactivée.

L'administrateur Informatica génère une clé asymétrique (clé publique-privée).

L'assertion signée peut être chiffrée par le fournisseur d'identité à l'aide d'une clé de chiffrement d'assertion, qui est une clé symétrique générée par le fournisseur d'identité.

Lorsque vous activez l'assertion chiffrée, le fournisseur d'identité chiffre également la clé symétrique à l'aide du certificat public que l'administrateur de sécurité a importé dans le fournisseur d'identité. La réponse SAML contiendra l'assertion chiffrée et une clé symétrique chiffrée. Agissant en tant que fournisseur de services, Informatica déchiffre la clé symétrique chiffrée à l'aide de la clé privée correspondante que l'administrateur Informatica importe dans le keystore SAML. Après avoir obtenu la clé symétrique, Informatica déchiffre l'assertion chiffrée.

Suivez les étapes de cette section pour activer la signature de demande, l'assertion chiffrée ou la réponse signée.

Signature de demande

Vous pouvez activer la signature de demande pendant ou après le processus d'installation/de mise à niveau à l'aide d'infasetup, de l'outil Administrator tool ou de l'outil Analyst tool.

Pendant le processus d'installation ou de mise à niveau, cochez l'option **Demande signée** dans l'utilitaire d'installation.

Une fois le processus d'installation ou de mise à niveau terminé, configurez la signature de demande à l'aide d'infasetup ou de l'outil Administrator tool.

infasetup

Pour utiliser infasetup, utilisez les options suivantes avec la commande `infasetup`

`updateDomainSamlConfig` :

```
[<-SignSamlRequest|-ssr> sign_saml_request]
[<-RequestSigningPrivateKeyAlias|-rspa> saml_request_signing_private_key_alias]
[<-RequestSigningPrivateKeyPassword|-rspp> saml_request_signing_private_key_password]
[<-RequestSigningAlgorithm|-rsa> saml_request_signing_algorithm]
```

Pour plus d'informations sur ces commandes, consultez le *Guide de référence des commandes Informatica*.

Outil Administrator

Configurez la signature de demande dans l'outil Administrator tool.

1. Dans le navigateur de domaine, sélectionnez le nœud de domaine.

2. Dans les propriétés du nœud, cliquez sur l'icône **Éditer** de la section **Configuration SAML**.
3. Sélectionnez **Activer la signature de demande**.
4. Renseignez les propriétés suivantes :
 - Alias de clé privée de signature
 - Mot de passe de clé privée de signature
 - Algorithme de signature
5. Cliquez sur **OK**.
6. Redémarrez le domaine.

Réponse signée

Activez la réponse signée pour permettre au fournisseur d'identité de signer les réponses aux demandes d'authentification du fournisseur de services.

Vous pouvez activer la réponse signée pendant ou après le processus d'installation/de mise à niveau à l'aide d'infasetup, de l'outil Administrator tool ou de l'outil Analyst tool.

Pendant le processus d'installation ou de mise à niveau, cochez l'option **Réponse signée** dans l'utilitaire d'installation.

Une fois le processus d'installation ou de mise à niveau terminé, configurez la signature de réponse à l'aide d'infasetup ou de l'outil Administrator tool.

Remarque: Le fournisseur d'identité Okta SSO ne prend pas en charge la réponse signée.

infasetup

Pour utiliser infasetup, utilisez les options suivantes avec la commande `infasetup updateDomainSamlConfig` :

```
[<-SamlResponseSigned|-srs> saml_response_signed]
[<-ResponseSigningCertificateAlias|-rsca> idp_response_signing_certificate_alias]
```

Pour plus d'informations sur ces commandes, consultez le *Guide de référence des commandes Informatica*.

Outil Administrator

Configurez la signature de réponse dans l'outil Administrator tool.

1. Dans le navigateur de domaine, sélectionnez le nœud de domaine.
2. Dans les propriétés du nœud, cliquez sur l'icône **Éditer** de la section **Configuration SAML**.
3. Sélectionnez **Activer la signature de réponse**.
4. Renseignez la propriété Alias de certificat de signature de réponse.
5. Cliquez sur **OK**.
6. Redémarrez le domaine.

Assertion chiffrée

Activez l'assertion chiffrée pour permettre au fournisseur d'identité de chiffrer les assertions d'authenticité à l'aide d'une clé symétrique.

Vous pouvez activer la signature d'assertion ou l'assertion chiffrée pendant ou après le processus d'installation/de mise à niveau à l'aide d'infasetup, de l'outil Administrator tool ou de l'outil Analyst tool.

Pendant le processus d'installation ou de mise à niveau, cochez l'option **Chiffrer l'assertion** dans l'utilitaire d'installation.

Une fois le processus d'installation ou de mise à niveau terminé, configurez l'assertion chiffrée à l'aide d'infasetup ou de l'outil Administrator tool.

infasetup

Pour utiliser infasetup, utilisez les options suivantes avec la commande `infasetup updateDomainSamlConfig` :

```
[<-SamlAssertionEncrypted|-sae> saml_assertion_encrypted]
[<-EncryptedAssertionPrivateKeyAlias|-eapa> saml_encrypted_assertion_private_key_alias]
[<-EncryptedAssertionPrivateKeyPassword|-eapp>
saml_encrypted_assertion_private_key_password]
```

Pour plus d'informations sur ces commandes, consultez le *Guide de référence des commandes Informatica*.

Outil Administrator tool

Configurez l'assertion chiffrée dans l'outil Administrator tool.

1. Dans le navigateur de domaine, sélectionnez le nœud de domaine.
2. Dans les propriétés du nœud, cliquez sur l'icône **Éditer** de la section **Configuration SAML**.
3. Sélectionnez **Activer le chiffrement d'assertion**.
4. Renseignez les propriétés suivantes :
 - Alias de clé privée de chiffrement d'assertion
 - Mot de passe de clé privée de chiffrement d'assertion
5. Cliquez sur **OK**.
6. Redémarrez le domaine.

Configurer les applications Web pour utiliser des fournisseurs d'identité différents

Vous pouvez configurer des applications Web Informatica qui s'exécutent dans un domaine permettant d'utiliser des fournisseurs d'identité différents. Par exemple, il est possible de configurer Informatica Administrator pour utiliser AD FS comme fournisseur d'identité et de configurer Informatica Analyst pour utiliser PingFederate comme fournisseur d'identité.

Lorsque vous activez un domaine pour utiliser l'authentification SAML, toutes les applications Web qui s'exécutent dans le domaine utilisent le fournisseur d'identité par défaut que vous spécifiez lorsque vous activez l'authentification SAML dans le domaine. Par exemple, si vous configurez AD FS comme fournisseur

d'identité, toutes les applications Web l'utilisent comme fournisseur d'identité, sauf si vous configurez une application Web permettant d'utiliser un fournisseur d'identité différent.

Vous spécifiez le fournisseur d'identité par défaut lorsque vous utilisez l'une des options suivantes permettant d'activer l'authentification SAML :

- Lorsque vous créez le domaine et que vous installez les services Informatica.
- Lorsque vous exécutez la commande `infasetup defineDomain` pour créer le domaine.
- Lorsque vous exécutez la commande `infasetup updateDomainSamlConfig` pour activer l'authentification SAML dans un domaine existant.

Vous utilisez l'outil Administrator tool pour configurer une application Web afin d'utiliser un fournisseur d'identité différent. Pour configurer l'outil Administrator tool ou l'application de surveillance afin d'utiliser un fournisseur d'identité différent, modifiez la configuration SAML sur le nœud où l'application s'exécute. Pour configurer d'autres applications Web permettant d'utiliser un fournisseur d'identité différent, modifiez la configuration SAML dans le processus d'application.

Préparer l'utilisation d'un fournisseur d'identité

Effectuez les tâches suivantes pour préparer une application Web Informatica à utiliser un fournisseur d'identité.

1. Créez une configuration LDAP pour le magasin de fournisseurs d'identité qui contient les comptes utilisateur de l'application Web Informatica. Vous créez également un domaine de sécurité LDAP, puis importez les comptes utilisateur dans le domaine de sécurité.
2. Exportez le certificat de signature d'assertion à partir du fournisseur d'identité.
3. Importez le certificat de signature d'assertion du fournisseur d'identité dans un fichier truststore sur chaque nœud de passerelle du domaine. Vous pouvez importer le certificat dans le fichier truststore Informatica par défaut ou dans un fichier truststore personnalisé.

Si vous modifiez le nom de l'alias, importez le certificat correspondant dans le fichier truststore de chaque nœud de passerelle, puis redémarrez le nœud.
4. Ajoutez un ou plusieurs tiers de confiance dans le fournisseur d'identité et mappez les attributs LDAP aux types correspondants utilisés dans les jetons de sécurité émis par le fournisseur d'identité.
5. Ajoutez l'URL de l'application Web Informatica au fournisseur d'identité.

Configurer Informatica Administrator pour utiliser un fournisseur d'identité

Utilisez l'outil Administrator tool pour configurer celui-ci ou l'application de surveillance afin d'utiliser un fournisseur d'identité SAML. Vous configurez l'outil Administrator tool ou l'application de surveillance afin d'utiliser un fournisseur d'identité sur le nœud où l'application s'exécute.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Services et nœuds**.
2. Sélectionnez le nœud de passerelle dans lequel l'outil Administrator tool et l'application de surveillance s'exécutent dans le navigateur de domaine.
3. Cliquez sur l'icône de modification en regard de Configuration SAML.
4. Entrez les propriétés requises afin d'activer l'application permettant d'utiliser un fournisseur d'identité.

Le tableau suivant décrit les propriétés que vous entrez :

Propriété	Description
URL du fournisseur d'identité	Facultatif. URL du serveur de fournisseur d'identité. Vous devez spécifier la chaîne complète de l'URL.
ID de fournisseur de services	Facultatif. Nom du tiers de confiance ou identificateur de fournisseur de services pour le domaine, tel que défini dans le fournisseur d'identité.
Alias de certificat de signature d'assertion	Facultatif. Nom d'alias spécifié lors de l'importation du certificat de signature d'assertion du fournisseur d'identité dans le fichier truststore utilisé pour l'authentification SAML. Si vous modifiez le nom de l'alias, importez le certificat correspondant dans le fichier truststore de chaque nœud de passerelle, puis redémarrez le nœud.
Tolérance de variation d'horloge	Facultatif. Différence temporelle autorisée entre l'horloge système de l'hôte du fournisseur d'identité et celle du nœud principal de passerelle. Facultatif. La durée de vie des jetons SAML émis par le fournisseur d'identité est définie selon l'horloge système de l'hôte du fournisseur d'identité. La durée de vie d'un jeton SAML émis par le fournisseur d'identité est valide si l'heure de début ou l'heure de fin définie dans le jeton est comprise dans le nombre de secondes spécifié de l'horloge système du nœud principal de passerelle. Les valeurs doivent être comprises entre 0 et 600 secondes. Définissez la valeur sur -1 pour utiliser la valeur configurée pour le domaine. La valeur par défaut est 120 secondes.

L'image suivante montre la configuration permettant à l'outil Administrator tool d'utiliser AD FS comme fournisseur d'identité. Si vous ne spécifiez aucune valeur pour une propriété, le domaine utilise la valeur définie dans la configuration SAML par défaut.

Edit SAML Configuration

Fields marked with an asterisk (*) are required.

Web Application ID *
monitoring

Identity Provider URL

Service Provider ID

Assertion Signing Certificate Alias

Clock Skew Tolerance
-1

Web Application ID *
AdministratorConsole

Identity Provider URL
https://server.company.com/adfs/ls/

Service Provider ID
ADFS_Prod

Assertion Signing Certificate Alias
adfs_cert

Clock Skew Tolerance
240

?
OK
Cancel

5. Cliquez sur **OK**.
6. Redémarrez l'application.

Configurer une application Web Informatica

Utilisez l'outil Administrator tool pour configurer une application Web Informatica afin d'utiliser un fournisseur d'identité SAML.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Services et nœuds**.
2. Sélectionnez l'application ou le service d'application dans le Navigateur de domaine.
 - Pour configurer l'outil Analyst tool afin d'utiliser un fournisseur d'identité, sélectionnez le service Analyst, puis cliquez sur l'onglet **Processus**.
 - Pour configurer l'application de l'outil Ingestion de masse afin d'utiliser un fournisseur d'identité, sélectionnez le service d'ingestion de masse, puis cliquez sur l'onglet **Processus**.
 - Pour configurer l'application Metadata Manager afin d'utiliser un fournisseur d'identité, sélectionnez le service Metadata Manager, puis cliquez sur l'onglet **Propriétés**.
 - Pour configurer l'application Enterprise Data Catalog ou Catalog Administrator afin d'utiliser un fournisseur d'identité, sélectionnez le service de catalogue, puis cliquez sur l'onglet **Processus**.
 - Pour configurer l'application Enterprise Data Preparation afin d'utiliser un fournisseur d'identité, sélectionnez le service Enterprise Data Preparation, puis cliquez sur l'onglet **Processus**.
 - Pour configurer l'application Data Privacy Management afin qu'elle utilise un fournisseur d'identité, sélectionnez le Service Data Privacy Management, puis cliquez sur l'onglet **Processus**.
3. Cliquez sur l'icône de modification en regard de **Configuration SAML**.
4. Entrez les propriétés requises afin d'activer l'application Web permettant d'utiliser un fournisseur d'identité.

Le tableau suivant décrit les propriétés que vous entrez :

Propriété	Description
URL du fournisseur d'identité	Facultatif. URL du serveur de fournisseur d'identité. Vous devez spécifier la chaîne complète de l'URL.
ID de fournisseur de services	Facultatif. Nom du tiers de confiance ou identificateur de fournisseur de services pour le domaine, tel que défini dans le fournisseur d'identité.
Alias de certificat de signature d'assertion	Facultatif. Nom d'alias spécifié lors de l'importation du certificat de signature d'assertion du fournisseur d'identité dans le fichier truststore utilisé pour l'authentification SAML. Si vous modifiez le nom de l'alias, importez le certificat correspondant dans le fichier truststore de chaque nœud de passerelle, puis redémarrez le nœud.
Tolérance de variation d'horloge	Facultatif. Différence temporelle autorisée entre l'horloge système de l'hôte du fournisseur d'identité et celle du nœud principal de passerelle. Facultatif. La durée de vie des jetons SAML émis par le fournisseur d'identité est définie selon l'horloge système de l'hôte du fournisseur d'identité. La durée de vie d'un jeton SAML émis par le fournisseur d'identité est valide si l'heure de début ou l'heure de fin définie dans le jeton est comprise dans le nombre de secondes spécifié de l'horloge système du nœud principal de passerelle. Les valeurs doivent être comprises entre 0 et 600 secondes. La valeur par défaut est 120 secondes.

L'image suivante montre la configuration permettant à Enterprise Data Catalog d'utiliser PingFederate comme fournisseur d'identité :

Edit Ldadmin SAML Configuration X

Fields marked with an asterisk (*) are required.

Web Application ID	catalog_service_ldadmin
IDP URL	https://10.70.140.70:9031/idp/startSSO.saml2
Service Provider ID	PingFed_Dev
Assertion Signing Certificate Alias	pingfed_cert
Clock Skew Tolerance	240

? OK Cancel

5. Cliquez sur **OK**.
6. Redémarrez l'application ou le service d'application après avoir configuré une application permettant d'utiliser un fournisseur d'identité SAML.

CHAPITRE 6

Sécurité de domaine

Ce chapitre comprend les rubriques suivantes :

- [Présentation de la sécurité de domaine, 79](#)
- [Communication sécurisée à l'intérieur du domaine, 80](#)
- [Connexions sécurisées à un service d'application Web, 93](#)
- [Suites de chiffres du domaine Informatica, 97](#)
- [Sources et cibles sécurisées, 100](#)
- [Stockage de données sécurisé, 102](#)
- [Services et ports d'application, 106](#)

Présentation de la sécurité de domaine

Vous pouvez activer des options dans le domaine Informatica pour configurer la communication sécurisée entre les composants du domaine et entre le domaine et les composants clients.

Vous pouvez activer différentes options pour sécuriser des composants spécifiques du domaine. Vous n'avez pas besoin de sécuriser tous les composants du domaine. Par exemple, vous pouvez sécuriser la communication entre les services du domaine, mais pas la connexion entre le service de référentiel modèle et la base de données du référentiel.

Informatica utilise les protocoles TCP/IP et HTTP pour la communication entre les composants du domaine. Le domaine utilise des certificats SSL pour sécuriser la communication entre les composants.

Lorsque vous installez les services Informatica, vous pouvez activer la communication sécurisée pour les services du domaine et l'outil Administrator tool. Après l'installation, vous pouvez configurer la communication sécurisée dans le domaine à partir de l'outil Administrator tool ou de la ligne de commande.

Lors de l'installation, le programme d'installation génère une clé de cryptage pour crypter les données sensibles; telles que les mots de passe, qui sont stockées dans le domaine. Vous pouvez fournir le mot-clé que le programme d'installation utilise pour générer la clé de cryptage. Après l'installation, vous pouvez modifier la clé de cryptage pour les données sensibles. Vous devez mettre à niveau le contenu des référentiels pour mettre à jour les données cryptées.

Vous pouvez activer la communication sécurisée dans les zones suivantes :

Domaine

Dans le domaine, vous pouvez sélectionner des options pour activer la communication sécurisée pour les composants suivants :

- Entre le gestionnaire de service, les services du domaine et les outils clients Informatica

- Entre le domaine et le référentiel de configuration du domaine
- Entre les services de référentiel et les bases de données de référentiel
- Entre le service d'intégration PowerCenter et les processus DTM

Services d'applications Web

Vous pouvez sécuriser la connexion entre un service d'application Web, tel que le service Analyst ou le service Hub des opérations REST, et le navigateur.

Sources et cibles

Vous pouvez activer la communication sécurisée entre le service d'intégration de données et le service d'intégration PowerCenter, d'une part, et les bases de données source et cible d'autre part.

Stockage des données

Informatica crypte les données sensibles, telles que les mots de passe, lors du stockage des données dans le domaine. Informatica génère une clé de cryptage basée sur un mot clé que vous indiquez lors de l'installation. Informatica utilise la clé de cryptage pour crypter et décrypter les données sensibles stockées dans le domaine.

Communication sécurisée à l'intérieur du domaine

Vous pouvez utiliser l'option de communication sécurisée pour sécuriser la connexion entre les services et entre les services et les gestionnaires de service du domaine. Par ailleurs, vous pouvez activer la sécurité pour les flux de travail et utiliser les bases de données sécurisées pour les référentiels que vous créez dans le domaine.

Après avoir sécurisé le domaine, configurez les applications clientes Informatica afin qu'elles fonctionnent avec un domaine.

Répertoire par défaut du keystore et du truststore

Le déploiement d'Informatica inclut les fichiers keystore et truststore par défaut dans le répertoire par défaut suivant :

```
<Informatica installation directory>\services\shared\security
```

Informatica vous recommande d'utiliser le keystore et le truststore par défaut uniquement pour la configuration et les cas d'utilisation de preuve de concept.

Pour sécuriser un environnement de production, utilisez les directives suivantes :

- Lorsque vous configurez une communication sécurisée, vous ne devez pas modifier, remplacer ni supprimer les fichiers du répertoire par défaut :

```
<Informatica installation directory>\services\shared\security
```
- Configurez un keystore et un truststore personnalisés pour la communication sécurisée dans un emplacement autre que le répertoire par défaut :

```
<Informatica installation directory>\services\shared\security
```
- Vous ne pouvez pas utiliser le keystore et le truststore par défaut pour configurer d'autres services ou clients.

Communication sécurisée pour les services et le gestionnaire de service

Vous pouvez configurer la communication sécurisée dans le domaine pendant l'installation. Après l'installation, vous pouvez configurer la communication sécurisée pour le domaine dans l'outil Administrator tool ou à partir de la ligne de commande.

Informatica fournit un certificat SSL que vous pouvez utiliser pour sécuriser le domaine. Cependant, vous devez fournir un certificat SSL personnalisé pour les domaines qui nécessitent un niveau supérieur de sécurité, comme un domaine dans un environnement de production. Spécifiez les fichiers entrepôt de clés et truststore contenant les certificats SSL à utiliser.

Remarque: Informatica fournit des certificats SSL à des fins d'évaluation. Si vous ne fournissez pas de certificat SSL, Informatica utilise la même clé privée par défaut pour toutes les installations d'Informatica. La sécurité de votre domaine peut être compromise. Fournissez un certificat SSL afin de garantir un niveau de sécurité élevé pour le domaine. Le certificat que vous fournissez peut être auto-signé ou émaner d'une autorité de certification (CA).

Lorsque vous configurez la communication sécurisée pour le domaine, vous sécurisez les connexions entre les composants suivants :

- Entre le gestionnaire de service et tous les services exécutés dans le domaine
- Entre le service d'intégration de données et le service de référentiel modèle
- Entre le service d'intégration de données et les processus de flux de travail
- Entre le service d'intégration PowerCenter et le service de référentiel PowerCenter
- Entre les services de domaine, les outils clients Informatica et les programmes de ligne de commande

Exigences pour la communication sécurisée dans le domaine

Avant d'activer la communication sécurisée dans le domaine, assurez-vous que les conditions suivantes sont respectées :

Vous avez créé une demande de signature de certificat (CSR) et une clé privée.

Vous pouvez utiliser keytool ou OpenSSL pour créer la CSR et la clé privée.

Si vous utilisez le cryptage RSA, vous devez utiliser plus de 512 bits.

Vous disposez d'un certificat SSL signé.

Le certificat peut être auto-signé ou signé par une autorité de certification. Informatica recommande un certificat signé par une autorité de certification.

Vous avez importé le certificat dans des keystores.

Vous devez disposer d'un keystore au format PEM nommé `infa_keystore.pem` et d'un keystore au format JKS nommé `infa_keystore.jks`.

Les fichiers keystore doivent contenir les certificats SSL racine et intermédiaire.

Remarque: Le mot de passe du keystore au format JKS doit être identique à la phrase secrète de la clé secrète utilisée pour générer le certificat SSL.

Vous avez importé le certificat dans des truststores.

Vous devez disposer d'un truststore au format PEM nommé `infa_truststore.pem` et d'un keystore au format JKS nommé `infa_truststore.jks`.

Les fichiers truststore doivent contenir les certificats SSL racine, intermédiaire et des utilisateurs finaux.

Les keystores et les truststores se trouvent dans le répertoire approprié.

Si vous activez la communication sécurisée lors de l'installation, le keystore et le truststore doivent se trouver dans un répertoire auquel le programme d'installation peut accéder.

Si vous activez la communication sécurisée après l'installation, le keystore et le truststore doivent se trouver dans un répertoire auquel les programmes de ligne de commande peuvent accéder.

Vous avez appliqué l'en-tête de réponse HSTS (HTTP Strict Transport Security).

Remarque: Vous pouvez utiliser cette option après avoir appliqué le Service Pack Informatica 10.4.1.2.

Vous pouvez choisir d'activer l'en-tête de réponse HSTS dans votre domaine pour éviter les menaces de sécurité de type MITM (man-in-the-middle). Si vous activez l'en-tête de réponse HSTS, vous pouvez empêcher les redirections HTTP vers HTTPS et vous assurer que seules les URL sécurisées (HTTPS) sont accessibles.

Important: Informatica prend en charge plusieurs applications et services s'exécutant à la fois avec les protocoles HTTP et HTTPS. Si vous activez cette option, vous ne pouvez pas accéder à ces applications ou services avec une URL HTTP.

Pour activer cette option, définissez la variable d'environnement `INFA_HSTS_HEADER_ENABLED` sur `True` et importez les certificats à partir de `infa_truststore` et le keystore Informatica Administrator dans votre navigateur.

Directives d'utilisation des fichiers truststore par défaut et personnalisés

Le programme d'installation place les fichiers par défaut `infa_truststore.jks` et keystore dans le répertoire `<Informatica installation directory>/services/shared/security` sur chaque nœud. Vous pouvez utiliser le truststore par défaut pour l'installation et la preuve de concept, mais les fichiers truststore et keystore par défaut offrent une sécurité limitée. Pour la production, Informatica recommande d'utiliser des fichiers truststore et keystore personnalisés pour une communication et une authentification SAML plus sécurisées.

Placez les fichiers truststore et keystore personnalisés dans un répertoire personnalisé. Le nom du fichier truststore doit être `infa_truststore.jks`.

Ne remplacez pas les fichiers par défaut, ne les supprimez pas, ni ne les remplacez. fichiers truststore et keystore par défaut. Ne placez pas les fichiers truststore et keystore personnalisés dans le répertoire `<Informatica installation directory>/services/shared/security`

Lorsque vous créez un alias pour les nouveaux certificats et clés privées, n'utilisez pas le nom par défaut « Informatica LLC », qui est utilisé par les fichiers truststore et keystore par défaut.

Directives de création de certificats et de fichiers truststore et keystore personnalisés

Vous pouvez utiliser l'utilitaire de gestion des clés et des certificats Java `keytool` pour créer un certificat SSL ou une demande de signature de certificat (CSR) ainsi que des fichiers keystore et truststore au format JKS.

`keytool` est disponible dans le répertoire suivant sur les nœuds de domaine :

```
<Informatica installation directory>\java\bin
```

Si ces derniers s'exécutent sur AIX, vous pouvez utiliser l'utilitaire `keytool` fourni avec IBM JDK pour créer un certificat SSL ou une demande de signature de certificat (CSR) ainsi que des fichiers keystore et truststore :

1. Copiez les fichiers de certificat dans un dossier local sur un nœud de passerelle dans le domaine Informatica.
2. À partir de la ligne de commande, accédez à l'emplacement de l'utilitaire `keytool` sur le nœud.
3. Exécutez l'utilitaire `keytool` pour importer le certificat.
4. Redémarrez le nœud.

Étapes suivantes

Pour plus d'informations sur la procédure à suivre pour créer un keystore et un truststore personnalisés et pour importer des certificats dans votre navigateur, consultez l'article How-To Library Informatica « How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain » :

<https://docs.informatica.com/data-integration/shared-content-for-data-integration/h2l/how-to-create-keystore-and-truststore-files-for-secure-communication/abstract.html>

Après avoir sécurisé le domaine, configurez les applications clientes Informatica afin qu'elles fonctionnent avec un domaine.

Activation de la communication sécurisée pour le domaine depuis la ligne de commande

Utilisez les commandes `infacmd` et `infasetup` pour activer la communication sécurisée pour le domaine. Lorsque vous activez la communication sécurisée, vous devez redémarrer le domaine pour appliquer la modification.

Pour utiliser vos fichiers de certificat SSL, spécifiez les fichiers keystore lorsque vous exécutez la commande `infasetup`.

Pour configurer la communication sécurisée pour le domaine à partir de la ligne de commande, utilisez les commandes suivantes :

infacmd isp UpdateDomainOptions

Utilisez la commande `UpdateDomainOptions` pour définir le mode de communication sécurisée pour le domaine.

infasetup UpdateGatewayNode

Utilisez la commande `UpdateGatewayNode` pour activer la communication sécurisée du gestionnaire de service sur un nœud de passerelle dans un domaine. Si le domaine comporte plusieurs nœuds de passerelle, exécutez la commande `UpdateGatewayNode` sur chaque nœud de passerelle.

infasetup UpdateWorkerNode

Utilisez la commande `UpdateWorkerNode` pour activer la communication sécurisée du gestionnaire de service sur un nœud de travail dans un domaine. Si le domaine comporte plusieurs nœuds de travail, exécutez la commande `UpdateWorkerNode` sur chaque nœud de travail.

1. Vérifiez que le domaine que vous voulez sécuriser est en cours d'exécution.
2. Mettez à jour le domaine.

Exécutez la commande suivante avec les options et les arguments requis :

- Windows : `infacmd isp UpdateDomainOptions`
- UNIX : `infacmd.sh isp UpdateDomainOptions`

Pour configurer la communication sécurisée pour le domaine, incluez l'option suivante lors de l'exécution de la commande `infacmd` :

Option	Argument	Description
-DomainOptions -do	option_name=value	Définissez l'option suivante pour configurer la communication sécurisée pour le domaine : TLSMode=True

3. Arrêtez le domaine.

Le domaine doit être arrêté avant l'exécution des commandes infasetup.

4. Exécutez la commande infasetup avec les options et les arguments requis.

Entrez la commande suivante :

- **Windows** : `infasetup UpdateGatewayNode` ou `infasetup UpdateWorkerNode`
- **UNIX** : `infasetup.sh UpdateGatewayNode` ou `infasetup.sh UpdateWorkerNode`

Pour configurer la communication sécurisée sur les nœuds, exécutez les commandes avec les options suivantes :

Option	Argument	Description
-EnableTLS -tls	enable_tls	Configure la communication sécurisée des services du domaine Informatica.
-NodeKeystore -nk	node_keystore_directory	Facultatif si vous utilisez le certificat SSL par défaut d'Informatica. Obligatoire si vous utilisez votre propre certificat SSL. Répertoire contenant les fichiers keystore. Le domaine Informatica requiert le certificat SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers keystore aux formats PEM et JKS. Les fichiers keystore doivent être nommés <code>infa_keystore.jks</code> et <code>infa_keystore.pem</code> . Vous pouvez utiliser le même fichier keystore pour plusieurs nœuds.
-NodeKeystorePass -nkp	node_keystore_password	Facultatif si vous utilisez le certificat SSL par défaut d'Informatica. Obligatoire si vous utilisez votre propre certificat SSL. Mot de passe du fichier <code>infa_keystore.jks</code> .
-NodeTruststore -nt	node_truststore_directory	Facultatif si vous utilisez le certificat SSL par défaut d'Informatica. Répertoire contenant les fichiers truststore. Vous pouvez utiliser le même fichier truststore pour plusieurs nœuds.
-NodeTruststorePass -ntp	node_truststore_password	Facultatif si vous utilisez le certificat SSL par défaut d'Informatica. Mot de passe du fichier <code>infa_truststore.jks</code> .

5. Exécutez la commande infasetup sur chaque nœud du domaine.

Si vous avez plusieurs nœuds de passerelle dans le domaine, exécutez la commande `infasetup UpdateGatewayNode` sur chaque nœud de passerelle. Si vous avez plusieurs nœuds de travail, exécutez la commande `infasetup UpdateWorkerNode` sur chaque nœud de travail. Vous devez utiliser les mêmes fichiers keystore pour tous les nœuds du domaine.

6. Redémarrez le domaine.

Activation de la communication sécurisée pour le domaine dans l'outil Administrator

Vous pouvez utiliser l'outil Administrator pour activer la communication sécurisée pour le domaine. Lorsque vous activez la communication sécurisée dans l'outil Administrator, vous devez également exécuter les commandes `infasetup` pour mettre à jour les nœuds.

Lorsque vous activez l'option Communication sécurisée dans l'outil Administrator, vous devez également exécuter la commande `infasetup` pour mettre à jour les fichiers de configuration Informatica sur chaque nœud. Pour spécifier les fichiers de certificat SSL à utiliser, indiquez les fichiers `truststore` lorsque vous exécutez la commande `infasetup`.

Pour mettre à jour les fichiers de configuration Informatica sur chaque nœud, utilisez les commandes suivantes :

infasetup UpdateGatewayNode

Utilisez la commande `UpdateGatewayNode` pour activer la communication sécurisée du gestionnaire de service sur un nœud de passerelle dans un domaine. Si le domaine comporte plusieurs nœuds de passerelle, exécutez la commande `UpdateGatewayNode` sur chaque nœud de passerelle.

infasetup UpdateWorkerNode

Utilisez la commande `UpdateWorkerNode` pour activer la communication sécurisée du gestionnaire de service sur un nœud de travail dans un domaine. Si le domaine comporte plusieurs nœuds de travail, exécutez la commande `UpdateWorkerNode` sur chaque nœud de travail.

Pour activer la communication sécurisée pour le domaine à partir de l'outil Administrator, procédez comme suit :

1. Dans l'outil Administrator, sélectionnez le domaine.
2. Dans le panneau de contenu, cliquez sur la vue **Propriétés**.
3. Accédez à la section **Propriétés générales** et cliquez sur **Modifier**.
4. Dans la fenêtre **Modifier les propriétés générales**, sélectionnez **Activer la communication sécurisée**.
5. Cliquez sur **OK**.
6. Arrêtez le domaine.

Le domaine doit être arrêté avant l'exécution des commandes `infasetup`.

7. Exécutez la commande `infasetup` avec les options et les arguments requis.

Entrez la commande suivante :

- **Windows** : `infasetup UpdateGatewayNode` **ou** `infasetup UpdateWorkerNode`
- **UNIX** : `infasetup.sh UpdateGatewayNode` **ou** `infasetup.sh UpdateWorkerNode`

Pour configurer la communication sécurisée sur les nœuds, exécutez les commandes avec les options suivantes :

Option	Argument	Description
-EnableTLS -tls	enable_tls	Configure la communication sécurisée des services du domaine Informatica.
-NodeKeystore -nk	node_keystore_directory	Facultatif si vous utilisez le certificat SSL par défaut d'Informatica. Obligatoire si vous utilisez votre propre certificat SSL. Répertoire contenant les fichiers keystore. Le domaine Informatica requiert le certificat SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir les fichiers keystore aux formats PEM et JKS. Les fichiers keystore doivent être nommés infa_keystore.jks et infa_keystore.pem. Vous pouvez utiliser le même fichier keystore pour plusieurs nœuds.
-NodeKeystorePass -nkp	node_keystore_password	Facultatif si vous utilisez le certificat SSL par défaut d'Informatica. Obligatoire si vous utilisez votre propre certificat SSL. Mot de passe du fichier infa_keystore.jks.
-NodeTruststore -nt	node_truststore_directory	Facultatif si vous utilisez le certificat SSL par défaut d'Informatica. Répertoire contenant les fichiers truststore. Vous pouvez utiliser le même fichier truststore pour plusieurs nœuds.
-NodeTruststorePass -ntp	node_truststore_password	Facultatif si vous utilisez le certificat SSL par défaut d'Informatica. Mot de passe du fichier infa_truststore.jks.

- Exécutez la commande infasetup sur chaque nœud du domaine.

Si vous avez plusieurs nœuds de passerelle dans le domaine, exécutez la commande infasetup UpdateGatewayNode sur chaque nœud de passerelle. Si vous avez plusieurs nœuds de travail, exécutez la commande infasetup UpdateWorkerNode sur chaque nœud de travail. Vous devez utiliser les mêmes fichiers keystore pour tous les nœuds du domaine.

- Redémarrez le domaine.

Configuration des applications clientes Informatica pour une utilisation avec un domaine

Lorsque vous activez la communication sécurisée au sein du domaine, vous sécurisez également les connexions entre le domaine et les applications clientes Informatica, telles que l'outil Developer. Vous devrez peut-être spécifier l'emplacement et le mot de passe des fichiers truststore utilisés pour sécuriser le domaine dans les variables d'environnement. Définissez les variables d'environnement sur les machines hébergeant les applications clientes qui accèdent aux services au sein du domaine.

Les certificats SSL utilisés pour sécuriser un domaine Informatica sont contenus dans les fichiers truststore nommés infa_truststore.jks et infa_truststore.pem. Les fichiers truststore doivent être disponibles sur chacun des hôtes clients.

Vous devrez peut-être définir les variables d'environnement suivantes sur chaque hôte client :

INFA_TRUSTSTORE

Définissez cette variable sur le répertoire qui contient les fichiers truststore `infa_truststore.jks` et `infa_truststore.pem`.

INFA_TRUSTSTORE_PASSWORD

Définissez cette variable sur le mot de passe pour le fichier truststore. Le mot de passe doit être crypté. Utilisez le programme de ligne de commande `mpasswd` pour crypter le mot de passe.

Informatica fournit un certificat SSL dans les fichiers truststore par défaut que vous pouvez utiliser pour sécuriser le domaine. Lorsque vous installez des clients Informatica, le programme d'installation définit les variables d'environnement et installe les fichiers truststore dans le répertoire suivant par défaut :

`<répertoire d'installation Informatica>\clients\shared\security`

Si vous utilisez le certificat SSL Informatica par défaut, et que les fichiers `infa_truststore.jks` et `infa_truststore.pem` se trouvent dans le répertoire par défaut, vous n'avez pas besoin de définir les variables d'environnement `INFA_TRUSTSTORE` ou `INFA_TRUSTSTORE_PASSWORD`.

Vous devez définir les variables d'environnement `INFA_TRUSTSTORE` et `INFA_TRUSTSTORE_PASSWORD` sur chaque hôte client dans les scénarios suivants :

Vous utilisez un certificat SSL personnalisé pour sécuriser le domaine.

Si vous fournissez un certificat SSL à utiliser pour sécuriser le domaine, importez le certificat dans les fichiers truststore nommés `infa_truststore.jks` et `infa_truststore.pem`, puis copiez les fichiers truststore sur chaque hôte client. Vous devez spécifier l'emplacement des fichiers et le mot de passe truststore.

Important : si vous transmettez le traitement à un cluster de calcul et que le service d'intégration de données s'exécute sur une grille, importez les certificats une seule fois, puis copiez-les dans chaque service d'intégration de données sur la grille. À chaque importation d'un certificat, les contenus du certificat sont identiques, mais les valeurs hexadécimales sont différentes. Par conséquent, les mappages actuels qui s'exécutent sur la grille échouent avec des erreurs d'initialisation.

Remplacez les fichiers truststore Informatica par défaut par vos propres fichiers truststore dans le répertoire par défaut.

Si vous remplacez les fichiers truststore `infa_truststore.jks` et `infa_truststore.pem` par défaut par vos propres fichiers truststore dans le répertoire Informatica par défaut, vous devez spécifier le mot de passe truststore. Les fichiers truststore doivent porter les mêmes noms de fichiers que les fichiers truststore par défaut.

Vous utilisez le certificat SSL d'Informatica par défaut, mais les fichiers truststore ne se trouvent pas dans le répertoire Informatica par défaut.

Si vous utilisez le certificat SSL Informatica par défaut, mais que les fichiers truststore `infa_truststore.jks` et `infa_truststore.pem` par défaut ne se trouvent pas dans le répertoire par défaut, vous devez spécifier l'emplacement des fichiers et le mot de passe truststore.

Base de données de référentiel de configuration du domaine sécurisée

Le référentiel de configuration du domaine Informatica stocke les informations de configuration ainsi que les privilèges et les autorisations des comptes utilisateur. Lorsque vous créez un domaine Informatica, vous devez créer un référentiel de configuration du domaine.

Vous pouvez créer un référentiel de configuration du domaine sur une base de données qui est sécurisée avec le protocole SSL. Le protocole SSL utilise les certificats SSL stockés dans un fichier truststore. L'accès à la base de données sécurisée requiert un fichier truststore contenant les certificats de la base de données.

Vous pouvez créer une base de données de référentiel de configuration du domaine sécurisée lorsque vous installez les services Informatica et créez un domaine. Pour plus d'informations sur la configuration d'un référentiel de configuration du domaine sécurisé pendant l'installation, consultez les guides d'installation Informatica.

Après l'installation, vous pouvez configurer une base de données de référentiel de configuration du domaine sécurisée à partir de la ligne de commande.

Remarque: avant de configurer une base de données de référentiel de configuration du domaine sécurisée, vous devez activer la communication sécurisée pour le domaine.

Vous pouvez créer un référentiel de configuration du domaine sécurisé sur les bases de données suivantes :

- Oracle
- Microsoft SQL Server
- IBM DB2

Configuration d'une base de données du référentiel de configuration du domaine sécurisé

Après l'installation, vous pouvez convertir le référentiel de configuration du domaine en base de données sécurisée. Vous pouvez utiliser une base de données de référentiel de configuration du domaine sécurisée uniquement si vous activez la communication sécurisée pour le domaine.

Vous devez arrêter le domaine avant de modifier sa base de données de référentiel de configuration. Utilisez la commande `infasetup` pour sauvegarder la base de données de référentiel de configuration du domaine et la restaurer dans une base de données sécurisée. Lorsque vous restaurez le référentiel de configuration du domaine dans la base de données sécurisée, spécifiez les paramètres de sécurité de cette dernière. Ensuite, mettez à jour le nœud de passerelle en indiquant les informations du référentiel de configuration du domaine.

Pour sauvegarder et restaurer la base de données de référentiel, puis mettre à jour le nœud de passerelle, utilisez les commandes suivantes :

infasetup BackupDomain

Utilisez l'option `BackupDomain` pour sauvegarder les données de la base de données de référentiel de configuration du domaine.

infasetup RestoreDomain

Utilisez l'option `RestoreDomain` pour restaurer les données du référentiel de configuration du domaine dans une base de données sécurisée.

infasetup UpdateGatewayNode

Utilisez l'option `UpdateGatewayNode` pour mettre à jour les paramètres du référentiel de configuration du domaine dans les nœuds de passerelle du domaine.

Pour convertir le référentiel de configuration du domaine en base de données sécurisée, procédez comme suit :

1. Vérifiez que la communication sécurisée est activée pour le domaine.

Le domaine doit être sécurisé pour que vous puissiez utiliser une base de données sécurisée pour le référentiel de configuration du domaine.

2. Arrêtez le domaine.

3. Exécutez la commande `infasetup BackupDomain` et indiquez les informations de connexion à la base de données.

Lorsque vous exécutez la commande `BackupDomain`, `infasetup` sauvegarde la plupart des tables de la base de données de configuration du domaine sous un nom de fichier que vous spécifiez.

Remarque: si la commande `infasetup` de sauvegarde ou de restauration échoue et renvoie une erreur de mémoire Java, augmentez la quantité de mémoire système disponible pour cette commande. Pour augmenter la quantité de mémoire système, définissez la valeur `-Xmx` dans la variable d'environnement `INFA_JAVA_CMD_OPTS`.

4. Faites appel à l'utilitaire de sauvegarde de base de données pour sauvegarder manuellement les tables supplémentaires du référentiel que la commande `infasetup` ne sauvegarde pas.

Sauvegardez le contenu de la table suivante :

- `ISP_RUN_LOG`

5. Pour restaurer le référentiel de configuration du domaine dans la base de données sécurisée, exécutez la commande `infasetup RestoreDomain` et indiquez les informations de connexion à la base de données.

Outre les informations de connexion, spécifiez les options suivantes requises pour la base de données sécurisée :

Option	Argument	Description
<code>-DatabaseTlsEnabled</code> <code>-dbtls</code>	<code>database_tls_enabled</code>	Obligatoire. Indique si la base de données dans laquelle le référentiel de configuration du domaine sera restauré est une base de données sécurisée. Définissez cette option sur <code>True</code> .
<code>-DatabaseTruststoreLocation</code> <code>-dbtl</code>	<code>database_truststore_location</code>	Obligatoire. Chemin et nom du fichier <code>truststore</code> contenant le certificat SSL pour la base de données.
<code>-DatabaseTruststorePassword</code> <code>-dbtp</code>	<code>database_truststore_password</code>	Obligatoire. Mot de passe du fichier <code>truststore</code> de la base de données sécurisée.

Dans la chaîne de connexion, incluez les paramètres de sécurité suivants :

EncryptionMethod

Requis. Indique si les données sont cryptées lorsqu'elles sont transmises sur le réseau. Ce paramètre doit être défini sur `SSL`.

ValidateServerCertificate

Facultatif. Indique si Informatica valide le certificat envoyé par le serveur de base de données.

Si ce paramètre est défini sur `True`, Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre `HostNameInCertificate`, Informatica valide également le nom d'hôte dans le certificat.

Si ce paramètre est défini sur False, Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de truststore que vous spécifiez.

La valeur par défaut est True.

HostNameInCertificate

Facultatif. Nom d'hôte de la machine qui héberge la base de données sécurisée. Si vous spécifiez un nom d'hôte, Informatica valide le nom d'hôte inclus dans la chaîne de connexion avec le nom d'hôte dans le certificat SSL.

cryptoProtocolVersion

Requis. Indique le protocole cryptographique à utiliser pour la connexion à une base de données sécurisée. Vous pouvez définir le paramètre sur `cryptoProtocolVersion=TLSv1.1` ou `cryptoProtocolVersion=TLSv1.2` en fonction du protocole cryptographique utilisé par le serveur de base de données.

6. Faites appel à l'utilitaire de restauration de base de données pour restaurer les tables du référentiel que vous avez sauvegardées manuellement.

Restaurez la table suivante :

- ISP_RUN_LOG

7. Pour mettre à jour les nœuds du domaine avec les informations relatives au référentiel de configuration du domaine sécurisé, exécutez la commande `infasetup UpdateGatewayNode` et indiquez les informations de connexion à la base de données sécurisée.

Outre les options de nœud, spécifiez les options suivantes requises pour la base de données sécurisée :

Option	Argument	Description
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Obligatoire. Indique si la base de données utilisée pour le référentiel de configuration du domaine est une base de données sécurisée. Définissez cette option sur True.
-DatabaseConnectionString -cs	database_connection_string	Obligatoire. Chaîne de connexion à utiliser pour se connecter à la base de données sécurisée. La chaîne de connexion doit inclure les paramètres de sécurité que vous avez inclus dans la chaîne de connexion lorsque vous avez exécuté la commande <code>infasetup RestoreDomain</code> dans l'étape 5
-DatabaseTruststorePassword -dbtp	database_truststore_password	Obligatoire. Mot de passe du fichier truststore de la base de données sécurisée.

Si vous avez plusieurs nœuds de passerelle dans le domaine, exécutez la commande `infasetup UpdateGatewayNode` sur chaque nœud de passerelle.

8. Redémarrez le domaine.

Base de données de référentiel PowerCenter sécurisée

Lorsque vous créez un service de référentiel PowerCenter, vous pouvez créer le référentiel PowerCenter associé dans une base de données sécurisée avec le protocole SSL.

Le service de référentiel PowerCenter se connecte à la base de données du référentiel PowerCenter via la connectivité native.

Lorsque vous créez un référentiel PowerCenter sur une base de données sécurisée, vérifiez que les fichiers client de base de données contiennent les informations de connexion sécurisée de la base de données. Par exemple, si vous créez un référentiel PowerCenter sur une base de données Oracle sécurisée, configurez les fichiers client de la base de données Oracle tnsnames.ora et sqlnet.ora avec les informations de connexion sécurisée.

Base de données du référentiel modèle sécurisée

Lorsque vous créez un service de référentiel modèle, vous pouvez créer le référentiel modèle associé dans une base de données sécurisée avec le protocole SSL.

Le service de référentiel modèle se connecte à la base de données du référentiel modèle à l'aide des pilotes JDBC.

1. Configurez une base de données sécurisée avec le protocole SSL.
2. Dans l'outil Administrator, créez un service de référentiel modèle.
3. Dans la boîte de dialogue **Nouveau service de référentiel modèle**, entrez les propriétés générales du service de référentiel modèle et cliquez sur **Suivant**.
4. Entrez les propriétés de la base de données et la chaîne de connexion JDBC du service de référentiel modèle.

Pour vous connecter à une base de données sécurisée, entrez ses paramètres dans le champ **Paramètres JDBC sécurisés**. Informatica traite la valeur du champ **Paramètres JDBC sécurisés** comme des données sensibles et stocke la chaîne de paramètres sous forme cryptée.

La liste suivante décrit les paramètres de base de données sécurisés :

EncryptionMethod

Requis. Indique si les données sont cryptées lorsqu'elles sont transmises sur le réseau. Ce paramètre doit être défini sur **SSL**.

ValidateServerCertificate

Facultatif. Indique si Informatica valide le certificat envoyé par le serveur de base de données.

Si ce paramètre est défini sur **True**, Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre **HostNameInCertificate**, Informatica valide également le nom d'hôte dans le certificat.

Si ce paramètre est défini sur **False**, Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de truststore que vous spécifiez.

La valeur par défaut est **True**.

HostNameInCertificate

Facultatif. Nom d'hôte de la machine qui héberge la base de données sécurisée. Si vous spécifiez un nom d'hôte, Informatica valide le nom d'hôte inclus dans la chaîne de connexion avec le nom d'hôte dans le certificat SSL.

cryptoProtocolVersion

Requis. Indique le protocole cryptographique à utiliser pour la connexion à une base de données sécurisée. Vous pouvez définir le paramètre sur `cryptoProtocolVersion=TLSv1.1` ou `cryptoProtocolVersion=TLSv1.2` en fonction du protocole cryptographique utilisé par le serveur de base de données.

TrustStore

Obligatoire. Chemin d'accès et nom du fichier truststore contenant le certificat SSL de la base de données.

Si vous n'incluez pas le chemin du fichier truststore, Informatica recherche ce fichier dans le répertoire par défaut suivant : `<InformaticaInstallationDirectory>/tomcat/bin`

TrustStorePassword

Obligatoire. Mot de passe du fichier truststore pour la base de données sécurisée.

Remarque: Informatica ajoute les paramètres JDBC sécurisés à la chaîne de connexion JDBC. Si vous incluez les paramètres JDBC sécurisés directement dans la chaîne de connexion, n'entrez pas de paramètres dans le champ **Paramètres JDBC sécurisés**.

5. Testez la connexion pour vérifier que la connexion à la base de données de référentiel sécurisée est valide.
6. Finalisez le processus pour créer un service de référentiel modèle.

Communication sécurisée pour les flux de travail et les sessions

Par défaut, lorsque vous activez l'option de communication sécurisée pour le domaine, Informatica sécurise la connexion entre, d'un côté, les services d'intégration de données et d'intégration PowerCenter et, de l'autre, les processus DTM.

En outre, si vous exécutez les sessions PowerCenter sur une grille, vous pouvez activer une option permettant de sécuriser la communication de données entre les processus DTM.

Pour activer la communication de données sécurisée entre les processus DTM dans les sessions PowerCenter, sélectionnez l'option **Activer le cryptage des données** pour le service d'intégration PowerCenter.

Remarque: Les sessions PowerCenter nécessitent davantage de ressources processeur et de mémoire lorsque les processus DTM s'exécutent en mode sécurisé. Avant d'activer la communication de données sécurisée entre les processus DTM pour les sessions PowerCenter, déterminez si les ressources du domaine sont adaptées à la charge supplémentaire.

Activation de la communication sécurisée pour les processus DTM de PowerCenter

Pour sécuriser la connexion entre les processus DTM dans les sessions PowerCenter exécutées sur une grille, configurez le service d'intégration PowerCenter pour activer le cryptage des données dans le cadre des processus DTM.

1. Dans le navigateur de l'outil Administrator, sélectionnez le service d'intégration PowerCenter.
2. Dans le panneau de contenu, cliquez sur la vue Propriétés.
3. Accédez à la section Propriétés du service d'intégration PowerCenter et cliquez sur Modifier.
4. Dans la fenêtre **Modifier les propriétés du service d'intégration PowerCenter**, sélectionnez **Activer le cryptage des données**.
5. Cliquez sur **OK**.

Lorsque vous exécutez une session PowerCenter sur une grille, les processus DTM envoient des données cryptées lorsqu'ils communiquent avec d'autres processus DTM.

Connexions sécurisées à un service d'application Web

Pour protéger les données transmises entre un service d'application Web et le navigateur, sécurisez la connexion entre le service d'application Web et le navigateur.

Vous pouvez sécuriser les connexions suivantes :

Connexions à l'outil Administrator tool

Vous pouvez sécuriser la connexion entre l'outil Administrator tool et le navigateur.

Connexions aux services d'application Web

Vous pouvez sécuriser la connexion entre les services d'application Web et le navigateur :

- Service Analyst
- Service Metadata Manager
- Service Hub des opérations REST
- Service Test Data Manager
- Service de la console Hub des services Web

Exigences pour les connexions sécurisées aux services d'application Web

Pour sécuriser la connexion à un service d'application Web, vérifiez que les conditions suivantes sont respectées :

Vous avez créé une demande de signature de certificat (CSR) et une clé privée.

Vous pouvez utiliser keytool ou OpenSSL pour créer la CSR et la clé privée.

Si vous utilisez le cryptage RSA, vous devez utiliser plus de 512 bits.

Vous disposez d'un certificat SSL signé.

Le certificat peut être auto-signé ou signé par une autorité de certification. Informatica recommande un certificat signé par une autorité de certification.

Vous avez importé le certificat dans un keystore au format JKS.

Un keystore ne doit contenir qu'un seul certificat. Si vous utilisez un certificat unique pour chaque service d'application Web, créez un keystore distinct pour chaque certificat. Vous pouvez également utiliser un certificat et un keystore partagés.

Si vous utilisez le certificat SSL généré par le programme d'installation pour l'outil Administrator, vous n'avez pas besoin de l'importer dans un keystore au format JKS.

Le keystore se trouve dans un répertoire accessible.

Le keystore doit se trouver dans un répertoire auquel l'outil Administrator et les programmes de ligne de commande peuvent accéder.

Activation des connexions sécurisées sur l'outil Administrator

Après l'installation, vous pouvez configurer des connexions sécurisées sur l'outil Administrator depuis la ligne de commande.

Vous devez mettre à jour les nœuds de passerelle du domaine avec les propriétés d'une connexion sécurisée entre le navigateur et le service Informatica Administrator.

Pour mettre à jour le nœud de passerelle avec les propriétés de la connexion sécurisée, exécutez la commande suivante : `infasetup UpdateGatewayNode`

Incluez les options suivantes :

Option	Argument	Description
-HttpsPort -hs	AdminConsole_https_port	Numéro de port à utiliser pour une connexion sécurisée au service Informatica Administrator.
-KeystoreFile -kf	AdminConsole_Keystore_File	Chemin et nom du fichier keystore à utiliser pour la connexion HTTPS au service Informatica Administrator.
-KeystorePass -kp	AdminConsole_Keystore_Password	Mot de passe du fichier keystore.

Si le domaine comporte plusieurs nœuds de passerelle, exécutez la commande sur chacun d'entre eux.

Services d'applications Web Informatica

Configurez une connexion sécurisée pour un service d'application Web lorsque vous le créez ou le configurez. Chaque service d'application possède des propriétés spécifiques concernant la connexion HTTPS sécurisée.

Sécurité de l'outil Analyst tool

Lorsque vous créez le service Analyst, vous pouvez configurer les propriétés HTTPS sécurisées de l'outil Analyst tool.

Pour sécuriser la connexion entre le navigateur et le service Analyst, configurez les propriétés suivantes de ce service :

Propriété	Description
Activer la communication sécurisée	Sélectionnez cette option pour activer la connexion sécurisée entre l'outil Analyst tool et le service Analyst.
Port HTTPS	Numéro du port sur lequel l'application Web Informatica Analyst est exécutée lorsque vous activez le protocole TLS. Utilisez un numéro différent de celui du port HTTP.
Fichier keystore	Répertoire dans lequel le fichier entrepôt de clés contenant les certificats numériques est stocké.

Propriété	Description
Mot de passe keystore	Mot de passe en texte brut du fichier keystore. Si cette propriété n'est pas définie, le service Analyst utilise le mot de passe par défaut <i>changeit</i> .
Protocole SSL	Informatica vous recommande de laisser ce champ vide. La version de TLS activée dépend de la valeur. Un champ vide active la version la plus élevée de TLS disponible. Si vous entrez une valeur, il est possible que les versions antérieures de TLS soient activées. Le comportement est basé sur la version Java de votre environnement. Pour obtenir plus d'informations, consultez la documentation de votre version Java.

Sécurité du service Hub des opérations REST

Lorsque vous utilisez le service Hub des opérations REST, vous pouvez configurer les propriétés HTTPS sécurisées pour le Hub des opérations REST.

Pour sécuriser la connexion entre le navigateur et le service Hub des opérations REST, configurez les propriétés suivantes du service Hub des opérations REST :

Propriété	Description
Port HTTP	Numéro de port HTTP unique pour le processus du service Hub des opérations REST lorsque le service utilise le protocole HTTP. La valeur par défaut est 6555.
Port HTTPS	Numéro de port sur lequel le service Hub des opérations REST est exécuté lorsque vous activez le protocole TLS (Transport Layer Security). Utilisez un numéro différent de celui du port HTTP.
Activer le protocole TLS	Sélectionnez cette option pour activer une connexion sécurisée entre le service Hub des opérations REST et le client REST.
Fichier keystore	Répertoire dans lequel le fichier entrepôt de clés contenant les certificats numériques est stocké.
Mot de passe keystore	Mot de passe en texte brut du fichier keystore. Si cette propriété n'est pas définie, le service Hub des opérations REST utilise le mot de passe par défaut.
Protocole SSL	Un champ vide active la version la plus élevée de TLS disponible. La version de TLS activée dépend de la valeur. Si vous entrez une valeur, il est possible que les versions antérieures de TLS soient activées. Le comportement est basé sur la version Java de votre environnement. Pour obtenir plus d'informations, consultez la documentation de votre version Java.

Sécurité de la console Hub de services Web

Lorsque vous créez le service Hub de services Web, vous pouvez configurer les propriétés HTTPS sécurisées de la console Hub de services Web.

Pour sécuriser la connexion entre le navigateur et le service Hub de services Web, configurez les propriétés du service Hub des services Web suivantes :

Propriété	Description
URLScheme	Indique le protocole de sécurité que vous configurez pour le hub de services Web : <ul style="list-style-type: none">- HTTP. Exécutez le hub de services Web uniquement sur HTTP.- HTTPS. Exécutez le hub de services Web uniquement sur HTTPS.- HTTP et HTTPS. Exécutez le hub de services Web en modes HTTP et HTTPS.
HubPortNumber (https)	Numéro de port du hub de services Web exécuté sur HTTPS. Apparaît lorsque le schéma URL sélectionné inclut HTTPS. Obligatoire si vous exécutez le hub de services Web sur HTTPS. La valeur par défaut est 7343.
Fichier entrepôt de clés	Chemin et nom du fichier entrepôt de clés qui contient les clés et les certificats requis pour une connexion HTTPS.
Mot de passe de l'entrepôt de clés	Mot de passe du fichier entrepôt de clés. Si cette propriété n'est pas définie, le hub de services Web utilise le mot de passe par défaut <i>changeit</i> .

Sécurité de Metadata Manager

Lorsque vous créez le service Metadata Manager, vous pouvez configurer les propriétés HTTPS sécurisées de l'application Web Metadata Manager.

Pour sécuriser la connexion entre le navigateur et le service Metadata Manager, configurez les propriétés suivantes du service Metadata Manager :

Propriété	Description
Activer le protocole SSL (Secure Sockets Layer)	Indique que vous voulez configurer une connexion sécurisée pour l'application Web Metadata Manager. Remarque: Cette propriété est affichée lorsque vous créez un service Metadata Manager. Pour sécuriser la connexion pour un service Metadata Manager, définissez la propriété de configuration Schéma URL sur HTTPS.
Numéro de port	Numéro de port sur lequel l'application Metadata Manager s'exécute. La valeur par défaut est 10250.
Fichier keystore	Fichier keystore qui contient les clés et les certificats requis si vous configurez une connexion sécurisée pour l'application Web Metadata Manager. Remarque: Le service Metadata Manager utilise le cryptage RSA. Par conséquent, Informatica vous recommande d'utiliser un certificat de sécurité généré avec l'algorithme RSA.
Mot de passe keystore	Mot de passe du fichier keystore.

Suites de chiffres du domaine Informatica

Vous pouvez configurer les suites de chiffres utilisées par le domaine Informatica lorsqu'il crypte ses connexions internes. Les connexions qui partent du domaine Informatica vers les ressources se trouvant en dehors du domaine ne sont pas affectées par la configuration de la suite de chiffres.

Lorsque vous activez la communication sécurisée du domaine Informatica ou des connexions sécurisées vers les services d'application Web, le domaine Informatica utilise des suites de chiffres pour crypter le trafic.

Informatica crée la liste de suites de chiffres effective qu'il utilise en fonction des listes suivantes :

Liste noire

Liste de suites de chiffres que vous souhaitez voir bloquées par le domaine Informatica. Lorsque vous placez une suite de chiffres dans une liste noire, le domaine Informatica la supprime de la liste effective. Vous pouvez ajouter à la liste noire des suites de chiffres se trouvant dans la liste par défaut.

Liste par défaut

Liste de suites de chiffres prises en charge par défaut par le domaine Informatica. Si vous ne configurez pas de liste blanche ou de liste noire, le domaine Informatica utilise la liste par défaut en tant que liste effective.

Pour plus d'informations, veuillez consulter ["Liste par défaut des suites de chiffres" à la page 98](#).

Liste blanche

Liste de suites de chiffres que vous souhaitez voir prises en charge par le domaine Informatica. Lorsque vous ajoutez une suite de chiffres à la liste blanche, le domaine Informatica l'ajoute à la liste effective. Il n'est pas nécessaire d'ajouter les suites de chiffres de la liste par défaut à la liste blanche.

Informatica crée la liste effective en ajoutant des suites de chiffres de la liste blanche dans la liste par défaut et en retirant des suites de chiffres de la liste noire.

Tenez compte des directives suivantes pour les listes effectives :

- Pour utiliser une liste effective personnalisée pour des connexions sécurisées à des clients Web, le domaine Informatica doit utiliser la communication sécurisée du domaine. Si le domaine n'utilise pas la communication sécurisée, Informatica utilise la liste par défaut en tant que liste effective.
- La liste effective gère uniquement les connexions dans le domaine Informatica. Les connexions aux sources de données n'utilisent pas la liste effective.
- La liste effective doit contenir au moins une suite de chiffres prise en charge par TLS v1.1 ou 1.2.
- La liste effective doit être une suite de chiffres valide pour Windows, l'environnement d'exécution Java et OpenSSL.

Créer des listes de suites de chiffres

Pour configurer le domaine Informatica pour utiliser des suites de chiffres spécifiques, créez une liste blanche spécifiant les suites de chiffres complémentaires prises en charge. Vous pouvez également créer une liste noire spécifiant les suites de chiffres à bloquer.

Collaborez avec votre administrateur de sécurité réseau afin de déterminer les suites de chiffres qui conviennent au domaine Informatica.

La liste des suites de chiffres doit être séparée par des virgules. Utilisez les noms de l'organisme IANA (Internet Assigned Numbers Authority) pour les suites de chiffres de la liste. Vous pouvez également utiliser une expression régulière Java.

Configurez la liste blanche et la liste noire avec `infasetup`. Vous pouvez fournir les listes directement dans les paramètres de commande ou spécifier des fichiers en texte brut qui contiennent des listes séparées par des virgules.

L'exemple suivant affiche une liste contenant deux suites de chiffres :

```
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Vous pouvez configurer la liste blanche et la liste noire de suites de chiffres pour le domaine Informatica lorsque vous créez le domaine. Utilisez `infasetup` pour créer le domaine Informatica, les nœuds de passerelle et les nœuds de travail. Pour plus d'informations sur les commandes `infasetup`, consultez la *Référence des commandes Informatica*.

Vous pouvez également configurer la liste blanche et la liste noire d'un domaine Informatica existant.

Liste par défaut des suites de chiffres

Par défaut, le domaine Informatica utilise les suites de chiffres suivantes pour sécuriser la communication dans le domaine et sécuriser les connexions clientes :

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

Configurer le domaine Informatica à l'aide d'une nouvelle liste effective de suites de chiffres

Pour configurer les suites de chiffres utilisées par le domaine Informatica, vous devez mettre à jour le domaine Informatica, tous les nœuds de passerelle et tous les nœuds de travail avec la même liste blanche ou la même liste noire.

Remarque: Les modifications apportées à la liste blanche, à la liste noire et à la liste effective ne sont pas cumulatives. Informatica crée une liste effective en fonction de la liste noire, de la liste par défaut et de la liste blanche lors de l'exécution de la commande. La nouvelle liste effective remplace la précédente.

Pour configurer un domaine Informatica existant avec une nouvelle liste effective de suites de chiffres, procédez comme suit :

1. Fermez le domaine Informatica.
2. Vous pouvez éventuellement exécuter la commande `infasetup listDomainCiphers` pour afficher les listes de suites de chiffres prises en charge ou bloquées par un domaine ou un nœud.

Par exemple, exécutez la commande suivante pour afficher toutes les listes de suites de chiffres :

```
infasetup listDomainCiphers -l ALL -dc true
```

3. Exécutez la commande `infasetup updateDomainCiphers` sur un nœud de passerelle et spécifiez une liste blanche, une liste noire ou les deux.

Par exemple, exécutez la commande suivante pour ajouter une suite de chiffres à la liste effective et en retirer deux :

```
infasetup updateDomainCiphers -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

4. Exécutez la commande `infasetup updateGatewayNode` sur chaque nœud de passerelle et spécifiez une liste blanche, une liste noire ou les deux.

Utilisez la même liste blanche ou noire que le domaine.

Par exemple, exécutez la commande suivante :

```
infasetup updateGatewayNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

5. Mettez à jour chaque nœud de travail avec le même ensemble de suites de chiffres que le domaine Informatica.

Utilisez la même liste blanche ou noire que le domaine.

Par exemple, exécutez la commande suivante :

```
infasetup updateWorkerNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

6. Démarrez le domaine Informatica.

7. Vous pouvez éventuellement exécuter la commande `infacmd isp listDomainCiphers` pour afficher les listes de suites de chiffres utilisées par un domaine ou un nœud.

Par exemple, exécutez la commande suivante pour afficher la liste effective de suites de chiffres utilisée par le domaine :

```
infacmd isp listDomainCiphers -l EFFECTIVE
```

Sources et cibles sécurisées

Informatica utilise des objets de connexion pour se connecter aux bases de données relationnelles en tant que source ou cible. Vous pouvez créer un objet de connexion à une base de données relationnelle qui est sécurisée avec un certificat SSL.

Vous créez les objets de connexion PowerCenter dans le gestionnaire de flux de travail. Vous créez une connexion Service de données, Data Quality ou Profilage dans l'outil Developer tool ou Administrator tool.

Vous pouvez créer une connexion sécurisée à une source ou une cible sur les bases de données suivantes :

- Oracle
- Microsoft SQL Server
- IBM DB2

Sources et cibles du service d'intégration de données

Lorsque vous créez un objet de connexion pour le service d'intégration de données afin de traiter les mappages, les profils de données, les fiches d'évaluation ou les services de données SQL, vous pouvez définir une connexion à une base de données sécurisée avec le protocole SSL.

Le service d'intégration de données se connecte à la base de données source ou cible via les pilotes JDBC. Lorsque vous configurez la connexion à une base de données de référentiel sécurisée, vous devez inclure les paramètres de connexion sécurisée dans la chaîne de connexion JDBC.

1. Configurez une base de données sécurisée à l'aide du protocole SSL, dans le but de l'utiliser comme source ou cible.
2. Dans l'outil Administrator, créez une connexion.
3. Dans la boîte de dialogue **Nouvelle connexion**, sélectionnez le type de connexion. Ensuite, cliquez sur **OK**.

Vous pouvez créer une connexion à une base de données DB2, Microsoft SQL Server ou Oracle sécurisée.

4. Dans la boîte de dialogue **Nouvelle connexion - Étape 1 sur 3**, entrez les propriétés de la connexion et cliquez sur **Suivant**.
5. Sur la page **Nouvelle connexion - Étape 2 sur 3**, entrez la chaîne de connexion à la base de données. Pour vous connecter à une base de données sécurisée, entrez les paramètres appropriés dans le champ **Options de sécurité JDBC avancées**. Informatica considère la valeur du champ **Options de sécurité JDBC avancées** comme des données sensibles et stocke la chaîne de paramètres sous une forme cryptée.

La liste suivante décrit les paramètres de base de données sécurisés :

EncryptionMethod

Requis. Indique si les données sont cryptées lorsqu'elles sont transmises sur le réseau. Ce paramètre doit être défini sur `SSL`.

ValidateServerCertificate

Facultatif. Indique si Informatica valide le certificat envoyé par le serveur de base de données.

Si ce paramètre est défini sur `True`, Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre `HostNameInCertificate`, Informatica valide également le nom d'hôte dans le certificat.

Si ce paramètre est défini sur `False`, Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de truststore que vous spécifiez.

La valeur par défaut est `True`.

HostNameInCertificate

Facultatif. Nom d'hôte de la machine qui héberge la base de données sécurisée. Si vous spécifiez un nom d'hôte, Informatica valide le nom d'hôte inclus dans la chaîne de connexion avec le nom d'hôte dans le certificat `SSL`.

TrustStore

Obligatoire. Chemin d'accès et nom du fichier truststore contenant le certificat `SSL` de la base de données.

TrustStorePassword

Obligatoire. Mot de passe du fichier truststore pour la base de données sécurisée.

Remarque: Informatica ajoute les paramètres `JDBC` sécurisés à la chaîne de connexion. Si vous ajoutez les paramètres `JDBC` sécurisés directement à la chaîne de connexion, n'entrez pas de paramètres dans le champ **Options de sécurité JDBC avancées**.

6. Testez la connexion pour vérifier que la connexion à la base de données sécurisée est valide.
7. Finalisez le processus pour créer la connexion relationnelle.

Sources et cibles PowerCenter

Lorsque vous créez un objet de connexion pour une session PowerCenter, vous pouvez définir une connexion à une base de données sécurisée avec le protocole `SSL`.

Vous pouvez vous connecter à des sources et des cibles PowerCenter relationnelles via la connectivité native ou les pilotes `ODBC`.

Si vous vous connectez à une source ou une cible relationnelle sécurisée via la connectivité native, vérifiez que le client de base de données contient les informations de connexion de la base de données sécurisée. Par exemple, si vous vous connectez à une cible PowerCenter sur une base de données Oracle sécurisée, configurez le fichier du client de base de données Oracle `tnsnames.ora` avec les informations de connexion de la base de données sécurisée.

Si vous vous connectez à une source ou une cible relationnelle sécurisée via les pilotes `ODBC`, vérifiez que le client de base de données contient les informations de connexion de la base de données sécurisée et que la source de données `ODBC` définit correctement la connexion à la base de données sécurisée.

Stockage de données sécurisé

Informatica crypte les données sensibles telles que les mots de passe et les paramètres de connexion sécurisée avant de stocker les données dans le référentiel de configuration du domaine. Informatica utilise un mot-clé que vous indiquez pour créer une clé de cryptage pour crypter les données sensibles.

Lors de l'installation, vous devez fournir un mot-clé que le programme d'installation utilise pour générer la clé de cryptage du domaine. Tous les nœuds du domaine doivent utiliser la même clé de cryptage. En cas d'installation sur plusieurs nœuds, le programme d'installation utilise la même clé de cryptage pour tous les nœuds du domaine. Pour plus d'informations sur la génération d'une clé de cryptage pour le domaine pendant l'installation, consultez les guides d'installation Informatica.

Après l'installation, vous pouvez modifier la clé de cryptage du domaine. Exécutez la commande `infasetup` pour générer une clé de cryptage et modifier la clé de cryptage du domaine. Après avoir modifié la clé de cryptage du domaine, vous devez mettre à niveau le contenu des référentiels du domaine pour mettre à jour les données cryptées.

Remarque: Vous devez conserver en lieu sûr le nom du domaine, le mot-clé de la clé de cryptage et le fichier de clé de cryptage. Le nom de domaine, le mot-clé et la clé de cryptage sont requis lorsque vous modifiez la clé de cryptage du domaine ou déplacez un référentiel vers un autre domaine. Si vous perdez le fichier de clé de cryptage, il vous faut le mot-clé pour générer de nouveau la clé de cryptage. Si vous perdez le mot-clé et la clé de cryptage, vous ne pouvez pas modifier la clé de cryptage du domaine ni déplacer un référentiel vers un autre domaine.

Répertoire sécurisé sous UNIX

Lorsque vous installez Informatica, le programme d'installation crée un répertoire pour stocker des fichiers Informatica qui nécessitent un accès restreint, tels que le fichier de clé de cryptage du domaine. Sous UNIX, le programme d'installation attribue des autorisations différentes au répertoire et aux fichiers dans le répertoire.

Par défaut, le programme d'installation crée le répertoire suivant dans le répertoire d'installation d'Informatica pour y stocker la clé de cryptage : `<INFA_HOME>/isp/config/keys`

Le répertoire `/keys` contient le fichier de clé de cryptage du nœud. Si vous configurez le domaine pour utiliser l'authentification Kerberos, le répertoire contient également les fichiers `keytab` Kerberos.

Lors de l'installation, vous pouvez spécifier un répertoire différent dans lequel stocker le fichier de cryptage. Le programme d'installation attribue les mêmes autorisations au répertoire spécifié en tant que le répertoire par défaut.

Le répertoire `/keys` et ses fichiers disposent des autorisations suivantes :

Autorisations des répertoires

Le propriétaire du répertoire dispose de `-wx` autorisations pour le répertoire mais aucune autorisation `r`. Le propriétaire du répertoire est le compte d'utilisateur utilisé pour exécuter le programme d'installation. Le groupe auquel le propriétaire appartient dispose également de `-wx` autorisations pour le répertoire mais aucune autorisation `R`.

Par exemple, le compte d'utilisateur `ediqa` possède le répertoire et appartient au groupe `infaadmin`. Le compte d'utilisateur `ediqa` et le groupe `infaadmin` disposent des autorisations suivantes : `-wx-wx---`

Le compte d'utilisateur `ediqa` et le groupe `infaadmin` peuvent écrire dans le répertoire et exécuter des fichiers dans celui-ci. Ils ne peuvent pas afficher la liste de fichiers du répertoire mais peuvent lister un fichier spécifique par nom.

Si vous connaissez le nom d'un fichier dans le répertoire, vous pouvez copier le fichier depuis le répertoire vers un autre emplacement. Si vous ne connaissez pas le nom du fichier, vous devez modifier

l'autorisation pour le répertoire afin d'inclure l'autorisation d'accès en lecture avant de pouvoir copier le fichier. Vous pouvez utiliser la commande `chmod 730` pour accorder l'autorisation d'accès en lecture au propriétaire du répertoire et des sous-répertoires.

Par exemple, vous devez copier le fichier de clé de cryptage nommé *siteKey* vers un répertoire temporaire afin de le rendre accessible à un autre nœud dans le domaine. Exécutez la commande `chmod 730` sur le répertoire `<Répertoire d'installation Informatica>/isp/config` pour attribuer les autorisations suivantes : `rw-x-wx---`. Vous pouvez ensuite copier le fichier de clé de cryptage du sous-répertoire `/keys` vers un autre répertoire.

Après avoir terminé la copie les fichiers, rétablissez les autorisations de lecture et d'exécution pour le répertoire. Vous pouvez utiliser la commande `chmod 330` pour supprimer l'autorisation d'accès en lecture.

Remarque: N'utilisez pas l'option `-R` pour modifier de façon récursive les autorisations pour le répertoire et fichiers. Le répertoire et les fichiers dans le répertoire ont des autorisations différentes.

Autorisations d'accès aux fichiers

Le propriétaire des fichiers du répertoire dispose des autorisations `rxwx` pour les fichiers. Le propriétaire des fichiers du répertoire est le compte d'utilisateur utilisé pour exécuter le programme d'installation. Le groupe auquel appartient le propriétaire dispose également d'une autorisation `rxwx` pour les fichiers du répertoire.

Le propriétaire et le groupe ont un accès complet au fichier et peuvent afficher ou modifier le fichier dans le répertoire.

Remarque: Vous devez connaître le nom du fichier pour pouvoir afficher ou modifier le fichier.

Modification de la clé de cryptage à partir de la ligne de commande

Après l'installation, vous pouvez modifier la clé de cryptage du domaine à partir de la ligne de commande. Vous devez arrêter le domaine avant de modifier la clé de cryptage.

Utilisez la commande `infasetup` pour générer une clé de cryptage et configurer le domaine pour utiliser la nouvelle clé de cryptage.

Les commandes `infasetup` suivantes permettent de générer et de modifier la clé de cryptage :

generateEncryptionKey

Génère une clé de cryptage dans un fichier nommé *sitekey*. Si le répertoire spécifié pour la clé de chiffrement contient un fichier nommé *sitekey*, Informatica le renomme *siteKey_old*.

migrateEncryptionKey

Modifie la clé de cryptage utilisée pour stocker les données sensibles dans le domaine Informatica.

Pour modifier la clé de cryptage d'un domaine, procédez comme suit :

1. Arrêtez le domaine.
2. Sauvegardez le domaine avant de modifier la clé de cryptage.
Pour être sûr de récupérer le domaine en cas de problèmes lors de la modification de la clé de cryptage, sauvegardez-le avant d'exécuter les commandes `infasetup`.
3. Pour générer une clé de chiffrement pour le domaine, exécutez la commande `infasetup generateEncryptionKey`.

Spécifiez l'option encryptionKeyLocation pour générer une clé de chiffrement :

Option	Argument	Description
-encryptionKeyLocation -kl	encryption_key_location	Répertoire contenant la clé de cryptage actuelle. Le nom du fichier de cryptage est <i>sitekey</i> . Informatica remplace le nom du fichier <i>sitekey</i> actuel par <i>sitekey_old</i> et génère une clé de cryptage dans un nouveau fichier nommé <i>sitekey</i> dans le même répertoire.

Remarque: Le programme d'installation crée une clé de chiffrement lors de l'installation et de la mise à niveau. Vous n'avez pas besoin des options de mot clé et de nom de domaine lors de la génération de la clé de site du fichier de chiffrement. Assurez-vous d'enregistrer une copie de cette clé de site unique. En cas de perte, vous ne pouvez plus la régénérer. Ne partagez la clé de site unique avec personne.

4. Pour modifier la clé de chiffrement du domaine, exécutez la commande `infasetup migrateEncryptionKey` et spécifiez l'emplacement de l'ancienne clé de chiffrement et de la nouvelle.

Spécifiez les options suivantes requises pour modifier la clé de cryptage du domaine :

Option	Argument	Description
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	<p>Répertoire dans lequel l'ancien fichier de clé de cryptage (<i>siteKey_old</i>) et le nouveau (<i>siteKey</i>) sont stockés.</p> <p>Le répertoire doit contenir les deux fichiers de clé de cryptage, l'ancien et le nouveau. S'ils sont stockés dans des répertoires différents, copiez-les dans le même répertoire.</p> <p>Si le domaine comporte plusieurs nœuds, ce répertoire doit être accessible au nœud du domaine depuis lequel vous exécutez la commande <code>migrateEncryptionKey</code>.</p> <p>Lorsque vous migrez un domaine multinœud, tous les nœuds du domaine doivent utiliser la même clé de chiffrement. Pour changer la clé de chiffrement du domaine, exécutez la commande <code>infasetup migrateEncryptionKey</code> sur tous les nœuds du domaine.</p> <p>Remarque: Sous UNIX, le nom de fichier <i>siteKey_old</i> est sensible à la casse. Si vous renommez manuellement le fichier de clé de cryptage précédent, vérifiez que le nouveau nom respecte la casse.</p>
-IsDomainMigrated -mig	is_domain_migrated	<p>Indique si le domaine a été mis à jour de manière à utiliser la clé de cryptage la plus récente.</p> <p>Lorsque vous exécutez la commande <code>migrateEncryptionKey</code> pour la première fois, définissez cette option sur <code>False</code> pour indiquer que le domaine utilise l'ancienne clé de cryptage.</p> <p>Par la suite, lorsque vous exécutez la commande <code>migrateEncryptionKey</code> pour mettre à jour d'autres nœuds du domaine, définissez cette option sur <code>True</code> pour indiquer que le domaine a été mis à jour et utilise la clé de cryptage la plus récente. Vous pouvez également exécuter la commande <code>migrateEncryptionKey</code> sans cette option.</p> <p>La valeur par défaut est <code>True</code>.</p>

5. Exécutez la commande `infasetup` sur chaque nœud du domaine.

Si le domaine comporte plusieurs nœuds, exécutez la commande `infasetup migrateEncryptionKey` sur chaque nœud. Exécutez la commande sur les nœuds de passerelle avant de l'exécuter sur les nœuds de travail. Vous pouvez omettre l'option `IsDomainMigrated` après la première exécution de la commande.

6. Redémarrez le domaine.

Vous devez mettre à niveau tous les services de référentiel du domaine pour mettre à jour et chiffrer les données sensibles des référentiels avec la nouvelle clé de chiffrement. Vous devez également migrer la clé de site après avoir mis à niveau le domaine.

7. Mettez à niveau l'ensemble des services de référentiel modèle, des services de référentiel PowerCenter et des services Metadata Manager.

Vous pouvez mettre à niveau un service de référentiel modèle et un service de référentiel PowerCenter dans l'outil Administrator ou à l'invite de commande. Vous pouvez mettre à niveau un service Metadata Manager dans l'outil Administrator.

Remarque: Vous devez désactiver le service Metadata Manager pour pouvoir le mettre à niveau.

Pour mettre à niveau un service dans l'outil Administrator, sélectionnez **Gérer > Mettre à niveau** dans la zone d'en-tête. Si vous sélectionnez plusieurs services, l'outil Administrator les met à niveau dans l'ordre approprié.

Pour mettre à niveau un service à l'invite de commande, utilisez les commandes suivantes :

Type de service de référentiel	Commande
Service de référentiel modèle	<code>infacmd mrs UpgradeContents</code>
Service de référentiel PowerCenter	<code>pmrep Upgrade</code>

Services et ports d'application

Les services du domaine Informatica et les services d'application dans le domaine Informatica ont des ports uniques.

Domaine Informatica

Le tableau suivant décrit les ports que vous pouvez définir :

Port	Description
Port de gestionnaire de service	Numéro de port utilisé par le Gestionnaire de service sur le nœud. Le gestionnaire de service écoute les demandes de connexions entrantes sur ce port. Les applications clientes utilisent ce port pour communiquer avec les services du domaine. Les programmes de ligne de commande Informatica utilisent ce port pour communiquer avec le domaine. Ce port est également utilisé par le pilote JDBC/ODBC du service de données SQL. La valeur par défaut est 6006.
Port d'arrêt du gestionnaire de service	Numéro de port qui contrôle l'arrêt du serveur pour le Gestionnaire de service du domaine. Le gestionnaire de service écoute les commandes d'arrêt sur ce port. La valeur par défaut est 6007.
Port d'Informatica Administrator	Numéro de port utilisé par Informatica Administrator. La valeur par défaut est 6008.
Port HTTPS d'Informatica Administrator	Aucun port par défaut. Entrez le numéro de port requis lorsque vous créez le service. Configurer le port sur 0 désactive la connexion HTTPS à l'outil Administrator tool.
Port d'arrêt d'Informatica Administrator	Numéro de port qui contrôle l'arrêt du serveur pour Informatica Administrator. Informatica Administrator écoute les demandes d'arrêt sur ce port. La valeur par défaut est 6009.

Port	Description
Numéro de port minimal	Plus petit numéro de port de la plage des numéros de port pouvant être attribués aux processus de service d'application exécutés sur ce nœud. Le numéro par défaut est 6014.
Numéro de port maximal	Plus grand numéro de port de la plage des numéros de port pouvant être attribués aux processus de service d'application exécutés sur ce nœud. Le numéro par défaut est 6114.

Service Analyst

Le tableau suivant présente le port par défaut associé au service Analyst :

Type	Port par défaut
Service Analyst (HTTP)	8085
Service Analyst (HTTPS)	Aucun port par défaut. Saisissez le numéro de port requis lorsque vous créez le service.

Service de gestion de contenu

Le tableau suivant présente le port par défaut associé au service de gestion de contenu :

Type	Port par défaut
Service de gestion de contenu (HTTP)	8105
Service de gestion de contenu (HTTPS)	Aucun port par défaut. Saisissez le numéro de port requis lorsque vous créez le service.

Service d'intégration de données

Le tableau suivant présente le port par défaut associé au service d'intégration de données :

Type	Port par défaut
Service d'intégration de données (proxy HTTP)	8080
Service d'intégration de données (HTTP)	8095
Service d'intégration de données (HTTPS)	Aucun port par défaut. Saisissez le numéro de port requis lorsque vous créez le service.
Base de données de l'entrepôt de profilage	Aucun port par défaut. Saisissez le numéro de port de la base de données.

Service d'accès aux métadonnées

Le tableau suivant présente le port par défaut associé au service d'accès aux métadonnées :

Type	Port par défaut
Service d'accès aux métadonnées (HTTP)	7080 Le service d'accès aux métadonnées utilise des numéros de port consécutifs pour se connecter à plusieurs distributions Hadoop.
Service d'accès aux métadonnées (HTTPS)	Aucun port par défaut. Saisissez le numéro de port requis lorsque vous créez le service. Le service d'accès aux métadonnées utilise des numéros de port consécutifs pour se connecter à plusieurs distributions Hadoop.

Service Metadata Manager

Le tableau suivant présente le port par défaut associé au service Metadata Manager :

Type	Port par défaut
Service Metadata Manager (HTTP)	10250
Service Metadata Manager (HTTPS)	Aucun port par défaut. Saisissez le numéro de port requis lorsque vous créez le service.

Service d'écoute PowerExchange®

Utilisez le même numéro de port que celui indiqué dans l'instruction SVCNODE du fichier DBMOVE.

Si vous définissez plusieurs services d'écoute à exécuter sur un nœud, vous devez définir un numéro de port SVCNODE unique pour chaque service.

Service de journalisation PowerExchange

Utilisez le même numéro de port que celui indiqué dans l'instruction SVCNODE du fichier DBMOVE.

Si vous définissez plusieurs services d'écoute à exécuter sur un nœud, vous devez définir un numéro de port SVCNODE unique pour chaque service.

Service Hub des services Web

Le tableau suivant présente le port par défaut associé au service Hub des services Web :

Type	Port par défaut
Service Hub des services Web (HTTP)	7333
Service Hub des services Web (HTTPS)	7343

CHAPITRE 7

Gestion de la sécurité dans Informatica Administrator

Ce chapitre comprend les rubriques suivantes :

- [Présentation de l'utilisation d'Informatica Administrator, 109](#)
- [Sécurité utilisateur, 110](#)
- [Onglet Sécurité, 112](#)
- [Gestion du mot de passe, 116](#)
- [Gestion de la sécurité de domaine, 117](#)
- [Gestion de la sécurité des utilisateurs, 118](#)

Présentation de l'utilisation d'Informatica Administrator

Informatica Administrator est l'outil que vous utilisez pour gérer le domaine et la sécurité Informatica.

Utilisez l'outil Administrator pour effectuer les types de tâches suivants :

- **Tâches d'administration du domaine.** Gérer des journaux, objets de domaine, autorisations d'utilisateurs et rapports de domaine. Générer et charger des diagnostics de nœuds. Surveiller les tâches et les applications du service d'intégration de données. Les objets de domaine comprennent des services d'applications, des nœuds, des grilles, des dossiers, des connexions de bases de données, des profils des systèmes d'exploitation et des licences.
- **Tâches d'administration de la sécurité.** Permet de gérer les utilisateurs, les groupes, les rôles et les privilèges.

L'outil Administrator comprend les onglets suivants :

- **Gérer.** Permet d'afficher et de modifier les propriétés du domaine et les objets à l'intérieur du domaine.
- **Surveiller.** Permet d'afficher l'état des tâches de profil, de fiche d'évaluation, d'aperçu et de mappage, des services de données SQL, des services Web et des flux de travail pour chaque service d'intégration de données.
- **Surveiller.** Permet d'afficher l'état des tâches de profil, les tâches d'aperçu, les tâches de mappage, les services de données SQL et les services Web pour chaque service d'intégration de données.

- **Journaux.** Permet d'afficher les événements du journal pour le domaine et les services à l'intérieur du domaine.
- **Rapports.** Permet d'exécuter un rapport des services Web ou de gestion des licences.
- **Sécurité.** Permet de gérer les utilisateurs, les groupes, les rôles et les privilèges.
- **Nuage.** Permet d'afficher les informations relatives à votre organisation Informatica Cloud®.

L'outil Administrator possède les éléments d'en-tête suivants :

- **Se déconnecter.** Permet de se déconnecter de l'outil Administrator tool.
- **Gérer.** Permet de gérer votre compte.
- **Aide.** Accédez à l'aide de l'onglet actuel et déterminez la version d'Informatica.

Sécurité utilisateur

Le gestionnaire de service et certains services d'application contrôlent la sécurité utilisateur dans les clients d'application. Les clients d'application incluent Informatica Administrator, Informatica Analyst, Informatica Developer, Metadata Manager et le client PowerCenter.

Le gestionnaire de service et les services d'application contrôlent la sécurité utilisateur à l'aide des fonctions suivantes :

Cryptage

Lorsque vous vous connectez à un client d'application, le gestionnaire de service crypte le mot de passe.

Authentification

Lorsque vous vous connectez à un client d'application, le gestionnaire de service authentifie votre compte utilisateur à l'aide de votre nom d'utilisateur et de votre mot de passe, ou de votre jeton d'authentification utilisateur.

Autorisation

Lorsque vous demandez un objet dans un client d'application, le gestionnaire de service et les services d'application autorisent la demande en fonction de vos privilèges, rôles et autorisations.

Vous pouvez également utiliser HTTPS pour sécuriser la connexion au domaine et aux services d'application. Les services d'application suivants fournissent une connexion HTTPS ainsi que le domaine Informatica :

- Service d'intégration de données
- Service Analyst
- Service de gestion de contenu
- Service d'accès aux métadonnées
- Service Metadata Manager
- Service du hub de services Web

Cryptage

Informatica chiffre les mots de passe envoyés depuis les clients d'application au gestionnaire de service. Informatica utilise le chiffrement AES avec des clés 128 bits multiples pour chiffrer les mots de passe et stocke les mots de passe cryptés dans la base de données de configuration du domaine. Configurez HTTPS pour chiffrer les mots de passe envoyés au gestionnaire de service depuis les clients d'application.

Authentification

Le gestionnaire de service authentifie les utilisateurs qui se connectent aux clients de l'application.

Lors de votre première connexion à un client d'application, vous saisissez un nom d'utilisateur, un mot de passe et un domaine de sécurité. Un domaine de sécurité est un regroupement de comptes et de groupes d'utilisateurs dans un domaine Informatica.

Le domaine de sécurité que vous utilisez détermine la méthode d'authentification que le gestionnaire de service utilise pour authentifier votre compte utilisateur :

- Native. Lorsque vous vous connectez à un client d'application en tant qu'utilisateur natif, le gestionnaire de service authentifie votre nom d'utilisateur et votre mot de passe par rapport aux comptes d'utilisateurs de la base de données de configuration du domaine.
- Protocole LDAP (Lightweight Directory Access Protocol) Lorsque vous vous connectez à un client d'application en tant qu'utilisateur LDAP, le gestionnaire de service communique votre nom d'utilisateur et votre mot de passe au service d'annuaire LDAP externe pour l'authentification.

Authentification unique

Après vous être connecté à un client d'application, le gestionnaire de service permet de lancer un autre client d'application ou d'accéder à plusieurs référentiels à l'intérieur du client d'application. Vous n'avez pas besoin de vous connecter à l'autre client d'application ou au référentiel.

Lorsque le gestionnaire de service authentifie votre compte d'utilisateur pour la première fois, il crée un jeton d'authentification crypté pour votre compte et renvoie le jeton d'authentification au client de l'application. Le jeton d'authentification contient votre nom d'utilisateur, domaine de sécurité et un délai d'expiration. Le gestionnaire de service renouvelle périodiquement le jeton d'authentification avant le délai d'expiration.

Lorsque vous accédez à plusieurs référentiels à l'intérieur d'un client d'application, ce dernier envoie le jeton d'authentification au gestionnaire de service pour l'authentification de l'utilisateur.

Lorsque vous lancez un client d'application Web à partir d'un autre client d'application, il transmet le jeton d'application au client d'application suivant. Le client d'application Web suivant envoie le jeton d'authentification au gestionnaire de service pour authentification de l'utilisateur. Vous devez vous déconnecter de chaque client d'application Web séparément. Par exemple, si vous ouvrez l'outil Analyst tool depuis l'outil Administrator tool, vous devez vous déconnecter des deux outils séparément.

Remarque: Pour utiliser l'authentification unique entre l'outil Administrator tool, l'outil Analyst tool et l'outil de surveillance, vous devez ajouter leur nom de domaine complet au fichier hôte de chaque nœud.

Vous ne pouvez pas utiliser l'authentification unique pour vous connecter à un client d'application Web depuis un outil client. Par exemple, si vous lancez l'outil Administrator tool depuis l'outil Developer tool, vous devez vous connecter à l'outil Administrator tool.

Autorisation

Le gestionnaire de service autorise les demandes utilisateur pour les objets de domaine. Les demandes peuvent provenir de l'outil Administrator. Les services d'application suivants autorisent les demandes utilisateur pour d'autres objets :

- Service d'intégration de données
- Service Metadata Manager
- Service de référentiel modèle
- Service de référentiel PowerCenter

Lorsque vous créez des utilisateurs et des groupes natifs, ou que vous importez des utilisateurs et des groupes LDAP, le gestionnaire de service stocke les informations dans la base de données de configuration du domaine, au sein des référentiels suivants :

- Référentiel modèle
- Référentiel PowerCenter
- Référentiel PowerCenter pour le gestionnaire de métadonnées

Le gestionnaire de service synchronise les informations concernant les utilisateurs et les groupes entre les référentiels et la base de données de configuration du domaine, lorsque les événements suivants se produisent :

- Redémarrez le service Metadata Manager, le service de référentiel modèle ou le service de référentiel PowerCenter.
- Vous ajoutez ou supprimez des utilisateurs ou des groupes natifs.
- Le gestionnaire de service synchronise la liste des utilisateurs et des groupes LDAP dans la base de données de configuration du domaine avec la liste des utilisateurs et des groupes dans le service d'annuaire LDAP.

Lorsque vous attribuez des permissions aux utilisateurs et aux groupes dans une application client, le service d'application stocke les affectations d'autorisation avec les informations concernant les utilisateurs et les groupes dans le référentiel approprié.

Lorsque vous demandez un objet dans une application client, le service d'application approprié autorise votre demande. Si par exemple vous essayez de modifier un projet dans Informatica Developer, le service de référentiel modèle autorise votre demande en fonction des privilèges, rôles et autorisations qui vous sont attribués.

Onglet Sécurité

Vous gérez la sécurité Informatica dans l'onglet Sécurité de l'outil Administrator tool.

L'onglet Sécurité possède les composants suivants :

- Section Rechercher. Recherche des utilisateurs, groupes ou rôles par nom.
- Navigateur. Le navigateur s'affiche dans le volet de gauche et affiche les groupes, les utilisateurs et les rôles.
- Panneau de contenu. Le panneau de contenu affiche les propriétés et options en fonction de l'objet sélectionné dans le navigateur et de l'onglet sélectionné dans le panneau de contenu.
- Menu Actions de sécurité. Contient des options pour créer ou supprimer un groupe, un utilisateur ou un rôle. Vous pouvez gérer les configurations LDAP et les profils du système d'exploitation. Vous pouvez également afficher les utilisateurs possédant les privilèges pour un service.

Utilisation de la section Rechercher

Utilisez la section Rechercher pour rechercher des utilisateurs, groupes et rôles par nom. La recherche n'est pas sensible à la casse.

1. Dans la section Rechercher, sélectionnez si vous souhaitez rechercher des utilisateurs, groupes ou rôles.
2. Entrez le nom complet ou partiel à rechercher.

Vous pouvez inclure un astérisque (*) dans un nom pour utiliser un caractère générique dans la recherche. Par exemple, saisissez « ad* » pour rechercher tous les objets commençant par « ad ». Saisissez « ad* » pour rechercher tous les objets se terminant par « ad ».

3. Cliquez sur Atteindre.

La section Résultats de la recherche apparaît et affiche un maximum de 100 objets. Si votre recherche renvoie plus de 100 objets, précisez vos critères de recherche pour affiner les résultats de la recherche.

4. Sélectionnez un objet dans la section Résultats de la recherche pour afficher des informations sur l'objet dans le volet de contenu.

Utilisation du navigateur de sécurité

Le navigateur s'affiche dans le panneau de contenu de l'onglet Sécurité. Lorsque vous sélectionnez un objet dans le navigateur, le panneau de contenu affiche des informations sur l'objet.

Le navigateur de l'onglet Sécurité affiche l'une des sections suivantes en fonction de ce que vous affichez :

- Section Groupes. Sélectionnez un groupe pour afficher les propriétés du groupe, les utilisateurs affectés au groupe, et les rôles et privilèges attribués au groupe.
- Section Utilisateurs. Sélectionnez un utilisateur pour afficher les propriétés de l'utilisateur, les groupes auxquels l'utilisateur appartient, et les rôles et privilèges attribués à l'utilisateur.
- Section Rôles. Sélectionnez un rôle pour afficher les propriétés du rôle, les utilisateurs et groupes auxquels le rôle est attribué, et les privilèges affectés au rôle.
- Section Profils d'exploitation. Sélectionnez un profil d'exploitation permettant d'afficher les propriétés du profil de système d'exploitation, ainsi que les autorisations attribuées aux utilisateurs et aux groupes qui utilisent le profil de système d'exploitation.
- Section Configuration LDAP. Sélectionnez une configuration permettant d'afficher les détails de la connexion au serveur LDAP, le domaine de sécurité LDAP qui contient les utilisateurs et groupes importés depuis le service d'annuaire LDAP et la planification de la synchronisation LDAP.

Le navigateur fournit différents moyens d'effectuer une tâche. Vous pouvez utiliser l'une des méthodes suivantes pour gérer les groupes, utilisateurs et rôles :

- Cliquez sur le menu **Actions**. Chaque section du navigateur comprend un menu Actions pour gérer des groupes, des utilisateurs, des rôles, des profils de systèmes d'exploitation ou des configurations LDAP.
- Cliquer avec le bouton droit de la souris sur un objet. Cliquez avec le bouton droit sur un objet dans le navigateur pour afficher les options disponibles dans le menu Actions.
- Utiliser les raccourcis clavier. Utilisez les raccourcis clavier pour passer à des sections différentes du navigateur.

Groupes

Un groupe est un ensemble d'utilisateurs et de groupes qui peuvent posséder les mêmes privilèges, rôles et autorisations.

La section Groupes du navigateur organise les groupes dans des dossiers du domaine de sécurité. Un domaine de sécurité est un regroupement de comptes et de groupes d'utilisateurs dans un domaine Informatica. L'authentification native utilise le domaine de sécurité natif qui contient les utilisateurs et groupes créés et gérés dans l'outil Administrator. L'authentification LDAP utilise les domaines de sécurité LDAP qui contiennent les utilisateurs et groupes importés à partir du service d'annuaire LDAP.

Lorsque vous sélectionnez un dossier de domaine de sécurité dans la section Groupes du navigateur, le volet de contenu affiche tous les groupes appartenant au domaine de sécurité.

Lorsque vous sélectionnez un groupe dans le navigateur, le volet de contenu affiche les onglets suivants :

- **Présentation.** Affiche les propriétés générales du groupe et les utilisateurs affectés au groupe.
- **Privilèges.** Affiche les privilèges et rôles attribués au groupe pour le domaine et pour les services d'application du domaine.
- **Autorisations.** Affiche le niveau d'accès dont disposent les utilisateurs au sein du groupe pour effectuer des tâches sur les objets du domaine, notamment les nœuds, les grilles et les services d'application. Affiche également le niveau d'accès dont disposent les utilisateurs au sein du groupe pour effectuer des tâches sur les objets de la connexion et les profils du système d'exploitation.

Utilisateurs

Un utilisateur avec un compte dans le domaine Informatica peut se connecter aux clients d'applications suivants :

- Informatica Administrator
- Client PowerCenter
- Informatica Developer
- Informatica Analyst
- Metadata Manager

La section Utilisateurs du navigateur organise les utilisateurs dans des dossiers du domaine de sécurité. Un domaine de sécurité est un regroupement de comptes et de groupes d'utilisateurs dans un domaine Informatica. L'authentification native utilise le domaine de sécurité natif qui contient les utilisateurs et groupes créés et gérés dans l'outil Administrator. L'authentification LDAP utilise les domaines de sécurité LDAP qui contiennent les utilisateurs et groupes importés à partir du service d'annuaire LDAP.

Lorsque vous sélectionnez un dossier de domaine de sécurité dans la section Utilisateurs du navigateur, le volet de contenu affiche tous les utilisateurs appartenant au domaine de sécurité.

Lorsque vous sélectionnez un utilisateur dans le navigateur, le volet de contenu affiche les onglets suivants :

- **Présentation.** Affiche les propriétés générales de l'utilisateur et tous les groupes auxquels l'utilisateur appartient.
- **Privilèges.** Affiche les privilèges et rôles attribués à l'utilisateur pour le domaine et pour les services d'application dans le domaine.
- **Autorisations.** Affiche le niveau d'accès dont dispose l'utilisateur pour effectuer des tâches sur les objets du domaine, comme les nœuds, les grilles et les services d'application. Affiche également le niveau d'accès dont dispose l'utilisateur pour effectuer des tâches sur les objets de connexion et les profils du système d'exploitation.

Rôles

Un rôle est un regroupement de privilèges que vous assignez à un utilisateur ou un groupe. Les privilèges déterminent les actions que les utilisateurs peuvent effectuer. Vous assignez un rôle à des utilisateurs et des groupes pour le domaine et les services d'application du domaine.

La section Rôles du navigateur organise les rôles dans les dossiers suivants :

- **Rôles définis par le système.** Contient des rôles que vous ne pouvez ni éditer ni supprimer. Le rôle Administrateur est un rôle défini par le système.
- **Rôles personnalisés.** Contient des rôles que vous pouvez créer, éditer et supprimer. L'outil Administrator comprend des rôles personnalisés que vous pouvez éditer et assigner à d'autres utilisateurs et groupes.

Lorsque vous sélectionnez un dossier dans la section Rôles du navigateur, le volet de contenu affiche tous les rôles appartenant au dossier.

Lorsque vous sélectionnez un rôle dans le navigateur, le volet de contenu affiche les onglets suivants :

- Présentation. Affiche les propriétés générales du rôle ainsi que les utilisateurs et groupes dont le rôle est assigné pour le domaine et les services d'application.
- Privilèges. Affiche les privilèges assignés au rôle pour le domaine ou les services d'application.

Profils de système d'exploitation

Un profil de système d'exploitation est un mécanisme de sécurité que le service d'intégration de données et le service d'intégration PowerCenter utilisent pour exécuter des mappages, des flux de travail et des tâches de profilage.

La section Profils de système d'exploitation du navigateur répertorie les profils de système d'exploitation configurés dans le domaine.

Lorsque vous sélectionnez un profil de système d'exploitation dans le navigateur, le volet de contenu affiche les onglets suivants :

- Propriétés. Affiche les propriétés générales du profil de système d'exploitation configuré pour le service d'intégration de données, pour le service d'intégration PowerCenter ou pour les deux services d'application.
- Autorisations. Affiche les autorisations attribuées aux utilisateurs et aux groupes qui utilisent le profil de système d'exploitation. Indique également si le profil de système d'exploitation est le profil par défaut attribué à un utilisateur ou à un groupe.

Configuration LDAP

Vous pouvez configurer un domaine Informatica pour permettre aux utilisateurs et aux groupes importés depuis un ou plusieurs services d'annuaire LDAP de se connecter aux nœuds, services et clients d'application Informatica.

La section Configuration LDAP du navigateur répertorie les configurations LDAP que le domaine utilise.

Lorsque vous sélectionnez une configuration LDAP, les onglets suivants s'affichent sous l'onglet Configuration LDAP :

- Présentation. Répertorie les détails de connexion du serveur LDAP qui contient le service d'annuaire à partir duquel vous voulez importer des utilisateurs et des groupes.
- Domaines de sécurité. Répertorie les détails du domaine de sécurité LDAP qui contient les utilisateurs et les groupes importés depuis le service d'annuaire LDAP.
- Planification. Répertorie les détails de planification de la synchronisation indiquant lorsque le gestionnaire de service met à jour le domaine de sécurité avec les utilisateurs et les groupes dans le service d'annuaire LDAP.

Gestion des comptes

Pour améliorer la sécurité dans le domaine Informatica, vous pouvez appliquer le verrouillage des comptes utilisateur et administrateur après un certain nombre d'échecs de connexion.

La section Configuration du verrouillage de compte de la page Gestion des comptes indique si le verrouillage de compte est activé pour les comptes utilisateur et les comptes administrateur. La section indique également le nombre maximum d'échecs de connexion autorisés.

La section Utilisateurs natifs verrouillés de la page répertorie les comptes utilisateurs verrouillés dans le domaine de sécurité natif. Vous pouvez déverrouiller un compte utilisateur dans le domaine de sécurité natif.

La section Utilisateurs LDAP verrouillés de la page répertorie les comptes utilisateurs verrouillés dans un domaine de sécurité LDAP. Vous pouvez déverrouiller un compte utilisateur dans le domaine Informatica. Toutefois, l'administrateur LDAP doit déverrouiller le compte utilisateur dans le serveur LDAP. L'utilisateur ne peut pas se connecter au domaine Informatica tant que l'administrateur LDAP n'a pas déverrouillé son compte utilisateur.

Rapports d'audit

Les rapports d'audit fournissent des informations sur les utilisateurs et les groupes du domaine Informatica, ainsi que sur les privilèges, rôles et autorisations attribués à chaque utilisateur ou groupe.

Vous sélectionnez le rapport d'audit à générer dans le menu Sélectionner un type de rapport. Vous pouvez générer les rapports d'audit suivants :

Informations personnelles de l'utilisateur

Affiche les informations de contact et les détails d'état des comptes utilisateurs dans le domaine. Vous pouvez sélectionner les utilisateurs ou les groupes pour lesquels vous voulez générer le rapport.

Association de groupes d'utilisateurs

Affiche des informations concernant les utilisateurs et les groupes auxquels ils appartiennent. Vous pouvez sélectionner les utilisateurs ou les groupes pour lesquels vous voulez générer le rapport.

Privilèges

Affiche les informations sur les privilèges attribués aux utilisateurs et aux groupes du domaine. Vous pouvez sélectionner les utilisateurs ou les groupes pour lesquels vous voulez générer le rapport.

Rôles

Affiche les informations sur les rôles attribués aux utilisateurs et aux groupes du domaine. Vous pouvez sélectionner les rôles pour lesquels vous voulez générer le rapport.

Autorisations d'objet de domaine

Affiche les informations sur les objets de domaine sur lesquels les utilisateurs et les groupes disposent d'une autorisation. Vous pouvez sélectionner les utilisateurs ou les groupes pour lesquels vous voulez générer le rapport.

Gestion du mot de passe

Vous pouvez changer le mot de passe via l'application de modification du mot de passe.

Vous pouvez ouvrir l'application de modification de mot de passe depuis l'outil Administrator tool ou à l'aide de l'URL suivante : `http://<fully qualified host name>:<port>/passwordchange/`

Le gestionnaire de service utilise le mot de passe utilisateur associé à un nœud de travail pour authentifier les utilisateurs du domaine. Si vous changez un mot de passe d'utilisateur associé à un ou à plusieurs nœuds de travail, le gestionnaire de service met à jour le mot de passe pour chaque nœud de travail. Le gestionnaire de service ne peut pas mettre à jour les nœuds qui ne sont pas en cours d'exécution. Pour les nœuds qui ne sont pas en cours d'exécution, le gestionnaire de service met à jour le mot de passe au redémarrage des nœuds.

Remarque: Pour un compte utilisateur LDAP, changez le mot de passe dans le service d'annuaire LDAP.

Pour un compte utilisateur natif, si vous activez la complexité du mot de passe, utilisez les directives suivantes lorsque vous créez ou modifiez un mot de passe :

- Le mot de passe doit contenir au moins huit caractères.
- Il doit être composé d'un caractère alphabétique, d'un caractère numérique et d'un caractère non alphanumérique, tels que :

! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { | } ~

Lorsque vous utilisez des caractères spéciaux dans un mot de passe, il arrive que l'interpréteur de commandes les lise différemment. Par exemple, \$ est interprété comme une variable. Dans ce cas, utilisez un caractère d'échappement pour échapper le caractère spécial.

Modification de votre mot de passe

Modifiez le mot de passe d'un compte utilisateur natif à tout moment. Pour un compte utilisateur créé par une autre personne, modifiez le mot de passe lors de la première connexion à l'outil Administrator.

1. Dans la zone d'en-tête de l'outil Administrator tool, cliquez sur **Gérer > Changer le mot de passe** .
L'application de modification du mot de passe s'ouvre dans une nouvelle fenêtre du navigateur.
2. Entrez le mot de passe actuel dans la zone **Mot de passe** et le nouveau mot de passe dans les zones **Nouveau mot de passe** et **Confirmer le mot de passe**.
3. Cliquez sur **Mettre à jour** .

Gestion de la sécurité de domaine

Vous pouvez configurer les composants du domaine Informatica pour utiliser le protocole SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) pour chiffrer les connexions avec les autres composants. Lorsque vous activez le protocole SSL ou TLS pour les composants du domaine, vous garantisiez une communication sécurisée.

Vous pouvez configurer une communication sécurisée des manières suivantes :

Entre les services du domaine

Vous pouvez configurer une communication sécurisée entre les services du domaine.

Entre le domaine et les composants externes

Vous pouvez configurer une communication sécurisée entre les composants du domaine Informatica et les navigateurs Web ou clients de service Web.

Chaque méthode de configuration de communication sécurisée est indépendante des autres méthodes. Lorsque vous configurez une communication sécurisée pour un ensemble de composants, il n'est pas nécessaire de configurer une communication sécurisée pour tout autre ensemble.

Remarque: Si vous faites passer un domaine de l'état sécurisé à l'état non sécurisé ou inversement, vous devez supprimer sa configuration dans l'outil Developer et les outils clients PowerCenter, puis reconfigurer le domaine dans le client.

Gestion de la sécurité des utilisateurs

Vous gérez la sécurité des utilisateurs à l'intérieur du domaine à l'aide de privilèges et d'autorisations.

Les privilèges déterminent les actions que l'utilisateur peut effectuer dans les objets du domaine. Les autorisations définissent le niveau d'accès d'un utilisateur à un objet du domaine. Les objets de domaine comprennent le domaine, les dossiers, les nœuds, les grilles, les licences, les connexions de bases de données, les profils de systèmes d'exploitation et les services d'application.

Même si un utilisateur possède le privilège pour effectuer certaines actions, l'utilisateur peut également demander l'autorisation d'effectuer l'action sur un objet spécifique. Par exemple, un utilisateur a le privilège de domaine Gérer les services qui permet de modifier les services d'application. Toutefois, l'utilisateur a également l'autorisation pour le service d'application. Un utilisateur avec le privilège de domaine Gérer les services et l'autorisation pour le service de référentiel de développement mais pas le service de référentiel de production peut modifier le premier mais pas le second.

Pour se connecter à l'outil Administrator, un utilisateur doit posséder le privilège de domaine Accéder à Informatica Administrator. Si un utilisateur a le privilège Accéder à Informatica Administrator et l'autorisation pour un objet, mais n'a pas le privilège de domaine qui permet de modifier le type d'objet, l'utilisateur peut uniquement consulter l'objet. Par exemple, si un utilisateur a l'autorisation pour un nœud, mais n'a pas le privilège Gérer les nœuds et les grilles, l'utilisateur peut consulter les propriétés du nœud mais ne peut ni configurer, ni arrêter ni supprimer le nœud.

Si un utilisateur n'a pas l'autorisation pour un objet sélectionné dans le navigateur, le volet de contenu affiche un message indiquant que l'autorisation pour l'objet est refusée.

CHAPITRE 8

Utilisateurs et groupes

Ce chapitre comprend les rubriques suivantes :

- [Présentation des utilisateurs et des groupes, 119](#)
- [Groupes par défaut, 120](#)
- [Comprendre les comptes utilisateurs, 121](#)
- [Gestion des utilisateurs, 123](#)
- [Gestion des groupes, 132](#)
- [Gestion des profils de systèmes d'exploitation, 133](#)
- [Verrouillage de compte, 143](#)

Présentation des utilisateurs et des groupes

Pour accéder aux objets et services d'application dans le domaine Informatica et pour utiliser les clients de l'application, vous devez avoir un compte utilisateur.

Lors de l'installation, un compte utilisateur administrateur par défaut est créé. Utilisez le compte d'administrateur par défaut pour vous connecter au domaine Informatica et gérer des services d'application, des objets de domaine et d'autres comptes utilisateurs. Lorsque vous vous connectez au domaine Informatica après l'installation, modifiez le mot de passe pour garantir la sécurité du domaine Informatica et des applications.

La gestion des comptes d'utilisateurs dans Informatica implique les composants clés suivants :

- **Utilisateurs.** Vous pouvez configurer différents types de comptes utilisateur dans le domaine Informatica. Les utilisateurs peuvent effectuer des tâches en fonction des rôles, privilèges et autorisations qui leurs sont attribués.
- **Authentification.** Lorsqu'un utilisateur se connecte à un client de l'application, le gestionnaire de service authentifie le compte utilisateur dans le domaine Informatica et vérifie que l'utilisateur peut utiliser le client de l'application. Le domaine Informatica peut utiliser l'authentification native ou LDAP pour authentifier les utilisateurs. Le gestionnaire de service organise les comptes et les groupes d'utilisateurs par domaine de sécurité. Il authentifie les utilisateurs selon le domaine de sécurité auquel ils appartiennent.
- **Groupes.** Vous pouvez configurer des groupes d'utilisateurs et attribuer différents rôles, privilèges et autorisations à chaque groupe. Les rôles, privilèges et autorisations attribués au groupe déterminent les tâches que les utilisateurs du groupe peuvent effectuer dans le domaine Informatica.

- **Privilèges et rôles.** Les privilèges déterminent les actions que les utilisateurs peuvent effectuer dans les clients de l'application. Un rôle est un regroupement de privilèges que vous pouvez attribuer à des utilisateurs et des groupes. Vous attribuez des rôles et des privilèges à des utilisateurs et des groupes pour le domaine et les services d'application du domaine.
- **Profils de système d'exploitation.** Si vous exécutez le service d'intégration sous UNIX ou Linux, vous pouvez configurer le service d'intégration pour qu'il utilise les profils de système d'exploitation. Utilisez les profils de système d'exploitation pour améliorer la sécurité et restreindre l'environnement d'exécution pour les utilisateurs. Vous pouvez créer et gérer des profils de système d'exploitation dans l'onglet Sécurité de l'outil Administrator.
- **Verrouillage de compte.** Vous pouvez configurer le verrouillage du compte pour verrouiller un compte utilisateur lorsque cet utilisateur indique une connexion incorrecte dans l'outil Administrator ou des clients d'application, comme l'outil Developer et l'outil Analyst. Vous pouvez également déverrouiller un compte utilisateur.

Groupes par défaut

Le domaine Informatica dispose d'un ensemble de groupes d'utilisateurs qui sont créés lors de l'installation.

Par défaut, il s'agit des groupes d'utilisateurs suivants :

- Administrateur
- Tout le monde
- Opérateur

Groupe d'administration

Le domaine Informatica inclut un groupe par défaut nommé Administrateur. Le compte administrateur par défaut créé lors de l'installation appartient à ce groupe.

Le groupe Administrateur possède des autorisations et des privilèges d'administration sur le domaine et sur tous les services d'application. Vous pouvez ajouter des utilisateurs au groupe d'administration ou en supprimer. Tous les utilisateurs du groupe Administrateur ont les mêmes autorisations et privilèges que l'administrateur par défaut créé lors de l'installation.

Vous ne pouvez pas supprimer le compte de l'administrateur par défaut depuis le groupe d'administrateurs ni supprimer le groupe d'administrateurs.

Groupe Tout le monde

Un domaine Informatica inclut un groupe par défaut nommé Tout le monde. Tous les utilisateurs du domaine appartiennent au groupe.

Par défaut, le groupe Tout le monde ne dispose d'aucun privilège. Vous pouvez attribuer des privilèges, des rôles et des autorisations au groupe Tout le monde pour accorder le même accès à tous les utilisateurs.

Vous ne pouvez pas effectuer les tâches suivantes relatives au groupe Tout le monde :

- Modifier ou supprimer le groupe Tout le monde.
- Ajouter des utilisateurs ou supprimer des utilisateurs du groupe Tout le monde.
- Déplacer un groupe vers le groupe Tout le monde.

Groupe d'opérateurs

Le domaine Informatica inclut un groupe par défaut nommé Opérateurs.

Par défaut, le groupe d'opérateurs dispose d'une autorisation sur tous les objets du domaine. Vous pouvez attribuer le rôle d'opérateur au groupe d'opérateurs et l'utiliser pour gérer les opérateurs dans le domaine.

Vous pouvez effectuer les tâches suivantes dans le groupe d'opérateurs :

- Attribuer des privilèges et des rôles au groupe.
- Ajouter des utilisateurs au groupe ou en supprimer.
- Déplacer un groupe vers le groupe.
- Modifier ou supprimer le groupe.

Comprendre les comptes utilisateurs

Un domaine Informatica peut posséder les types de compte suivants :

- Administrateur par défaut
- Administrateur de domaine
- Administrateur de client d'application
- Utilisateur

Administrateur par défaut

Lorsque vous installez les services Informatica, le programme d'installation crée l'administrateur par défaut avec un nom d'utilisateur et un mot de passe que vous indiquez. Vous pouvez utiliser le compte de l'administrateur par défaut pour vous connecter la première fois à l'outil Administrator.

L'administrateur par défaut possède les autorisations et privilèges administrateur sur le domaine et tous les services d'application.

L'administrateur par défaut peut effectuer les tâches suivantes :

- Créer, configurer et gérer tous les objets du domaine, y compris les nœuds, services d'application et les comptes utilisateur et administrateur.
- Configurer et gérer tous les objets et comptes d'utilisateurs créés par d'autres administrateurs de domaine et administrateurs de client d'application.
- Se connecter à n'importe quel client d'application.

Vous ne pouvez pas désactiver ou modifier le nom d'utilisateur ou les privilèges de l'administrateur par défaut. Vous pouvez modifier le mot de passe de l'administrateur par défaut.

Administrateur de domaine

Un administrateur de domaine peut créer et gérer des objets dans le domaine.

L'administrateur de domaine peut se connecter à l'outil Administrator, créer et configurer les services d'application du domaine. Cependant, par défaut, l'administrateur de domaine ne peut pas se connecter aux clients d'application. L'administrateur par défaut doit explicitement donner à l'administrateur de domaine les

autorisations et privilèges complets des services d'application pour qu'il puisse se connecter et effectuer des tâches d'administration dans les clients d'application.

Pour créer un administrateur de domaine, attribuez à un utilisateur le rôle Administrateur d'un domaine.

Administrateur de client d'application

Un administrateur de client d'application peut créer et gérer l'ensemble des objets d'un client d'application. Vous devez créer des comptes administrateur pour les clients d'application. Pour limiter les privilèges administrateur et sécuriser les clients d'application, créez un compte administrateur distinct pour chacun d'eux.

Par défaut, l'administrateur de client d'application ne dispose pas d'autorisation ni de privilège dans le domaine. Sans autorisation ni privilège dans le domaine, l'administrateur de client d'application ne peut pas se connecter à l'outil Administrator pour gérer le service d'application.

Vous pouvez paramétrer l'administrateur de client d'application suivant :

Administrateur Informatica Analyst

Dispose de toutes les autorisations et de tous les privilèges dans Informatica Analyst. L'administrateur Informatica Analyst peut se connecter à Informatica Analyst pour créer et gérer des projets et des objets dans des projets, ainsi que pour effectuer toutes les tâches dans le client d'application.

Pour créer un administrateur Informatica Analyst, attribuez le rôle administrateur à un utilisateur pour un service Analyst et pour le service de référentiel modèle associé.

Administrateur Informatica Developer

Dispose de toutes les autorisations et de tous les privilèges dans Informatica Developer. L'administrateur Informatica Developer peut se connecter à Informatica Developer pour créer et gérer des projets et des objets dans des projets, ainsi que pour effectuer toutes les tâches dans le client d'application.

Pour créer un administrateur Informatica Developer, attribuez à un utilisateur le rôle d'administrateur pour un service de référentiel modèle.

Administrateur Metadata Manager

Dispose de toutes les autorisations et de tous les privilèges dans Metadata Manager. L'administrateur Metadata Manager peut se connecter à Metadata Manager pour créer des objets Metadata Manager et les gérer, ainsi que pour effectuer toutes les tâches dans le client d'application.

Pour créer un administrateur Metadata Manager, attribuez à un utilisateur le rôle administrateur pour un service Metadata Manager.

Administrateur Test Data

Dispose de l'ensemble des autorisations et des privilèges dans Test Data Manager. L'administrateur Test Data Manager peut se connecter à Test Data Manager pour créer des objets Test Data Manager et les gérer, ainsi que pour effectuer toutes les tâches dans le client d'application.

Pour créer un administrateur Test Data, attribuez à un utilisateur le rôle d'administrateur pour un service Test Data Manager.

Administrateur du client PowerCenter

Dispose de toutes les autorisations et de tous les privilèges sur tous les objets dans le client PowerCenter. L'administrateur du client PowerCenter peut se connecter au client PowerCenter pour gérer des objets du référentiel PowerCenter et effectuer toutes les tâches dans le client PowerCenter. L'administrateur du client PowerCenter peut aussi effectuer toutes les tâches dans les programmes de ligne de commande pmrep et pmcmd

Pour créer un administrateur du client PowerCenter, attribuez à un utilisateur le rôle administrateur pour un service de référentiel PowerCenter.

Utilisateur

Un utilisateur avec un compte dans le domaine Informatica peut effectuer des tâches dans les clients d'application.

Généralement, l'administrateur par défaut ou un administrateur de domaine crée et gère les comptes utilisateur et attribue les rôles, autorisations et privilèges dans le domaine Informatica. Cependant, les utilisateurs possédant les privilèges et autorisations de domaine nécessaires peuvent créer un compte utilisateur et attribuer les rôles, autorisations et privilèges.

Les utilisateurs peuvent effectuer des tâches dans les clients d'application Informatica en fonction des privilèges et autorisations qui leur sont attribués.

Gestion des utilisateurs

Vous pouvez créer, modifier et supprimer des utilisateurs dans le domaine de sécurité natif. Vous ne pouvez pas supprimer ou modifier les propriétés des comptes d'utilisateurs dans les domaines de sécurité LDAP. Vous ne pouvez pas modifier les attributions des utilisateurs pour les groupes LDAP.

Vous pouvez attribuer des rôles, des autorisations et des privilèges à un compte utilisateur dans le domaine de sécurité natif ou dans un domaine de sécurité LDAP. Les rôles, autorisations et privilèges attribués à l'utilisateur déterminent les tâches que l'utilisateur peut effectuer dans le domaine Informatica.

Vous pouvez également déverrouiller un compte utilisateur.

Création d'utilisateurs natifs

Ajoutez, modifiez ou supprimez des utilisateurs natifs dans l'onglet Sécurité.

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans le menu Actions de sécurité, cliquez sur Créer utilisateur.
3. Saisissez les informations suivantes pour l'utilisateur :

Propriété	Description
Nom de connexion	Nom de connexion du compte utilisateur. Le nom de connexion d'un compte utilisateur doit être unique dans le domaine de sécurité auquel il appartient. Le nom n'est pas sensible à la casse et ne doit pas dépasser 128 caractères. Il ne peut pas inclure de tabulation, de retour à la ligne, ni les caractères spéciaux suivants : , + " \ < > ; / * % ? & Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Tous les autres caractères d'espacement sont interdits.
Mot de passe	Mot de passe du compte utilisateur. Le mot de passe peut contenir entre 1 et 80 caractères.

Propriété	Description
Confirmer le mot de passe	Entrez une nouvelle fois le mot de passe pour le confirmer. Vous devez entrer une nouvelle fois le mot de passe. Ne faites pas de copier-coller du mot de passe.
Nom complet	Nom complet du compte utilisateur. Le nom complet ne peut pas inclure les caractères spéciaux suivants : < > "
Description	Description du compte utilisateur. La description ne peut pas dépasser 765 caractères, ni inclure les caractères spéciaux suivants : < > "
Courriel	Adresse de courriel de l'utilisateur. L'adresse de courriel ne peut pas inclure les caractères spéciaux suivants : < > " Entrez l'adresse de courriel au format UserName@Domain.
Téléphone	Numéro de téléphone de l'utilisateur. Le numéro de téléphone ne peut pas inclure les caractères spéciaux suivants : < > "

4. Cliquez sur OK pour enregistrer le compte utilisateur.

Après avoir créé le compte utilisateur, le panneau d'informations en affiche les propriétés, ainsi que les groupes auxquels l'utilisateur appartient.

Modification des propriétés générales d'utilisateurs natifs

Vous ne pouvez pas modifier le nom de connexion d'un utilisateur natif. Vous ne pouvez pas modifier le mot de passe et les autres informations d'un compte utilisateur natif.

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans la section Utilisateurs du navigateur, sélectionnez un compte utilisateur natif et cliquez sur Modifier.
3. Pour modifier le mot de passe, sélectionnez Changer le mot de passe.
L'onglet Sécurité efface les champs Mot de passe et Confirmer le mot de passe.
4. Entrez un nouveau mot de passe et confirmez.
5. Modifiez le nom complet, la description, l'adresse e-mail et le téléphone si nécessaire.
6. Cliquez sur OK pour enregistrer les modifications.

Assignation des utilisateurs natifs aux groupes natifs

Assignez des utilisateurs natifs aux groupes natifs dans l'onglet sécurité.

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans la section Utilisateurs du navigateur, sélectionnez un compte utilisateur natif et cliquez sur **Modifier**.
3. Cliquez sur l'onglet Groupes.

4. Pour attribuer un utilisateur natif à un groupe, sélectionnez un nom de groupe dans la colonne Tous les groupes, puis cliquez sur **Ajouter**.
Si des groupes imbriqués ne s'affichent pas dans la colonne Tous les groupes, développez chaque groupe pour les afficher.
Vous pouvez attribuer un utilisateur natif à plusieurs groupes. Utilisez les touches Ctrl ou Shift pour sélectionner plusieurs groupes en même temps.
5. Pour supprimer un utilisateur d'un groupe, sélectionnez un groupe dans la colonne Groupes attribués et cliquez sur **Supprimer**.
6. Cliquez sur **OK** pour enregistrer les attributions de groupe.

Assignation des utilisateurs LDAP aux groupes natifs

Vous pouvez assigner les comptes utilisateur LDAP aux groupes natifs. Vous ne pouvez pas modifier l'assignation des comptes utilisateur LDAP aux groupes LDAP.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Sécurité**.
2. Dans la section Groupes du navigateur, sélectionnez un groupe natif, puis cliquez sur **Modifier**.
3. Cliquez sur l'onglet **Utilisateurs**.
4. Pour attribuer un utilisateur LDAP à un groupe, sélectionnez un utilisateur LDAP dans la colonne Tous les utilisateurs, puis cliquez sur **Ajouter**.
5. Pour supprimer un utilisateur LDAP d'un groupe, sélectionnez un utilisateur LDAP dans la colonne Utilisateurs attribués, puis cliquez sur **Supprimer**.
6. Cliquez sur **OK** pour enregistrer les attributions d'utilisateur.

Activation et désactivation des comptes utilisateurs

Les utilisateurs ayant un compte actif peuvent se connecter à des clients d'application et effectuer des tâches en fonction de leurs autorisations et privilèges. Si vous ne voulez pas que les utilisateurs accèdent temporairement aux clients d'applications, vous pouvez désactiver leurs comptes. Vous pouvez activer ou désactiver les comptes d'utilisateurs dans un domaine de sécurité LDAP ou dans un domaine natif. Lorsque vous désactivez un compte utilisateur, ce dernier ne peut plus se connecter à des clients d'application.

Pour désactiver un compte utilisateur, sélectionnez un compte utilisateur dans la section Utilisateurs du navigateur, puis cliquez sur Désactiver. Lorsque vous sélectionnez un compte utilisateur désactivé, l'onglet Sécurité affiche un message indiquant que le compte est désactivé. Lorsqu'un compte utilisateur est désactivé, le bouton Activer est disponible. Pour activer un compte utilisateur, cliquez sur Activer.

Vous ne pouvez pas désactiver le compte administrateur par défaut.

Remarque: Lorsque le gestionnaire de service importe un compte utilisateur du service d'annuaire LDAP, il n'importe pas les attributs LDAP qui indiquent si le compte utilisateur est activé ou désactivé. Le gestionnaire de service importe tous les comptes d'utilisateurs comme étant des comptes activés. Vous devez désactiver un compte utilisateur LDAP dans l'outil Administrator si vous ne voulez pas que l'utilisateur accède aux clients d'application. Lors des synchronisations suivantes avec le serveur LDAP, le compte utilisateur conserve l'état actif ou inactif défini dans l'outil Administrator.

Suppression d'utilisateurs natifs

Pour supprimer un compte utilisateur natif, cliquez avec le bouton droit de la souris sur le nom de compte utilisateur dans la section Utilisateurs du navigateur, puis sélectionnez Supprimer l'utilisateur. Confirmez la suppression du compte utilisateur.

Vous ne pouvez pas supprimer le compte administrateur par défaut. Lorsque vous vous connectez à l'outil Administrator, vous ne pouvez pas supprimer votre compte utilisateur.

Suppression des utilisateurs de PowerCenter

Lorsque vous supprimez un utilisateur détenant des objets dans le référentiel PowerCenter, vous supprimez la propriété de l'utilisateur sur les dossiers, objets de connexion, groupes de déploiement, libellés ou requêtes. Après avoir supprimé un utilisateur, l'administrateur par défaut devient le propriétaire de tous les objets détenus par l'utilisateur supprimé.

Lorsque vous affichez l'historique d'un objet avec version précédemment détenu par un utilisateur supprimé, le nom de l'utilisateur supprimé s'affiche avec le préfixe « supprimé ».

Suppression des utilisateurs de Metadata Manager

Lorsque vous supprimez un utilisateur détenant des raccourcis et des dossiers, Metadata Manager déplace le dossier personnel de l'utilisateur vers un dossier nommé Utilisateurs supprimés détenu par l'administrateur par défaut. Le dossier personnel de l'utilisateur supprimé contient tous les raccourcis et dossiers créés par l'utilisateur. Tout dossier partagé reste partagé après que l'utilisateur a été supprimé.

Si le dossier Utilisateurs supprimés contient un dossier avec le même nom d'utilisateur, Metadata Manager nomme le dossier supplémentaire « Copie (n) de <nom d'utilisateur> ».

Utilisateurs LDAP

Vous ne pouvez pas ajouter, modifier ou supprimer des utilisateurs LDAP dans l'outil Administration. Vous devez gérer les comptes utilisateur LDAP dans le service d'annuaire LDAP.

Déverrouillage d'un compte utilisateur

L'administrateur de domaine peut déverrouiller un compte utilisateur qui est verrouillé hors du domaine. Si l'utilisateur est un utilisateur natif, l'administrateur peut lui demander de réinitialiser le mot de passe avant de se reconnecter au domaine.

L'utilisateur doit avoir une adresse électronique valide configurée dans le domaine pour recevoir les notifications lorsque son mot de passe de compte a été réinitialisé.

Si le compte de l'utilisateur est verrouillé dans le serveur d'authentification LDAP, l'administrateur LDAP doit le déverrouiller dans le serveur LDAP.

1. Dans l'outil Administrator, cliquez sur l'onglet **Sécurité**.
2. Cliquez sur **Gestion de comptes**.

La page Gestion des comptes affiche les listes d'utilisateurs dont le compte est verrouillé suivantes :

Utilisateurs natifs verrouillés

Inclut les comptes utilisateur du domaine de sécurité natif qui sont verrouillés.

Utilisateurs LDAP verrouillés

Inclut les comptes utilisateur des domaines de sécurité LDAP qui sont verrouillés.

3. Sélectionnez les utilisateurs que vous voulez déverrouiller.
4. Sélectionnez **Déverrouiller l'utilisateur et réinitialiser le mot de passe** afin de générer un nouveau mot de passe pour l'utilisateur après avoir déverrouillé le compte.
L'utilisateur reçoit le nouveau mot de passe par courrier électronique.
5. Cliquez sur **Déverrouiller les utilisateurs sélectionnés**.

Augmentation de la mémoire système pour un grand nombre d'utilisateurs

Le temps de traitement pour le redémarrage d'un domaine Informatica, pour la synchronisation des utilisateurs LDAP et pour certaines commandes infacmd et infasetup augmente proportionnellement au nombre d'utilisateurs du domaine Informatica.

Le nombre d'utilisateurs affecte le temps de traitement des commandes suivantes :

- infasetup BackupDomain, DeleteDomain et RestoreDomain
- infacmd isp ExportDomainObjects, ExportUsersandGroups, ImportDomainObjects et ImportUsersandGroups
- infacmd tools ExportObjects et ImportObjects

Vous aurez peut-être besoin d'augmenter la mémoire système utilisée par les services Informatica, infasetup et infacmd lorsque vous aurez un grand nombre d'utilisateurs dans le domaine. Pour augmenter la taille maximale du tas mémoire, configurez les variables d'environnement suivantes et spécifiez la valeur en mégaoctets :

- INFA_JAVA_OPTS. Détermine la taille maximale du tas mémoire utilisée par les services Informatica. Configurez cette variable pour chaque nœud sur lequel les services Informatica sont installés.
- ICMD_JAVA_OPTS. Détermine la taille maximale du tas mémoire utilisée par infacmd. Configurez cette variable pour chaque machine sur laquelle s'exécute infacmd.
- INFA_JAVA_CMD_OPTS. Détermine la taille maximale du tas mémoire utilisée par infasetup. Configurez cette variable pour chaque machine sur laquelle s'exécute infasetup.

Par exemple, pour configurer 2 048 Mo de mémoire système sur UNIX pour la variable d'environnement INFA_JAVA_OPTS, utilisez la commande suivante :

```
setenv INFA_JAVA_OPTS "-Xmx2048m"
```

Sous Windows, configurez les variables en tant que variables système.

Le tableau suivant décrit la configuration minimale requise pour les paramètres de taille maximum du tas, selon le nombre d'utilisateurs et de services dans le domaine :

Nombre d'utilisateurs du domaine	Taille maximum du tas (1-5 Services)	Taille maximum du tas (6-10 Services)
1000 maximum	512 Mo (par défaut)	1024 Mo
5 000	2048 Mo	3072 Mo
10 000	3072 Mo	5120 Mo
20 000	5120 Mo	6144 Mo
30 000	5120 Mo	6144 Mo

Remarque: Les paramètres de taille maximale du tas mémoire dans le tableau sont basés sur le nombre de services d'application dans le domaine.

Après avoir configuré ces variables d'environnement, redémarrez le nœud pour que les changements soient pris en compte.

Affichage de l'activité utilisateur

Utilisez l'onglet Journaux de l'outil Administrator tool pour afficher les journaux d'activité utilisateur. Affichez les journaux d'activité utilisateur pour vérifier les tentatives d'ouverture de session des applications clientes Informatica. Vous pouvez également afficher les journaux pour déterminer quand un utilisateur a créé, mis à jour ou supprimé des services, des nœuds, des utilisateurs, des groupes ou des rôles.

Consultez le *Guide de l'administrateur Informatica* pour plus d'informations sur les journaux d'activité utilisateur et l'onglet Journaux de l'outil Administrator tool.

Vous pouvez également utiliser la commande `infacmd isp getUserActivityLog` pour afficher les données des journaux d'activité utilisateur. La commande `infacmd isp getUserActivityLog` utilise la syntaxe suivante :

```
infacmd isp getUserActivityLog -dn domain_name -un user_name -pd password
```

La commande `infacmd isp getUserActivityLog` requiert le rôle administrateur ou l'appartenance au groupe administrateur. Pour plus d'informations sur la commande `isp getUserActivityLog`, consultez la *Référence des commandes Informatica*.

Les données des journaux d'activité utilisateur incluent les tentatives d'ouverture de session réussies et non réussies des clients d'Informatica. Si le client définit des propriétés personnalisées sur les demandes de connexion, les données du journal incluent les propriétés personnalisées.

Remarque: Les journaux d'activité utilisateur n'incluent pas les tentatives d'ouverture de session dans un domaine configuré pour utiliser l'authentification Kerberos.

Les données d'activité utilisateur incluent les propriétés suivantes pour chaque tentative d'ouverture de session d'un client Informatica :

- Nom de l'application
- Version de l'application
- Nom d'hôte ou adresse IP de l'hôte d'application

Vous pouvez afficher les événements du journal en fonction des filtres facultatifs suivants :

- Nom d'utilisateur
- Domaine de sécurité
- Date et heure
- Ordre chronologique
- Code d'activité
- Texte d'activité

Vous pouvez afficher les événements du journal à l'invite de commandes ou écrire les événements dans un fichier dans l'un des formats suivants :

- Binaire
- Texte
- XML

Si vous imprimez un journal au format binaire, vous pouvez le convertir au format texte ou XML à l'aide de la commande `infacmd isp convertUserActivityLog`. Pour plus d'informations sur l'utilisation de la commande `infacmd isp convertUserActivityLog`, consultez la *Référence des commandes Informatica*.

Codes d'activité utilisateur

Les journaux d'activité utilisateur incluent des codes qui indiquent la réussite ou l'échec de chaque activité.

Les codes d'activité valides sont les suivants :

- CCM_10437. Indique la réussite d'une activité.
- CCM_10438. Indique l'échec d'une activité.
- CCM_10778. Indique qu'une tentative de connexion avec des propriétés personnalisées a réussi.
- CCM_10779. Indique qu'une tentative de connexion avec des propriétés personnalisées a échoué.
- CCM_10786. Indique qu'une tentative de connexion sans propriétés personnalisées a réussi.
- CCM_10787. Indique qu'une tentative de connexion sans propriétés personnalisées a échoué.

Filtres des journaux d'activité utilisateur

Utilisez un ou plusieurs filtres pour récupérer des événements du journal pour des utilisateurs, des dates ou des événements spécifiques.

Utilisez un ou plusieurs des paramètres suivants pour la commande `infacmd isp getUserActivityLog` pour filtrer les événements du journal :

Utilisateurs et domaines de sécurité

Facultatif. Liste des utilisateurs pour lesquels vous souhaitez obtenir les événements du journal. Séparez plusieurs utilisateurs par un espace. Utilisez le symbole de caractère générique (*) pour afficher les journaux de plusieurs utilisateurs sur tous les domaines de sécurité ou un seul d'entre eux. Par exemple, les chaînes suivantes sont les valeurs valides pour cette option :

```
user:Native
"user:*"
"user*"
"*_users_*"
"*:Native"
```

Ajoutez le paramètre suivant à la commande `getUserActivityLog` pour filtrer les événements du journal en fonction de l'utilisateur ou du domaine de sécurité :

```
-usrs <UserName>:<SecurityDomain>
```

Par exemple, ajoutez le paramètre suivant pour récupérer l'activité utilisateur pour un utilisateur nommé User1 sur tous les domaines de sécurité :

```
-usrs "User1:*
```

Date et heure

Facultatif. Plage de dates pour laquelle vous voulez afficher les événements du journal.

Si vous entrez une date de fin qui est antérieure à la date de début, la commande ne renvoie aucun événement du journal.

Entrez la date et l'heure dans l'un des formats suivants :

- MM/jj/aaaa
- MM/jj/aaaa HH:mm:ss
- aaaa-MM-jj
- aaaa-MM-jj HH:mm:ss

Ajoutez le paramètre suivant à la commande `getUserActivityLog` pour filtrer le journal par date de début ou date de fin :

```
-sd <start_date> -ed <end_date>
```

Par exemple, ajoutez le paramètre suivant pour récupérer l'activité utilisateur entre le 1er janvier 2014 et le 3 février 2014 :

```
-sd 01/01/2014 -ed 02/03/2014
```

Code d'activité

Facultatif. Renvoie les événements du journal en fonction du code d'activité.

Utilisez le symbole de caractère générique (*) pour récupérer les événements du journal pour plusieurs codes d'activité. Les codes d'activité valides sont notamment les suivants :

- CCM_10437. Indique la réussite d'une activité.
- CCM_10438. Indique l'échec d'une activité.
- CCM_10778. Indique qu'une tentative de connexion avec des propriétés personnalisées a réussi.
- CCM_10779. Indique qu'une tentative de connexion avec des propriétés personnalisées a échoué.
- CCM_10786. Indique qu'une tentative de connexion sans propriétés personnalisées a réussi.
- CCM_10787. Indique qu'une tentative de connexion sans propriétés personnalisées a échoué.

Ajoutez le paramètre suivant à la commande getUserActivityLog pour filtrer par code d'activité :

```
-ac <activity_code>
```

Par exemple, ajoutez le paramètre suivant pour récupérer les événements du journal qui se sont correctement déroulés :

```
-ac CCM_10437
```

Si vous utilisez le symbole de caractère générique, placez l'argument entre guillemets.

Texte d'activité

Facultatif. Renvoie les événements du journal en fonction d'une chaîne trouvée dans le texte d'activité.

Ajoutez le paramètre suivant à la commande getUserActivityLog pour filtrer par texte d'activité :

```
-atxt <activity_text>
```

Utilisez le symbole de caractère générique (*) pour récupérer les journaux liés à plusieurs événements. Par exemple, le paramètre suivant renvoie tous les événements du journal qui contiennent « Activation du service » dans leur description :

```
-atxt "**Enabling service**"
```

Si vous utilisez le symbole de caractère générique, placez l'argument entre guillemets.

Ordre chronologique

Facultatif. Imprime les événements du journal dans l'ordre chronologique inverse. Si vous ne spécifiez pas ce paramètre, la commande affiche les événements du journal dans l'ordre chronologique.

Ajoutez le paramètre suivant à la commande getUserActivityLog pour imprimer d'abord l'événement le plus récent :

```
-ro true
```

Écriture et affichage des événements du journal d'activité utilisateur

Vous pouvez écrire les événements du journal d'activité utilisateur dans un fichier ou les afficher sur la ligne de commande lorsque vous utilisez la commande infacmd isp getUserActivityLog. Écrivez les événements du

journal d'activité utilisateur dans le format adapté à l'utilisation prévue du fichier d'événements du journal exporté.

Écriture et affichage des fichiers journaux

Pour écrire les événements du journal d'activité utilisateur dans un fichier, exécutez la commande avec le paramètre de fichier de sortie `-lo` :

```
-lo output_file_name
```

Si vous ne spécifiez pas de format de sortie, la commande écrit les événements du journal dans un fichier texte. Par exemple, exécutez la commande suivante pour écrire les événements du journal dans un fichier nommé `log.txt` :

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -lo log.txt
```

Pour spécifier un format de sortie, exécutez la commande avec le paramètre de format `-fm` :

```
-fm output_format_BIN_TEXT_XML
```

Les formats valides sont les suivants :

- **Bin (binaire).** Utilisez le format binaire pour sauvegarder les événements du journal dans ce format. Ce format peut être utile pour envoyer les événements du journal au service clientèle international d'Informatica.
- **Texte.** Utilisez le format texte si vous voulez analyser les événements du journal dans un éditeur de texte.
- **XML.** Utilisez le format XML si vous voulez analyser les événements du journal dans un outil externe qui utilise le format XML ou si vous souhaitez utiliser des outils XML tels que XSLT.

Si vous spécifiez le format texte ou XML comme format de sortie, mais sans indiquer de fichier de sortie, la commande affiche le journal au format texte ou XML sur la ligne de commande.

Si vous spécifiez le format binaire comme format de sortie, vous devez indiquer un nom de fichier de sortie.

Par exemple, exécutez la commande suivante pour imprimer les événements du journal dans un fichier nommé `log.xml` :

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -fm xml -lo log.xml
```

Conversion de fichiers journaux

Si vous utilisez la commande `getUserActivity` pour écrire des événements du journal dans un fichier binaire, vous pouvez convertir le fichier au format texte ou XML.

Exécutez la commande suivante pour convertir au format texte ou XML un journal binaire récupéré :

```
infacmd isp convertUserActivityLogFile -in BIN_input_file_name -fm output_format_TEXT_XML -lo output_file_name
```

Par exemple, exécutez la commande suivante pour convertir un fichier d'entrée binaire nommé `log.bin` au format XML et obtenir un fichier de sortie nommé `convertedlog.xml` :

```
infacmd isp convertUserActivityLogFile -in log.bin -fm XML -lo convertedLog.xml
```

Pour afficher le journal sur la ligne de commande, omettez le nom du fichier de sortie.

Si vous omettez le format, la commande utilise le format texte.

Gestion des groupes

Vous pouvez créer, modifier et supprimer des groupes dans le domaine de sécurité natif.

Vous pouvez attribuer des rôles, autorisations et privilèges à un groupe dans le domaine de sécurité natif ou LDAP. Vous ne pouvez pas supprimer ou modifier les propriétés des comptes de groupe dans les domaines de sécurité LDAP. Les rôles, autorisations et privilèges attribués au groupe déterminent les tâches que les utilisateurs du groupe peuvent effectuer dans le domaine.

Ajout d'un groupe natif

Ajouter, modifier ou supprimer des groupes natifs dans l'onglet Sécurité.

Un groupe natif peut contenir des comptes d'utilisateurs natifs ou LDAP, ou d'autres groupes natifs. Il est possible de créer plusieurs niveaux de groupes natifs. Par exemple, le groupe Finance contient le groupe AccountsPayable qui contient le groupe OfficeSupplies. Le groupe Finance est le groupe parent du groupe AccountsPayable, et le groupe AccountsPayable est le groupe parent du groupe OfficeSupplies. Chaque groupe peut contenir d'autres groupes natifs.

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans le menu Actions de sécurité, cliquez sur Créer groupe.
3. Saisissez les informations suivantes pour le groupe :

Propriété	Description
Nom	Nom du groupe. Le nom n'est pas sensible à la casse et ne doit pas dépasser 128 caractères. Les tabulations, retours à la ligne et caractères spéciaux suivants ne sont pas admis : , + " \ < > ; / * % ? Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Tous les autres caractères d'espacement sont interdits.
Groupe parent	Groupe auquel le nouveau groupe appartient. Si vous sélectionnez un groupe natif avant de cliquer sur Créer groupe, le groupe sélectionné devient le groupe du parent. Sinon, le champ Groupe parent affiche Natif, ce qui indique que le nouveau groupe n'appartient pas à un autre groupe.
Description	Description du groupe. La description du groupe ne peut pas excéder 765 caractères ou inclure les caractères spéciaux suivants : < > "

4. Cliquez sur Parcourir pour sélectionner un autre groupe parent.
Vous pouvez créer plusieurs niveaux de groupes et de sous-groupes.
5. Cliquez sur OK pour enregistrer le groupe.

Modification des propriétés d'un groupe natif

Après avoir créé un groupe, vous pouvez modifier sa description et la liste des utilisateurs du groupe. Vous ne pouvez pas modifier le nom du groupe ou le parent du groupe. Pour modifier le parent du groupe, vous devez déplacer le groupe vers un autre groupe.

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans la section Groupes du navigateur, sélectionnez un groupe natif et cliquez sur Modifier.

3. Modifiez la description du groupe.
4. Pour modifier la liste des utilisateurs du groupe, cliquez sur l'onglet Utilisateurs.
L'onglet Utilisateurs affiche la liste des utilisateurs du domaine et la liste des utilisateurs assignés au groupe.
5. Pour attribuer des utilisateurs au groupe, sélectionnez un compte utilisateur dans la colonne Tous les utilisateurs et cliquez sur Ajouter.
6. Pour supprimer un utilisateur d'un groupe, sélectionnez un compte utilisateur dans la colonne Utilisateurs assignés et cliquez sur Supprimer.
7. Cliquez sur OK pour enregistrer les modifications.

Déplacement d'un groupe natif vers un autre groupe natif

Pour organiser les groupes d'utilisateurs dans le domaine de sécurité natif, vous pouvez configurer des groupes imbriqués et déplacer un groupe vers un autre groupe.

Pour déplacer un groupe natif vers un autre groupe natif, cliquez avec le bouton droit de la souris sur le nom d'un groupe natif dans la section Groupes du navigateur, puis sélectionnez Déplacer un groupe.

Suppression d'un groupe natif

Pour supprimer un groupe natif, cliquez avec le bouton droit de la souris sur le nom du groupe dans la section Groupes du navigateur et sélectionnez Supprimer le groupe.

Lorsque vous supprimez un groupe, les utilisateurs du groupe perdent leur appartenance au groupe et toutes les autorisations ou privilèges hérités du groupe.

Lorsque vous supprimez un groupe, le gestionnaire de service supprime tous les groupes et sous-groupes appartenant au groupe.

Groupes LDAP

Vous ne pouvez pas ajouter, modifier ou supprimer des groupes LDAP ou modifier les attributions d'utilisateur des groupes LDAP dans l'outil Administration. Vous devez gérer les groupes et attributions d'utilisateur dans le service d'annuaire LDAP.

Gestion des profils de systèmes d'exploitation

Créez et gérez des profils de système d'exploitation sous l'onglet Sécurité de l'outil Administrator tool ou depuis la ligne de commande. Vous pouvez créer, modifier et supprimer des profils de système d'exploitation. Vous pouvez attribuer le profil de système d'exploitation par défaut aux utilisateurs et aux groupes ou le modifier.

Si le service d'intégration de données est configuré pour utiliser des profils de système d'exploitation, il exécute des mappages, des profils et des flux de travail avec ce profil. Si le service d'intégration PowerCenter est configuré pour utiliser des profils de système d'exploitation, il exécute des mappages, des profils et des flux de travail avec ce profil.

Créez, modifiez et supprimez des profils de système d'exploitation dans la vue **Profils de système d'exploitation** de l'onglet **Sécurité**.

Procédez comme suit pour créer un profil de système d'exploitation :

1. Entrez un nom pour le profil de système d'exploitation et un nom d'utilisateur système.
2. Sélectionnez les services d'intégration et configurez les propriétés du profil de système d'exploitation.
3. Vous pouvez éventuellement attribuer des autorisations sur le profil de système d'exploitation.

Vous pouvez attribuer des utilisateurs et des groupes aux profils de système d'exploitation et attribuer un profil par défaut aux utilisateurs et aux groupes après l'avoir créé.

Propriétés du profil de système d'exploitation du service d'intégration PowerCenter

Les variables de processus de service qui sont définies dans les propriétés de session et les fichiers de paramètres remplacent les paramètres des profils de système d'exploitation.

Le tableau suivant décrit les propriétés du profil de système d'exploitation du service d'intégration PowerCenter :

Propriété	Description
Nom	Nom en lecture seule du profil de système d'exploitation. Le nom ne peut pas dépasser 128 caractères. Il ne peut pas inclure d'espaces ni les caractères spéciaux suivants : \ / : * ? " < > [] = + ; ,
Nom d'utilisateur système	Nom en lecture seule d'un utilisateur de système d'exploitation qui existe sur les machines sur lesquelles le service d'intégration PowerCenter est exécuté. Le service d'intégration PowerCenter exécute les flux de travail à l'aide de l'accès système de l'utilisateur système défini pour le profil de système d'exploitation.
\$PMRootDir	Répertoire racine auquel le nœud peut accéder. Il s'agit du répertoire racine d'autres variables de processus de service. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " ,
\$PMSessionLogDir	Répertoire des journaux de sessions. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/SessLogs.
\$PMBadFileDir	Répertoire des fichiers de rejet. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/BadFiles.
\$PMCacheDir	Répertoire des fichiers d'index et de cache de données. Vous pouvez augmenter les performances lorsque le répertoire de cache est un lecteur local du processus de service d'intégration PowerCenter. N'utilisez pas de lecteur mappé ou monté pour les fichiers de cache. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/Cache.
\$PMTargetFileDir	Répertoire des fichiers cibles. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/TgtFiles.

Propriété	Description
\$PMSourceFileDir	Répertoire des fichiers sources. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/SrcFiles.
\$PmExtProcDir	Répertoire des procédures externes. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/ExtProc.
\$PMTempDir	Répertoire des fichiers temporaires. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/Temp.
\$PMLookupFileDir	Répertoire des fichiers de recherche. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/LkpFiles.
\$PMStorageDir	Répertoire des fichiers d'exécution. Les fichiers de récupération de flux de travail sont enregistrés dans le répertoire \$PMStorageDir configuré dans les propriétés du service d'intégration PowerCenter. Les fichiers de récupération de session sont enregistrés dans le répertoire \$PMStorageDir configuré dans le profil de système d'exploitation. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/Storage.
Variables d'environnement	Nom et valeur des variables d'environnement utilisées par le service d'intégration lors de l'exécution. Si vous indiquez la variable d'environnement LD_LIBRARY_PATH dans les propriétés du profil de système d'exploitation, le service d'intégration ajoute la valeur de cette variable à sa variable d'environnement LD_LIBRARY_PATH. Le service d'intégration utilise la valeur de sa variable d'environnement LD_LIBRARY_PATH pour définir les variables d'environnement des processus enfants générés pour le profil de système d'exploitation. Si vous n'indiquez pas la variable d'environnement LD_LIBRARY_PATH dans les propriétés du profil de système d'exploitation, le service d'intégration utilise sa variable d'environnement LD_LIBRARY_PATH.

Propriétés du profil de système d'exploitation du service d'intégration de données

Le tableau suivant décrit les propriétés du profil de système d'exploitation du service d'intégration de données :

Propriété	Description
Nom	Nom en lecture seule du profil de système d'exploitation. Le nom ne peut pas dépasser 128 caractères. Il ne peut pas inclure d'espaces ou les caractères spéciaux suivants : % * + \ / ? ; < >
Nom d'utilisateur système	Nom en lecture seule d'un utilisateur du système d'exploitation qui existe sur les machines sur lesquelles le service d'intégration PowerCenter est exécuté. Le service d'intégration de données exécute des mappages, des flux de travail et des tâches de profilage à l'aide de l'accès système de l'utilisateur du système d'exploitation.
\$DISRootDir	Répertoire racine auquel le nœud peut accéder. Il s'agit du répertoire racine d'autres variables de processus de service. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , []
\$DISTempDir	Répertoire des fichiers temporaires créés lors de l'exécution des tâches. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/disTemp. Remarque: Si le service d'intégration de données est configuré de manière à utiliser plusieurs profils de système d'exploitation, spécifiez un répertoire commun pour tous les profils, car un répertoire distinct pour chaque profil entraîne une utilisation excessive de l'espace disque.
\$DISCacheDir	Répertoire des fichiers d'index et de cache de données des transformations. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/cache.
\$DISSourceDir	Répertoire des fichiers plats sources utilisés dans un mappage. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/source.
\$DISTargetDir	Répertoire des fichiers plats cibles utilisés dans un mappage. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/cible.
\$DISRejectedFilesDir	Répertoire des fichiers de rejet. Les fichiers de rejet contiennent des lignes qui ont été rejetées lors de l'exécution d'un mappage. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/rejet.
\$DISLogDir	Répertoire des journaux. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , [] La valeur par défaut est <répertoire racine>/disLogs.

Propriété	Description
Activer les propriétés d'emprunt d'identité Hadoop	<p>Indique que le service d'intégration de données emploie l'utilisateur identifié en tant qu'utilisateur Hadoop pour exécuter des mappages, des flux de travail et des tâches de profilage dans un environnement Hadoop.</p> <p>L'utilisateur identifié en tant qu'utilisateur Hadoop par défaut est l'utilisateur connecté. Pour spécifier un autre utilisateur identifié en tant qu'utilisateur Hadoop, sélectionnez Utiliser l'utilisateur spécifié en tant qu'utilisateur Hadoop identifié et entrez un nom d'utilisateur.</p>
Variables d'environnement	<p>Nom et valeur des variables d'environnement utilisées par le service d'intégration lors de l'exécution.</p> <p>Si vous indiquez la variable d'environnement LD_LIBRARY_PATH dans les propriétés du profil de système d'exploitation, le service d'intégration ajoute la valeur de cette variable à sa variable d'environnement LD_LIBRARY_PATH. Le service d'intégration utilise la valeur de sa variable d'environnement LD_LIBRARY_PATH pour définir les variables d'environnement des processus enfants générés pour le profil de système d'exploitation.</p> <p>Si vous n'indiquez pas la variable d'environnement LD_LIBRARY_PATH dans les propriétés du profil de système d'exploitation, le service d'intégration utilise sa variable d'environnement LD_LIBRARY_PATH.</p> <p>Remarque: Sous AIX, vous devez définir la variable d'environnement LD_LIBRARY_PATH sur INFA_HOME/services/shared/bin pour que le service d'intégration de données puisse exécuter correctement les mappages, les profils et les flux de travail sur les profils de système d'exploitation.</p>
Répertoire de cache de fichier plat	<p>Répertoire de cache de fichier plat dans lequel l'outil Analyst tool stocke les fichiers plats chargés.</p> <p>Si le service Analyst se connecte à un service d'intégration de données qui utilise les profils de système d'exploitation, l'utilisateur du système d'exploitation spécifié dans le profil de système d'exploitation doit avoir accès à ce répertoire de cache de fichier plat. Lorsque vous importez une source de table de référence ou de fichier plat, l'outil Analyst utilise les fichiers de ce répertoire pour créer un objet de données de table de référence ou de fichier plat. Redémarrez le service Analyst si vous modifiez l'emplacement du fichier plat.</p>

Propriétés du profil de système d'exploitation du service d'accès aux métadonnées

Le tableau suivant décrit les propriétés du profil de système d'exploitation du service d'accès aux métadonnées :

Propriété	Description
Nom	Nom en lecture seule du profil de système d'exploitation. Le nom ne peut pas dépasser 128 caractères. Il ne peut pas inclure d'espaces ou les caractères spéciaux suivants : % * + \ / ? ; < >
Nom d'utilisateur système	Nom en lecture seule d'un utilisateur du système d'exploitation qui existe sur les machines sur lesquelles le service d'accès aux métadonnées est exécuté. Le service d'accès aux métadonnées permet à l'outil Developer d'accéder aux informations de connexion Hadoop pour importer et prévisualiser les métadonnées à l'aide de l'accès système de l'utilisateur du système d'exploitation.
Activer les propriétés d'emprunt d'identité Hadoop	Indique que le service d'accès aux métadonnées utilise l'utilisateur identifié en tant qu'utilisateur Hadoop pour importer et prévisualiser les métadonnées. L'utilisateur identifié en tant qu'utilisateur Hadoop par défaut est l'utilisateur connecté. Pour spécifier un autre utilisateur identifié en tant qu'utilisateur Hadoop, sélectionnez Utiliser l'utilisateur spécifié en tant qu'utilisateur Hadoop identifié et entrez un nom d'utilisateur.

Création d'un profil de système d'exploitation

Créez un profil de système d'exploitation et attribuez-le aux utilisateurs et aux groupes afin d'améliorer la sécurité et d'isoler l'environnement d'exécution de l'utilisateur. Vous pouvez créer un ou plusieurs profils de système d'exploitation. Le service d'intégration PowerCenter utilise le profil de système d'exploitation pour exécuter des flux de travail. Le service d'intégration de données utilise le profil de système d'exploitation pour exécuter des mappages, des profils et des flux de travail. Le service d'accès aux métadonnées utilise le profil du système d'exploitation pour accéder aux informations de connexion Hadoop et importer et prévisualiser les métadonnées.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Sécurité**.
2. Dans le menu Actions de sécurité, cliquez sur **Créer un profil de système d'exploitation**.

La boîte de dialogue **Créer un profil de système d'exploitation - Étape 1 sur 3** s'affiche.

3. Entrez les propriétés générales suivantes pour le profil de système d'exploitation :

Propriété	Description
Nom	Nom du profil de système d'exploitation. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Il ne peut pas dépasser 128 caractères ni commencer par @. Il ne peut pas non plus contenir les caractères spéciaux suivants : % * + \ / ? ; < > Le nom peut inclure des espaces ASCII, sauf en première et en dernière position. Tous les autres caractères d'espacement sont interdits.
Nom d'utilisateur système	Nom d'un utilisateur du système d'exploitation qui existe sur les machines sur lesquelles le service d'intégration s'exécute. Le service d'intégration exécute les flux de travail à l'aide de l'accès système de l'utilisateur système défini pour le profil de système d'exploitation. Remarque: Lorsque vous créez des profils de système d'exploitation, vous ne pouvez pas spécifier le nom d'utilisateur du système comme racine ou utiliser un utilisateur non racine dont l'uid==0.

4. Cliquez sur **Suivant**.

La boîte de dialogue **Configurer le profil de système d'exploitation - Étape 2 sur 3** s'affiche.

5. Sélectionnez le service qui utilisera le profil du système d'exploitation.
- Service d'intégration PowerCenter
 - Service d'intégration de données
 - Service d'accès aux métadonnées
6. Configurez les propriétés du profil du système d'exploitation des services sélectionnés. Pour créer un profil de système d'exploitation pour le service d'accès aux métadonnées, vous devez également sélectionner Service d'intégration des données avec Service d'accès aux métadonnées et spécifier la variable \$DISRootDir pour le service d'intégration des données.
7. Si les services accèdent à un environnement Hadoop au moment de la conception ou de l'exécution, configurez les propriétés d'imitation Hadoop comme suit :
- a. Sélectionnez **Activer les propriétés d'emprunt d'identité Hadoop**.
 - b. Employez l'utilisateur connecté ou spécifiez un utilisateur identifié en tant qu'utilisateur Hadoop pour exécuter les tâches Hadoop.
8. Vous pouvez éventuellement configurer les variables d'environnement.
9. Si le service Analyst se connecte à un service d'intégration de données qui utilise les profils de système d'exploitation, configurez les propriétés du service Analyst.
10. Cliquez sur **Suivant**.
- La boîte de dialogue **Attribuer des groupes et des utilisateurs au profil de système d'exploitation - Étape 3 sur 3** s'affiche.
11. Dans l'onglet **Groupes**, attribuez des groupes au profil de système d'exploitation comme suit :
- a. Pour attribuer des groupes spécifiques au profil de système d'exploitation, sélectionnez un ou plusieurs groupes et cliquez sur **Ajouter**.
 - b. Pour attribuer tous les groupes disponibles au profil de système d'exploitation, cliquez sur **Ajouter tout**.
12. Vous pouvez éventuellement attribuer le profil de système d'exploitation en tant que profil par défaut à un ou plusieurs groupes. Pour attribuer un profil par défaut, définissez le groupe de la liste Groupe(s) sélectionné(s) sur **Profil par défaut**.

13. Dans l'onglet **Utilisateurs**, attribuez des utilisateurs au profil de système d'exploitation comme suit :
 - a. Pour attribuer des utilisateurs spécifiques au profil de système d'exploitation, sélectionnez un ou plusieurs utilisateurs et cliquez sur **Ajouter**.
 - b. Pour attribuer tous les utilisateurs disponibles au profil de système d'exploitation, cliquez sur **Ajouter tout**.
14. Vous pouvez éventuellement attribuer le profil de système d'exploitation en tant que profil par défaut à un ou plusieurs utilisateurs. Pour attribuer un profil par défaut, définissez l'utilisateur de la liste Utilisateur(s) sélectionné(s) sur **Profil par défaut**.
15. Cliquez sur **Terminer**.

Après avoir créé le profil de système d'exploitation, le panneau d'informations en affiche les propriétés ainsi que les groupes et les utilisateurs auxquels le profil est attribué.

Modification d'un profil de système d'exploitation

Vous pouvez modifier un profil de système d'exploitation pour en changer les propriétés.

Vous ne pouvez pas modifier le nom ou le nom de l'utilisateur système après avoir créé un profil de système d'exploitation. Si vous ne voulez pas employer l'utilisateur du système d'exploitation spécifié dans le profil de ce dernier, supprimez-le.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Sécurité**.
2. Sélectionnez la vue **Profils de système d'exploitation**.
3. Sélectionnez le profil de système d'exploitation.
4. Dans l'onglet **Propriétés**, cliquez sur **Modifier**.

La boîte de dialogue **Modifier les propriétés** s'affiche.
5. Sélectionnez le service d'intégration des données, le service d'intégration PowerCenter ou le service d'accès aux métadonnées que vous souhaitez configurer.
6. Modifiez les propriétés du service.
7. Cliquez sur **OK**.

Attribution d'un profil de système d'exploitation par défaut à un utilisateur ou à un groupe

Lorsqu'un utilisateur ou un groupe a accès à plusieurs profils de système d'exploitation, attribuez un profil de système d'exploitation par défaut utilisé par le service d'intégration pour exécuter des tâches et des flux de travail. Vous pouvez attribuer à un utilisateur ou à un groupe un profil de système d'exploitation avec autorisations directes comme profil par défaut. Un utilisateur ou un groupe ne peut avoir qu'un seul profil de système d'exploitation par défaut. Cependant, vous pouvez attribuer le même profil de système d'exploitation que le profil par défaut à plusieurs utilisateurs ou à plusieurs groupes.

1. Dans l'onglet **Sécurité**, sélectionnez la vue **Utilisateurs** ou **Groupes**.
2. Dans le navigateur, sélectionnez l'utilisateur ou le groupe.
3. Dans le panneau de contenu, cliquez sur la vue **Autorisations**.
4. Cliquez sur l'onglet **Profils de systèmes d'exploitation**.
5. Cliquez sur le bouton **Attribuer ou modifier le profil de système d'exploitation par défaut**.

La boîte de dialogue **Attribuer ou modifier le profil de système d'exploitation par défaut** s'affiche.

6. Sélectionnez un profil dans la liste **Profil de système d'exploitation par défaut** ou sélectionnez **Ne pas assigner un profil de système d'exploitation par défaut** dans la liste pour supprimer le profil par défaut affecté à un utilisateur ou un groupe.

7. Cliquez sur **OK**.

Dans le panneau d'informations, la colonne **Profil par défaut** correspondant au profil de système d'exploitation indique **Oui (direct)**.

Suppression d'un profil de système d'exploitation

Pour supprimer un profil de système d'exploitation, cliquez avec le bouton droit de la souris sur le nom du profil dans la section Profil de système d'exploitation du navigateur et sélectionnez **Supprimer un profil**.

Après avoir supprimé un profil de système d'exploitation, attribuez-en un autre aux utilisateurs et aux groupes auxquels le profil de système d'exploitation était attribué en tant que profil par défaut. Si le service d'intégration PowerCenter utilise les profils de système d'exploitation, attribuez un autre aux dossiers du référentiel et aux flux de travail auxquels le profil de système d'exploitation était attribué.

Utilisation des profils du système d'exploitation dans un domaine sécurisé

Vous pouvez utiliser les profils du système d'exploitation dans un domaine Informatica sur lequel la communication sécurisée est activée.

Tenez compte des règles et directives suivantes lorsque vous utilisez les profils du système d'exploitation dans un domaine sur lequel la communication sécurisée est activée :

- Vous devez définir la variable d'environnement suivante pour le profil du système d'exploitation :

INFA_TRUSTSTORE

Définissez la valeur sur le répertoire qui contient les fichiers truststore pour les certificats SSL pour le domaine sécurisé. Le répertoire doit contenir un fichier truststore nommé infa_truststore.pem.

INFA_TRUSTSTORE_PASSWORD

Si vous utilisez un fichier truststore personnalisé, définissez la valeur du mot de passe infa_truststore.pem qui contient le certificat SSL pour le domaine sécurisé. Le mot de passe doit être crypté. Utilisez le programme de ligne de commande pmpasswd pour crypter le mot de passe.

- Par ailleurs, si le service d'intégration PowerCenter utilise l'option Session ou Grille, vous devez définir les variables d'environnement suivantes du profil du système d'exploitation :

INFA_KEYSTORE

Définissez la valeur sur le répertoire qui contient les fichiers entrepôt de clés pour les certificats SSL du domaine sécurisé. Le répertoire doit contenir un fichier entrepôt de clés nommé infa_keystore.pem.

Vous pouvez définir les variables d'environnement pour le profil du système d'exploitation dans l'outil Administrator. Pour définir les variables d'environnement du profil du système d'exploitation, cliquez sur **Sécurité > Profils de système d'exploitation**. Modifiez les propriétés du profil de système d'exploitation et définissez les variables d'environnement.

Utilisation des profils du système d'exploitation dans un domaine avec l'authentification Kerberos

Vous pouvez utiliser les profils du système d'exploitation dans un domaine Informatica qui s'exécute sur un réseau avec l'authentification Kerberos.

Tenez compte des règles et directives suivantes lorsque vous utilisez les profils du système d'exploitation dans un domaine qui s'exécute sur un réseau avec l'authentification Kerberos :

- Le compte d'utilisateur du profil du système d'exploitation doit être un principal dans le service Active Directory utilisé pour l'authentification Kerberos et importé dans un domaine de sécurité LDAP dans le domaine Informatica.
- Le compte d'utilisateur doit disposer d'un fichier cache de justificatifs d'identité Kerberos accessible au compte d'utilisateur du profil du système d'exploitation. Chaque compte d'utilisateur du profil du système d'exploitation doit disposer d'un fichier cache de justificatifs d'identité séparé.
- Le fichier cache de justificatifs d'identité pour le compte d'utilisateur du profil du système d'exploitation doit être transférable. Par exemple, si vous utilisez l'utilitaire *kinit* pour créer le fichier cache de justificatifs d'identité, vous devez inclure l'option *-f*.
- Le fichier cache de justificatifs d'identité pour le compte d'utilisateur du profil du système d'exploitation doit être disponible lorsque vous exécutez un flux de travail qui utilise un profil de système d'exploitation.
- Le fichier cache de justificatifs d'identité pour le compte d'utilisateur du profil du système d'exploitation doit toujours disposer des derniers justificatifs d'identité. Vous pouvez exécuter un utilitaire planificateur de tâches, tel que *cron*, pour effectuer régulièrement la mise à jour les justificatifs d'identité de l'utilisateur dans le fichier cache de justificatifs d'identité.
- Vous devez définir les variables d'environnement suivantes pour le profil du système d'exploitation :

INFA_OSPI_SECURITY_DOMAIN

Définissez la valeur sur le nom du domaine de sécurité qui contient le compte d'utilisateur pour le profil du système d'exploitation. Si le compte d'utilisateur est dans le domaine de sécurité de la zone de l'utilisateur pour Kerberos, vous n'avez pas besoin de définir cette variable. Le domaine de sécurité de la zone de l'utilisateur pour Kerberos est le domaine de sécurité créé lors de l'installation qui a le même nom que la zone de l'utilisateur Kerberos.

KRB5_CONFIG

Définissez la valeur pour le chemin et le nom du fichier de configuration Kerberos. Le nom du fichier de configuration Kerberos est *krb5.conf*.

KRB5CCNAME

Définissez la valeur pour le chemin et le nom du fichier cache de justificatifs d'identité Kerberos pour le compte d'utilisateur du profil du système d'exploitation.

Vous pouvez définir les variables d'environnement pour le profil du système d'exploitation dans l'outil Administrator. Pour définir les variables d'environnement du profil du système d'exploitation, cliquez sur **Sécurité > Profils de système d'exploitation**. Modifiez les propriétés du profil de système d'exploitation et définissez les variables d'environnement.

Verrouillage de compte

Pour améliorer la sécurité dans le domaine Informatica, un administrateur peut appliquer le verrouillage de comptes utilisateur du domaine, y compris les comptes d'autres administrateurs, après plusieurs échecs de connexion.

L'administrateur peut spécifier le nombre autorisé d'échecs de tentative de connexion d'un utilisateur avant le verrouillage de son compte. Si un compte est verrouillé, l'administrateur peut le déverrouiller dans le domaine Informatica.

Lorsque l'administrateur déverrouille un compte utilisateur, il peut sélectionner l'option « Déverrouiller l'utilisateur et réinitialiser le mot de passe » pour réinitialiser le mot de passe de l'utilisateur. L'administrateur peut envoyer un courriel à l'utilisateur pour lui demander de changer le mot de passe avant de se reconnecter au domaine. Pour activer le domaine afin d'envoyer des courriers électroniques aux utilisateurs lorsque leur mot de passe est réinitialisé, configurez les paramètres du serveur de messagerie pour le domaine.

Si le compte de l'utilisateur est verrouillé dans le domaine Informatica et dans le serveur LDAP, l'administrateur Informatica peut le déverrouiller depuis le domaine Informatica. L'utilisateur ne peut pas se connecter au domaine Informatica tant que l'administrateur LDAP n'a pas également déverrouillé son compte dans le serveur LDAP.

Remarque: Si le domaine Informatica utilise l'authentification réseau Kerberos, vous ne pouvez pas configurer le verrouillage de comptes utilisateur. La vue **Gestion des comptes** n'est pas disponible dans l'onglet **Sécurité** de l'outil Administrator.

Configuration du verrouillage de compte

Sélectionnez les options de verrouillage de compte pour verrouiller des comptes utilisateur dans le domaine Informatica après plusieurs échecs de connexion.

1. Dans l'outil Administrator, cliquez sur **Sécurité > Gestion des comptes**.
2. Dans la section **Configuration du verrouillage de compte**, cliquez sur **Modifier**.
3. Définissez les propriétés suivantes :

Propriété	Description
Activer le verrouillage de compte	Applique le verrouillage de compte utilisateur du domaine Informatica après un nombre d'échecs de connexion spécifié. Par défaut, cette option n'applique pas le verrouillage des comptes d'administrateurs. Vous devez sélectionner l'option Activer le verrouillage du compte d'administration pour appliquer le verrouillage des comptes d'administrateurs.
Activer le verrouillage du compte d'administration	Applique le verrouillage d'un compte d'administrateur du domaine Informatica après un nombre d'échecs de connexion spécifié. Vous devez sélectionner l'option Activer le verrouillage de compte pour pouvoir appliquer le verrouillage de comptes d'administrateurs.
Nombre maximum de tentatives de connexion	Spécifie le nombre maximal d'échecs de connexion consécutifs autorisés avant le verrouillage d'un compte utilisateur du domaine Informatica.

Règles et directives de verrouillage de compte

Tenez compte des règles et directives suivantes lorsque vous appliquez le verrouillage de compte aux utilisateurs d'Informatica :

- Si un service d'application fonctionne sous un compte d'utilisateur et qu'un mot de passe incorrect est fourni pour ce service, le compte d'utilisateur peut être verrouillé lorsque le service d'applications tente de démarrer. Le service d'intégration de données, le service Hub de services Web et le service d'intégration PowerCenter sont résilients des services d'application qui utilisent un nom d'utilisateur et un mot de passe pour s'authentifier auprès du service de référentiel modèle ou du service de référentiel PowerCenter. Si le service d'intégration de données, le service Hub de services Web ou le service d'intégration PowerCenter tente en permanence de redémarrer après un échec de connexion, le domaine verrouille le compte utilisateur associé.
- Si un compte utilisateur LDAP est verrouillé dans le domaine Informatica et le serveur d'authentification LDAP, l'administrateur de domaine Informatica peut le déverrouiller dans le domaine Informatica. L'administrateur LDAP peut déverrouiller le compte utilisateur dans le serveur LDAP.
- Si vous activez le verrouillage de compte dans le domaine Informatica et dans le serveur LDAP, configurez le même seuil pour les échecs de connexion dans le domaine Informatica et le serveur LDAP pour éviter toute confusion concernant la stratégie de verrouillage de compte.
- Si le verrouillage de compte n'est pas activé dans le domaine Informatica mais que le compte d'un utilisateur est verrouillé, vérifiez qu'il ne l'est pas dans le serveur LDAP.

CHAPITRE 9

Privilèges et rôles

Ce chapitre comprend les rubriques suivantes :

- [Privilèges, 145](#)
- [Rôles, 147](#)
- [Privilèges du domaine, 147](#)
- [Privilèges du service Analyst, 155](#)
- [Privilèges du service de gestion de contenu, 156](#)
- [Privilèges du service d'intégration de données, 157](#)
- [Privilège du service d'ingestion de masse, 157](#)
- [Privilèges du Metadata Manager Service, 158](#)
- [Privilèges du service de référentiel modèle, 161](#)
- [Privilèges du PowerCenter Repository Service, 163](#)
- [Privilèges du service d'écoute PowerExchange, 177](#)
- [Privilèges du service de journalisation PowerExchange, 177](#)
- [Privilèges du service de planificateur, 178](#)
- [Privilèges du service Test Data Manager, 179](#)
- [Gestion des rôles, 183](#)
- [Attribution de privilèges et de rôles aux utilisateurs et aux groupes, 186](#)
- [Affichage des utilisateurs avec des privilèges pour un service, 188](#)
- [Dépannage des problèmes de privilèges et de rôles, 188](#)

Privilèges

Les privilèges déterminent les actions que les utilisateurs peuvent effectuer dans les clients de l'application. Informatica inclut les privilèges suivants :

- Privilèges du domaine. Déterminent les actions que les utilisateurs peuvent effectuer sur le domaine Informatica à l'aide de l'outil Administrator tool et des programmes de ligne de commande infacmd et pmrep.
- Privilège du service Analyst. Détermine les actions que l'utilisateur peut effectuer à l'aide d'Informatica Analyst.
- Privilège du service de gestion de contenu. Détermine les actions que les utilisateurs peuvent effectuer à l'aide de tables de référence dans les outils Informatica Developer tool et Informatica Analyst tool.

- Privilège du service d'intégration de données. Déterminent les actions dans les applications que l'utilisateur peut effectuer à l'aide de l'outil Administrator tool et du programme de ligne de commande infacmd. Ce privilège détermine également si les utilisateurs peuvent développer et exporter les résultats du profil.
- Privilège du service d'ingestion de masse. Détermine les actions que les utilisateurs peuvent effectuer à l'aide de l'outil Ingestion de masse.
- Privilèges du service Metadata Manager. Déterminent les actions que l'utilisateur peut effectuer à l'aide de Metadata Manager.
- Privilège du service de référentiel modèle. Détermine les actions dans les projets que l'utilisateur peut effectuer à l'aide d'Informatica Analyst et d'Informatica Developer.
- Privilèges du service de référentiel PowerCenter. Déterminent les actions du référentiel PowerCenter que l'utilisateur peut effectuer à l'aide du Repository Manager, du Concepteur, du gestionnaire de workflow, du moniteur de workflow et des programmes de ligne de commande pmrep et pmcmd.
- Privilèges du service d'application PowerExchange. Déterminent les actions que l'utilisateur peut effectuer dans le service d'écoute PowerExchange et dans le service de journalisation PowerExchange à l'aide des commandes infacmd pwx.
- Privilèges du service de planificateur. Déterminent les actions que les utilisateurs peuvent effectuer à l'aide du service de planificateur.
- Privilèges du service Test Data Manager. Déterminent les tâches de découverte de données, de masquage des données, de sous-ensemble de données et de Test Data Generation que les utilisateurs peuvent effectuer à l'aide de Test Data Manager.

Vous assignez des privilèges aux utilisateurs et groupes pour les services d'application. Vous pouvez assigner des privilèges différents à un utilisateur pour chaque service d'application du même type de service.

Vous attribuez des privilèges aux utilisateurs et aux groupes dans l'**onglet Sécurité** de l'outil Administrator tool.

L'outil Administrator tool organise les privilèges en niveaux. Un privilège est indiqué au-dessous de celui qu'il inclut. Certains privilèges en incluent d'autres. Lorsque vous assignez un privilège à des utilisateurs et des groupes, l'outil Administrator tool assigne également les privilèges inclus.

Groupes de privilèges

Les privilèges de service d'application et de domaine sont organisés en groupes de privilèges. Un groupe de privilèges est une organisation de privilèges qui définissent les actions classiques des utilisateurs. Par exemple, les privilèges du domaine incluent les groupes de privilèges suivants :

- Outils. Inclut les privilèges de connexion à l'outil Administrator.
- Administration de la sécurité. Inclut les privilèges de gestion des utilisateurs, groupes, rôles et privilèges.
- Administration de domaine. Inclut les privilèges de gestion du domaine, des dossiers, nœuds, grilles, licences et services d'application.

Astuce: Lorsque vous attribuez des privilèges aux utilisateurs et groupes d'utilisateurs, vous pouvez sélectionner un groupe de privilèges pour attribuer tous les privilèges du groupe.

Rôles

Un rôle est un regroupement de privilèges que vous attribuez à un utilisateur ou un groupe. Chaque utilisateur au sein d'une organisation a un rôle spécifique, qu'il soit développeur, administrateur, utilisateur de base ou utilisateur avancé.

Par exemple, le rôle Développeur de PowerCenter comprend tous les privilèges du service de référentiel PowerCenter ou actions qu'un développeur effectue.

Vous attribuez un rôle à des utilisateurs et des groupes pour le domaine et les services d'application du domaine.

Astuce: Si vous organisez des utilisateurs en groupes puis attribuez des rôles et des autorisations aux groupes, vous pouvez simplifier les tâches d'administration des utilisateurs. Par exemple, si un utilisateur change de poste au sein d'une organisation, déplacez-le vers un autre groupe. Si un nouvel utilisateur rejoint l'organisation, ajoutez l'utilisateur à un groupe. L'utilisateur hérite des rôles et des autorisations attribués au groupe. Vous n'avez pas besoin de réattribuer des privilèges, de rôles et de autorisations. Pour plus d'informations, consultez l'article suivant de la Bibliothèque de procédures Informatica

<https://kb.informatica.com/h2l/HowTo%20Library/1/0236-GroupsAndRolesToManageAccessControl.pdf>.

Privilèges du domaine

Les privilèges du domaine déterminent les actions que les utilisateurs peuvent effectuer à l'aide de l'outil Administrator tool et des programmes de ligne de commande infacmd et pmrep.

Le tableau suivant décrit chaque groupe de privilèges du domaine :

Groupe de privilèges	Description
Administration de la sécurité	Inclut les privilèges de gestion des utilisateurs, groupes, rôles et privilèges.
Administration de domaine	Inclut des privilèges pour gérer le domaine, les dossiers, les nœuds, les grilles, les licences, les services d'application, les connexions et les configurations de grappe.
Surveillance	Inclut les privilèges de configuration des statistiques et des rapports de surveillance, d'affichage de la surveillance des objets d'intégration et d'accès à la surveillance.
Outils	Inclut les privilèges de connexion à l'outil Administrator tool.
Administration Cloud	Inclut les privilèges permettant d'ajouter des organisations Informatica Cloud dans l'outil Administrator tool et les afficher.

Groupe de privilèges Administration de la sécurité

Les privilèges du groupe de privilèges Administration de la sécurité et les autorisations d'objet de domaine déterminent les actions de gestion de la sécurité que les utilisateurs peuvent effectuer.

Certaines tâches de gestion de la sécurité sont déterminées par le rôle Administrateur, et non pas par les privilèges ni par les autorisations. Un utilisateur auquel est attribué le rôle Administrateur sur le domaine peut effectuer les tâches suivantes :

- Créez, modifiez et supprimez des profils de système d'exploitation.
- Accordez une autorisation sur des profils de système d'exploitation.

Remarque: Pour réaliser des tâches de gestion de la sécurité dans l'outil Administrator, les utilisateurs doivent également posséder le privilège Accès à Informatica Administrator.

Privilège Attribuer les privilèges et les rôles

Les utilisateurs auxquels est attribué le rôle Attribuer les privilèges et les rôles peuvent assigner des privilèges et les rôles aux utilisateurs et aux groupes.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Attribuer les privilèges et les rôles :

Autorisation pour	Description
Domaine ou service d'application	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Accorder des privilèges et des rôles aux utilisateurs et groupes pour le domaine ou service d'application.- Modifier et supprimer les privilèges et rôles assignés aux utilisateurs et aux groupes.

Privilège Gérer les utilisateurs, les groupes et les rôles

Les utilisateurs possédant le privilège Gérer les utilisateurs, les groupes et les rôles peuvent configurer une authentification LDAP et gérer les utilisateurs, groupes et rôles.

Le privilège Gérer les utilisateurs, les groupes et les rôles inclut le privilège Attribuer les privilèges et les rôles.

Le tableau suivant répertorie les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Gérer les utilisateurs, les groupes et les rôles :

Autorisation pour	Description
-	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Configurer l'authentification LDAP pour le domaine.- Créer, modifier et supprimer des utilisateurs, des groupes et des rôles.- Importer des utilisateurs et groupes LDAP.
Profil du système d'exploitation	L'utilisateur peut modifier les propriétés de profil du système d'exploitation.

Groupe de privilèges Administration de domaine

Les actions de gestion de domaine que les utilisateurs peuvent effectuer dépendent des privilèges du groupe Administration de domaine et des autorisations sur les objets de domaine.

Certaines tâches de gestion de domaine sont déterminées par le rôle Administrateur et non pas par les privilèges ni par les autorisations. Un utilisateur auquel est assigné le rôle Administrateur sur le domaine peut effectuer les tâches suivantes :

- Configurer les propriétés du domaine.

- Configurer les configurations de grappe.
- Accorder des autorisations sur le domaine.
- Gérer et purger des événements de journaux.
- Recevoir des alertes de domaine.
- Exécuter le rapport de licence.
- Afficher les événements du journal d'activité utilisateur.
- Arrêter le domaine.
- Accéder à l'assistant de mise à niveau de service.

Les utilisateurs auxquels sont attribuées les autorisations d'objet de domaine, mais pas les privilèges, peuvent effectuer certaines tâches de gestion de domaine. Le tableau suivant répertorie les actions que les utilisateurs peuvent effectuer lorsque seules les autorisations d'objet de domaine leur sont assignées :

Autorisation pour	Description
Domaine	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Afficher les propriétés de domaine et les événements du journal. - Configurer les paramètres de surveillance.
Dossier	L'utilisateur peut afficher les propriétés de dossier.
Service d'application	L'utilisateur peut afficher les propriétés du service d'application et les événements du journal.
Objet de licence	L'utilisateur peut afficher les propriétés de l'objet de licence.
Grille	L'utilisateur peut afficher les propriétés de la grille.
Nœud	L'utilisateur peut afficher les propriétés du nœud.
Hub des services Web	L'utilisateur peut exécuter le rapport de services Web.

Remarque: Pour réaliser des tâches de gestion de domaine dans l'outil Administrator tool, les utilisateurs doivent également posséder le privilège Accès à Informatica Administrator.

Privilège Gérer l'exécution des services

Les utilisateurs possédant le privilège Gérer l'exécution des services peuvent activer et désactiver les services d'application et recevoir les alertes de service d'application.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Gérer l'exécution des services :

Autorisation pour	Description
Service d'application	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Activer et désactiver les services d'application et les processus de service. Pour activer et désactiver un service du gestionnaire de métadonnées, les utilisateurs doivent également avoir l'autorisation sur le service d'intégration PowerCenter et le service de référentiel PowerCenter associés. - Recevoir les alertes de service d'application.

Privlège Gérer les services

Les utilisateurs possédant le privilège Gérer les services peuvent créer, configurer, déplacer, supprimer et accorder des autorisations pour les services d'application et les objets de licence.

Le privilège Gérer les services comprend le privilège Gérer l'exécution des services.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Gérer les services :

Autorisation pour	Description
Domaine ou dossier parent	L'utilisateur peut créer des objets de licence.
Domaine ou dossier parent, nœud ou grille d'exécution du service d'application, objet de licence et tout service d'application associé	L'utilisateur peut créer des services d'application.
Service d'application	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Configurer des services d'application.- Accorder l'autorisation pour les services d'application.
Dossiers d'origine et de destination	L'utilisateur peut déplacer des services d'application ou des objets de licence d'un dossier vers un autre.
Domaine ou dossier parent et service d'application	L'utilisateur peut supprimer des services d'application.
Service Analyst	L'utilisateur peut créer et supprimer des tables de suivi d'audit.
Service Metadata Manager	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Sauvegarder le contenu du référentiel Metadata Manager.- Supprimer le contenu du référentiel Metadata Manager.- Mettre à niveau le contenu du service Metadata Manager. Remarque: Pour créer ou restaurer le contenu du référentiel Metadata Manager, l'utilisateur doit faire partie du groupe Administrateur par défaut.
Service Metadata Manager Service de référentiel PowerCenter	L'utilisateur peut restaurer le référentiel PowerCenter pour Metadata Manager.
Service de référentiel modèle	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Créer et supprimer le contenu du référentiel modèle.- Créer, supprimer et réindexer l'index de la recherche.- Mettre à niveau le contenu du service de référentiel modèle à partir du menu Actions ou de la ligne de commande. L'utilisateur doit également disposer des privilèges Créer, Modifier et Supprimer sur le service de référentiel modèle et de l'autorisation d'écriture sur les projets.
Service d'intégration PowerCenter	L'utilisateur peut exécuter le service d'intégration PowerCenter en mode sécurisé.

Autorisation pour	Description
Service de référentiel PowerCenter	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Sauvegarder, restaurer et mettre à niveau le référentiel PowerCenter. - Configurer le lignage de données pour le référentiel PowerCenter. - Copier le contenu d'un autre référentiel PowerCenter. - Fermer les connexions utilisateurs et déverrouiller les verrous du référentiel PowerCenter. - Créer et supprimer le contenu du référentiel PowerCenter. - Créer, modifier et supprimer les extensions de métadonnées réutilisables dans PowerCenter Repository Manager. - Activer le contrôle de version pour le référentiel PowerCenter. - Gérer un domaine du référentiel PowerCenter. - Effectuer une purge avancée des versions d'objets au niveau du référentiel dans PowerCenter Repository Manager. - Inscrire et désinscrire les plug-ins du référentiel PowerCenter. - Exécuter le référentiel PowerCenter en mode exclusif. - Envoyer les notifications du référentiel PowerCenter aux utilisateurs. - Mettre à jour les statistiques du référentiel PowerCenter. - Mettre à niveau le contenu du service de référentiel PowerCenter.
Service Test Data Manager	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Créez et supprimez le contenu du référentiel Test Data Manager. - Mettez à niveau le contenu du service Test Data Manager.
Objet de licence	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Modifier des objets de licence. - Accorder l'autorisation pour les objets de licence.
Objet de licence et service d'application	L'utilisateur peut attribuer une licence à un service d'application.
Domaine ou dossier parent et objet de licence	L'utilisateur peut supprimer des objets de licence.

Privilège Gérer les nœuds et les grilles

Les utilisateurs possédant le privilège Gérer les nœuds et les grilles peuvent créer, configurer, déplacer, supprimer, arrêter et accorder des autorisations sur les nœuds et les grilles.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Gérer les nœuds et les grilles :

Autorisation pour	Description
Domaine ou dossier parent	L'utilisateur peut créer des nœuds.
Domaine ou dossier parent et nœuds assignés à la grille	L'utilisateur peut créer des grilles.
Nœud ou grille	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Configurer et arrêter des nœuds et des grilles. - Accorder des autorisations sur les nœuds et grilles.

Autorisation pour	Description
Dossiers d'origine et de destination	L'utilisateur peut déplacer les nœuds et les grilles d'un dossier vers un autre.
Domaine ou dossier parent et nœud ou grille	L'utilisateur peut retirer les nœuds et les grilles.

Privilège Gérer les dossiers de domaine

Les utilisateurs possédant le privilège Gérer les dossiers de domaine peuvent créer, modifier, supprimer et accorder des autorisations sur les dossiers de domaine.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Gérer les dossiers de domaine :

Autorisation pour	Description
Domaine ou dossier parent	L'utilisateur peut créer des dossiers.
Dossier	L'utilisateur peut effectuer les actions suivantes : - Modifier des dossiers. - Accorder des autorisations sur les dossiers.
Dossiers d'origine et de destination	L'utilisateur peut déplacer des dossiers depuis un dossier parent vers un autre.
Domaine ou dossier parent et dossier en cours de suppression	L'utilisateur peut retirer des dossiers.

Privilège Gérer les connexions

L'utilisateur ayant le privilège Gérer les connexions peut créer, modifier et supprimer des connexions dans l'outil Administrator, l'outil Analyst, l'outil Developer et le programme de ligne de commande infacmd. Les utilisateurs peuvent également copier les connexions dans l'outil Developer et attribuer des autorisations sur des connexions dans l'outil Administrator et le programme de ligne de commande infacmd.

Les utilisateurs disposant du privilège Gérer les connexions peuvent également créer, actualiser et supprimer des configurations de grappe et définir et effacer des propriétés de configuration dans l'outil Administrator tool et le programme de ligne de commande infacmd.

L'utilisateur ayant les autorisations de connexion mais pas le privilège Gérer les connexions peut effectuer les actions de gestion des connexions suivantes :

- Afficher toutes les métadonnées de connexion, à l'exception des mots de passe. Exige l'autorisation de lecture pour la connexion.
- Prévisualiser les données ou exécuter un mappage, une fiche d'évaluation ou un profil. Exige l'autorisation d'exécution pour la connexion.

Le tableau suivant présente les autorisations requises et les actions que l'utilisateur peut effectuer avec le privilège Gérer les connexions :

Autorisation	Description
-	L'utilisateur peut créer des connexions et des configurations de grappe.
Écrire sur la connexion	L'utilisateur est capable de copier, modifier et supprimer des connexions.
Accorder sur connexion	L'utilisateur peut attribuer et révoquer les autorisations sur les connexions.
Écrire dans la configuration de grappe	L'utilisateur peut créer, actualiser et supprimer des configurations de grappe. L'utilisateur peut définir et effacer des propriétés de configuration de grappe.

Groupe de privilèges Surveillance

Les privilèges du groupe de privilèges Surveillance déterminent quels utilisateurs peuvent afficher et configurer la surveillance.

Le tableau suivant répertorie les autorisations requises et les actions que l'utilisateur peut effectuer avec les privilèges du groupe Gérer la surveillance :

Privilège parent	Privilège	Autorisation pour	Description
Gérer la surveillance	Configuration de surveillance	Domaine	L'utilisateur peut configurer les paramètres de surveillance.
Gérer la surveillance	Paramètres Rapport et Statistiques	Domaine	L'utilisateur peut configurer les statistiques et les rapports de surveillance.
Afficher	Afficher les tâches de tous les utilisateurs dans les groupes auxquels l'utilisateur appartient	Domaine	Un utilisateur d'un groupe peut surveiller les tâches exécutées par d'autres utilisateurs du groupe. Si l'utilisateur appartient à plusieurs groupes, il peut voir les tâches de tous les groupes.
Afficher les tâches de tous les utilisateurs dans les groupes auxquels l'utilisateur appartient	Afficher les tâches d'autres utilisateurs	Domaine	L'utilisateur peut afficher les tâches d'autres utilisateurs.
Afficher	Afficher les statistiques	Domaine	L'utilisateur peut afficher la vue Résumé des statistiques ainsi que les statistiques des objets de domaine. Remarque: Dans un domaine qui utilise l'authentification Kerberos, les utilisateurs doivent également avoir le rôle Administrateur pour le service de référentiel modèle de surveillance afin d'afficher la vue Résumé des statistiques ainsi que les statistiques des objets de domaine.

Privilège parent	Privilège	Autorisation pour	Description
Afficher	Afficher les rapports	Domaine	L'utilisateur peut afficher des rapports des objets de domaine.
Accéder à la surveillance	Accéder à partir de l'outil Analyst tool	Domaine	L'utilisateur peut accéder à l'espace de travail État de la tâche de l'outil Analyst tool.
Accéder à la surveillance	Accéder à partir de l'outil Developer tool	Domaine	L'utilisateur peut accéder à l'outil Monitoring tool depuis l'outil Developer tool.
Accéder à la surveillance	Accéder à partir de l'outil Administrator tool	Domaine	L'utilisateur peut accéder à l'onglet Surveiller de l'outil Administrator tool.
s.o.	Exécuter des actions sur des tâches	Domaine	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Abandonner les tâches. - Réexécuter les tâches de mappage. - Afficher les journaux des tâches.

Les utilisateurs n'ont pas besoin du privilège Accès à Informatica Administrator pour accéder à l'outil Monitoring tool.

Groupe de privilèges Outils

Le privilège du groupe Outils du domaine détermine les utilisateurs pouvant accéder à l'outil Administrator.

Le tableau suivant répertorie les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège dans le groupe Outils :

Privilège	Description
Accès à Informatica Administrator	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Se connecter à l'outil Administrator. - Gérer leur compte utilisateur dans l'outil Administrator. - Exporter les événements du journal.

Les utilisateurs doivent avoir le privilège Accès à Informatica Administrator pour effectuer les tâches dans l'outil Administrator tool. Les utilisateurs n'ont pas besoin du privilège Accès à Informatica Administrator pour exécuter les commandes infacmd ou accéder à l'outil Monitoring tool.

Groupe de privilèges d'administration Cloud

Les privilèges du groupe Administration Cloud déterminent les utilisateurs qui peuvent afficher et configurer les organisations Informatica Cloud.

Le tableau suivant répertorie les autorisations requises et les actions que les utilisateurs peuvent effectuer avec les privilèges du groupe d'administration Cloud :

Privilège	Autorisation pour	Description
Afficher l'organisation	Domaine	L'utilisateur peut afficher les organisations Informatica Cloud ainsi que les agents sécurisés et les connexions Cloud associés.
Gérer l'organisation	Domaine	L'utilisateur peut ajouter des organisations Informatica Cloud dans l'outil Administrator.

Privilèges du service Analyst

Le privilège du service Analyst détermine les actions que les utilisateurs sous licence peuvent effectuer sur les projets à l'aide de l'outil Analyst.

Le tableau suivant répertorie les privilèges et autorisations requis pour gérer les projets et les objets des projets :

Privilège	Autorisation	Description
Exécuter les profils et les fiches d'évaluation	Lire les projets. Exécuter sur la connexion de la source de données relationnelle.	L'utilisateur peut exécuter des profils et des fiches d'évaluation pour des utilisateurs sous licence dans l'outil Analyst tool.
Accéder aux spécifications de mappage	Lire les projets.	L'utilisateur peut accéder aux spécifications de mappage pour les utilisateurs sous licence dans l'outil Analyst tool.
Charger les résultats de spécification de mappage	Écrire dans les projets.	L'utilisateur peut charger les résultats d'une spécification de mappage pour des utilisateurs sous licence dans une table ou un fichier plat. Remarque: Sélectionnez ce privilège pour accorder également le privilège Accéder aux spécifications de mappage par défaut.
Gérer des glossaires	-	L'utilisateur peut gérer Business Glossary.
Afficher les glossaires	-	L'utilisateur peut afficher les ressources de Business Glossary dans l'espace de travail Bibliothèque. Ceci revient à fournir une autorisation d'accès en lecture pour les glossaires et les ressources du glossaire dans l'espace de travail Sécurité du glossaire.

Privilège	Autorisation	Description
Accès à l'espace de travail	-	L'utilisateur peut accéder aux espaces de travail suivants dans l'outil Analyst tool : - Espace de travail . - Espace de travail Découverte . - Espace de travail Glossaire . - Espace de travail Fiches d'évaluation . Remarque: Sélectionnez ce privilège pour accorder également l'accès aux projets dans l'outil Analyst. Si l'utilisateur ne dispose pas de ce privilège, il doit posséder le privilège Espace de travail Conception , Espace de travail Découverte , Espace de travail Glossaire ou Espace de travail Fiches d'évaluation pour accéder aux projets.
Espace de travail Conception	-	L'utilisateur peut accéder à l'espace de travail Conception .
Espace de travail Découverte	-	L'utilisateur peut accéder à l'espace de travail Découverte .
Espace de travail Glossaire	-	L'utilisateur peut accéder à l'espace de travail Glossaire .
Espace de travail Fiches d'évaluation	-	L'utilisateur peut accéder à l'espace de travail Fiches d'évaluation .

Privilèges du service de gestion de contenu

Les privilèges du service de gestion de contenu déterminent les actions que les utilisateurs sous licence peuvent effectuer sur les tables de référence.

Le tableau suivant répertorie les privilèges et les autorisations requises pour gérer les tables de référence :

Privilège	Autorisation	Description
Créer des tables de référence	Accès en écriture sur le projet	<ul style="list-style-type: none"> - Créer une table de référence dans les outils Analyst et Developer. - Créer une table de référence avec la commande d'importation infacmd rtm. - Importer un objet de table de référence de l'objet pour le référentiel modèle. - Copier une table de référence dans les outils Analyst et Developer. - Créer une table de référence à partir des données de profil. Remarque: Le privilège de création accorde également par défaut le privilège de modification.
Modifier les données et les métadonnées de la table de référence	Accès en lecture sur le projet	<ul style="list-style-type: none"> - Modifier les valeurs de la table de référence dans les outils Analyst et Developer. - Ajouter des données de profil à une table de référence. - Ajouter ou supprimer les colonnes d'une table de référence. Modifier les métadonnées de la table de référence, comme les noms de colonne, les descriptions et les valeurs par défaut.

Privilèges du service d'intégration de données

Les privilèges du service d'intégration de données déterminent les actions que les utilisateurs peuvent effectuer sur les applications à l'aide de l'outil Administrator et du programme de ligne de commande infacmd. Ils déterminent également si les utilisateurs peuvent explorer et exporter les résultats de profil à l'aide des outils Analyst et Developer.

Le tableau suivant répertorie les actions que les utilisateurs peuvent effectuer avec le privilège du groupe de privilèges Administration des applications :

Nom du privilège	Description
Gérer les applications	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Sauvegarder et restaurer une application dans un fichier.- Déployer une application sur un service d'intégration de données et résoudre les conflits de nom.- Démarrer une application après son déploiement.- Rechercher une application.- Vous pouvez démarrer ou arrêter des objets dans une application.- Configurer les propriétés d'application.

Le tableau suivant répertorie les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège du groupe de privilèges Administration des profilages :

Nom du privilège	Autorisation pour	Description
Explorer et exporter les résultats	Lire le projet L'exécution sur la connexion de la source de données relationnelles est également requise pour explorer les données en direct.	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Explorer les résultats de profilage.- Exporter les résultats de profilage.

Privilège du service d'ingestion de masse

Le privilège du service d'ingestion de masse détermine les actions que les utilisateurs peuvent effectuer à l'aide de l'outil Ingestion de masse.

Le tableau suivant décrit les actions que les utilisateurs peuvent effectuer avec le privilège du service d'ingestion de masse :

Privilège	Description
Accès à la spécification d'ingestion de masse	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Parcourir toutes les spécifications d'ingestion de masse- Modifier une spécification d'ingestion de masse- Exécuter une spécification d'ingestion de masse- Supprimer une spécification d'ingestion de masse

Remarque: Un utilisateur qui ne reçoit pas le privilège d'accès à la spécification d'ingestion de masse ou le rôle Administrateur sur le domaine peut effectuer ces actions uniquement dans les spécifications d'ingestion de masse que l'utilisateur crée lui-même.

Privilèges du Metadata Manager Service

Les privilèges du Metadata Manager Service déterminent les actions Metadata Manager que les utilisateurs peuvent effectuer à l'aide de Metadata Manager.

Le tableau suivant décrit chaque groupe de privilèges du Metadata Manager Service :

Groupe de privilèges	Description
Catalogue	Inclut les privilèges permettant de gérer les objets dans la page Parcourir de l'interface Metadata Manager.
Chargement	Inclut les privilèges permettant de gérer les objets dans la page Chargement de l'interface Metadata Manager.
Modèle	Inclut les privilèges permettant de gérer les objets dans la page Modèle de l'interface Metadata Manager.
Sécurité	Inclut les privilèges permettant de gérer les objets dans la page Sécurité de l'interface Metadata Manager.

Groupe de privilèges Catalogue

Les privilèges du groupe de privilèges Catalogue déterminent les tâches que les utilisateurs peuvent effectuer sur l'onglet **Parcourir** de l'application Metadata Manager. Un utilisateur disposant du privilège nécessaire pour effectuer une action a également besoin d'autorisations pour exécuter cette action sur un objet spécifique. Configurez les autorisations dans l'onglet **Sécurité** de l'application Metadata Manager.

Le tableau suivant contient la liste des privilèges du groupe de privilèges Catalogue, ainsi que les autorisations requises pour effectuer des tâches sur un objet :

Privilège	Inclut les privilèges	Autorisation	Description
Partager des raccourcis	S. O.	Écrire	L'utilisateur peut partager un dossier contenant un raccourci avec d'autres utilisateurs et d'autres groupes.
Afficher le lignage	S. O.	Lire	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Exécuter une analyse de lignage de données sur des objets de métadonnées, des catégories et des termes d'entreprise.- Exécuter une analyse de lignage à partir du concepteur PowerCenter. Les utilisateurs doivent également avoir l'autorisation en écriture sur le dossier du référentiel PowerCenter.
Afficher les catalogues associés	S. O.	Lire	L'utilisateur peut afficher les catalogues associés.
Afficher les résultats de profil	S. O.	Lire	L'utilisateur peut afficher les informations de profilage pour des objets de métadonnées dans le catalogue depuis une source relationnelle.

Privilège	Inclut les privilèges	Autorisation	Description
Afficher le catalogue	S. O.	Lire	L'utilisateur peut effectuer les actions suivantes : - Afficher les ressources et les objets de métadonnées dans le catalogue de métadonnées. - Rechercher dans le catalogue de métadonnées.
Afficher les relations	S. O.	Lire	L'utilisateur peut afficher les relations pour des objets de métadonnées, des catégories et des termes d'entreprise.
Gérer les relations	Afficher les relations	Écrire	L'utilisateur peut créer, modifier et supprimer des relations pour des objets de métadonnées personnalisés, des catégories et des termes d'entreprise.
Afficher les commentaires	S. O.	Lire	L'utilisateur peut afficher les commentaires pour des objets de métadonnées, des catégories et des termes d'entreprise.
Publier des commentaires	Afficher les commentaires	Écrire	L'utilisateur peut ajouter les commentaires pour des objets de métadonnées, des catégories et des termes d'entreprise.
Supprimer les commentaires	- Publier des commentaires - Afficher les commentaires	Écrire	L'utilisateur peut supprimer des commentaires pour des objets de métadonnées, des catégories et des termes d'entreprise.
Afficher les liens	S. O.	Lire	L'utilisateur peut afficher les liens pour des objets de métadonnées, des catégories et des termes d'entreprise.
Gérer les liens	Afficher les liens	Écrire	L'utilisateur peut créer, modifier et supprimer des liens pour des objets de métadonnées, des catégories et des termes d'entreprise.
Afficher le glossaire	S. O.	Lire	L'utilisateur peut effectuer les actions suivantes : - Affichez les glossaires d'entreprise dans la vue Glossaire . - Rechercher des glossaires d'entreprise.
Gérer les objets	S. O.	Écrire	L'utilisateur peut effectuer les actions suivantes : - Modifier des objets de métadonnées dans le catalogue. - Créer, modifier et supprimer des objets de métadonnées personnalisés. Les utilisateurs doivent également avoir le privilège Afficher modèle. - Créer, modifier et supprimer des ressources de métadonnées personnalisées. Les utilisateurs doivent également avoir le privilège Gérer les ressources.

Groupe de privilèges Chargement

Les privilèges du groupe de privilèges Chargement déterminent les tâches que les utilisateurs peuvent effectuer sur l'onglet **Chargement** de l'application Metadata Manager. Un utilisateur disposant du privilège

nécessaire pour effectuer une action a également besoin d'autorisations pour exécuter cette action sur un objet spécifique. Configurez les autorisations dans l'onglet **Sécurité** de l'application Metadata Manager.

Le tableau suivant présente les privilèges et autorisations nécessaires pour gérer une instance d'une ressource dans l'entrepôt Metadata Manager :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher la ressource	-	Lecture	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Afficher les ressources et les propriétés des ressources dans l'entrepôt du gestionnaire de métadonnées. - Exporter les configurations de ressource. - Télécharger le programme d'installation de l'agent Metadata Manager.
Charger la ressource	Afficher la ressource	Écriture	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Charger les métadonnées d'une ressource dans l'entrepôt du gestionnaire de métadonnées.* - Créer des liens entre les objets dans des ressources connectées pour le lignage des données. - Configurer l'indexation de la recherche pour les ressources. - Importer les configurations de ressource.
Gérer les planifications	Afficher la ressource	Écriture	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Créer des planifications et les modifier. - Ajouter des planifications aux ressources.
Purger les métadonnées	Afficher la ressource	Écriture	L'utilisateur peut supprimer des métadonnées pour une ressource depuis l'entrepôt Metadata Manager.
Gérer la ressource	<ul style="list-style-type: none"> - Purger les métadonnées - Afficher la ressource 	Écriture	L'utilisateur peut créer, modifier et supprimer des ressources.
* Pour charger des métadonnées pour des ressources Business Glossary, les privilèges Charger la ressource, Gérer la ressource et Afficher le modèle sont requis.			

Groupe de privilèges du modèle

Les privilèges du groupe de privilèges Modèle déterminent les tâches que les utilisateurs peuvent effectuer sur l'onglet **Modèle** de l'application Metadata Manager. Vous ne pouvez pas configurer d'autorisations sur un modèle.

Le tableau suivant répertorie les privilèges requis pour gérer les modèles :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher le modèle	-	-	L'utilisateur peut ouvrir des modèles et des classes, ainsi qu'en afficher les propriétés. Afficher les relations et les attributs de classes.
Gérer le modèle	Afficher le modèle	-	L'utilisateur peut créer, modifier et supprimer des modèles personnalisés. Ajoutez des attributs aux modèles intégrés et universels.
Exporter/Importer des modèles	Afficher le modèle	-	L'utilisateur peut importer et exporter des modèles personnalisés. Importez et exportez des modèles intégrés modifiés et universels.

Groupe de privilèges Sécurité

Les privilèges du groupe de privilèges Sécurité déterminent les tâches que les utilisateurs peuvent effectuer sur l'onglet **Sécurité** de l'application Metadata Manager.

Par défaut, le privilège Gérer les autorisations du catalogue dans le groupe de privilèges Sécurité est assigné à l'administrateur, ou à un utilisateur avec le rôle Administrateur dans le service Metadata Manager. Vous pouvez assigner le privilège Gérer les autorisations du catalogue à d'autres utilisateurs.

Le tableau suivant présente le privilège et l'autorisation requis pour gérer la sécurité de Metadata Manager :

Privilège	Inclut les privilèges	Autorisation	Description
Gérer les autorisations du catalogue	-	Contrôle complet	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Assigner les autorisations d'utilisateurs et de groupes aux ressources, objets de métadonnées, catégories et termes commerciaux.- Modifier les autorisations pour les ressources, objets de métadonnées, catégories et termes métier.

Privilèges du service de référentiel modèle

Les privilèges du service de référentiel modèle déterminent les actions que les utilisateurs peuvent effectuer sur les projets à l'aide d'Informatica Analyst et d'Informatica Developer.

Les autorisations de l'objet de référentiel modèle déterminent les tâches que les utilisateurs peuvent effectuer sur les objets dans des projets.

Le tableau suivant répertorie les autorisations requises et les actions que les utilisateurs peuvent effectuer avec les privilèges du service de référentiel modèle :

Privilège	Autorisation	Description
N/D	Lire dans le projet	L'utilisateur peut afficher des projets et des objets dans des projets.
N/D	Écrire dans le projet	L'utilisateur peut créer, modifier et supprimer des objets dans des projets.
N/D	Attribuer sur le projet	L'utilisateur peut accorder et révoquer des autorisations sur les projets pour les utilisateurs et les groupes.
Accéder à Analyst	N/D	L'utilisateur peut accéder au référentiel modèle depuis l'outil Analyst tool.
Accès à Developer	N/D	L'utilisateur peut accéder au référentiel modèle depuis l'outil Developer tool.
Créer, modifier et supprimer des projets	N/D	L'utilisateur peut créer des projets.
Créer, modifier et supprimer des projets	Écrire dans les projets.	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Modifier des projets. - Supprimer des projets si l'utilisateur les a créés. - Mettre à niveau le contenu du service de référentiel modèle. Pour mettre à niveau le service à partir du menu Actions ou de la ligne de commande, l'utilisateur doit également disposer du privilège Gérer le service pour le domaine et de l'autorisation sur le service de référentiel modèle. Pour mettre à niveau le service à l'aide de l'assistant de mise à niveau de service, l'utilisateur doit également disposer du rôle Administrateur pour le domaine.
Gérer les domaines de données	N/D	L'utilisateur peut créer, modifier et supprimer des domaines de données dans le glossaire de domaine de données. Ce privilège fait partie du groupe de privilèges Administration de domaine de données .
Gérer les notifications	N/D	L'utilisateur peut configurer les notifications de fiche d'évaluation. Ce privilège fait partie du groupe de privilèges Administration de profilage .
Gérer le développement basé sur l'équipe	N/D	L'utilisateur peut gérer les états verrouillé et déverrouillé des objets du référentiel modèle. Si le référentiel modèle est intégré à un système de contrôle de version, l'utilisateur peut gérer les états extrait et archivé des objets. L'utilisateur peut également gérer la propriété des objets extraits.
Afficher les détails de sécurité	N/D	L'utilisateur peut afficher les détails suivants : <ul style="list-style-type: none"> - Noms des projets pour lesquels les utilisateurs ne disposent d'aucune autorisation d'accès en lecture. - Détails des messages d'erreur et d'avertissement.

Privilèges du PowerCenter Repository Service

Les privilèges du PowerCenter Repository Service déterminent les actions correspondantes que l'utilisateur peut effectuer à l'aide du PowerCenter Repository Manager, du Concepteur, du gestionnaire de workflow, du moniteur de Workflow et des programmes de ligne de commande pmrep et pmcmd.

Le tableau suivant décrit chaque groupe de privilèges pour le PowerCenter Repository Service :

Groupe de privilèges	Description
Outils	Comprend les privilèges pour accéder aux outils du client PowerCenter et programmes de ligne de commande.
Dossiers	Comprend les privilèges pour gérer les dossiers du référentiel.
Objets de conception	Comprend les privilèges pour gérer les composants d'entreprise, les paramètres de mappage et les variables, les mappages, les mapplets, les transformations et les fonctions définies par l'utilisateur.
Sources et cibles	Comprend les privilèges pour gérer les cubes, dimensions, définitions source et cible.
Objets d'exécution	Comprend les privilèges pour gérer les objets de configuration des sessions, les tâches, les workflows et les worklets.
Objets globaux	Comprend les privilèges pour gérer les objets de connexion, les groupes de déploiement, les libellés et les requêtes.

L'utilisateur doit disposer du privilège de domaine Gérer les services et de l'autorisation pour le PowerCenter Repository Service de l'outil Administrator pour effectuer les actions suivantes dans le Repository Manager :

- Effectuer une purge avancée des versions d'objets au niveau du référentiel PowerCenter.
- Créer, modifier et supprimer des extensions de métadonnées réutilisables.

Groupe de privilèges Outils

Les privilèges du groupe de privilèges Outils du service de référentiel PowerCenter déterminent les outils clients PowerCenter et les programmes de ligne de commande auxquels l'utilisateur peut accéder.

Le tableau suivant répertorie les actions que les utilisateurs peuvent effectuer pour les privilèges dans le groupe Outils :

Privilège	Autorisation	Description
Accéder au concepteur	-	L'utilisateur peut se connecter au référentiel PowerCenter à l'aide du concepteur.
Accéder au Repository Manager	-	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Se connecter au référentiel PowerCenter à l'aide du Repository Manager.- Exécuter les commandes <i>pmrep</i>.

Privilège	Autorisation	Description
Accéder au gestionnaire de flux de travail	-	L'utilisateur peut effectuer les actions suivantes : - Connectez-vous au référentiel PowerCenter à l'aide du gestionnaire de flux de travail. - Supprimez un service d'intégration PowerCenter du gestionnaire de flux de travail.
Accéder au moniteur de flux de travail	-	L'utilisateur peut effectuer les actions suivantes : - Connectez-vous au référentiel PowerCenter à l'aide du moniteur de flux de travail. - Connectez-vous au service d'intégration PowerCenter dans le moniteur de flux de travail.

Remarque: Lorsque le service d'intégration PowerCenter est exécuté en mode sécurisé, l'utilisateur doit avoir le rôle administrateur pour le service de référentiel PowerCenter associé.

Le privilège approprié dans le groupe de privilèges Outils est obligatoire pour tous les utilisateurs effectuant des tâches dans les outils clients PowerCenter dans les programmes de ligne de commande. Par exemple, pour créer des dossiers dans le Repository Manager, un utilisateur doit avoir les privilèges Création des dossiers et Accès au Repository Manager.

Si l'utilisateur a un privilège dans le groupe de privilèges Outils et l'autorisation pour un objet de référentiel PowerCenter, mais pas le privilège pour modifier le type d'objet, il peut néanmoins effectuer des actions dans l'objet. Par exemple, un utilisateur a le privilège Accès au Repository Manager et l'autorisation de lecture dans certains dossiers. L'utilisateur n'a pas de privilèges dans le groupe de privilèges Dossiers. L'utilisateur peut afficher les objets dans les dossiers et comparer ces derniers.

Groupe de privilèges Dossiers

Les actions de gestion des dossiers sont déterminées par les privilèges du groupe de privilèges Dossiers, les autorisations d'objet du référentiel PowerCenter et les autorisations d'objet de domaine. Les utilisateurs gèrent les dossiers dans le Repository Manager et à l'aide du programme de ligne de commande pmrep.

Certaines tâches de gestion des dossiers sont déterminées par le propriétaire du dossier et par le rôle de l'administrateur ; pas par les privilèges ou les autorisations. Le propriétaire du dossier ou un utilisateur ayant le rôle Administrateur pour le service de référentiel PowerCenter peut effectuer les tâches de gestion des dossiers suivantes :

- Assigner les profils de système d'exploitation aux dossiers si le service d'intégration PowerCenter utilise les profils des systèmes d'exploitation. Nécessite une autorisation sur le profil du système d'exploitation.
- Modifier le propriétaire du dossier.
- Configurer les autorisations d'accès au dossier.
- Supprimer le dossier.
- Désigner le dossier à partager.
- Modifier le nom et la description du dossier.

Les utilisateurs auxquels sont assignées les autorisations de dossier mais pas les privilèges peuvent effectuer certaines tâches de gestion des dossiers. Le tableau suivant répertorie les actions que les utilisateurs peuvent effectuer lorsqu'ils possèdent uniquement les autorisations de dossier :

Autorisation	Description
Lire dans le dossier	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Comparer des dossiers.- Afficher des objets dans des dossiers.

Remarque: Pour effectuer des actions sur les dossiers, les utilisateurs doivent également posséder le privilège Accès au Repository Manager.

Privilège Créer des dossiers

Les utilisateurs auxquels est assigné le privilège Créer des dossiers peuvent créer des dossiers de référentiel PowerCenter.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Créer des dossiers :

Autorisation	Description
-	L'utilisateur peut créer des dossiers.

Privilège Copier des dossiers

Les utilisateurs auxquels est assigné le privilège Copier des dossiers peuvent copier des dossiers dans un référentiel PowerCenter ou vers un autre référentiel PowerCenter.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Copier des dossiers :

Autorisation	Description
Lire dans le dossier	L'utilisateur peut copier les dossiers dans le même référentiel PowerCenter ou dans un autre référentiel PowerCenter. Les utilisateurs doivent également avoir le privilège Créer des dossiers dans le référentiel de destination.

Gérer les versions de dossier

Si vous disposez d'une option de développement basée sur une équipe, attribuez à des utilisateurs le privilège Gérer les versions de dossier dans un référentiel PowerCenter versionné. Les utilisateurs peuvent modifier le statut des dossiers et effectuer une purge avancée des versions d'objet au niveau du dossier.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Gérer les versions de dossier :

Autorisation	Description
Lire et écrire dans le dossier.	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Modifier le statut des dossiers.- Effectuer une purge avancée des versions d'objet au niveau du dossier.

Groupe de privilèges Objets de conception

Les privilèges du groupe de privilèges Objets de conception et les autorisations des objets du référentiel PowerCenter déterminent les actions que l'utilisateur peut effectuer dans les objets de conception suivants :

- Composants métier
- Paramètres et variables de mappage
- Mappages
- Mapplets
- Transformations
- Fonctions définies par l'utilisateur

Les utilisateurs ayant les autorisations, mais pas de privilèges, peuvent effectuer certaines actions pour les objets de conception. Le tableau suivant présente les actions que l'utilisateur peut effectuer lorsqu'il a uniquement les autorisations :

Autorisation	Description
Lire dans le dossier	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Comparer les objets de conception.- Copier les objets de conception en tant qu'image.- Exporter des objets de conception.- Générer un code pour les procédures de transformation personnalisée et externes.- Recevoir les messages de notification du référentiel PowerCenter.- Exécuter un lignage de données sur les objets de conception. Les utilisateurs doivent également posséder le privilège Afficher le lignage pour le service du gestionnaire de métadonnées et l'autorisation de lecture sur les objets de métadonnées dans le catalogue du gestionnaire de métadonnées.- Rechercher des objets de conception.- Afficher des objets de conception, les dépendances des objets de conception et l'historique des objets de conception.
Lire dans le dossier partagé Lire et écrire dans le dossier de destination	L'utilisateur peut créer des raccourcis.

Remarque: Pour effectuer les actions sur les objets de conception, les utilisateurs doivent également posséder le privilège approprié dans le groupe de privilèges Outils.

Privilège Création, modification et suppression d'objets de conception

Les utilisateurs bénéficiant du privilège Création, modification et suppression d'objets de conception peuvent créer, modifier et supprimer des composants commerciaux, des paramètres de mappage, des variables de mappage, des mappages, des mapplets, des transformations et des fonctions définies par l'utilisateur.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Création, modification et suppression d'objets de conception :

Autorisation	Description
Lire dans le dossier d'origine Lire et écrire dans le dossier de destination	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Copier des objets de conception d'un dossier vers un autre.- Copier des objets de conception dans un autre référentiel PowerCenter. Les utilisateurs doivent également avoir le privilège Création, modification et suppression d'objets de conception dans le référentiel de destination.
Lire et écrire dans le dossier.	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Modifier les commentaires d'un objet de conception à version gérée.- Archiver et annuler les extractions des objets de conception effectuées par leur propre compte utilisateur.- Extraire des objets de conception.- Copier et coller des objets de conception dans le même dossier.- Créer, modifier et supprimer des profils de données et lancer le gestionnaire de profils. Les utilisateurs doivent également avoir le privilège Créer, modifier et supprimer des objets d'exécution.- Créer, modifier et supprimer des objets de conception.- Générer et nettoyer des programmes ABAP SAP.- Générer des mappages d'intégration de contenu commercial. Les utilisateurs doivent également avoir le privilège Création, modification et suppression des sources et des cibles.- Importer des objets de conception en utilisant le concepteur. Les utilisateurs doivent également avoir le privilège Création, modification et suppression des sources et des cibles.- Importer des objets de conception en utilisant le gestionnaire de référentiel. Les utilisateurs doivent également disposer des privilèges Créer, modifier et supprimer des objets d'exécution et Créer, modifier et supprimer des sources et cibles.- Revenir à une version antérieure des objets de conception.- Valider les mappages, les mapplets et les fonctions définies par les utilisateurs.

Gérer les versions d'objets de conception

Si vous disposez d'une option de développement basée sur une équipe, attribuez à des utilisateurs le privilège Gérer les versions d'objets de conception dans un référentiel PowerCenter versionné. Les utilisateurs peuvent modifier le statut, récupérer et purger les versions d'objet de conception. Les utilisateurs peuvent également archiver et annuler les extractions effectuées par d'autres utilisateurs.

Le privilège Gérer les versions d'objets de conception comprend le privilège Créer, modifier et supprimer des objets de conception.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Gérer les versions d'objets de conception :

Autorisation	Description
Lire et écrire dans le dossier.	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Modifier le statut des objets de conception. - Archiver et annuler les extractions des objets de conception effectuées par d'autres utilisateurs. - Purger les versions des objets de conception. - Récupérer des objets de conception supprimés.

Groupe de privilèges Sources et cibles

Les privilèges du groupe de privilèges Sources et cibles et les autorisations des objets du référentiel PowerCenter déterminent les actions que l'utilisateur peut effectuer dans les objets source et cible suivants :

- Cubes
- Dimensions
- Définitions de sources
- Définitions de cibles

Les utilisateurs ayant les autorisations, mais pas de privilèges, peuvent effectuer des actions pour les objets source et cible. Le tableau suivant présente les actions que l'utilisateur peut effectuer lorsqu'il a uniquement les autorisations :

Autorisation	Description
Lire dans le dossier	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Comparer les objets source et cible. - Exporter les objets source et cible. - Prévisualiser les données source et cible. - Recevoir les messages de notification du référentiel PowerCenter. - Exécuter un lignage de données sur les objets source et cible. Les utilisateurs doivent également posséder le privilège Afficher le lignage pour le service du gestionnaire de métadonnées et l'autorisation de lecture sur les objets de métadonnées dans le catalogue du gestionnaire de métadonnées. - Rechercher des objets source et cible. - Afficher des objets source et cible, des dépendances d'objets source et cible ainsi qu'un historique d'objets source et cible.
Lire dans le dossier partagé Lire et écrire dans le dossier de destination	Créer des raccourcis.

Remarque: Pour effectuer les actions sur les objets source et cible, les utilisateurs doivent également posséder le privilège approprié dans le groupe de privilèges Outils.

Privilège Création, édition et suppression des sources et des cibles

Les utilisateurs ayant le privilège Création, édition et suppression des sources et des cibles peuvent créer, modifier et supprimer des cubes, des dimensions et des définitions de sources et de cibles.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Création, édition et suppression des sources et des cibles :

Autorisation	Description
Lire dans le dossier d'origine Lire et écrire dans le dossier de destination	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Copier des objets source et cible dans un autre dossier.- Copier des objets source et cible dans un autre référentiel PowerCenter. Les utilisateurs doivent également avoir le privilège Création, édition et suppression des sources et des cibles dans le référentiel de destination.
Lire et écrire dans le dossier.	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Modifier les commentaires d'un objet source ou cible à version gérée.- Archiver et annuler les extractions des objets source ou cible effectuées par leur propre compte utilisateur.- Extraire des objets source et cible.- Copier et coller des objets source et cible dans le même dossier.- Créer, modifier et supprimer des objets source et cible.- Importer des fonctions SAP.- Importer des objets source et cible en utilisant le concepteur. Les utilisateurs doivent également disposer du privilège Création, modification et suppression des objets de conception.- Importer des objets source et cible en utilisant le gestionnaire de référentiel. Les utilisateurs doivent également avoir les privilèges Création, édition et suppression des objets de conception et des objets d'exécution.- Générer et exécuter SQL pour créer des cibles dans une base de données relationnelle.- Revenir à une version antérieure des objets source et cible.

Privilège Gérer les versions source et cible

Si vous disposez d'une option de développement basée sur une équipe, attribuez à des utilisateurs le privilège Gérer les versions source et cible dans un référentiel PowerCenter versionné. L'utilisateur peut modifier l'état, récupérer et purger les versions des objets source et cible. Les utilisateurs peuvent également archiver et annuler les extractions effectuées par d'autres utilisateurs.

Le privilège Gérer les versions source et cible comprend le privilège Créer, modifier et supprimer des sources et cibles.

Le tableau suivant présente les autorisations requises et les actions que l'utilisateur peut effectuer avec le privilège Gérer les versions source et cible :

Autorisation	Description
Lire et écrire dans le dossier.	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Modifier l'état des objets source et cible. - Archiver et annuler les extractions des objets source et cible extraits par d'autres utilisateurs. - Purger la version des objets source et cible. - Récupérer les objets source et cible supprimés.

Groupe de privilèges Objets d'exécution

Les privilèges dans le groupe des privilèges Objets d'exécution, les autorisations des objets du référentiel PowerCenter et les autorisations des objets du domaine déterminent les actions que l'utilisateur peut effectuer dans les objets d'exécution suivants :

- Objets de configuration des sessions
- Tâches
- Flux de travail
- Worklets

Certaines tâches des objets d'exécution sont déterminées par le rôle Administrateur ; pas par les privilèges ou les autorisations. Un utilisateur ayant le rôle Administrateur pour le service de référentiel PowerCenter peut supprimer un service d'intégration PowerCenter du navigateur du gestionnaire de flux de travail.

Les utilisateurs ayant les autorisations mais pas les privilèges peuvent effectuer certaines actions pour les objets d'exécution. Le tableau suivant présente les actions que l'utilisateur peut effectuer lorsqu'il a uniquement les autorisations :

Autorisation	Description
Lire dans le dossier	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Comparer les objets d'exécution. - Exporter les objets d'exécution. - Recevoir les messages de notification du référentiel PowerCenter. - Rechercher les objets d'exécution. - Utiliser les paramètres et variables de mappage dans une session. - Afficher les objets d'exécution, les dépendances des objets d'exécution et l'historique des objets d'exécution.
Lire et exécuter dans le dossier	<p>Arrêter et abandonner les tâches et flux de travail démarrés par leur propre compte utilisateur.</p> <p>Lorsque le service d'intégration PowerCenter est exécuté en mode sécurisé, l'utilisateur doit avoir le rôle administrateur pour le service de référentiel PowerCenter associé.</p>

Remarque: Pour effectuer les actions dans les objets d'exécution, l'utilisateur doit avoir également le privilège approprié dans le groupe de privilèges Outils.

Privilège Création, modification et suppression d'objets d'exécution

Les utilisateurs possédant le privilège Création, modification et suppression d'objets d'exécution peuvent créer, modifier et supprimer des objets, des tâches, des flux de travail et des worklets de configuration de session.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Création, modification et suppression d'objets d'exécution :

Autorisation	Description
Lire dans le dossier d'origine Lire et écrire dans le dossier de destination	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Copier des tâches, des flux de travail ou des worklets d'un dossier vers un autre.- Copier des tâches, des flux de travail ou des worklets vers un autre référentiel PowerCenter. Les utilisateurs doivent également avoir le privilège Création, modification et suppression d'objets d'exécution dans le référentiel de destination.
Lire et écrire dans le dossier.	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Assigner un service d'intégration PowerCenter à un flux de travail dans les propriétés du flux de travail.- Assigner un niveau de service à un flux de travail.- Modifier les commentaires d'un objet d'exécution à version gérée.- Archiver et annuler les extractions des objets d'exécution effectuées par leur propre compte utilisateur.- Extraire des objets d'exécution.- Copier et coller des tâches, des flux de travail et des worklets dans le même dossier.- Créer, modifier et supprimer des profils de données et lancer le gestionnaire de profils. Les utilisateurs doivent également disposer du privilège Création, modification et suppression des objets de conception.- Créer, modifier et supprimer des objets de configuration de session.- Supprimer et valider des tâches, des flux de travail et des worklets.- Importer les objets d'exécution en utilisant le gestionnaire de référentiel. Les utilisateurs doivent également disposer des privilèges Créer, modifier et supprimer des objets de conception et Créer, modifier et supprimer des sources et cibles.- Importer des objets d'exécution en utilisant le gestionnaire de flux de travail.- Revenir à une version antérieure des objets d'exécution.
Lire et écrire dans le dossier. Lire dans l'objet de connexion	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Créer et modifier des tâches, des flux de travail et des worklets.- Remplacer une connexion de base de données relationnelle pour toutes les sessions qui utilisent cette connexion.

Privilège Gérer les versions d'objets d'exécution

Si vous disposez d'une option de développement basée sur une équipe, attribuez à des utilisateurs le privilège Gérer les versions d'objets d'exécution dans un référentiel PowerCenter versionné. Les utilisateurs peuvent modifier le statut, récupérer et purger les versions d'objet d'exécution. Les utilisateurs peuvent également archiver et annuler les extractions effectuées par d'autres utilisateurs.

Le privilège Gérer les versions d'objets d'exécution comprend le privilège Créer, modifier et supprimer des objets d'exécution.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Gérer les versions d'objets d'exécution :

Autorisation	Description
Lire et écrire dans le dossier.	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Modifier le statut des objets d'exécution. - Archiver et annuler les extractions des objets d'exécution effectuées par d'autres utilisateurs. - Purger les versions des objets d'exécution. - Récupérer des objets d'exécution supprimés.

Privilège Surveiller les objets d'exécution

Les utilisateurs auxquels est assigné le privilège Surveiller les objets d'exécution peuvent surveiller les flux de travail et tâches dans le moniteur de flux de travail.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Surveiller les objets d'exécution :

Autorisation	Permet à l'utilisateur de
Lire dans le dossier	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Afficher les propriétés des objets d'exécution dans le moniteur de flux de travail. - Afficher les journaux de session et de flux de travail dans le moniteur de flux de travail. - Afficher les détails des performances et de l'objet d'exécution dans le moniteur de flux de travail. <p>Lorsque le service d'intégration PowerCenter est exécuté en mode sécurisé, l'utilisateur doit avoir le rôle administrateur pour le service de référentiel PowerCenter associé.</p>

Privilège Exécuter des objets d'exécution

Les utilisateurs ayant le privilège Exécuter des objets d'exécution peuvent démarrer, démarrer à froid et récupérer des tâches et des flux de travail.

Le privilège Exécuter des objets d'exécution inclut le privilège Surveillance d'objets d'exécution.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Exécuter les objets d'exécution :

Autorisation	Description
Lire et exécuter dans le dossier	L'utilisateur peut assigner un service d'intégration PowerCenter pour un flux de travail en utilisant le menu de service ou le navigateur.
<p>Lire, écrire et exécuter dans le dossier</p> <p>Lire et exécuter dans l'objet de connexion</p>	<p>L'utilisateur peut déboguer un mappage en créant une instance de session de débogage ou en utilisant une session réutilisable. Les utilisateurs doivent également avoir le privilège Créer, modifier et supprimer des objets d'exécution.</p> <p>Lorsque le service d'intégration PowerCenter est exécuté en mode sécurisé, l'utilisateur doit avoir le rôle administrateur pour le service de référentiel PowerCenter associé.</p>

Autorisation	Description
Lire et exécuter dans le dossier Lire et exécuter dans l'objet de connexion	L'utilisateur peut déboguer un mappage en utilisant une session non réutilisable. Lorsque le service d'intégration PowerCenter est exécuté en mode sécurisé, l'utilisateur doit avoir le rôle administrateur pour le service de référentiel PowerCenter associé.
Lire et exécuter dans le dossier Lire et exécuter dans l'objet de connexion	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Démarrez, démarrez à froid et redémarrez des tâches et des flux de travail. - Récupérez les tâches et flux de travail démarrés par leur propre compte utilisateur. Si le service d'intégration PowerCenter utilise les profils des systèmes d'exploitation, l'utilisateur doit avoir l'autorisation pour le profil du système d'exploitation. Lorsque le service d'intégration PowerCenter est exécuté en mode sécurisé, l'utilisateur doit avoir le rôle administrateur pour le service de référentiel PowerCenter associé.

Privlège Gérer l'exécution des objets d'exécution

L'utilisateur ayant le privilège Gérer l'exécution des objets d'exécution peut planifier et annuler la planification des flux de travail. L'utilisateur peut également arrêter, abandonner et récupérer les tâches et flux de travail démarrés par d'autres utilisateurs.

Le privilège Gérer l'exécution des objets d'exécution comprend le privilège Exécuter des objets d'exécution et le privilège Contrôler les objets d'exécution.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Gérer l'exécution des objets d'exécution :

Autorisation	Description
Lire et exécuter dans le dossier	L'utilisateur peut écouter les flux de travail et les entrées du journal de session.
Lire et exécuter dans le dossier	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Arrêter et abandonner les tâches et flux de travail démarrés par d'autres utilisateurs. - Arrêter et abandonner les tâches récupérées automatiquement. - Annuler la planification des flux de travail. Lorsque le service d'intégration PowerCenter est exécuté en mode sécurisé, l'utilisateur doit avoir le rôle administrateur pour le service de référentiel PowerCenter associé.

Autorisation	Description
Lire et exécuter dans le dossier Lire et exécuter dans l'objet de connexion	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Récupérer les tâches et flux de travail démarrés par d'autres utilisateurs. - Restaurer les tâches récupérées automatiquement. Si le service d'intégration PowerCenter utilise les profils des systèmes d'exploitation, l'utilisateur doit avoir l'autorisation pour le profil du système d'exploitation. Lorsque le service d'intégration PowerCenter est exécuté en mode sécurisé, l'utilisateur doit avoir le rôle administrateur pour le service de référentiel PowerCenter associé.
Lire, écrire et exécuter dans le dossier Lire et exécuter dans l'objet de connexion	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Créez et éditez un planificateur réutilisable dans le menu Flux de travail > Planificateurs. - Éditez un planificateur non réutilisable dans les propriétés du flux de travail. - Éditez un planificateur réutilisable dans les propriétés du flux de travail. Les utilisateurs doivent également avoir le privilège Créer, modifier et supprimer des objets d'exécution. Si le service d'intégration PowerCenter utilise les profils des systèmes d'exploitation, l'utilisateur doit avoir l'autorisation pour le profil du système d'exploitation. Lorsque le service d'intégration PowerCenter est exécuté en mode sécurisé, l'utilisateur doit avoir le rôle administrateur pour le service de référentiel PowerCenter associé.

Groupe de privilèges des objets globaux

Les privilèges du groupe des privilèges d'objets globaux et les autorisations des objets du référentiel PowerCenter déterminent les actions que l'utilisateur peut effectuer sur les objets globaux suivants :

- Objets de connexion
- Groupes de déploiement
- Libellés
- Demandes

Certaines tâches des objets globaux sont déterminées par le propriétaire de l'objet global et par le rôle de l'administrateur, pas par les privilèges, ni par les autorisations. Le propriétaire de l'objet global ou un utilisateur ayant le rôle Administrateur pour le service de référentiel PowerCenter peut effectuer les tâches d'objets globaux suivantes :

- Configurer les autorisations des objets globaux.
- Changer le propriétaire de l'objet global.
- Supprimer l'objet global.

Les utilisateurs ayant les autorisations, mais pas de privilèges, peuvent effectuer des actions pour les objets globaux. Le tableau suivant présente les actions que l'utilisateur peut effectuer lorsqu'il a uniquement les autorisations :

Autorisation	Description
Lire dans l'objet de connexion	L'utilisateur peut afficher des objets de connexion.
Lire dans le groupe de déploiement	L'utilisateur peut afficher des groupes de déploiement.
Lire dans le libellé	L'utilisateur peut afficher des libellés.

Autorisation	Description
Lire dans la demande	L'utilisateur peut afficher des demandes.
Lire et écrire dans l'objet de connexion	L'utilisateur peut modifier des objets de connexion.
Lire et écrire dans le libellé	L'utilisateur peut modifier et verrouiller des libellés.
Lire et écrire dans la demande	L'utilisateur peut modifier et valider les demandes d'objets.
Lire et exécuter dans la demande	L'utilisateur peut exécuter des demandes d'objets.
Lire dans le dossier Lire et exécuter dans le libellé.	L'utilisateur peut appliquer des libellés et en retirer les références.

Remarque: Pour effectuer les actions dans les objets globaux, l'utilisateur doit avoir également le privilège approprié dans le groupe de privilèges Outils.

Privilège Créer des connexions

Les utilisateurs auxquels est assigné le privilège Créer des connexions peuvent créer des objets de connexion.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Créer des connexions :

Autorisation	Description
-	L'utilisateur peut créer et copier des objets de connexion.

Privilège Gérer les groupes de déploiement

Si vous disposez d'une option de développement basée sur une équipe, les utilisateurs auxquels le privilège Gérer les groupes de déploiement a été assigné dans un référentiel PowerCenter versionné peuvent créer, éditer, copier et annuler le déploiement de groupes. Dans un référentiel sans version, l'utilisateur peut créer, modifier et copier les groupes de déploiement.

Le tableau suivant présente les autorisations requises et les actions que l'utilisateur peut effectuer avec le privilège Gérer les groupes de déploiement :

Autorisation	Description
-	L'utilisateur peut créer des groupes de déploiement.
Lire et écrire dans le groupe de déploiement	L'utilisateur peut effectuer les actions suivantes : - Modifier les groupes de déploiement. - Supprimer les objets d'un groupe de déploiement.
Lire dans le dossier d'origine Lire et écrire dans le groupe de déploiement	L'utilisateur peut ajouter des objets vers un groupe de déploiement.

Autorisation	Description
Lire dans le dossier d'origine Lire et écrire dans le dossier de destination Lire et exécuter dans le groupe de déploiement	L'utilisateur peut copier des groupes de déploiement.
Lire et écrire dans le dossier de destination	L'utilisateur peut restaurer les groupes de déploiement.

Privilège Exécuter les groupes de déploiement

Les utilisateurs auxquels est assigné le privilège Exécuter les groupes de déploiement peuvent copier un groupe de déploiement sans autorisation d'écriture sur les dossiers cible.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Exécuter les groupes de déploiement :

Autorisation	Description
Lire dans le dossier d'origine Exécuter le groupe de déploiement	L'utilisateur peut copier des groupes de déploiement.

Privilège Créer des libellés

Si vous avez une option de développement basée sur une équipe, les utilisateurs assignés au privilège Créer des libellés dans un référentiel PowerCenter versionné peuvent créer des libellés.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Créer des libellés :

Autorisation	Description
-	L'utilisateur peut créer des libellés.

Privilège Créer des demandes

Les utilisateurs auxquels est assigné le privilège Créer des demandes peuvent créer des demandes d'objet.

Le tableau suivant présente les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège Créer des demandes :

Autorisation	Description
-	L'utilisateur peut créer des demandes d'objets.

Privilèges du service d'écoute PowerExchange

Les privilèges du service d'écoute PowerExchange déterminent les commandes infacmd pwx que les utilisateurs peuvent exécuter.

Le tableau suivant décrit le privilège du service d'écoute PowerCenter dans le groupe de privilèges des commandes d'information :

Nom du privilège	Description
listtask	Exécute la commande infacmd pwx ListTaskListener.

Le tableau suivant décrit chaque privilège du service d'écoute PowerCenter dans le groupe de privilèges des commandes de gestion :

Nom du privilège	Description
close	Exécute la commande infacmd pwx CloseListener.
closeforce	Exécute la commande infacmd pwx CloseForceListener.
stoptask	Exécute la commande infacmd pwx StopTaskListener.

Privilèges du service de journalisation PowerExchange

Les privilèges du service de journalisation PowerExchange déterminent les commandes infacmd pwx que les utilisateurs peuvent exécuter.

Le tableau suivant décrit chaque privilège du service de journalisation PowerCenter dans le groupe de privilèges des commandes d'information :

Nom du privilège	Description
displayall	Exécutez la commande infacmd pwx DisplayAllLogger.
displaycpu	Exécutez la commande infacmd pwx DisplayCPULogger.
displaycheckpoints	Exécutez la commande infacmd pwx DisplayCheckpointsLogger.
displayevents	Exécutez la commande infacmd pwx DisplayEventsLogger.
displaymemory	Exécutez la commande infacmd pwx DisplayMemoryLogger.
displayrecords	Exécutez la commande infacmd pwx DisplayRecordsLogger.
displaystatus	Exécutez la commande infacmd pwx DisplayStatusLogger.

Le tableau suivant décrit chaque privilège du service de journalisation PowerCenter dans le groupe de privilèges Commandes de gestion :

Nom du privilège	Description
condense	Exécutez la commande infacmd pwx CondenseLogger.
fileswitch	Exécutez la commande infacmd pwx FileSwitchLogger.
shutdown	Exécutez la commande infacmd pwx ShutDownLogger.

Privilèges du service de planificateur

Les privilèges du service de planificateur déterminent les actions que les utilisateurs peuvent effectuer sur les planifications et les tâches planifiées.

Le tableau suivant décrit les privilèges du service de planificateur et les autorisations requises :

Privilège	Description	Nécessite une autorisation sur
Créer une planification	L'utilisateur peut créer des planifications. Pour créer une planification, l'utilisateur doit également avoir le privilège d'administration de l'application sur le service d'intégration de données.	<ul style="list-style-type: none"> - Service de planificateur - Service d'intégration de données qui exécute les tâches que l'utilisateur souhaite planifier
Modifier une planification	L'utilisateur peut modifier, interrompre et reprendre des planifications. Pour modifier une planification, l'utilisateur doit également avoir le privilège d'administration de l'application sur le service d'intégration de données.	<ul style="list-style-type: none"> - Service de planificateur - Service d'intégration de données qui exécute les tâches que l'utilisateur souhaite planifier
Supprimer une planification	L'utilisateur peut supprimer des planifications.	Service de planificateur
Afficher les planifications	L'utilisateur peut afficher la vue Planifications et les planifications.	Service de planificateur

Privilèges du service Test Data Manager

Les privilèges du service Test Data Manager déterminent les actions que les utilisateurs peuvent effectuer à l'aide de Test Data Manager. Configurez les autorisations dans l'onglet **Sécurité** de l'outil Administrator tool.

Le tableau suivant décrit chaque groupe de privilèges de Test Data Manager :

Groupe de privilèges	Description
Administration	Inclut des privilèges pour créer et gérer des connexions, des phrases secrètes, des rôles et attribuer des privilèges aux utilisateurs et aux groupes d'utilisateurs dans Informatica Administrator, gérer des référentiels, ajouter des licences et configurer des attributs de flux de travail et de projet. Remarque: Pour créer des utilisateurs et des groupes, l'administrateur Informatica par défaut doit au préalable attribuer des privilèges d'administration de sécurité à l'administrateur des données de test.
Domaines de données	Inclut des privilèges pour afficher et gérer des domaines de données dans Test Data Manager.
Masquage des données	Inclut des privilèges pour afficher et gérer des règles de masquage et des affectations de stratégies dans Test Data Manager.
Stratégies	Inclut des privilèges pour afficher et gérer des stratégies dans Test Data Manager.
Projets	Inclut des privilèges pour afficher et gérer des projets, effectuer un audit et importer des métadonnées, et exécuter des plans et des flux de travail dans Test Data Manager.

Groupe de privilèges Administration

Les privilèges du groupe de privilèges Administration déterminent les tâches d'administration que les administrateurs des données de test peuvent effectuer.

Le tableau suivant répertorie les privilèges du groupe de privilèges Administration, ainsi que les autorisations requises pour effectuer une tâche sur un objet :

Groupe de privilèges Connexions

Les privilèges du groupe de privilèges Connexions déterminent les tâches que les utilisateurs peuvent effectuer sur la page Connexions de l'espace de travail TDM. Le tableau suivant répertorie les privilèges du groupe de privilèges Connexions, ainsi que les autorisations requises pour effectuer une tâche sur un objet :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher des connexions	-	Lire	L'utilisateur peut afficher et tester les connexions dans l'espace de travail TDM.
Gérer des connexions	Afficher des connexions	Écrire	L'utilisateur peut effectuer les actions suivantes sur la page Connexion dans l'espace de travail TDM : <ul style="list-style-type: none">- Créer des connexions.- Modifier des connexions.- Supprimer des connexions.- Afficher des connexions.- Tester des connexions.

Groupe de privilèges Domaines de données

Les privilèges du groupe de privilèges Domaines de données déterminent les tâches que les utilisateurs peuvent effectuer sur des domaines de données dans la page Stratégies de Test Data Manager.

Le tableau suivant répertorie les privilèges du groupe de privilèges Domaines de données, ainsi que les autorisations requises pour effectuer une tâche sur un objet :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher des domaines de données	-	Lire	Les utilisateurs peuvent visualiser les domaines de données dans Test Data Manager.
Gérer des domaines de données	Afficher des domaines de données	Écrire	Les utilisateurs peuvent effectuer les actions suivantes sur les domaines de données dans Test Data Manager : <ul style="list-style-type: none">- Créer des domaines de données.- Modifier des domaines de données.- Supprimer des domaines de données.- Afficher des domaines de données.

Groupe de privilèges Masquage des données

Les privilèges du groupe de privilèges Masquage des données déterminent les tâches que les utilisateurs peuvent effectuer dans la vue Projet | Définir | Masquage des données de Test Data Manager. Vous pouvez affecter des règles et des stratégies aux colonnes du tableau dans cette vue.

Le tableau suivant répertorie les privilèges du groupe de privilèges Masquage des données, ainsi que les autorisations requises pour effectuer une tâche sur un objet :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher un masquage des données	-	Lire	Les utilisateurs peuvent afficher les affectations de masquage des données dans Test Data Manager.
Gérer un masquage des données	Afficher un masquage des données	Écrire	Les utilisateurs peuvent effectuer les actions de masquage des données suivantes dans Test Data Manager : <ul style="list-style-type: none">- Ajouter des affectations de règles et de stratégies.- Supprimer des affectations de règles et de stratégies.- Remplacer des propriétés de règle.- Afficher des affectations de masquage des données.

Groupe de privilèges Sous-ensemble de données

Les privilèges du groupe de privilèges Sous-ensemble de données déterminent les tâches que les utilisateurs peuvent effectuer sur des objets de sous-ensemble de données dans Test Data Manager.

Le tableau suivant répertorie les privilèges du groupe de privilèges Sous-ensemble de données, ainsi que les autorisations requises pour effectuer une tâche sur un objet :

Groupe de privilèges Stratégies

Les privilèges du groupe de privilèges Stratégies déterminent les tâches que les utilisateurs peuvent effectuer sur des stratégies dans Test Data Manager.

Le tableau suivant répertorie les privilèges du groupe de privilèges Stratégies, ainsi que les autorisations requises pour effectuer une tâche sur un objet :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher des stratégies	-	Lire	L'utilisateur peut visualiser les stratégies dans Test Data Manager.
Gérer des stratégies	Afficher des stratégies	Écrire	L'utilisateur peut effectuer les actions de stratégie suivantes dans Test Data Manager : <ul style="list-style-type: none">- Créer des stratégies.- Modifier des stratégies.- Supprimer des stratégies.- Afficher des stratégies.

Groupe de privilèges Projets

Les privilèges du groupe de privilèges Projets déterminent les tâches que les utilisateurs peuvent effectuer sur des projets dans Test Data Manager.

Le tableau suivant répertorie les privilèges du groupe de privilèges Projets, ainsi que les autorisations requises pour effectuer une tâche sur un objet :

Remarque: Un utilisateur disposant du privilège Gérer le projet doit disposer au moins des niveaux de privilèges suivants pour pouvoir créer un plan avec chaque composant.

- Affichez la connexion depuis le groupe de privilèges Administration. Pour créer un plan.
- Affichez les sous-ensembles de données depuis le groupe de privilèges Sous-ensemble de données. Pour créer un plan avec des composants de sous-ensemble.
- Affichez les règles de masquage depuis le groupe de privilèges Règles. Pour créer un plan avec des composants de masquage.

Groupe de privilèges Règles

Le tableau suivant répertorie les privilèges du groupe de privilèges Masquage des données, ainsi que les autorisations requises pour effectuer une tâche sur un objet :

Groupe de privilèges Génération de données

Les privilèges du groupe de privilèges Génération de données déterminent les tâches de génération des données que les utilisateurs peuvent effectuer dans Test Data Manager.

Le tableau suivant répertorie les privilèges du groupe de privilèges Génération de donnée de , ainsi que les autorisations requises pour effectuer une tâche sur un objet :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher une génération des données	-	Lire	Les utilisateurs peuvent visualiser les affectations de règles de génération de données dans Test Data Manager.
Gérer une génération des données	Afficher une génération des données	Écrire	L'utilisateur peut effectuer les actions suivantes sur la génération de données dans Test Data Manager : <ul style="list-style-type: none">- Afficher des affectations de règles de génération des données- Ajouter des affectations de règles de génération de données.- Supprimer des affectations de règles de génération de données.- Remplacer des affectations de règles de génération de données.

Gestion des rôles

Un rôle est un regroupement de privilèges que vous pouvez attribuer à des utilisateurs et des groupes. Vous pouvez assigner les types de rôles suivants :

- Défini par le système. Des rôles que vous ne pouvez ni éditer ni supprimer.
- Personnalisé. Des rôles que vous pouvez créer, éditer et supprimer.

Un rôle comprend des privilèges pour le domaine ou un type de service d'application. Vous devez attribuer des rôles à des utilisateurs ou des groupes pour le domaine ou pour chacun de ses services d'application. Par exemple, vous pouvez créer un rôle Développeur qui comprend les privilèges du service de référentiel PowerCenter. Un domaine peut contenir plusieurs services de référentiel PowerCenter. Vous pouvez attribuer le rôle Développeur à un utilisateur pour le service de référentiel PowerCenter en phase de développement. Vous pouvez attribuer un rôle différent à un utilisateur pour le service de référentiel PowerCenter en phase de production.

Lorsque vous sélectionnez un rôle dans la section Rôles du navigateur, vous pouvez afficher tous les utilisateurs et groupes dont le rôle leur a été directement attribué pour le domaine et les services d'application. Vous pouvez afficher les assignations de rôle par utilisateurs et par groupes ou par services. Pour accéder à un utilisateur ou à un groupe indiqué dans la section Assignations, cliquez avec le bouton droit sur l'utilisateur ou le groupe et sélectionnez Naviguer dans un élément.

Vous pouvez rechercher des rôles personnalisés et définis par le système.

Rôles définis par le système

Un rôle défini par le système est un rôle que vous ne pouvez ni modifier ni supprimer. Le rôle Administrateur est un rôle défini par le système.

Lorsque vous attribuez le rôle Administrateur à un utilisateur ou groupe du domaine, le service Analyst, le service d'intégration de données, le service d'ingestion de masse, le service Metadata Manager, le service de référentiel modèle ou le service de référentiel PowerCenter, l'utilisateur ou le groupe se voit accorder tous les privilèges pour le service. Le rôle Administrateur contourne la vérification des autorisations. Les utilisateurs possédant le rôle Administrateur peuvent accéder à tous les objets gérés par le service.

Rôle Administrateur

Lorsque vous attribuez le rôle administrateur à un utilisateur ou à un groupe du domaine, du service d'intégration de données ou du service de référentiel PowerCenter, l'utilisateur ou le groupe peut effectuer certaines tâches déterminées par le rôle administrateur, et non pas par les privilèges ou les autorisations.

Vous pouvez attribuer à un utilisateur ou à un groupe tous les privilèges du domaine, du service d'intégration de données ou du service de référentiel PowerCenter, puis accorder à l'utilisateur ou au groupe toutes les autorisations sur tout le domaine ou sur les objets du référentiel PowerCenter. Toutefois, cet utilisateur ou ce groupe ne peut pas effectuer les tâches déterminées par le rôle administrateur.

Par exemple, un utilisateur ayant le rôle administrateur du domaine peut configurer des propriétés du domaine dans l'outil Administrator. Un utilisateur ayant tous les privilèges et toutes les autorisations du domaine ne peut pas configurer des propriétés du domaine.

Le tableau suivant donne la liste des tâches déterminées par le rôle administrateur du domaine, du service d'intégration de données, du service d'ingestion de masse et du service de référentiel PowerCenter :

Service	Tâches
Domaine	<ul style="list-style-type: none"> - Configurer les propriétés du domaine. - Configurer les configurations de grappe. - Créer des profils de système d'exploitation. - Supprimer des profils de système d'exploitation. - Accorder des autorisations sur le domaine et sur les profils de système d'exploitation. - Gérer et purger des événements de journaux. - Recevoir des alertes de domaine. - Exécuter le rapport de licence. - Afficher les événements du journal d'activité utilisateur. - Arrêter le domaine. - Accéder à l'assistant de mise à niveau de service.
Service d'intégration de données	<ul style="list-style-type: none"> - Mettre à jour le service d'intégration de données dans le menu Actions.
Service d'ingestion de masse	<ul style="list-style-type: none"> - Parcourir toutes les spécifications d'ingestion de masse. - Modifier une spécification d'ingestion de masse. - Exécuter une spécification d'ingestion de masse. - Supprimer une spécification d'ingestion de masse.
Service de référentiel PowerCenter	<ul style="list-style-type: none"> - Attribuer les profils de systèmes d'exploitation aux dossiers du référentiel si le service d'intégration PowerCenter utilise ces profils.* - Modifier le propriétaire des dossiers et des objets globaux.* - Configurer les autorisations des dossiers et des objets globaux.* - Connecter le PowerCenter Integration Service à partir du client PowerCenter lorsque le PowerCenter Integration Service est exécuté en mode sans échec. - Supprimer un PowerCenter Integration Service à partir du navigateur du gestionnaire de workflow. - Supprimer des dossiers et des objets globaux.* - Désigner les dossiers à partager.* - Modifier le nom et la description des dossiers.* <p>*Le propriétaire du dossier du référentiel PowerCenter ou le propriétaire de l'objet global peut également effectuer ces tâches.</p>

Rôles personnalisés

Un rôle personnalisé est un rôle que vous pouvez modifier ou supprimer.

Par défaut, l'outil Administrator tool inclut les rôles personnalisés suivants :

- Rôle personnalisé du service Analyst
- Rôles personnalisés du service Metadata Manager
- Rôle personnalisé de l'opérateur
- Rôles personnalisés du service de référentiel PowerCenter
- Rôles personnalisés du service Test Data Manager

Vous pouvez modifier les privilèges de ces rôles ou supprimer les rôles. Vous pouvez également créer vos propres rôles personnalisés.

Création des rôles personnalisés

Lorsque vous créez un rôle personnalisé, vous attribuez des privilèges au rôle pour le domaine ou pour le type de service d'application. Un rôle peut inclure des privilèges pour un ou plusieurs services.

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans le menu Actions de sécurité, cliquez sur Créer un rôle.
La boîte de dialogue Créer un rôle s'affiche.
3. Entrez les propriétés suivantes pour le rôle :

Propriété	Description
Nom	Nom du rôle. Le nom du rôle n'est pas sensible à la casse et ne doit pas dépasser 128 caractères. Il ne peut pas inclure de tabulation, retour à la ligne ou les caractères spéciaux suivants : , + " \ < > ; / * % ? Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Tous les autres caractères d'espacement sont interdits.
Description	Description du rôle. La description ne peut pas excéder 765 caractères ou contenir de tabulation, de retour à la ligne ou les caractères spéciaux suivants : < > "

4. Cliquez sur l'onglet Privilèges.
5. Développez le domaine ou un type de service d'application.
6. Sélectionnez les privilèges à attribuer au rôle pour le domaine ou le type de service d'application.
7. Cliquez sur OK.

Modification des propriétés pour les rôles personnalisés

Lorsque vous modifiez un rôle personnalisé, vous pouvez modifier sa description. Vous ne pouvez pas modifier le nom du rôle.

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans la section Rôles du navigateur, sélectionnez un rôle.
3. Cliquez sur Modifier.
4. Modifiez la description du rôle et cliquez sur OK.

Modification des privilèges associés aux rôles personnalisés

Vous pouvez modifier les privilèges attribués à un rôle personnalisé pour le domaine et pour chaque type de service d'application.

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans la section Rôles du navigateur, sélectionnez un rôle.
3. Cliquez sur l'onglet Privilèges.
4. Cliquez sur Modifier.
La boîte de dialogue Modifier les rôles et les privilèges s'affiche.
5. Développez le domaine ou un type de service d'application.
6. Pour attribuer des privilèges au rôle, sélectionnez-les pour le domaine ou le type de service d'application.
7. Pour retirer des privilèges du rôle, supprimez-les pour le domaine ou le type de service d'application.

8. Reprenez cette procédure pour modifier les privilèges de chaque type de service.
9. Cliquez sur OK.

Suppression des rôles personnalisés

Lorsque vous supprimez un rôle personnalisé, ce dernier et tous les privilèges qu'il contient sont supprimés de tous les utilisateurs ou groupes assignés au rôle.

Pour supprimer un rôle personnalisé, cliquez avec le bouton droit de la souris sur le rôle dans la section Rôles du navigateur et sélectionnez Supprimer le rôle. Confirmez la suppression du rôle.

Attribution de privilèges et de rôles aux utilisateurs et aux groupes

Vous pouvez déterminer les actions que les utilisateurs peuvent effectuer en attribuant les éléments suivants aux utilisateurs et aux groupes :

- Privilèges. Un privilège détermine les actions que l'utilisateur peut effectuer dans les clients d'application.
- Rôles. Un rôle est un ensemble de privilèges. Lorsque vous attribuez un rôle à un utilisateur ou à un groupe, vous attribuez l'ensemble des privilèges appartenant au rôle.

Servez-vous des règles et des instructions suivantes lorsque vous attribuez des privilèges et des rôles aux utilisateurs et aux groupes :

- Vous pouvez attribuer des privilèges et des rôles à des utilisateurs et des groupes pour le domaine et pour chaque service d'application en cours d'exécution dans le domaine.

Vous ne pouvez pas attribuer de privilèges et de rôles aux utilisateurs et groupes pour un service Metadata Manager ou un service de référentiel PowerCenter dans les cas suivants :

- Le service d'application est désactivé.
- Le service de référentiel PowerCenter s'exécute en mode exclusif.
- Vous pouvez attribuer différents privilèges et rôles à un utilisateur ou à un groupe pour chaque service d'application du même type de service.
- Un rôle peut comprendre des privilèges pour le domaine et plusieurs types de service d'application. Lorsque vous attribuez un rôle à un utilisateur ou à un groupe pour un service d'application, les privilèges pour ce type de service d'application sont attribués à l'utilisateur ou au groupe.

Si vous modifiez les privilèges ou les rôles attribués à un utilisateur, les modifications prennent effet lors de la prochaine connexion de l'utilisateur.

Remarque: Vous ne pouvez pas modifier les privilèges ou les rôles attribués au compte administrateur par défaut.

Privilèges hérités

Un utilisateur ou un groupe peut hériter de privilèges venant des objets suivants :

- Groupe. Lorsque vous attribuez des privilèges à un groupe, tous les sous-groupes et tous les utilisateurs appartenant au groupe héritent de ses privilèges.

- Rôle. Lorsque vous attribuez un rôle à un utilisateur, l'utilisateur hérite des privilèges appartenant à ce rôle. Lorsque vous attribuez un rôle à un groupe, le groupe, tous les sous-groupes et tous les utilisateurs appartenant au groupe héritent des privilèges appartenant à ce rôle. Le sous-groupe et les utilisateurs n'héritent pas du rôle.

On ne peut pas révoquer des privilèges hérités d'un groupe ou d'un rôle. Vous pouvez attribuer des privilèges supplémentaires n'étant pas hérités d'un groupe ou d'un rôle à un utilisateur ou à un groupe.

L'onglet Privilèges pour un utilisateur ou un groupe affiche tous les rôles et privilèges attribués à un utilisateur ou à un groupe pour le domaine et pour chaque service d'application. Étendez le domaine ou le service d'application pour afficher les rôles et les privilèges attribués au domaine ou au service. Cliquez sur les éléments suivants pour afficher des informations supplémentaires sur les rôles et privilèges attribués :

- Nom d'un rôle attribué. Affiche les informations du rôle sur le panneau d'informations.
- Icône d'information pour un rôle attribué. Met en valeur tous les privilèges hérités avec ce rôle.

Les privilèges hérités d'un rôle ou d'un groupe affichent une icône d'héritage. L'info-bulle pour un privilège hérité affiche de quel rôle ou de quel groupe l'utilisateur a hérité de son privilège.

Assignation de privilèges et de rôles à un utilisateur ou un groupe par navigation

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans le navigateur, sélectionnez un utilisateur ou groupe.
3. Cliquez sur l'onglet Privilèges.
4. Cliquez sur Modifier.
La boîte de dialogue Modifier les rôles et les privilèges s'ouvre.
5. Pour attribuer des rôles, développez le domaine ou un service d'application dans l'onglet Rôles.
6. Pour accorder des rôles, sélectionnez les rôles à attribuer à l'utilisateur ou au groupe pour le domaine ou le service d'application.
Vous pouvez sélectionner tout rôle incluant des privilèges pour le domaine ou le type de service d'application sélectionné.
7. Pour révoquer des rôles, cliquez sur les rôles attribués à l'utilisateur ou au groupe.
8. Répétez les étapes [5](#) à [7](#) pour attribuer des rôles pour un autre service.
9. Pour attribuer des privilèges, cliquez sur l'onglet Privilèges.
10. Développez le domaine ou un service d'application.
11. Pour accorder des privilèges, sélectionnez les privilèges à attribuer à l'utilisateur ou groupe pour le domaine ou le service d'application.
12. Pour révoquer des privilèges, cliquez sur les privilèges attribués à l'utilisateur ou au groupe.
Vous ne pouvez pas révoquer des privilèges hérités d'un groupe ou d'un rôle.
13. Répétez les étapes [10](#) à [12](#) pour attribuer des privilèges pour un autre service.
14. Cliquez sur OK.

Affichage des utilisateurs avec des privilèges pour un service

Vous pouvez afficher tous les utilisateurs qui ont des privilèges pour le domaine ou un service d'application.

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans le menu Actions de sécurité, cliquez sur Privilèges de l'utilisateur du service.
La boîte de dialogue Services s'affiche.
3. Sélectionnez le domaine ou un service d'application.
Le panneau d'informations affiche tous les utilisateurs qui ont des privilèges pour le domaine ou le service d'application.
4. Cliquez avec le bouton droit de la souris et cliquez sur Naviguer dans un élément pour accéder à l'utilisateur.

Dépannage des problèmes de privilèges et de rôles

Je ne peux attribuer ni privilège ni rôle aux utilisateurs pour un service Metadata Manager ou un service de référentiel PowerCenter.

Vous ne pouvez pas attribuer de privilèges et de rôles aux utilisateurs et groupes pour un service Metadata Manager ou un service de référentiel PowerCenter existant dans les cas suivants :

- Le service d'application est désactivé.
- Le service de référentiel PowerCenter s'exécute en mode exclusif.

J'ai supprimé un privilège d'un groupe. Pourquoi certains utilisateurs du groupe ont-ils encore ce privilège ?

Vous pouvez utiliser l'une des méthodes suivantes pour attribuer des privilèges à un utilisateur :

- Attribuer un privilège directement à un utilisateur.
- Attribuer un rôle à un utilisateur.
- Attribuer un privilège ou un rôle à un groupe auquel l'utilisateur appartient.

Si vous supprimez un privilège d'un groupe, les utilisateurs qui appartiennent à ce groupe peuvent recevoir directement le privilège ou peuvent hériter du privilège d'un rôle attribué.

Tous les privilèges du domaine et les autorisations me sont attribués pour tous les objets du domaine, mais je ne peux pas effectuer toutes les tâches dans l'outil Administrator tool.

Certaines tâches de l'outil Administrator tool sont déterminées par le rôle Administrateur, pas par les privilèges ou les autorisations. Vous pouvez vous voir attribuer tous les privilèges du domaine et des autorisations complètes sur tous les objets qu'il contient. Toutefois, vous ne pouvez pas effectuer les tâches déterminées par le rôle Administrateur.

Le rôle Administrateur m'a été attribué pour un service d'application, mais je ne peux pas configurer le service d'application dans l'outil Administrator tool.

Quand vous avez le rôle Administrateur pour un service d'application, vous êtes administrateur de client d'application. Un administrateur de client d'application possède l'ensemble des autorisations et des privilèges dans un client d'application.

Toutefois, un administrateur de client d'application ne dispose ni d'autorisation ni de privilège dans le domaine Informatica. Un administrateur de client d'application ne peut pas se connecter à l'outil Administrator tool pour gérer le service du client d'application pour lequel il dispose de privilèges d'administrateur.

Pour gérer un service d'application dans l'outil Administrator tool, vous devez posséder les autorisations et privilèges du domaine approprié.

Le rôle Administrateur m'est attribué pour le service de référentiel PowerCenter, mais je ne peux pas utiliser Repository Manager pour effectuer une purge avancée des objets ou pour créer des extensions de métadonnées réutilisables.

Vous devez disposer de l'autorisation et du privilège de domaine Gérer les services dans le service de référentiel PowerCenter de l'outil Administrator tool pour effectuer les actions suivantes dans Repository Manager :

- Effectuer une purge avancée des versions d'objets au niveau du référentiel PowerCenter.
- Créer, éditer et supprimer des extensions de métadonnées réutilisables.

Mes privilèges indiquent que je dois pouvoir éditer des objet dans un client d'application, mais je ne peux pas éditer les métadonnées.

Il se peut que vous n'ayez pas les autorisations d'objet requises dans le client d'application. Même si vous disposez du privilège requis pour effectuer certaines actions, il vous faut peut-être aussi l'autorisation de les effectuer sur un objet spécifique.

Je ne peux pas utiliser pmrep pour me connecter à un nouveau service de référentiel PowerCenter exécuté en mode exclusif.

Il se peut que le gestionnaire de service n'ait pas synchronisé la liste d'utilisateurs et de groupes du référentiel PowerCenter avec la liste de la base de données de configuration du domaine. Pour synchroniser la liste d'utilisateurs et de groupes, redémarrez le service de référentiel PowerCenter.

Tous les privilèges me sont attribués dans le groupe de privilèges Dossiers pour le service de référentiel PowerCenter et je possède l'autorisation de lecture, d'écriture et d'exécution pour un dossier. Cependant, je ne peux pas configurer les autorisations d'accès au dossier.

Seul le propriétaire du dossier ou un utilisateur ayant le rôle Administrateur pour le service de référentiel PowerCenter peut effectuer les tâches de gestion suivantes du dossier :

- Attribuer les profils de systèmes d'exploitation aux dossiers si le service d'intégration PowerCenter utilise les profils de systèmes d'exploitation. Exige l'autorisation pour le profil de système d'exploitation.
- Modifier le propriétaire du dossier.
- Configurer les autorisations d'accès au dossier.
- Supprimer le dossier.
- Désigner le dossier à partager.
- Éditer le nom et la description du dossier.

Le rôle d'administrateur du service Metadata Manager m'a été attribué, mais je ne parviens pas à créer ou à restaurer le référentiel Metadata Manager.

Pour créer ou restaurer le référentiel Metadata Manager, vous devez faire partie du groupe Administrateur par défaut. Les utilisateurs faisant partie du groupe Administrateur par défaut disposent de plus de privilèges que les utilisateurs à qui le rôle d'administrateur d'un service d'application a été attribué.

Le privilège Charger des ressources m'a été attribué pour le service Metadata Manager, mais j'obtiens une erreur « Privilèges insuffisants » lorsque j'essaie de charger des ressources Business Glossary.

Pour charger des ressources Business Glossary, les privilèges Charger la ressource, Gérer la ressource et Afficher le modèle sont requis. Vous devez également avoir l'autorisation d'écriture sur toute ressource Business Glossary que vous voulez charger.

CHAPITRE 10

Autorisations

Ce chapitre comprend les rubriques suivantes :

- [Présentation des autorisations, 191](#)
- [Autorisations d'objets de domaines, 193](#)
- [Autorisations de connexion, 197](#)
- [Autorisations de configuration de grappe, 200](#)
- [Autorisations d'applications et d'objets d'applications, 200](#)
- [Autorisations du service de données SQL, 203](#)
- [Autorisations du service web, 207](#)

Présentation des autorisations

Vous gérez la sécurité utilisateur à l'aide des privilèges et autorisations. Les autorisations définissent le niveau d'accès des utilisateurs et des groupes à un objet.

Même si un utilisateur dispose du privilège pour effectuer certaines actions, il peut également demander l'autorisation d'effectuer l'action sur un objet spécifique.

Par exemple, un utilisateur dispose du privilège de domaine Gérer les services et de l'autorisation sur le service de référentiel PowerCenter en phase de développement, mais pas sur le service de référentiel PowerCenter en phase de production. L'utilisateur peut modifier ou supprimer le service de référentiel PowerCenter en phase de développement mais pas le service de référentiel PowerCenter en phase de production. Pour gérer un service d'application, un utilisateur doit avoir le privilège de domaine Gérer les services et l'autorisation pour le service d'application.

Vous pouvez utiliser différents outils pour configurer les autorisations sur les objets suivants :

Type d'objet	Outil	Description
Applications et objets d'application	Outil Administrator tool	Vous pouvez attribuer des autorisations sur les applications et les objets d'application tels que les mappages et les flux de travail.
Objets de connexion	Outil Administrator tool Outil Analyst tool Outil Developer tool	Vous pouvez attribuer des autorisations sur les connexions définies dans les outils Administrator tool, Analyst tool ou Developer tool. Ces outils partagent les autorisations de connexion.

Type d'objet	Outil	Description
Objets de domaine	Outil Administrator tool	Vous pouvez attribuer des autorisations sur les objets de domaine suivants : domaine, dossiers, nœuds, grilles, licences, services d'application et profils de système d'exploitation.
Objets du catalogue Metadata Manager	Metadata Manager	Vous pouvez attribuer des autorisations sur les dossiers et objets du catalogue Metadata Manager.
Projets du référentiel modèle	Outil Analyst tool Outil Developer tool	Vous pouvez attribuer des autorisations sur les projets définis dans les outils Analyst tool et Developer tool. Ces outils partagent les autorisations de projet.
Objets du référentiel PowerCenter	Client PowerCenter	Vous pouvez attribuer des autorisations sur les dossiers, groupes de déploiement, libellés, requêtes et objets de connexion de PowerCenter.
Objets du service de données SQL	Outil Administrator tool	Vous pouvez attribuer des autorisations sur les objets de données SQL tels que les services de données SQL, les schémas virtuels, les tables virtuelles et les procédures stockées virtuelles.
Objets du service Web	Outil Administrator tool	Vous pouvez attribuer des autorisations sur les services Web ou les opérations du service Web.

Types d'autorisations

Les utilisateurs et groupes peuvent avoir les types suivants d'autorisations dans un domaine :

Autorisations directes

Autorisations qui sont assignées directement à un utilisateur ou à un groupe. Lorsque des utilisateurs et groupes ont l'autorisation pour un objet, ils peuvent effectuer des tâches administratives dans cet objet s'ils ont le privilège approprié. Vous pouvez modifier des autorisations directes.

Autorisations héritées

Autorisations dont héritent les utilisateurs. Quand des utilisateurs ont l'autorisation pour un domaine ou un dossier, ils héritent de l'autorisation pour tous les objets du domaine ou du dossier. Quand des groupes ont l'autorisation pour un objet du domaine, tous les sous-groupes et utilisateurs appartenant au groupe héritent de l'autorisation pour l'objet du domaine. Par exemple, un domaine comprend un dossier nommé Nœud qui contient plusieurs nœuds. Si vous assignez une autorisation de groupe pour le dossier, tous les sous-groupes et utilisateurs appartenant au groupe héritent de l'autorisation pour l'objet et pour tous les nœuds du dossier.

Vous ne pouvez pas révoquer les autorisations héritées. Vous ne pouvez pas non plus révoquer des autorisations d'utilisateurs ou de groupes ayant le rôle Administrateur. Le rôle Administrateur contourne la vérification des autorisations. Les utilisateurs possédant le rôle Administrateur peuvent accéder à tous les objets.

Vous pouvez refuser les autorisations héritées pour certains types d'objets. Lorsque vous refusez des autorisations, vous configurez des exceptions aux autorisations dont les utilisateurs et groupes disposent déjà.

Autorisations effectives

Sur-ensemble de toutes les autorisations pour un utilisateur ou un groupe. Inclut les autorisations directes et héritées.

Quand vous affichez les détails des autorisations, vous pouvez afficher l'origine des autorisations effectives. Les détails des autorisations affichent les autorisations directes assignées à l'utilisateur ou au groupe, celles assignées aux groupes parents et les autorisations héritées des objets parents. En outre, les détails d'autorisations indiquent si l'utilisateur ou le groupe reçoit le rôle Administrateur qui contourne la vérification des autorisations.

Filtres de recherche des autorisations

Lorsque vous attribuez des autorisations, affichez les détails d'une autorisation ou modifiez les autorisations d'un utilisateur ou d'un groupe, vous pouvez utiliser les filtres pour rechercher un utilisateur ou un groupe.

Lorsque vous gérez les autorisations d'un utilisateur ou groupe, vous pouvez utiliser les filtres de recherche suivants :

Domaine de sécurité

Sélectionnez le domaine de sécurité pour rechercher des utilisateurs ou groupes.

Chaîne de forme

Entrez une chaîne pour rechercher des utilisateurs ou groupes. L'outil Administrator renvoie tous les noms contenant la chaîne de recherche. La chaîne n'est pas sensible à la casse. Par exemple, la chaîne « DA » peut renvoyer « iasdaemon », « daphne » et « DA_AdminGroup ».

Vous pouvez également trier la liste des utilisateurs ou groupes. Cliquez avec le bouton droit de la souris sur un nom de colonne pour la trier dans l'ordre croissant ou décroissant.

Autorisations d'objets de domaines

Vous pouvez configurer les privilèges et les autorisations vous permettant de gérer la sécurité utilisateur dans le domaine. Les autorisations définissent le niveau d'accès d'un utilisateur à un objet du domaine. Pour se connecter à l'outil Administrator, un utilisateur doit avoir une autorisation sur au moins un objet du domaine. Si l'utilisateur a une autorisation sur un objet, mais n'a pas le privilège de domaine qui lui permet de modifier le type d'objet, il peut uniquement consulter cet objet.

Par exemple, si un utilisateur dispose d'une autorisation sur un nœud, mais pas du privilège Gérer les nœuds et les grilles, il peut consulter les propriétés du nœud, mais ne peut ni le configurer, ni l'arrêter, ni le supprimer.

Vous pouvez configurer les autorisations sur les types d'objets de domaine suivants :

Type d'objet de domaine	Description de l'autorisation
Domaine	Autorise les utilisateurs de l'outil Administrator tool à accéder à tous les objets du domaine. Lorsque des utilisateurs ont l'autorisation sur un domaine, ils héritent de l'autorisation sur tous les objets du domaine.
Dossier	Autorise les utilisateurs de l'outil Administrator tool à accéder à tous les objets du dossier de ce dernier. Quand des utilisateurs ont l'autorisation sur un dossier, ils héritent de l'autorisation sur tous les objets du dossier.
Nœud	Permet aux utilisateurs de l'outil Administrator tool de consulter et de modifier les propriétés de nœuds. Sans autorisation, un utilisateur ne peut pas utiliser un nœud lorsqu'il définit un service d'application ou lorsqu'il crée une grille.

Type d'objet de domaine	Description de l'autorisation
Grille	Permet aux utilisateurs de l'outil Administrator tool de consulter et de modifier les propriétés de grilles. Sans autorisation, un utilisateur ne peut pas affecter la grille à un service d'intégration de données ou un service d'intégration PowerCenter.
Licence	Permet aux utilisateurs de l'outil Administrator tool de consulter et de modifier les propriétés de licences. Sans autorisation, un utilisateur ne peut pas se servir d'une licence lorsqu'il crée un service d'application.
Service d'application	Permet aux utilisateurs de l'outil Administrator tool de consulter et de modifier les propriétés de services d'applications.
Profil de système d'exploitation	Permet aux développeurs Informatica, aux analystes et aux opérateurs associés au profil de système d'exploitation d'exécuter des mappages, des profils et des flux de travail. Permet aux utilisateurs PowerCenter d'exécuter des flux de travail associés au profil de système d'exploitation. Si l'utilisateur qui exécute un flux de travail n'a pas l'autorisation sur le profil de système d'exploitation qui lui est attribué, le flux de travail se termine en échec.

Vous pouvez utiliser les méthodes suivantes pour gérer les autorisations d'objet de domaine :

- Gérer les autorisations par objet de domaine. Utilisez la vue Autorisations d'un objet de domaine pour attribuer et modifier les autorisations sur l'objet à plusieurs utilisateurs ou groupes.
- Gérer les autorisations par utilisateur ou par groupe. Utilisez la boîte de dialogue Gérer autorisations pour attribuer et modifier les autorisations d'un utilisateur ou d'un groupe spécifique sur des objets de domaine.

Remarque: Vous pouvez configurer des autorisations sur un profil de système d'exploitation différemment de la manière dont vous avez configuré les autorisations sur d'autres objets de domaine.

Autorisations par objet de domaine

La vue **Autorisations** d'un objet de domaine permet d'attribuer, d'afficher et de modifier les autorisation sur l'objet de domaine pour plusieurs utilisateurs ou groupes.

Attribution d'autorisations sur un objet de domaine

Lorsque vous attribuez des autorisations sur un objet de domaine, vous accordez aux utilisateurs et aux groupes l'accès à cet objet.

1. Dans l'onglet Gérer, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez l'objet de domaine.
3. Dans le volet de contenu, cliquez sur la vue **Autorisations**.
4. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**.
5. Cliquez sur **Actions > Attribuer l'autorisation**.

La boîte de dialogue **Attribuer des autorisations** affiche tous les utilisateurs ou groupes n'ayant pas d'autorisation sur l'objet.

6. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
7. Sélectionnez un utilisateur ou un groupe et cliquez sur **Suivant**.
8. Sélectionnez **Autoriser**, puis cliquez sur **Terminer**.

Affichage des détails des autorisations pour un objet de domaine

Quand vous affichez les détails des autorisations, vous pouvez afficher l'origine des autorisations effectives.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez l'objet de domaine.
3. Dans le volet de contenu, cliquez sur la vue **Autorisations**.
4. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**.
5. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
6. Sélectionnez un utilisateur ou un groupe, puis cliquez sur **Actions > Afficher les détails des autorisations**.

La boîte de dialogue **Détails des autorisations** s'affiche. La boîte de dialogue affiche les autorisations directes attribuées à l'utilisateur ou au groupe, celles attribuées aux groupes parents et les autorisations héritées des objets parents. En outre, les détails des autorisations indiquent si l'utilisateur ou le groupe reçoit le rôle Administrateur qui contourne la vérification des autorisations.

7. Cliquez sur **Fermer**.
8. Ou cliquez sur **Modifier les autorisations** pour modifier les autorisations directes.

Modification des autorisations dans un objet de domaine

Vous pouvez modifier les autorisations directes sur un objet de domaine pour un utilisateur ou un groupe. Vous ne pouvez pas révoquer les autorisations héritées ou vos propres autorisations.

Remarque: Si vous révoquez une autorisation directe sur un objet, l'utilisateur ou le groupe peut toujours hériter d'une autorisation d'un groupe ou objet parent.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez l'objet de domaine.
3. Dans le volet de contenu, cliquez sur la vue **Autorisations**.
4. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**.
5. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.

6. Sélectionnez un utilisateur ou un groupe et cliquez sur **Actions > Modifier les autorisations directes**.

La boîte de dialogue **Modifier les autorisations directes** s'affiche.

7. Pour attribuer une autorisation sur un objet, sélectionnez **Autoriser**.
8. Pour révoquer une autorisation sur un objet, sélectionnez **Révoquer**.

Vous pouvez voir si l'autorisation est attribuée directement ou héritée en cliquant sur **Afficher les détails des autorisations**.

9. Cliquez sur **OK**.

Autorisations par utilisateur ou groupe

La boîte de dialogue **Gérer les autorisations** permet d'afficher, d'attribuer et de modifier les autorisations d'objet de domaine d'un utilisateur ou groupe spécifique.

Affichage des détails d'autorisations pour un utilisateur ou un groupe

Quand vous affichez les détails d'autorisations, vous pouvez afficher l'origine des autorisations effectives.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Sécurité**.
2. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**.
3. Sélectionnez un utilisateur ou un groupe.
4. Cliquez dans l'onglet **Autorisations**.

Attribution ou modification des autorisations d'un utilisateur ou d'un groupe.

Lorsque vous modifiez les autorisations d'objet de domaine d'un utilisateur ou d'un groupe, vous pouvez attribuer des autorisations et modifier des autorisations directes existantes. Vous ne pouvez pas révoquer les autorisations héritées ou vos propres autorisations.

Vous pouvez voir si l'autorisation est attribuée directement ou héritée en cliquant sur **Afficher les détails des autorisations**. Si vous révoquez une autorisation sur l'objet, l'utilisateur ou le groupe peut toujours hériter d'une autorisation d'un groupe ou d'un objet parent.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Sécurité**.
2. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**.
3. Sélectionnez un utilisateur ou un groupe.
4. Cliquez dans l'onglet **Autorisations**.
5. Sélectionnez un objet de domaine, puis cliquez sur **Modifier les autorisations directes**.
6. Pour attribuer une autorisation sur l'objet, sélectionnez **Autoriser**.
7. Pour révoquer une autorisation sur un objet, sélectionnez **Révoquer**.
8. Cliquez sur **OK**.

Autorisations du profil de système d'exploitation

Attribuez, affichez et modifiez les autorisations sur les profils de système d'exploitation dans la page Sécurité de l'outil Administrator tool.

Le groupe Administrator dispose des autorisations sur tous les profils de système d'exploitation.

Attribution d'autorisations sur un profil de système d'exploitation

Lorsque vous attribuez des autorisations sur un profil de système d'exploitation, les utilisateurs Informatica exécutent des mappages, des profils et des flux de travail à l'aide de ce profil. Les utilisateurs de PowerCenter exécutent des flux de travail attribués au profil de système d'exploitation.

1. Dans l'outil Administrator, cliquez sur l'onglet **Sécurité**.
2. Cliquez sur l'onglet **Profils de systèmes d'exploitation**.
3. Sélectionnez un profil de système d'exploitation, puis cliquez sur l'onglet **Autorisations**.
4. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**, puis sélectionnez **Modifier les autorisations directes**.
5. Sélectionnez un objet de domaine, puis cliquez sur **Modifier les autorisations directes**.
6. Pour attribuer une autorisation sur l'objet, sélectionnez **Autoriser**.
7. Pour révoquer une autorisation sur un objet, sélectionnez **Révoquer**.
8. Cliquez sur **OK**.

Affichage des détails des autorisations sur un profil de système d'exploitation

Quand vous affichez les détails des autorisations, vous pouvez afficher l'origine des autorisations effectives.

1. Dans l'onglet **Sécurité**, sélectionnez la vue **Profils de systèmes d'exploitation**.
2. Sélectionnez le profil de système d'exploitation, puis cliquez sur l'onglet **Autorisations**.
3. Sélectionnez la vue **Groupes** ou **Utilisateurs**.
4. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
5. Sélectionnez un utilisateur ou un groupe, puis cliquez sur **Afficher les détails des autorisations**.
La boîte de dialogue **Détails des autorisations** s'affiche. La boîte de dialogue affiche les autorisations directes attribuées à l'utilisateur ou au groupe, celles attribuées aux groupes parents et les autorisations héritées des objets parents. En outre, les détails des autorisations indiquent si l'utilisateur ou le groupe reçoit le rôle Administrateur qui contourne la vérification des autorisations.
6. Cliquez sur **Fermer**.
7. Ou cliquez sur **Modifier les autorisations** pour modifier les autorisations directes.

Modification des autorisations sur un profil de système d'exploitation

Vous pouvez modifier les autorisations directes sur un profil de système d'exploitation pour un utilisateur ou un groupe. Vous ne pouvez pas révoquer les autorisations héritées ou vos propres autorisations.

Remarque: Si vous révoquez une autorisation directe sur un objet, l'utilisateur ou le groupe peut toujours hériter d'une autorisation d'un groupe ou objet parent.

1. Dans l'onglet **Sécurité**, sélectionnez la vue **Profils de systèmes d'exploitation**.
2. Sélectionnez le profil de système d'exploitation, puis cliquez sur l'onglet **Autorisations**.
3. Sélectionnez la vue **Groupes** ou **Utilisateurs**.
4. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
5. Sélectionnez un utilisateur ou un groupe et cliquez sur **Modifier les autorisations directes**.
La boîte de dialogue **Modifier les autorisations directes** s'affiche.
6. Pour attribuer une autorisation sur le profil de système d'exploitation, sélectionnez **Autoriser**.
7. Pour révoquer une autorisation sur le profil de système d'exploitation, sélectionnez **Révoquer**.
Vous pouvez voir si l'autorisation est attribuée directement ou héritée en cliquant sur **Afficher les détails des autorisations**.
8. Cliquez sur **OK**.

Autorisations de connexion

Les autorisations contrôlent le niveau d'accès d'un utilisateur ou d'un groupe sur une connexion.

Vous pouvez configurer les autorisations sur une connexion dans l'outil Analyst ou dans l'outil Administrator.

Toute autorisation de connexion affectée à un utilisateur ou un groupe dans un des programmes s'applique aussi dans les autres outils. Vous pouvez par exemple accorder au groupe A une autorisation sur la connexion A dans l'outil Developer. Le groupe A aura une autorisation sur la connexion A dans l'outil Analyst, mais aussi dans l'outil Administrator.

Toute autorisation de connexion affectée à un utilisateur ou un groupe dans un des programmes s'applique aussi dans les autres outils. Vous pouvez par exemple accorder au groupe A une autorisation sur la connexion A dans l'outil Developer. Le Group A dispose également d'une autorisation sur la Connexion A dans l'outil Administrator.

Les composants Informatica suivants utilisent des autorisations de connexion :

- Outil Administrator. Applique les autorisations de lecture, d'écriture et d'exécution sur les connexions.
- Outil Analyst. Applique les autorisations de lecture, d'écriture et d'exécution sur les connexions.
- Interface de ligne de commande Informatica. Applique les autorisations de lecture, d'écriture et d'accord sur les connexions.
- Outil Developer. Applique les autorisations de lecture, d'écriture et d'exécution sur les connexions. L'outil Developer n'applique pas les autorisations de connexion sur les services de données SQL. Au lieu de cela, il applique la sécurité au niveau des colonnes et de l'intercommunication pour restreindre l'accès aux données.
- Service d'intégration de données. Applique les autorisations d'exécution lorsqu'un utilisateur tente de prévisualiser des données ou d'exécuter un mappage, une fiche d'évaluation ou un profil.

Remarque: Vous ne pouvez pas attribuer d'autorisations sur les connexions suivantes : entrepôt de profilage, base de données du cache d'objet de données et référentiel modèle.

Types d'autorisations de connexion

Vous pouvez assigner différents types d'autorisation aux utilisateurs pour effectuer les actions suivantes :

Action	Types d'autorisation
Afficher toutes les métadonnées de connexion, à l'exception des mots de passe, comme le nom de la connexion, le type, la description, les chaînes de connexion et les noms d'utilisateur.	Lire
Modifier toutes les métadonnées de connexion, y compris les mots de passe. Supprimer la connexion. Les utilisateurs disposant de l'autorisation d'écriture héritent de l'autorisation de lecture.	Écrire
Accéder aux données physiques dans la source de données sous-jacentes définies par la connexion. Les utilisateurs peuvent prévisualiser les données, exécuter un mappage, exécuter un mappage dans un flux de travail de tâche de mapping, exécuter une fiche d'évaluation ou exécuter un profil qui utilise la connexion.	Exécuter
Accorder et révoquer les autorisations de connexion.	Accorder

Autorisations de connexion par défaut

L'administrateur de domaine dispose de toutes les autorisations sur toutes les connexions. L'utilisateur qui crée une connexion dispose des autorisations de lecture, d'écriture, d'exécution et d'attribution sur la connexion. Par défaut, tous les utilisateurs ont l'autorisation d'effectuer les actions suivantes sur les connexions :

- Afficher des métadonnées de connexion basiques, telles que le nom, la description et le type de connexion.
- Utiliser la connexion dans des mappages de l'outil Developer.
- Créer des profils dans l'outil Analyst sur les objets de la connexion.

Attribution d'autorisations à une connexion

Lorsque vous attribuez des autorisations à une connexion, vous définissez le niveau d'accès qu'un utilisateur ou groupe possède pour la connexion.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Connexions**.
2. Dans le navigateur, sélectionnez la connexion.
3. Dans le volet de contenu, cliquez sur la vue **Autorisations**.
4. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**.
5. Cliquez sur **Actions** > **Attribuer l'autorisation**.

La boîte de dialogue **Attribuer des autorisations** affiche tous les utilisateurs ou groupes n'ayant pas d'autorisation sur la connexion.

6. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
7. Sélectionnez un utilisateur ou un groupe et cliquez sur **Suivant**.
8. Sélectionnez **Autoriser** pour chaque type d'autorisation que vous voulez attribuer.
9. Cliquez sur **Terminer**.

Affichage des détails des autorisations pour une connexion

Quand vous affichez les détails des autorisations, vous pouvez afficher l'origine des autorisations effectives.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Connexions**.
2. Dans le navigateur, sélectionnez la connexion.
3. Dans le volet de contenu, cliquez sur la vue **Autorisations**.
4. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**.
5. Sélectionnez un utilisateur ou un groupe, puis cliquez sur **Actions** > **Afficher les détails des autorisations**.

La boîte de dialogue **Afficher les détails des autorisations** s'affiche. La boîte de dialogue affiche les autorisations directes attribuées à l'utilisateur ou au groupe et celles attribuées aux groupes parents. En outre, les détails des autorisations indiquent si l'utilisateur ou le groupe reçoit le rôle Administrateur qui contourne la vérification de l'autorisation.

6. Cliquez sur **Fermer**.
7. Ou cliquez sur **Modifier les autorisations** pour modifier les autorisations directes.

Modification des autorisations sur une connexion

Vous pouvez modifier les autorisations directes sur une connexion pour un utilisateur ou un groupe. Vous ne pouvez pas révoquer les autorisations héritées ou vos propres autorisations.

Remarque: Si vous révoquez une autorisation directe sur un objet, l'utilisateur ou le groupe peut toujours hériter d'une autorisation d'un groupe ou objet parent.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Connexions**.
2. Dans le navigateur, sélectionnez la connexion.
3. Dans le volet de contenu, cliquez sur la vue **Autorisations**.
4. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**.

5. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
6. Sélectionnez un utilisateur ou un groupe et cliquez sur **Actions > Modifier les autorisations directes**. La boîte de dialogue **Modifier les autorisations directes** s'affiche.
7. Choisissez d'autoriser ou de révoquer les autorisations.
 - Sélectionnez **Autoriser** pour attribuer une autorisation.
 - Décochez **Autoriser** pour révoquer une autorisation simple.
 - Sélectionnez **Révoquer** pour révoquer toutes les autorisations.

Vous pouvez voir si l'autorisation est attribuée directement ou héritée en cliquant sur **Afficher les détails des autorisations**.
8. Cliquez sur **OK**.

Autorisations de configuration de grappe

Les autorisations contrôlent le niveau d'accès d'un utilisateur ou d'un groupe sur une configuration de grappe.

Vous pouvez configurer des autorisations sur une configuration de grappe dans l'outil Administrator tool et l'interface de ligne de commande Informatica.

Un utilisateur ou un groupe peut disposer des autorisations suivantes sur une configuration de grappe :

- Lecture. L'utilisateur ou les membres du groupe peuvent afficher la configuration de grappe.
- Écriture. L'utilisateur ou les membres du groupe peuvent modifier la configuration de grappe. Inclut l'autorisation de lecture.
- Exécute. L'utilisateur ou les membres du groupe peuvent exécuter des mappages dans l'environnement Hadoop.
- Grant. L'utilisateur ou les membres du groupe peuvent accorder l'autorisation sur la configuration de grappe à d'autres utilisateurs et groupes. Inclut l'autorisation de lecture.
- Tous. L'utilisateur hérite de toutes les autorisations accordées.

Par défaut, tous les utilisateurs disposent de l'autorisation d'afficher le nom de configuration de grappe.

Autorisations d'applications et d'objets d'applications

Les autorisations contrôlent le niveau d'accès d'un utilisateur ou d'un groupe aux applications et aux objets d'application tels que les mappages et les flux de travail.

Vous pouvez configurer les autorisations d'applications et d'objets d'application dans l'outil Administrator tool ou depuis la ligne de commande.

Types d'autorisations sur les applications et les objets d'application

Vous pouvez attribuer, afficher, accorder et exécuter des autorisations pour les utilisateurs et les groupes.

Vous pouvez attribuer les autorisations suivantes aux utilisateurs et groupes :

Autorisation d'afficher

Affichez les applications et les objets d'application.

Accorder une autorisation

Accordez et révoquez des autorisations sur les applications et les objets d'application.

Autorisation d'exécuter

Exécutez des applications et des objets d'application.

Remarque: Pour effectuer des opérations telles que le démarrage, l'arrêt ou la sauvegarde dans l'outil Administrator tool ou depuis la ligne de commande, l'utilisateur doit disposer de l'autorisation d'exécution et du privilège Gérer les applications pour l'application.

Attribution d'autorisations sur une application ou un objet d'application

Lorsque vous attribuez des autorisations sur une application ou un objet d'application, vous définissez le niveau d'accès d'un utilisateur ou d'un groupe sur une application ou un objet d'application.

1. Dans l'onglet Gérer, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un service d'intégration de données.
3. Dans le volet de contenu, cliquez sur la vue **Applications**.
4. Sélectionnez une application, un mappage ou un flux de travail.
5. Dans le panneau d'informations, sélectionnez la vue **Autorisations du groupe** ou **Autorisations de l'utilisateur**.
6. Cliquez sur le bouton **Attribuer une autorisation**.
La boîte de dialogue **Attribuer des autorisations** affiche tous les utilisateurs ou groupes qui ne disposent pas d'autorisation sur l'application ou sur l'objet d'application.
7. Entrez les conditions de filtre pour rechercher les utilisateurs et les groupes, puis cliquez sur le bouton **Filtrer**.
8. Sélectionnez un utilisateur ou un groupe et cliquez sur **Suivant**.
9. Sélectionnez **Autoriser** pour chaque type d'autorisation que vous voulez attribuer.
10. Cliquez sur **Terminer**.

Affichage des détails des autorisations sur une application ou un objet d'application

Quand vous affichez les détails des autorisations, vous pouvez afficher l'origine des autorisations effectives.

1. Dans l'onglet Gérer, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un service d'intégration de données.
3. Dans le volet de contenu, cliquez sur la vue **Applications**.
4. Sélectionnez l'application, le mappage ou le flux de travail.

5. Dans le panneau d'informations, sélectionnez la vue **Autorisations du groupe** ou **Autorisations de l'utilisateur**.
6. Entrez les conditions de filtre pour rechercher les utilisateurs et les groupes, puis cliquez sur le bouton **Filtrer**.
7. Sélectionnez un utilisateur ou un groupe, puis cliquez sur le bouton **Afficher les détails des autorisations**.

La boîte de dialogue **Détails des autorisations** s'affiche. La boîte de dialogue affiche les autorisations directes attribuées à l'utilisateur ou au groupe, celles attribuées aux groupes parents et les autorisations héritées des objets parents. En outre, les détails des autorisations indiquent si l'utilisateur ou le groupe reçoit le rôle Administrateur qui contourne la vérification des autorisations.
8. Cliquez sur **Fermer**.
9. Ou cliquez sur **Modifier les autorisations** pour modifier les autorisations directes.

Modification des autorisations sur une application ou un objet d'application

Vous pouvez modifier les autorisations directes sur une application ou un objet d'application pour un utilisateur ou un groupe. Vous ne pouvez pas révoquer les autorisations héritées ou vos propres autorisations.

Remarque: Si vous révoquez une autorisation directe sur un objet, l'utilisateur ou le groupe peut toujours hériter d'une autorisation d'un groupe ou objet parent.

1. Dans l'onglet Gérer, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un service d'intégration de données.
3. Dans le volet de contenu, cliquez sur la vue **Applications**.
4. Sélectionnez l'application ou l'objet d'application.
5. Dans le panneau d'informations, sélectionnez la vue **Autorisations du groupe** ou **Autorisations de l'utilisateur**.
6. Entrez les conditions de filtre pour rechercher les utilisateurs et les groupes, puis cliquez sur le bouton **Filtrer**.
7. Sélectionnez un utilisateur ou un groupe et cliquez sur le bouton **Modifier les autorisations directes**.

La boîte de dialogue **Modifier les autorisations directes** s'affiche.
8. Choisissez d'autoriser ou de révoquer les autorisations.
 - Sélectionnez **Autoriser** pour attribuer une autorisation.
 - Décochez **Autoriser** pour révoquer une autorisation simple.
 - Sélectionnez **Révoquer** pour révoquer toutes les autorisations.

Vous pouvez voir si l'autorisation est attribuée directement ou héritée en cliquant sur **Afficher les détails des autorisations**.
9. Cliquez sur **OK**.

Refus d'autorisations sur une application ou un objet d'application

Vous pouvez explicitement refuser des autorisations sur une application et des objets d'application. Lorsque vous refusez une autorisation, vous appliquez une exception à l'autorisation effective.

Autorisations du service de données SQL

L'utilisateur final peut se connecter à un service de données SQL via un outil client JDBC ou ODBC. Après la connexion, l'utilisateur peut exécuter les requêtes SQL par rapport aux tables virtuelles d'un service de données SQL, ou l'utilisateur peut exécuter une procédure virtuelle stockée dans un service de données SQL. Les autorisations contrôlent le niveau d'accès d'un utilisateur à un service de données SQL.

Vous pouvez attribuer des autorisations à des utilisateurs et groupes sur les objets de service de données SQL suivants :

- service de données SQL
- Table virtuelle
- Procédure virtuelle stockée

Lorsque vous attribuez des autorisations sur un objet de service de données SQL, l'utilisateur ou le groupe hérite des mêmes autorisations sur tous les objets qui appartiennent à l'objet du service de données SQL. Par exemple, vous attribuez l'autorisation de sélection utilisateur sur un service de données SQL. L'utilisateur hérite de l'autorisation sélectionnée sur toutes les tables virtuelles du service de données SQL.

Vous pouvez refuser des autorisations à des utilisateurs et groupes dans certains objets du service de données SQL. Lorsque vous refusez des autorisations, vous configurez des exceptions aux autorisations dont les utilisateurs et groupes disposent déjà. Par exemple, vous ne pouvez pas attribuer des autorisations à une colonne d'une table virtuelle, mais vous pouvez refuser à un utilisateur d'exécuter une instruction SQL SELECT qui inclut la colonne.

Types d'autorisations de service de données SQL

Vous pouvez attribuer les autorisations suivantes aux utilisateurs et groupes :

- Autorisation d'accorder. L'utilisateur peut accorder et révoquer des autorisations dans les objets du service de données SQL à l'aide de l'outil Administrator ou du programme de ligne de commande *infacmd*.
- Autorisation d'exécuter. L'utilisateur peut exécuter des procédures stockées virtuelles dans le service de données SQL à l'aide d'un outil client JDBC ou ODBC.
- Autorisation de sélectionner. L'utilisateur peut exécuter des instructions SQL SELECT dans les tables virtuelles du service de données SQL à l'aide d'un outil client JDBC ou ODBC.

Certaines autorisations ne sont pas applicables à tous les objets de services de données SQL.

Le tableau suivant décrit les autorisations pour chaque objet de service de données SQL :

Objet	Autorisation d'accorder	Autorisation d'exécuter	Autorisation de sélectionner
service de données SQL	Autorisation d'accepter et de révoquer l'autorisation dans le service de données SQL et tous les objets à l'intérieur du service de données SQL.	Exécutez toutes les procédures stockées virtuelles dans le service de données SQL.	Exécutez les instructions SQL SELECT dans toutes les tables virtuelles du service de données SQL.
Table virtuelle	Autorisation d'accorder et de révoquer dans la table virtuelle.	-	Exécutez les instructions SQL SELECT dans la table virtuelle.
Procédure stockée virtuelle	Autorisation d'accorder et de révoquer dans la procédure stockée virtuelle.	Exécutez la procédure stockée virtuelle.	-

Attribuer des autorisations pour un service de données SQL.

Lorsque vous attribuez des autorisations sur un objet de service de données SQL, vous définissez le niveau d'accès qu'un utilisateur ou groupe possède pour l'objet.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un service d'intégration de données.
3. Dans le volet de contenu, cliquez sur la vue **Applications**.
4. Sélectionnez l'objet de service de données SQL.
5. Dans le panneau d'informations, sélectionnez la vue **Autorisations du groupe** ou **Autorisations de l'utilisateur**.

6. Cliquez sur le bouton **Attribuer une autorisation**.

La boîte de dialogue **Attribuer des autorisations** affiche tous les utilisateurs ou groupes n'ayant pas d'autorisation sur l'objet du service de données SQL.

7. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
8. Sélectionnez un utilisateur ou un groupe et cliquez sur **Suivant**.
9. Sélectionnez **Autoriser** pour chaque type d'autorisation que vous voulez attribuer.
10. Cliquez sur **Terminer**.

Affichage des détails des autorisations pour un service de données SQL

Quand vous affichez les détails des autorisations, vous pouvez afficher l'origine des autorisations effectives.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un service d'intégration de données.
3. Dans le volet de contenu, cliquez sur la vue **Applications**.
4. Sélectionnez l'objet de service de données SQL.
5. Dans le panneau d'informations, sélectionnez la vue **Autorisations du groupe** ou **Autorisations de l'utilisateur**.
6. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.

7. Sélectionnez un utilisateur ou un groupe, puis cliquez sur le bouton **Afficher les détails des autorisations**.

La boîte de dialogue **Détails des autorisations** s'affiche. La boîte de dialogue affiche les autorisations directes attribuées à l'utilisateur ou au groupe, celles attribuées aux groupes parents et les autorisations héritées des objets parents. En outre, les détails des autorisations indiquent si l'utilisateur ou le groupe reçoit le rôle Administrateur qui contourne la vérification des autorisations.

8. Cliquez sur **Fermer**.
9. Ou cliquez sur **Modifier les autorisations** pour modifier les autorisations directes.

Modification des autorisations pour un service de données SQL

Vous pouvez modifier les autorisations directes sur un service de données SQL pour un utilisateur ou un groupe. Vous ne pouvez pas révoquer les autorisations héritées ou vos propres autorisations.

Remarque: Si vous révoquez une autorisation directe sur un objet, l'utilisateur ou le groupe peut toujours hériter d'une autorisation d'un groupe ou objet parent.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Services et nœuds**.
 2. Dans le navigateur, sélectionnez un service d'intégration de données.
 3. Dans le volet de contenu, cliquez sur la vue **Applications**.
 4. Sélectionnez l'objet de service de données SQL.
 5. Dans le panneau d'informations, sélectionnez la vue **Autorisations du groupe** ou **Autorisations de l'utilisateur**.
 6. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
 7. Sélectionnez un utilisateur ou un groupe et cliquez sur le bouton **Modifier les autorisations directes**. La boîte de dialogue **Modifier les autorisations directes** s'affiche.
 8. Choisissez d'autoriser ou de révoquer les autorisations.
 - Sélectionnez **Autoriser** pour attribuer une autorisation.
 - Décochez **Autoriser** pour révoquer une autorisation simple.
 - Sélectionnez **Révoquer** pour révoquer toutes les autorisations.
- Vous pouvez voir si l'autorisation est attribuée directement ou héritée en cliquant sur **Afficher les détails des autorisations**.
9. Cliquez sur **OK**.

Refus d'autorisations pour un service de données SQL

Vous pouvez explicitement refuser des autorisations sur certains objets de service de données SQL. Lorsque vous refusez une autorisation sur un objet d'un service de données SQL, vous appliquez une exception à l'autorisation effective.

Pour refuser les autorisations, utilisez l'une des commandes infacmd suivantes :

- `infacmd sql SetStoredProcedurePermissions`. Refuse les autorisations Exécuter ou Accorder au niveau de la procédure stockée.
- `infacmd sql SetTablePermissions`. Refuse les autorisations Sélectionner ou Accorder au niveau de la table virtuelle.
- `infacmd sql SetColumnPermissions`. Refuse l'autorisation Sélectionner au niveau de la colonne.

Chaque commande possède les options Appliquer des autorisations (-ap) et Refuser des autorisations (-dp). La commande `SetColumnPermissions` n'inclut pas l'option Appliquer les autorisations.

Remarque: Vous ne pouvez pas refuser des autorisations depuis l'outil Administrator.

Le Data Integration Service vérifie les autorisations avant d'exécuter les requêtes SQL et les procédures stockées par rapport à la base de données virtuelle. Le Data Integration Service valide les autorisations des utilisateurs ou groupes en commençant au niveau du service de données SQL. Lorsque les autorisations s'appliquent à un objet parent d'un service de données SQL, les objets enfant héritent de l'autorisation. Le Data Integration Service vérifie les autorisations refusées au niveau des colonnes.

Sécurité au niveau des colonnes

Un administrateur peut refuser l'accès aux colonnes dans la table virtuelle d'un objet de données SQL. L'administrateur peut configurer le comportement du service d'intégration de données des requêtes par rapport à une colonne restreinte.

Les résultats suivants peuvent se produire lorsque l'utilisateur demande une colonne pour laquelle il ne possède pas d'autorisation :

- La requête renvoie une valeur de substitution à la place des données. La requête renvoie une valeur de substitution dans chaque ligne qu'elle renvoie. La valeur de substitution remplace la valeur de colonne dans la requête. Si la requête inclut des filtres ou des jointures, des résultats de substitution s'affichent dans les résultats.
- La requête échoue avec une erreur Autorisation insuffisante.

Pour plus d'informations sur la configuration de la sécurité pour les services de données SQL, consultez l'article « Méthode de configuration de la sécurité pour les services de données SQL » de la Bibliothèque de procédures Informatica :

https://kb.informatica.com/h2l/HowTo%20Library/1/0266_ConfiguringSecurityForSQLDataServices.pdf.

Colonnes restreintes

Lorsque vous configurez la sécurité au niveau des colonnes, définissez une option de colonne qui détermine ce qui se passe lorsqu'un utilisateur sélectionne la colonne restreinte dans une requête. Vous pouvez remplacer les données restreintes par une valeur par défaut. Ou, vous pouvez faire échouer la requête si un utilisateur sélectionne la colonne restreinte.

Par exemple, un administrateur refuse à un utilisateur l'accès à la colonne Salaire dans la table Employé. L'administrateur configure une valeur de remplacement de 100 000 pour la colonne Salaire. Lorsque l'utilisateur sélectionne la colonne Salaire dans une requête SQL, le Data Integration Service renvoie 100 000 pour le salaire dans chaque ligne.

Exécutez la commande `infacmd sql UpdateColumnOptions` pour configurer les options de colonne. Vous ne pouvez pas définir les options de colonne dans l'outil Administrator.

Lorsque vous exécutez `infacmd sql UpdateColumnOptions`, entrez les options suivantes :

ColumnOptions.DenyWith=option

Détermine s'il convient de substituer la valeur de colonne restreinte ou de faire échouer la requête. Si vous remplacez la valeur de colonne, vous pouvez choisir de remplacer la valeur par NULL ou par une valeur constante. Sélectionnez l'une des options suivantes :

- **ERROR.** Fait échouer la requête et renvoie une erreur lorsqu'une requête SQL sélectionne une colonne restreinte.
- **NULL.** Renvoie les valeurs null pour une colonne restreinte dans chaque ligne.
- **VALUE.** Renvoie une valeur de constante dans la colonne restreinte au niveau de chaque ligne. Configurez la valeur de constante dans l'option `ColumnOptions.InsufficientPermissionValue`.

ColumnOptions.InsufficientPermissionValue=value

Remplace la valeur de colonne restreinte par une constante. La valeur par défaut est une chaîne vide. Si le Data Integration Service remplace la colonne par une chaîne vide, mais que la colonne est un nombre ou une date, la requête renvoie des erreurs. Si vous ne configurez pas une valeur pour l'option `DenyWith`, le Data Integration Service ne tient pas compte de l'option `InsufficientPermissionValue`.

Pour configurer une valeur de remplacement pour une colonne, entrez la commande avec la syntaxe suivante :

```
infacmd sql UpdateColumnOptions -dn empDomain -sn DISService -un Administrator -pd
Adminpass -sqlds employee_APP.employees_SQL -t Employee -c Salary -o
ColumnOptions.DenyWith=VALUE ColumnOptions.InsufficientPermissionValue=100000
```

Si vous ne configurez pas l'une des deux options pour une colonne restreinte, la requête échoue par défaut. La requête est exécutée et le Data Integration Service remplace la valeur de la colonne par NULL.

Ajout d'un niveau de sécurité de colonne

Configurez le niveau de sécurité de colonne à l'aide de la commande `infacmd sql SetColumnPermissions`. Vous ne pouvez pas définir le niveau de sécurité de colonne dans l'outil Administrator.

Une table Employé contient les colonnes Prénom, Nom, Service et Salaire. Vous autorisez un utilisateur à accéder à la table Employé, mais n'autorisez pas l'utilisateur à accéder à la colonne Salaire.

Pour restreindre l'accès de l'utilisateur à la colonne Salaire, désactivez le Data Integration Service et entrez une commande `infacmd` similaire à la commande suivante :

```
infacmd sql SetColumnPermissions -dn empDomain -sn DISService -un Administrator -pd
Adminpass -sqlds employee_APP.employees -t Employee -c Salary gun -Tom -dp SQL_Select
```

Les instructions SQL renvoient la valeur NULL dans la colonne Salaire :

```
Select * from Employee
Select LastName, Salary from Employee
```

Le comportement par défaut renvoie des valeurs null.

Autorisations du service web

Les utilisateurs finaux peuvent envoyer des requêtes du service Web et recevoir des réponses correspondantes à travers un client de service Web. Les autorisations contrôlent le niveau d'accès de l'utilisateur à un service Web.

Vous pouvez attribuer des autorisations aux utilisateurs et groupes dans les objets suivants du service Web :

- Service Web
- Ressource du service Web REST
- Opération du service Web SOAP

Quand vous attribuez des autorisations pour un objet de service Web, l'utilisateur ou le groupe hérite des mêmes autorisations pour tous les objets qui appartiennent à l'objet du service Web. Par exemple, vous attribuez une autorisation d'exécution à l'utilisateur pour un service Web. L'utilisateur hérite de l'autorisation d'exécution pour les opérations du service Web.

Vous pouvez refuser des autorisations aux utilisateurs et groupes pour une opération de service Web. Lorsque vous refusez des autorisations, vous configurez des exceptions aux autorisations dont les utilisateurs et groupes disposent déjà. Par exemple, un utilisateur a des autorisations d'exécution pour un service Web comportant trois opérations. Vous pouvez refuser à un utilisateur d'exécuter une opération associée à un service Web.

Types d'autorisations de service Web

Un administrateur affecte les autorisations du service Web aux types d'utilisateurs et de groupes suivants :

- Consommateur du service Web. Utilisateur du domaine natif qui envoie une demande au service Web et reçoit une réponse du service Web. L'utilisateur doit disposer d'une autorisation d'exécution sur le service Web.
- Administrateur du service Web. Utilisateur qui peut se connecter à l'outil Administrator tool, modifier les propriétés du service Web et accorder des autorisations aux autres utilisateurs.
- Opérateur du service Web. Utilisateur qui peut se connecter à l'outil Administrator tool, surveiller un service Web et démarrer ou arrêter un service Web.

Un administrateur peut attribuer les autorisations suivantes aux utilisateurs et groupes :

- Autorisation d'accorder. L'utilisateur peut gérer des autorisations dans les objets du service Web à l'aide de l'outil Administrator ou du programme de ligne de commande *infacmd*.
- Autorisation d'exécuter. L'utilisateur peut envoyer des demandes de services Web et recevoir des réponses de service.

Le tableau suivant décrit les autorisations pour chaque objet de service Web SOAP :

Objet	Autorisation d'accorder	Autorisation d'exécuter
Service Web SOAP	Autorisation d'accorder et de révoquer pour le service Web et toutes les opérations à l'intérieur du service Web.	Envoyez les demandes de service Web et recevez les réponses correspondantes provenant de toutes les opérations à l'intérieur du service Web.
Opération du service Web SOAP	Autorisation d'accorder, de révoquer et de refuser pour l'utilisation du service Web.	Envoyez les demandes de service Web et recevez les réponses correspondantes provenant des opérations du service Web.

Le tableau suivant décrit les autorisations pour chaque objet de service Web REST :

Objet	Autorisation d'accorder	Autorisation d'exécuter
Service Web REST	Autorisation d'accorder et de révoquer pour le service Web REST et toutes les ressources à l'intérieur du service Web.	Envoyez les demandes de service Web et recevez les réponses correspondantes provenant de toutes les ressources à l'intérieur du service Web REST.
Ressource REST	Autorisation d'accorder, de révoquer et de refuser pour la ressource du service Web REST.	Envoyez les demandes de service Web et recevez les réponses correspondantes provenant de la ressource du service Web REST.

Attribution des autorisations pour un service Web

Lorsque vous attribuez des autorisations sur un objet de service Web, vous définissez le niveau d'accès qu'un utilisateur ou groupe possède pour l'objet.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un service d'intégration de données.
3. Dans le volet de contenu, cliquez sur la vue **Applications**.
4. Sélectionnez l'objet de service Web.
5. Dans le panneau d'informations, sélectionnez la vue **Autorisations du groupe** ou **Autorisations de l'utilisateur**.
6. Cliquez sur le bouton **Attribuer une autorisation**.

La boîte de dialogue **Attribuer des autorisations** affiche tous les utilisateurs ou groupes n'ayant pas d'autorisation sur l'objet du service de données SQL.

7. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
8. Sélectionnez un utilisateur ou un groupe et cliquez sur **Suivant**.
9. Sélectionnez **Autoriser** pour chaque type d'autorisation que vous voulez attribuer.
10. Cliquez sur **Terminer**.

Affichage des détails des autorisations pour un service Web

Quand vous affichez les détails des autorisations, vous pouvez afficher l'origine des autorisations effectives.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un service d'intégration de données.
3. Dans le volet de contenu, cliquez sur la vue **Applications**.
4. Sélectionnez l'objet de service Web.
5. Dans le panneau d'informations, sélectionnez la vue **Autorisations du groupe** ou **Autorisations de l'utilisateur**.
6. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
7. Sélectionnez un utilisateur ou un groupe, puis cliquez sur le bouton **Afficher les détails des autorisations**.

La boîte de dialogue **Détails des autorisations** s'affiche. La boîte de dialogue affiche les autorisations directes attribuées à l'utilisateur ou au groupe, celles attribuées aux groupes parents et les autorisations héritées des objets parents. En outre, les détails des autorisations indiquent si l'utilisateur ou le groupe reçoit le rôle Administrateur qui contourne la vérification des autorisations.

8. Cliquez sur **Fermer**.
9. Ou cliquez sur **Modifier les autorisations** pour modifier les autorisations directes.

Modification des autorisations dans un service Web

Vous pouvez modifier les autorisations directes sur un service Web pour un utilisateur ou un groupe. Lorsque vous modifiez les autorisations sur un objet de service Web, vous pouvez refuser les autorisations sur l'objet. Vous ne pouvez pas révoquer les autorisations héritées ou vos propres autorisations.

Remarque: Si vous révoquez une autorisation directe sur un objet, l'utilisateur ou le groupe peut toujours hériter d'une autorisation d'un groupe ou objet parent.

1. Dans l'onglet **Gérer**, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un service d'intégration de données.
3. Dans le volet de contenu, cliquez sur la vue **Applications**.
4. Sélectionnez l'objet de service Web.
5. Dans le panneau d'informations, sélectionnez la vue **Autorisations du groupe** ou **Autorisations de l'utilisateur**.
6. Entrez les conditions de filtre pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
7. Sélectionnez un utilisateur ou un groupe et cliquez sur le bouton **Modifier les autorisations directes**.

La boîte de dialogue **Modifier les autorisations directes** s'affiche.

8. Choisissez d'autoriser ou de révoquer les autorisations.

- Sélectionnez **Autoriser** pour attribuer une autorisation.
- Sélectionnez **Refuser** pour refuser une autorisation sur un objet de service Web.
- Décochez **Autoriser** pour révoquer une autorisation simple.
- Sélectionnez **Révoquer** pour révoquer toutes les autorisations.

Vous pouvez voir si l'autorisation est attribuée directement ou héritée en cliquant sur **Afficher les détails des autorisations**.

9. Cliquez sur **OK**.

CHAPITRE 11

Rapports d'audit

Ce chapitre comprend les rubriques suivantes :

- [Présentation des rapports d'audit, 211](#)
- [Informations personnelles de l'utilisateur, 212](#)
- [Association de groupes d'utilisateurs, 213](#)
- [Privilèges, 214](#)
- [Association de rôles, 214](#)
- [Autorisation d'objet de domaine, 215](#)
- [Sélection d'utilisateurs pour un rapport d'audit, 215](#)
- [Sélection des groupes pour un rapport d'audit , 216](#)
- [Sélection des rôles pour un rapport d'audit, 217](#)

Présentation des rapports d'audit

Utilisez les rapports d'audit pour afficher les informations concernant les utilisateurs et les groupes du domaine Informatica, ainsi que les privilèges et les autorisations qui leur sont attribués.

Vous pouvez générer les rapports d'audit suivants :

Informations personnelles de l'utilisateur

Affiche les informations sur les comptes utilisateur du domaine, y compris le statut de l'utilisateur. Vous pouvez sélectionner les utilisateurs ou les groupes pour lesquels vous voulez générer le rapport.

Association de groupes d'utilisateurs

Affiche des informations concernant les utilisateurs et les groupes auxquels ils appartiennent. Vous pouvez sélectionner les utilisateurs ou les groupes pour lesquels vous voulez générer le rapport.

Privilèges

Affiche les informations sur les privilèges attribués aux utilisateurs et aux groupes du domaine. Vous pouvez sélectionner les utilisateurs ou les groupes pour lesquels vous voulez générer le rapport.

Rôles

Affiche les informations sur les rôles attribués aux utilisateurs et aux groupes du domaine. Vous pouvez sélectionner les rôles pour lesquels vous voulez générer le rapport.

Autorisations d'objet de domaine

Affiche les informations sur les objets de domaine sur lesquels les utilisateurs et les groupes disposent d'une autorisation. Vous pouvez sélectionner les utilisateurs ou les groupes pour lesquels vous voulez générer le rapport.

Vous pouvez générer les rapports d'audit dans différents formats de fichier, y compris CSV, texte ou PDF. Vous pouvez également afficher le rapport à l'écran.

Vous pouvez générer les rapports d'audit dans l'outil Administrator ou à partir de la ligne de commande. Pour exécuter les rapports d'audit à partir de la ligne de commande, exécutez `infacmd` et le programme de ligne de commande.

Informations personnelles de l'utilisateur

Le rapport Informations personnelles de l'utilisateur affiche les informations de contact et le statut des comptes utilisateur du domaine.

Si vous exécutez le rapport pour les groupes, il organise la liste des utilisateurs par groupe et affiche le nom du groupe et le domaine de sécurité de chaque groupe. Le rapport affiche les groupes imbriqués séparément.

Le rapport Informations personnelles de l'utilisateur affiche les informations suivantes :

Nom de connexion

Nom de connexion du compte utilisateur.

Nom complet

Nom complet du compte utilisateur.

Domaine de sécurité

Domaine de sécurité auquel l'utilisateur appartient.

Description

Description du compte utilisateur.

ID de courriel

Adresse de courriel du compte utilisateur.

Téléphone

Numéro de téléphone du compte utilisateur.

Compte verrouillé

Indique si le compte est verrouillé ou non. Le rapport affiche Oui si le compte est verrouillé et Non s'il ne l'est pas.

Compte désactivé

Indique si le compte est désactivé ou non. Le rapport affiche Oui si le compte est désactivé et Non s'il est activé.

Association de groupes d'utilisateurs

Le rapport Association de groupes d'utilisateurs affiche des informations sur les utilisateurs et les groupes qui leur sont associés.

Si vous exécutez le rapport pour les utilisateurs, il affiche la liste des utilisateurs et les groupes auxquels ceux-ci appartiennent.

Le rapport Association de groupes d'utilisateurs affiche les informations suivantes :

Nom de connexion

Nom de connexion du compte utilisateur.

Nom complet

Nom complet du compte utilisateur.

Domaine de sécurité

Domaine de sécurité auquel le compte utilisateur appartient.

Nom du groupe

Nom du groupe auquel l'utilisateur appartient.

Chemin du groupe

Si le groupe est un groupe unique, c'est son nom qui est indiqué ici. Si le groupe est un groupe imbriqué, c'est sa position dans la hiérarchie des groupes imbriqués qui est indiquée.

Domaine de sécurité du groupe

Domaine de sécurité du groupe auquel l'utilisateur appartient.

Si vous exécutez le rapport pour les groupes, il organise la liste des utilisateurs par groupe et affiche le nom du groupe et le domaine de sécurité de chaque groupe. Le rapport affiche les groupes imbriqués séparément. Pour chaque groupe, il affiche la liste des utilisateurs et des groupes enfants.

Le rapport Association de groupes d'utilisateurs affiche les informations suivantes pour les utilisateurs qui appartiennent au groupe :

Nom de connexion

Nom de connexion du compte utilisateur.

Nom complet

Nom complet du compte utilisateur.

Domaine de sécurité

Domaine de sécurité auquel le compte utilisateur appartient.

Le rapport Association de groupes d'utilisateurs affiche les informations suivantes pour les groupes enfants qui appartiennent au groupe :

Nom du groupe

Nom du groupe.

Domaine de sécurité

Domaine de sécurité auquel le groupe appartient.

Chemin du groupe

Si le groupe est un groupe unique, c'est son nom qui est indiqué ici. Si le groupe est un groupe imbriqué, c'est sa position dans la hiérarchie des groupes imbriqués qui est indiquée.

Privilèges

Le rapport Privilèges affiche les utilisateurs et les groupes, ainsi que les privilèges qui leur sont attribués.

Si vous exécutez le rapport pour les utilisateurs, il affiche la liste des utilisateurs et les privilèges attribués à chacun d'entre eux. Si vous exécutez le rapport pour les groupes, il affiche la liste des groupes et les privilèges attribués à chacun d'entre eux.

Le rapport Privilèges affiche les informations suivantes :

Nom du privilège

Nom du privilège.

Chemin de privilège

Hérarchie du groupe de privilèges auquel appartient le privilège.

Nom de l'objet

Nom de l'objet sur lequel le privilège est autorisé.

Type d'objet

Type de l'objet sur lequel le privilège est autorisé.

Association de rôles

Le rapport Association de rôles affiche une liste de rôles et les utilisateurs et groupes auxquels les rôles sont attribués.

Le rapport Association de rôles affiche les informations suivantes :

Nom de connexion

Nom de connexion du compte utilisateur auquel le rôle est attribué. Il s'affiche pour la liste des utilisateurs.

Nom complet

Nom complet du compte utilisateur auquel le rôle est attribué. Il s'affiche pour la liste des utilisateurs.

Nom du groupe

Nom du groupe auquel le rôle est attribué. Il s'affiche pour la liste des groupes.

Domaine de sécurité

Domaine de sécurité auquel l'utilisateur ou le groupe appartient.

Nom de l'objet

Nom de l'objet pour lequel l'ensemble de privilèges dans le rôle est autorisé.

Type d'objet

Type de l'objet pour lequel l'ensemble de privilèges dans le rôle est autorisé.

Autorisation d'objet de domaine

Le rapport Autorisation d'objet de domaine affiche les utilisateurs et les groupes ainsi que les objets sur lesquels ces utilisateurs et ces groupes disposent d'une autorisation.

Si vous exécutez le rapport pour les utilisateurs, il affiche la liste des utilisateurs et les objets sur lesquels ils disposent d'autorisations. Si vous exécutez le rapport pour les groupes, il affiche la liste des groupes et les objets sur lesquels ils disposent d'autorisations.

Le rapport Autorisation d'objet de domaine affiche les informations suivantes :

Nom de l'objet

Nom de l'objet sur lequel l'utilisateur ou le groupe dispose d'une autorisation.

Type d'objet

Type de l'objet sur lequel l'utilisateur ou le groupe dispose d'une autorisation.

Chemin de l'objet

Emplacement de l'objet dans le référentiel.

Sélection d'utilisateurs pour un rapport d'audit

Vous pouvez générer un rapport d'audit pour plusieurs utilisateurs.

1. Dans l'outil Administrator, cliquez sur **Sécurité > Rapports d'audit**.
2. Dans la liste **Sélectionner le type de rapport**, sélectionnez le type de rapport d'audit que vous voulez exécuter.
3. Dans la liste **Générer un rapport pour**, sélectionnez **Utilisateurs** et cliquez sur **Atteindre**.
La boîte de dialogue **Sélectionner les utilisateurs** s'affiche. Par défaut, l'icône **Utilisateurs** est sélectionnée et la liste de tous les utilisateurs disponibles s'affiche. La liste affiche le nom complet de l'utilisateur et le domaine de sécurité auquel il appartient.
4. Dans la liste **Utilisateurs disponibles**, sélectionnez les utilisateurs pour lesquels vous voulez exécuter le rapport.
Utilisez la touche Maj ou Ctrl pour sélectionner plusieurs utilisateurs.
5. Pour sélectionner les utilisateurs par groupe, cliquez sur l'icône **Groupes**.
La liste **Groupes disponibles** affiche tous les groupes du domaine et la liste **Membres** affiche les utilisateurs qui sont membres des groupes. Dans la liste **Membres**, sélectionnez les utilisateurs pour lesquels vous voulez exécuter le rapport. Vous pouvez sélectionner des utilisateurs de plusieurs groupes.
6. Cliquez sur **Ajouter**.
Pour exécuter le rapport pour tous les utilisateurs, cliquez sur l'icône **Utilisateurs** et cliquez sur **Ajouter tout** sans sélectionner d'utilisateur.
Pour exécuter le rapport pour tous les utilisateurs d'un groupe, cliquez sur l'icône **Groupes**. Sélectionnez un groupe et cliquez sur **Ajouter tout** sans sélectionner d'utilisateur dans la liste **Membres**.
Les utilisateurs sélectionnés sont placés dans la liste **Utilisateurs sélectionnés**.
7. Dans la liste **Format de sortie du rapport**, sélectionnez le format dans lequel vous voulez afficher le rapport.

Par défaut, le rapport s'affiche à l'écran.

Vous pouvez également afficher un rapport d'audit dans l'un des formats suivants :

- Texte. Génère le rapport d'audit sous forme de fichier texte avec les valeurs indiquées dans des colonnes.
- CSV. Génère le rapport d'audit sous forme de fichier texte avec les valeurs séparées par des virgules.
- PDF. Génère le rapport d'audit au format .pdf. Vous devez installer Acrobat Reader pour afficher le rapport.

8. Cliquez sur **Générer le rapport**.

Sélection des groupes pour un rapport d'audit

Vous pouvez exécuter des rapports d'audit pour plusieurs groupes.

1. Dans l'outil Administrator, cliquez sur **Sécurité > Rapports d'audit**.
2. Dans la liste **Sélectionner le type de rapport**, sélectionnez le type de rapport d'audit que vous voulez exécuter.
3. Dans la liste **Générer un rapport pour**, sélectionnez **Groupes** et cliquez sur **Atteindre**.
La boîte de dialogue **Sélectionner les groupes** s'ouvre. Les listes de groupes sont organisées par domaine de sécurité.
4. Dans la liste **Groupes disponibles**, sélectionnez les groupes pour lesquels vous voulez exécuter le rapport.
Utilisez la touche Maj ou Ctrl pour sélectionner plusieurs groupes.
5. Cliquez sur **Ajouter**.
Pour exécuter le rapport pour tous les groupes, ne sélectionnez aucun groupe et cliquez sur **Ajouter tout**.
Les groupes sélectionnés sont placés dans la liste **Groupes sélectionnés**.
6. Dans la liste **Format de sortie du rapport**, sélectionnez le format dans lequel vous voulez afficher le rapport.
Par défaut, les rapports s'affichent à l'écran.
Vous pouvez également exécuter un rapport d'audit dans l'un des formats suivants :
 - Texte. Génère le rapport d'audit sous forme de fichier texte avec les valeurs indiquées dans des colonnes.
 - CSV. Génère le rapport d'audit sous forme de fichier texte avec les valeurs séparées par des virgules.
 - PDF. Génère le rapport d'audit au format .pdf. Vous devez installer Acrobat Reader pour afficher le rapport.
7. Cliquez sur **Générer le rapport**.

Sélection des rôles pour un rapport d'audit

Lorsque vous exécutez le rapport Association de rôles, vous devez sélectionner les rôles à inclure dans le rapport.

1. Dans l'outil Administrator, cliquez sur **Sécurité > Rapports d'audit**.
2. Dans la liste **Sélectionner le type de rapport**, sélectionnez le rapport **Association de rôles**.
3. Dans la liste **Générer un rapport pour**, sélectionnez **Rôles** et cliquez sur **Atteindre**.
La boîte de dialogue **Sélectionner les rôles** s'affiche. La liste des rôles définis par le système s'affiche séparément de la liste des rôles personnalisés.
4. Dans la liste **Rôles disponibles**, sélectionnez les rôles pour lesquels vous voulez exécuter le rapport.
Utilisez la touche Maj ou Ctrl pour sélectionner plusieurs rôles.
5. Cliquez sur **Ajouter**.
Pour exécuter le rapport pour tous les rôles, ne sélectionnez aucun rôle et cliquez sur **Ajouter tout**.
Les rôles sélectionnés sont placés dans la liste **Rôles sélectionnés**.
6. Dans la liste **Format de sortie du rapport**, sélectionnez le format dans lequel vous voulez afficher le rapport.
Par défaut, les rapports s'affichent à l'écran.
Vous pouvez également exécuter un rapport d'audit dans l'un des formats suivants :
 - Texte. Génère le rapport d'audit sous forme de fichier texte avec les valeurs indiquées dans des colonnes.
 - CSV. Génère le rapport d'audit sous forme de fichier texte avec les valeurs séparées par des virgules.
 - PDF. Génère le rapport d'audit au format .pdf. Vous devez installer Acrobat Reader pour afficher le rapport.
7. Cliquez sur **Générer le rapport**.

ANNEXE A

Privilèges et autorisations de ligne de commande

Cette annexe comprend les rubriques suivantes :

- [Commandes infacmd as, 218](#)
- [commandes infacmd cluster, 219](#)
- [Commandes infacmd dis , 220](#)
- [Commandes infacmd dp, 222](#)
- [commandes infacmd es, 222](#)
- [Commandes infacmd ipc, 222](#)
- [Commandes infacmd isp, 223](#)
- [Commandes infacmd mas, 233](#)
- [Commandes infacmd mi, 233](#)
- [Commandes infacmd mrs, 233](#)
- [Commandes infacmd ms, 236](#)
- [Commandes infacmd tools, 236](#)
- [Commandes infacmd ps, 236](#)
- [Commandes infacmd pwx, 237](#)
- [Commandes infacmd rms, 238](#)
- [Commandes infacmd rtm, 239](#)
- [Commandes infacmd sch, 239](#)
- [Commandes infacmd sql, 240](#)
- [Commandes infacmd wfs, 241](#)
- [Commandes pmcmd, 241](#)
- [Commandes pmrep, 244](#)

Commandes infacmd as

Pour exécuter les commandes *infacmd as*, les utilisateurs doivent avoir l'un des ensembles de privilèges du domaine répertorié, des privilèges du service Analyst et des autorisations d'objet de domaine.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd as* :

Commande <i>infacmd as</i>	Groupe de privilèges	Nom du privilège	Autorisation pour...
CreateAuditTables	Administration de domaine	Gérer le service	Domaine ou nœud d'exécution du service Analyst
CreateService	Administration de domaine	Gérer le service	Domaine ou nœud d'exécution du service Analyst
DeleteAuditTables	Administration de domaine	Gérer le service	Domaine ou nœud d'exécution du service Analyst
ListServiceOptions	-	-	Service Analyst
ListServiceProcessOptions	-	-	Service Analyst
UpdateServiceOptions	Administration de domaine	Gérer le service	Domaine ou nœud d'exécution du service Analyst
UpdateServiceProcessOptions	Administration de domaine	Gérer le service	Domaine ou nœud d'exécution du service Analyst

commandes *infacmd cluster*

Pour exécuter les commandes *infacmd cluster*, les utilisateurs doivent disposer de l'un des ensembles répertoriés de privilèges de domaine et d'autorisations de configuration de grappe.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd cluster* :

Commande <i>infacmd cluster</i>	Groupe de privilèges	Nom du privilège	Autorisation pour...
clearConfigurationProperties	Administration de domaine	Gérer les connexions	Écrire dans la configuration de grappe
createConfiguration	Administration de domaine	Gérer les connexions	Écrire dans les configurations de grappe
deleteConfiguration	Administration de domaine	Gérer les connexions	Écrire dans les configurations de grappe
exportConfiguration avec des propriétés sensibles	-	-	Écrire dans la configuration de grappe

Commande infacmd cluster	Groupe de privilèges	Nom du privilège	Autorisation pour...
exportConfiguration sans propriétés sensibles	-	-	Lire les configurations de grappe
listAssociatedConnections	-	-	-
listConfigurations	-	-	-
listConfigurationGroupPermissions	-	-	-
listConfigurationProperties	-	-	Lire les configurations de grappe
listConfigurationSets	-	-	Lire les configurations de grappe
listConfigurationUserPermissions	-	-	-
refreshConfiguration	Administration de domaine	Gérer les connexions	Écrire dans les configurations de grappe
setConfigurationPermissions	-	-	Octroyer des autorisations sur la configuration de grappe
setConfigurationProperties	Administration de domaine	Gérer les connexions	Écrire dans les configurations de grappe

Commandes infacmd dis

Pour exécuter les commandes *infacmd dis*, les utilisateurs doivent avoir l'un des ensembles de privilèges du domaine répertorié, des privilèges de service d'intégration de données et des autorisations d'objet de domaine.

Le tableau suivant répertorie les privilèges et les autorisations nécessaires pour les commandes *infacmd dis* :

Commande infacmd dis	Groupe de privilèges	Nom du privilège	Autorisation pour...
BackupApplication	Administration des applications	Gérer les applications	Application
CancelDataObjectCacheRefresh	-	-	-
CreateService	Administration de domaine	Gérer les services	Domaine ou nœud d'exécution du service d'intégration de données.

Commande infacmd dis	Groupe de privilèges	Nom du privilège	Autorisation pour...
DeployApplication	Administration des applications	Gérer les applications	Application
ListApplicationObjects	-	-	-
ListApplications	-	-	-
ListComputeOptions	Administration de domaine	Gérer les services	Service d'intégration de données
ListDataObjectOptions	-	-	-
ListServiceOptions	Administration de domaine	Gérer les services	Service d'intégration de données
ListServiceProcessOptions	Administration de domaine	Gérer les services	Service d'intégration de données
PurgeDataObjectCache	-	-	-
RefreshDataObjectCache	-	-	-
RenameApplication	Administration des applications	Gérer les applications	Application
RestoreApplication	Administration des applications	Gérer les applications	Application
StartApplication	Administration des applications	Gérer les applications	Application
StopApplication	Administration des applications	Gérer les applications	Application
stopBlazeService	Administration des applications	Gérer les applications	Application
UndeployApplication	Administration des applications	Gérer les applications	Application
UpdateApplication	Administration des applications	Gérer les applications	Application
UpdateApplicationOptions	Administration des applications	Gérer les applications	Application
UpdateDataObjectOptions	Administration des applications	Gérer les applications	-
UpdateComputeOptions	Administration de domaine	Gérer les services	Service d'intégration de données

Commande infacmd dis	Groupe de privilèges	Nom du privilège	Autorisation pour...
UpdateServiceOptions	Administration de domaine	Gérer les services	Service d'intégration de données
UpdateServiceProcessOptions	Administration de domaine	Gérer les services	Service d'intégration de données

Commandes infacmd dp

Les utilisateurs doivent être natifs ou recevoir le rôle d'administrateur pour exécuter les commandes infacmd dp suivantes :

- startSparkJobServer
- stopSparkJobServer

commandes infacmd es

Les utilisateurs doivent avoir le rôle d'administrateur sur le domaine afin d'exécuter les commandes infacmd es suivantes :

- ListServiceOptions
- UpdateServiceOptions
- UpdateSMTPOptions

Commandes infacmd ipc

Pour exécuter les commandes *infacmd ipc*, les utilisateurs doivent posséder l'une des autorisations d'objet du référentiel modèle répertoriées.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd ipc* :

Commande infacmd ipc	Groupe de privilèges	Nom du privilège	Autorisation pour...
ExportToPC	-	-	Lire le dossier qui crée les tables de référence à exporter
genReuseReportFromPC	Outils	Accéder à Repository Manager	-

Commandes infacmd isp

Pour exécuter les commandes *infacmd isp*, les utilisateurs doivent avoir l'un des ensembles indiqués de privilèges du domaine, privilèges de service, autorisations d'objet de domaine et autorisations de connexion.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd isp* :

Commande infacmd isp	Groupe de privilèges	Nom du privilège	Autorisation pour
AddAlertUser (pour les autres utilisateurs)	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
AddAlertUser (pour votre compte utilisateur)	-	-	-
AddConnectionPermissions	-	-	Accorder sur connexion
AddDomainLink*	-	-	-
AddDomainNode	Administration de domaine	Gérer les nœuds et les grilles	Domaine et nœud
AddGroupPrivilege	Administration de la sécurité	Attribuer des privilèges et des rôles	Domaine, Service Metadata Manager, Service de référentiel modèle ou Service de référentiel PowerCenter.
AddLicense	Administration de domaine	Gérer les services	Domaine ou dossier parent
AddNodeResource	Administration de domaine	Gérer les nœuds et les grilles	Nœud
AddRolePrivilege	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
AddServiceLevel*	-	-	-
AddUserToGroup	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
AssignGroupPermission (sur les services d'application ou les objets de licence)	Administration de domaine	Gérer les services	Service d'application ou objet de licence
AssignGroupPermission (sur le domaine)*	-	-	-
AssignGroupPermission (sur les dossiers)	Administration de domaine	Gérer les dossiers de domaine	Dossier
AssignGroupPermission (sur les nœuds et les grilles)	Administration de domaine	Gérer les nœuds et les grilles	Nœud ou grille

Commande infacmd isp	Groupe de privilèges	Nom du privilège	Autorisation pour
AssignGroupPermission (sur les profils de système d'exploitation)*	-	-	-
AssignISTOMMSERVICE	Administration de domaine	Gérer les services	Service Metadata Manager
AssignLicense	Administration de domaine	Gérer les services	Objet de licence et service d'application
AssignRSToWSHubService	Administration de domaine	Gérer les services	Service de référentiel PowerCenter et Hub des services Web
AssignRoleToGroup	Administration de la sécurité	Attribuer des privilèges et des rôles	Domaine, Service Metadata Manager, Service de référentiel modèle ou Service de référentiel PowerCenter.
AssignRoleToUser	Administration de la sécurité	Attribuer des privilèges et des rôles	Domaine, Service Metadata Manager, Service de référentiel modèle ou Service de référentiel PowerCenter.
AssignUserPermission (sur des services d'application ou des objets de licence)	Administration de domaine	Gérer les services	Service d'application ou objet de licence
AssignUserPermission (sur un domaine)*	-	-	-
AssignUserPermission (sur des dossiers)	Administration de domaine	Gérer les dossiers de domaine	Dossier
AssignUserPermission (sur des nœuds et des grilles)	Administration de domaine	Gérer les nœuds et les grilles	Nœud ou grille
AssignUserPermission (sur des profils de système d'exploitation)*	-	-	-
AssignUserPrivilege	Administration de la sécurité	Attribuer des privilèges et des rôles	Domaine, Service Metadata Manager, Service de référentiel modèle ou Service de référentiel PowerCenter.
AssignedToLicense	Administration de domaine	Gérer les services	Objet de licence et service d'application
ConvertLogFile	-	-	Service de domaine ou d'application
CreateConnection*	-	-	-

Commande infacmd isp	Groupe de privilèges	Nom du privilège	Autorisation pour
CreateFolder	Administration de domaine	Gérer les dossiers de domaine	Domaine ou dossier parent
CreateGrid	Administration de domaine	Gérer les nœuds et les grilles	Domaine ou dossier parent et nœuds attribués à la grille
CreateGroup	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
CreateIntegrationService	Administration de domaine	Gérer les services	Domaine ou dossier parent, nœud ou grille sur lequel ou laquelle s'exécute le service d'intégration PowerCenter, objet de licence et service de référentiel PowerCenter associé
CreateMMService	Administration de domaine	Gérer les services	Domaine ou dossier parent, nœud sur lequel s'exécute le service Metadata Manager, objet de licence, service d'intégration PowerCenter associé et service de référentiel PowerCenter
CreateOSProfile*	-	-	-
CreateRepositoryService	Administration de domaine	Gérer les services	Domaine ou dossier parent, nœud sur lequel s'exécute le service de référentiel PowerCenter et objet de licence
CreateRole	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
CreateSAPBWSservice	Administration de domaine	Gérer les services	Domaine ou dossier parent, nœud ou grille sur lequel ou laquelle s'exécute le service SAP BW, objet de licence et service d'intégration PowerCenter associé
CreateUser	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-

Commande infacmd isp	Groupe de privilèges	Nom du privilège	Autorisation pour
CreateWSHubService	Administration de domaine	Gérer les services	Domaine ou dossier parent, nœud ou grille sur lequel ou laquelle s'exécute le hub des services Web, objet de licence et service de référentiel PowerCenter associé
DisableNodeResource	Administration de domaine	Gérer les nœuds et les grilles	Nœud
DisableService (pour le service Metadata Manager)	Administration de domaine	Gérer l'exécution des services	Service Metadata Manager, service d'intégration PowerCenter associé et service de référentiel PowerCenter
DisableService (pour tous les autres services d'application)	Administration de domaine	Gérer l'exécution des services	Service d'application
DisableServiceProcess	Administration de domaine	Gérer l'exécution des services	Service d'application
DisableUser	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
EditUser	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
EnableNodeResource	Administration de domaine	Gérer les nœuds et les grilles	Nœud
EnableService (pour le service Metadata Manager)	Administration de domaine	Gérer l'exécution des services	Service Metadata Manager, service d'intégration PowerCenter associé et service de référentiel PowerCenter
EnableService (pour tous les autres services d'application)	Administration de domaine	Gérer l'exécution des services	Service d'application
EnableServiceProcess	Administration de domaine	Gérer l'exécution des services	Service d'application
EnableUser	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
ExportDomainObjects (pour les connexions)	Administration de domaine	Gérer les connexions	Lire sur les connexions

Commande infacmd isp	Groupe de privilèges	Nom du privilège	Autorisation pour
ExportDomainObjects (pour les utilisateurs, groupes et rôles)	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
ExportUsersAndGroups	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
GetFolderInfo	-	-	Dossier
GetLastError	-	-	Service d'application
GetLog	-	-	Service de domaine ou d'application
GetNodeName	-	-	Nœud
GetServiceOption	-	-	Service d'application
GetServiceProcessOption	-	-	Service d'application
GetServiceProcessStatus	-	-	Service d'application
GetServiceStatus	-	-	Service d'application
GetSessionLog	Objets d'exécution	Surveiller	Lire dans le dossier du référentiel
GetWorkflowLog	Objets d'exécution	Surveiller	Lire dans le dossier du référentiel
Aide	-	-	-
ImportDomainObjects (pour les connexions)	Administration de domaine	Gérer les connexions	Écrire sur les connexions
ImportDomainObjects (pour les utilisateurs, groupes et rôles)	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
ImportUsersAndGroups	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
ListAlertUsers	-	-	Domaine
ListAllGroups	-	-	-
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	Lire sur la connexion

Commande infacmd isp	Groupe de privilèges	Nom du privilège	Autorisation pour
ListConnectionPermissions	-	-	-
ListConnectionPermissions par groupe	-	-	-
ListConnectionPermissions par utilisateur	-	-	-
ListConnections	-	-	-
ListDomainLinks	-	-	Domaine
ListDomainOptions	-	-	Domaine
ListFolders	-	-	Dossiers
ListGridNodes	-	-	-
ListGroupPermissions	-	-	-
ListGroupPrivilege	Administration de la sécurité	Attribuer des privilèges et des rôles	Domaine, Service Metadata Manager, Service de référentiel modèle ou Service de référentiel PowerCenter.
ListGroupsForUser	-	-	Domaine
ListLDAPConnectivity	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
ListLicenses	-	-	Objets de licence
ListNodeOptions	-	-	Nœud
ListNodeResources	-	-	Nœud
ListNodes	-	-	-
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	Domaine
ListRolePrivileges	-	-	-
ListSMTPOptions	-	-	Domaine
ListSecurityDomains	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
ListServiceLevels	-	-	Domaine
ListServiceNodes	-	-	Service d'application

Commande infacmd isp	Groupe de privilèges	Nom du privilège	Autorisation pour
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListUserPermissions	-	-	-
ListUserPrivilege	Administration de la sécurité	Attribuer des privilèges et des rôles	Domaine, Service Metadata Manager, Service de référentiel modèle ou Service de référentiel PowerCenter.
MoveFolder	Administration de domaine	Gérer les dossiers de domaine	Dossiers d'origine et de destination
MoveObject (pour les services d'application ou objets de licence)	Administration de domaine	Gérer les services	Dossiers d'origine et de destination
MoveObject (pour les nœuds et grilles)	Administration de domaine	Gérer les nœuds et les grilles	Dossiers d'origine et de destination
Ping	-	-	-
PurgeLog*	-	-	-
RemoveAlertUser (pour les autres utilisateurs)	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
RemoveAlertUser (pour votre compte utilisateur)	-	-	-
RemoveConnection	-	-	Écrire sur la connexion
RemoveConnectionPermissions	-	-	Accorder sur connexion
RemoveDomainLink*	-	-	-
RemoveFolder	Administration de domaine	Gérer les dossiers de domaine	Domaine ou dossier parent et dossier en cours de suppression
RemoveGrid	Administration de domaine	Gérer les nœuds et les grilles	Domaine ou dossier parent et grille
RemoveGroup	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
RemoveGroupPrivilege	Administration de la sécurité	Attribuer des privilèges et des rôles	Domaine, Service Metadata Manager, Service de référentiel modèle ou Service de référentiel PowerCenter.

Commande infacmd isp	Groupe de privilèges	Nom du privilège	Autorisation pour
RemoveLicense	Administration de domaine	Gérer les services	Domaine ou dossier parent et objet de licence
RemoveNode	Administration de domaine	Gérer les nœuds et les grilles	Domaine ou dossier parent et nœud
RemoveNodeResource	Administration de domaine	Gérer les nœuds et les grilles	Nœud
RemoveOSProfile*	-	-	-
RemoveRole	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
RemoveRolePrivilege	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
RemoveService	Administration de domaine	Gérer les services	Domaine ou dossier parent et service d'application
RemoveServiceLevel*	-	-	-
RemoveUser	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
RemoveUserFromGroup	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
RemoveUserPrivilege	Administration de la sécurité	Attribuer des privilèges et des rôles	Domaine, Service Metadata Manager, Service de référentiel modèle ou Service de référentiel PowerCenter.
RenameConnection	-	-	Écrire sur la connexion
ResetPassword (pour les autres utilisateurs)	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
ResetPassword (pour votre compte utilisateur)	-	-	-
RunCPUProfile	Administration de domaine	Gérer les nœuds et les grilles	Nœud
SetConnectionPermission	-	-	Accorder sur connexion

Commande infacmd isp	Groupe de privilèges	Nom du privilège	Autorisation pour
SetLDAPConnectivity	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	-
SetRepositoryLDAPConfiguration	-	-	Domaine
ShowLicense	-	-	Objet de licence
ShutdownNode	Administration de domaine	Gérer les nœuds et les grilles	Nœud
SwitchToGatewayNode*	-	-	-
SwitchToWorkerNode*	-	-	-
UnAssignISMMService	Administration de domaine	Gérer les services	Service d'intégration PowerCenter et service Metadata Manager
UnAssignRoleFromGroup	Administration de la sécurité	Attribuer des privilèges et des rôles	Domaine, Service Metadata Manager, Service de référentiel modèle ou Service de référentiel PowerCenter.
UnAssignRoleFromUser	Administration de la sécurité	Attribuer des privilèges et des rôles	Domaine, Service Metadata Manager, Service de référentiel modèle ou Service de référentiel PowerCenter.
UnassignLicense	Administration de domaine	Gérer les services	Objet de licence et service d'application
UnassignRSWSHubService	Administration de domaine	Gérer les services	Service de référentiel PowerCenter et Hub des services Web
UnassociateDomainNode	Administration de domaine	Gérer les nœuds et les grilles	Nœud
UpdateConnection	-	-	Écrire sur la connexion
UpdateDomainOptions*	-	-	-
UpdateFolder	Administration de domaine	Gérer les dossiers de domaine	Dossier
UpdateGatewayInfo*	-	-	-
UpdateGrid	Administration de domaine	Gérer les nœuds et les grilles	Grille et nœuds
UpdateIntegrationService	Administration de domaine	Gérer les services	Service d'intégration PowerCenter

Commande infacmd isp	Groupe de privilèges	Nom du privilège	Autorisation pour
UpdateLicense	Administration de domaine	Gérer les services	Objet de licence
UpdateMMService	Administration de domaine	Gérer les services	Service Metadata Manager
UpdateNodeOptions	Administration de domaine	Gérer les nœuds et les grilles	Nœud
UpdateNodeRole	Administration de domaine	Gérer les nœuds et les grilles	Nœud
UpdateOSProfile	Administration de la sécurité	Gérer les utilisateurs, les groupes et les rôles	Profil de système d'exploitation
UpdateRepositoryService	Administration de domaine	Gérer les services	Service de référentiel PowerCenter
UpdateSAPBWService	Administration de domaine	Gérer les services	Service SAP BW
UpdateSMTPOptions*	-	-	-
UpdateServiceLevel*	-	-	-
UpdateServiceProcess	Administration de domaine	Gérer les services	Service d'intégration PowerCenter Chaque nœud ajouté au service d'intégration PowerCenter
UpdateWSHubService	Administration de domaine	Gérer les services	Hub des services Web
generateHadoopConnectionFromHiveConnection	-	-	-
listMonitoringOptions	Surveillance	Configuration de surveillance	Domaine
purgeMonitoringData	Surveillance	Configuration de surveillance	Domaine
updateMonitoringOptions	Surveillance	Configuration de surveillance	Domaine
* Pour exécuter ces commandes, les utilisateurs doivent se voir attribuer le rôle Administrateur pour le domaine.			

Commandes infacmd mas

Pour exécuter les commandes *infacmd mas*, les utilisateurs doivent avoir l'un des ensembles répertoriés de privilèges du domaine, de privilèges de service d'accès aux métadonnées et d'autorisations d'objet de domaine.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd mas* :

Commande infacmd dis	Groupe de privilèges	Nom du privilège	Autorisation pour...
CreateService	Administration de domaine	Gérer les services	Domaine ou nœud d'exécution du service d'accès aux métadonnées
ListServiceOptions	Administration de domaine	Gérer les services	Service d'accès aux métadonnées
ListServiceProcessOptions	Administration de domaine	Gérer les services	Service d'accès aux métadonnées
UpdateServiceOptions	Administration de domaine	Gérer les services	Service d'accès aux métadonnées
UpdateServiceProcessOptions	Administration de domaine	Gérer les services	Service d'accès aux métadonnées

Commandes infacmd mi

Le rôle Administrateur doit être attribué aux utilisateurs dans le service d'ingestion de masse pour exécuter les commandes *infacmd mi* suivantes :

- clearSamlConfig
- updateSamlConfig

Commandes infacmd mrs

Pour exécuter les commandes *infacmd mrs*, les utilisateurs doivent avoir l'un des ensembles indiqués de privilèges du Service de Référentiel Modèle et les autorisations des objets de référentiel modèle.

Les utilisateurs peuvent exécuter les commandes suivantes qui sont associées à des opérations de verrouillage et de déverrouillage sur les objets qui leur appartiennent. L'exécution des commandes sur des objets appartenant à d'autres utilisateurs requiert le privilège Gérer le développement basé sur l'équipe :

- CheckInObject
- ListCheckedOutObjects
- ListLockedObjects
- UndoCheckout

- UnlockObject

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd mrs* :

Commande infacmd mrs	Groupe de privilèges	Nom du privilège	Autorisation pour...
BackupContents	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service de référentiel modèle est exécuté
CheckInObject	Administration de domaine	Gérer le développement basé sur l'équipe	Service de référentiel modèle
CreateContents	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service de référentiel modèle est exécuté
CreateFolder	Administration de domaine	Pour l'outil Developer tool : - Accès à Developer Pour l'outil Analyst tool : - Accéder à Analyst - Accéder à l'espace de travail Découverte	Service de référentiel modèle
CreateProject	Administration de domaine	Création, modification et suppression de projets	Service de référentiel modèle
CreateService	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service de référentiel modèle est exécuté
DeleteContents	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service de référentiel modèle est exécuté
DeleteFolder	Administration de domaine	Pour l'outil Developer tool : - Accès à Developer Pour l'outil Analyst tool : - Accéder à Analyst - Accéder à l'espace de travail Découverte	Service de référentiel modèle
DeleteProject	Administration de domaine	Création, modification et suppression de projets	Service de référentiel modèle
ListBackupFiles	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service de référentiel modèle est exécuté
ListCheckedOutObjects	Administration de domaine	Gérer le développement basé sur l'équipe	Service de référentiel modèle

Commande infacmd mrs	Groupe de privilèges	Nom du privilège	Autorisation pour...
ListFolders	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service de référentiel modèle est exécuté
ListLockedObjects	Administration de domaine	Gérer le développement basé sur l'équipe	Service de référentiel modèle
ListProjects	Administration des domaines	Pour l'outil Developer tool : - Accès à Developer Pour l'outil Analyst tool : - Accéder à Analyst - Accéder à l'espace de travail Découverte	Domaine ou nœud sur lequel le service de référentiel modèle est exécuté
ListServiceOptions	-	-	Service de référentiel modèle
ListServiceProcessOptions	-	-	Service de référentiel modèle
PopulateVCS	Administration de domaine	Gérer le développement basé sur l'équipe	Service de référentiel modèle
ReassignCheckedOutObject	Administration de domaine	Gérer le développement basé sur l'équipe	Service de référentiel modèle
RebuildDependencyGraph	-	-	Service de référentiel modèle
RenameFolder	Administration de domaine	Pour l'outil Developer tool : - Accès à Developer Pour l'outil Analyst tool : - Accéder à Analyst - Accéder à l'espace de travail Découverte	Service de référentiel modèle
RestoreContents	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service de référentiel modèle est exécuté
UndoCheckout	Administration de domaine	Gérer le développement basé sur l'équipe	Service de référentiel modèle
UnlockObject	Administration de domaine	Gérer le développement basé sur l'équipe	Service de référentiel modèle
UpdateServiceOptions	Administration de domaine	Gérer le service	Service de référentiel modèle
UpdateServiceProcessOptions	Administration de domaine	Gérer le service	Service de référentiel modèle
UpgradeContents	Administration du service de référentiel modèle	Gérer le service	Service de référentiel modèle

Commandes infacmd ms

Pour exécuter les commandes *infacmd ms*, les utilisateurs doivent avoir l'un des ensembles répertoriés d'autorisations d'objet de domaine.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd ms* :

Commande infacmd ms	Groupe de privilèges	Nom du privilège	Autorisation pour...
deleteMappingPersistedOutputs	-	-	Exécuter dans l'application
getRequestLog	-	-	-
listMappingParams	-	-	-
listMappingPersistedOutputs	-	-	Afficher dans l'application
listMappings	-	-	-
runMapping	-	-	Exécuter sur les objets de connexion utilisés par le mappage

Commandes infacmd tools

Pour exécuter les commandes *infacmd tools*, les utilisateurs doivent posséder l'une des autorisations d'objet du référentiel modèle répertoriées.

Le tableau suivant répertorie les autorisations nécessaires pour les commandes *infacmd tools* :

Commande infacmd tools	Groupe de privilèges	Nom du privilège	Autorisation pour...
ExportObjects	-	-	Lire dans le projet
ImportObjects	-	-	Écrire dans le projet

Commandes infacmd ps

Pour exécuter les commandes *infacmd ps*, les utilisateurs doivent avoir l'un des ensembles répertoriés de privilèges de profilage et les autorisations d'objets de domaine.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd ps* :

Commande <i>infacmd ps</i>	Groupe de privilèges	Nom du privilège	Autorisation pour...
CreateWH	-	-	-
DropWH	-	-	-
Exécuter	-	-	Lire dans le projet Exécuter sur l'objet de connexion de source
Liste	-	-	Lire dans le projet
Purger	-	-	Lire et écrire dans le projet

Commandes *infacmd pwx*

Pour exécuter les commandes *infacmd pwx*, l'utilisateur doit avoir l'un des ensembles répertoriés d'autorisations et de privilèges du service d'application PowerExchange.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd pwx* :

Commande <i>infacmd pwx</i>	Groupe de privilèges	Nom du privilège	Autorisation pour...
CloseForceListener	Commandes de gestion	closeforce	-
CloseListener	Commandes de gestion	close	-
CondenseLogger	Commandes de gestion	condense	-
CreateListenerService	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service d'application PowerExchange est exécuté
CreateLoggerService	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service d'application PowerExchange est exécuté
DisplayAllLogger	Commandes d'information	displayall	-
DisplayCPULogger	Commandes d'information	displaycpu	-
DisplayEventsLogger	Commandes d'information	displayevents	-

Commande infacmd pwx	Groupe de privilèges	Nom du privilège	Autorisation pour...
DisplayMemoryLogger	Commandes d'information	displaymemory	-
DisplayRecordsLogger	Commandes d'information	displayrecords	-
DisplayStatusLogger	Commandes d'information	displaystatus	-
FileSwitchLogger	Commandes de gestion	fileswitch	-
ListTaskListener	Commandes d'information	listtask	-
ShutDownLogger	Commandes de gestion	shutdown	-
StopTaskListener	Commandes de gestion	stoptask	-
UpdateListenerService	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service d'application PowerExchange est exécuté
UpdateLoggerService	Administration de domaine	Gérer le service	Domaine ou nœud sur lequel le service d'application PowerExchange est exécuté

Commandes infacmd rms

Pour exécuter les commandes *infacmd rms*, les utilisateurs doivent avoir l'un des ensembles répertoriés d'autorisations et de privilèges de domaine.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd rms* :

commande infacmd rms	Groupe de privilèges	Nom du privilège	Autorisation pour
ListComputeNodeAttributes	Administration de domaine	-	Service du gestionnaire de ressource
ListServiceOptions	Administration de domaine	-	Service du gestionnaire de ressource
SetComputeNodeAttributes	Administration de domaine	Gérer les services	Service du gestionnaire de ressource
UpdateServiceOptions	Administration de domaine	Gérer les services	Service du gestionnaire de ressource

Commandes infacmd rtm

Pour exécuter les commandes *infacmd rtm*, les utilisateurs doivent avoir l'un des ensembles indiqués de privilèges de Service de Référentiel Modèle et les autorisations des objets de domaine.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd rtm* :

Commande infacmd rtm	Groupe de privilèges	Nom du privilège	Autorisation pour...
Deployimport	-	-	-
Export	-	-	L'écriture sur le projet contenant les tables de référence à exporter
Importer	-	-	La lecture et l'écriture sur le projet dans lequel les tables de référence sont importées

Commandes infacmd sch

Pour exécuter les commandes *infacmd sch*, les utilisateurs doivent avoir l'un des ensembles répertoriés d'autorisations et de privilèges.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd sch* :

commande infacmd sch	Groupe de privilèges	Nom du privilège	Autorisation pour
CreateSchedule	Privilèges du planificateur	Créer une planification	Service de planificateur
DeleteSchedule	Privilèges du planificateur	Supprimer une planification	Service de planificateur
ListSchedule	Privilèges du planificateur	Afficher les planifications	Service de planificateur
ListServiceOptions	Privilèges de domaine	Gérer les services	Service de planificateur
ListServiceProcessOptions	Privilèges de domaine	Gérer les services	Service de planificateur
PauseAll	Privilèges du planificateur	Modifier une planification	Service de planificateur
PauseSchedule	Privilèges du planificateur	Modifier une planification	Service de planificateur
ResumeAll	Privilèges du planificateur	Modifier une planification	Service de planificateur
ResumeSchedule	Privilèges du planificateur	Modifier une planification	Service de planificateur
UpdateSchedule	Privilèges du planificateur	Modifier une planification	Service de planificateur
UpdateService	Privilèges de domaine	Gérer les services	Service de planificateur

commande infacmd sch	Groupe de privilèges	Nom du privilège	Autorisation pour
UpdateServiceProcess	Privilèges de domaine	Gérer les services	Service de planificateur
Mettre à niveau	Privilèges de domaine	Gérer les services	Service de planificateur

Commandes infacmd sql

Pour exécuter les commandes *infacmd sql*, les utilisateurs doivent avoir l'un des ensembles indiqués de privilèges du domaine, les Data Integration Service et les autorisations des objets du domaine.

Le tableau suivant répertorie les privilèges et autorisations nécessaires pour les commandes *infacmd sql* :

Commande infacmd sql	Groupe de privilèges	Nom du privilège	Autorisation pour...
ExecuteSQL	-	-	Selon les objets auxquels vous souhaitez accéder dans votre instruction SQL
ListColumnPermissions	-	-	-
ListSQLDataServiceOptions	-	-	-
ListSQLDataServicePermissions	-	-	-
ListSQLDataServices	-	-	-
ListStoredProcedurePermissions	-	-	-
ListTableOptions	-	-	-
ListTablePermissions	-	-	-
PurgeTableCache	-	-	-
RefreshTableCache	-	-	-
RenameSQLDataService	Administration des applications	Gérer les applications	-
SetColumnPermissions	-	-	Accorder pour l'objet
SetSQLDataServicePermissions	-	-	Accorder pour l'objet
SetStoredProcedurePermissions	-	-	Accorder pour l'objet
SetTablePermissions	-	-	Accorder pour l'objet
StartSQLDataService	Administration des applications	Gérer les applications	-

Commande infacmd sql	Groupe de privilèges	Nom du privilège	Autorisation pour...
StopSQLDataService	Administration des applications	Gérer les applications	-
UpdateColumnOptions	Administration des applications	Gérer les applications	-
UpdateSQLDataServiceOptions	Administration des applications	Gérer les applications	-
UpdateTableOptions	Administration des applications	Gérer les applications	-

Commandes infacmd wfs

Pour exécuter des commandes infacmd wfs, les utilisateurs ne requièrent aucun privilège ni autorisation.

Commandes pmcmd

Pour exécuter les commandes *pmcmd*, les utilisateurs doivent avoir les ensembles indiqués de privilèges du PowerCenter Repository Service et les autorisations des objets du référentiel PowerCenter.

Lorsque le PowerCenter Integration Service est exécuté en mode sans échec, l'utilisateur doit avoir le rôle Administrateur pour que le PowerCenter Repository Service associé exécute les commandes suivantes :

- aborttask
- abortworkflow
- getrunningsessionsdetails
- getservicedetails
- getsessionstatistics
- gettaskdetails
- getworkflowdetails
- recoverworkflow
- scheduleworkflow
- starttask
- startworkflow
- stoptask
- stopworkflow
- unscheduleworkflow

Le tableau suivant présente les privilèges et autorisations nécessaires pour les commandes *pmcmd* :

Commande <i>pmcmd</i>	Groupe de privilèges	Nom du privilège	Autorisation
aborttask (démarrée par le compte utilisateur)	-	-	Lire et exécuter dans le dossier
aborttask (démarrée par d'autres utilisateurs)	Objets d'exécution	Gérer l'exécution	Lire et exécuter dans le dossier
abortworkflow (démarrée par le compte utilisateur)	-	-	Lire et exécuter dans le dossier
abortworkflow (démarrée par d'autres utilisateurs)	Objets d'exécution	Gérer l'exécution	Lire et exécuter dans le dossier
connect	-	-	-
disconnect	-	-	-
exit	-	-	-
getrunningsessionsdetails	Objets d'exécution	Surveiller	-
getservicedetails	Objets d'exécution	Surveiller	Lire dans le dossier
getserviceproperties	-	-	-
getsessionstatistics	Objets d'exécution	Surveiller	Lire dans le dossier
gettaskdetails	Objets d'exécution	Surveiller	Lire dans le dossier
getworkflowdetails	Objets d'exécution	Surveiller	Lire dans le dossier
help	-	-	-
pingservice	-	-	-
recoverworkflow (démarrée par le compte utilisateur)	Objets d'exécution	Exécuter	Lire et exécuter dans le dossier Lire et exécuter dans l'objet de connexion Autorisation sur le profil du système d'exploitation (si applicable)
recoverworkflow (démarrée par d'autres utilisateurs)	Objets d'exécution	Gérer l'exécution	Lire et exécuter dans le dossier Lire et exécuter dans l'objet de connexion Autorisation sur le profil du système d'exploitation (si applicable)

Commande pmcmd	Groupe de privilèges	Nom du privilège	Autorisation
scheduleworkflow	Objets d'exécution	Gérer l'exécution	Lire et exécuter dans le dossier Lire et exécuter dans l'objet de connexion Autorisation sur le profil du système d'exploitation (si applicable)
setfolder	-	-	Lire dans le dossier
setnowait	-	-	-
setwait	-	-	-
showsettings	-	-	-
starttask	Objets d'exécution	Exécuter	Lire et exécuter dans le dossier Lire et exécuter dans l'objet de connexion Autorisation sur le profil du système d'exploitation (si applicable)
startworkflow	Objets d'exécution	Exécuter	Lire et exécuter dans le dossier Lire et exécuter dans l'objet de connexion Autorisation sur le profil du système d'exploitation (si applicable)
stoptask (démarrée par le compte utilisateur)	-	-	Lire et exécuter dans le dossier
stoptask (démarrée par d'autres utilisateurs)	Objets d'exécution	Gérer l'exécution	Lire et exécuter dans le dossier
stopworkflow (démarrée par le compte utilisateur)	-	-	Lire et exécuter dans le dossier
stopworkflow (démarrée par d'autres utilisateurs)	Objets d'exécution	Gérer l'exécution	Lire et exécuter dans le dossier
unscheduleworkflow	Objets d'exécution	Gérer l'exécution	Lire et exécuter dans le dossier
unsetfolder	-	-	Lire dans le dossier
version	-	-	-
waittask	Objets d'exécution	Surveiller	Lire dans le dossier
waitworkflow	Objets d'exécution	Surveiller	Lire dans le dossier

Commandes pmrep

L'utilisateur doit avoir le privilège Accès au Repository Manager pour exécuter toutes les commandes *pmrep*, à l'exception des commandes suivantes :

- Exécuter
- Créer
- Restaurer
- Mettre à niveau
- Version
- Aide

Pour exécuter les commandes *pmrep*, l'utilisateur doit avoir l'un des ensembles indiqués de privilèges de domaine, les privilèges du PowerCenter Repository Service, les autorisations des objets de domaine, et les autorisations des objets du référentiel PowerCenter.

L'utilisateur doit être le propriétaire de l'objet ou avoir le rôle Administrateur pour le PowerCenter Repository Service pour exécuter les commandes suivantes :

- AssignPermission
- ChangeOwner
- CreateQuery
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- DeleteQuery
- ModifyFolder (pour changer de propriétaire, configurer les autorisations, désigner le dossier comme étant partagé, ou modifier le nom ou la description du dossier)

Le tableau suivant présente les privilèges et autorisations nécessaires pour les commandes *pmrep* :

Commandes pmrep	Groupe de privilèges	Nom du privilège	Autorisation
AddToDeploymentGroup	Objets globaux	Gérer les groupes de déploiement	Lire dans le dossier d'origine Lire et écrire dans le groupe de déploiement
ApplyLabel	-	-	Lire dans le dossier Lire et exécuter dans le libellé
AssignPermission	-	-	-
BackUp	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
ChangeOwner	-	-	-
CheckIn (pour vos propres extractions)	Objets de conception	Créer, modifier et supprimer	Lire et écrire dans le dossier.

Commandes pmrep	Groupe de privilèges	Nom du privilège	Autorisation
CheckIn (pour vos propres extractions)	Sources et cibles	Créer, modifier et supprimer	Lire et écrire dans le dossier.
CheckIn (pour vos propres extractions)	Objets d'exécution	Créer, modifier et supprimer	Lire et écrire dans le dossier.
CheckIn (pour les extractions des autres)	Objets de conception	Gérer les versions	Lire et écrire dans le dossier.
CheckIn (pour les extractions des autres)	Sources et cibles	Gérer les versions	Lire et écrire dans le dossier.
CheckIn (pour les extractions des autres)	Objets d'exécution	Gérer les versions	Lire et écrire dans le dossier.
CleanUp	-	-	-
ClearDeploymentGroup	Objets globaux	Gérer les groupes de déploiement	Lire et écrire dans le groupe de déploiement
Connect	-	-	-
Créer	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
CreateConnection	Objets globaux	Créer des connexions	-
CreateDeploymentGroup	Objets globaux	Gérer les groupes de déploiement	-
CreateFolder	Dossiers	Créer	-
CreateLabel	Objets globaux	Créer des libellés	-
CreateQuery	Objets globaux	Créer des requêtes	-
Supprimer	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-
DeleteObject	Objets de conception	Créer, modifier et supprimer	Lire et écrire dans le dossier.
DeleteObject	Sources et cibles	Créer, modifier et supprimer	Lire et écrire dans le dossier.
DeleteObject	Objets d'exécution	Créer, modifier et supprimer	Lire et écrire dans le dossier.

Commandes pmrep	Groupe de privilèges	Nom du privilège	Autorisation
DeleteQuery	-	-	-
DeployDeploymentGroup	Objets globaux	Gérer les groupes de déploiement	Lire dans le dossier d'origine Lire et écrire dans le dossier de destination Lire et exécuter dans le groupe de déploiement
DeployFolder	Dossiers	Copier dans le référentiel d'origine Créer dans le référentiel de destination	Lire dans le dossier
ExecuteQuery	-	-	Lire et exécuter dans la demande
Exit	-	-	-
FindCheckout	-	-	Lire dans le dossier
GetConnectionDetails	-	-	Lire dans l'objet de connexion
Aide	-	-	-
DétruireConnexionUtilisateur	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
ListConnections	-	-	Lire dans l'objet de connexion
ListObjectDependencies	-	-	Lire dans le dossier
ListObjects	-	-	Lire dans le dossier
ListTablesBySess	-	-	Lire dans le dossier
ListUserConnections	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
ModifyFolder (pour changer de propriétaire, configurer les autorisations, désigner le dossier comme étant partagé, ou modifier le nom ou la description du dossier)	-	-	-
ModifyFolder (pour changer d'état)	Dossiers	Gérer les versions	Lire et écrire dans le dossier.
Notifier	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
ObjectExport	-	-	Lire dans le dossier

Commandes pmrep	Groupe de privilèges	Nom du privilège	Autorisation
ObjectImport	Objets de conception	Créer, modifier et supprimer	Lire et écrire dans le dossier.
ObjectImport	Sources et cibles	Créer, modifier et supprimer	Lire et écrire dans le dossier.
ObjectImport	Objets d'exécution	Créer, modifier et supprimer	Lire et écrire dans le dossier.
PurgeVersion	Objets de conception	Gérer les versions	Lire et écrire dans le dossier. Lire, écrire et exécuter dans la requête si vous indiquez un nom de requête
PurgeVersion	Sources et cibles	Gérer les versions	Lire et écrire dans le dossier. Lire, écrire et exécuter dans la requête si vous indiquez un nom de requête
PurgeVersion	Objets d'exécution	Gérer les versions	Lire et écrire dans le dossier. Lire, écrire et exécuter dans la requête si vous indiquez un nom de requête
PurgeVersion (pour purger les objets au niveau du dossier)	Dossiers	Gérer les versions	Lire et écrire dans le dossier.
PurgeVersion (pour purger les objets au niveau du référentiel)	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
Register	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
RegisterPlugin	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
Restaurer	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
RetourArrièreDeploiement	Objets globaux	Gérer les groupes de déploiement	Lire et écrire dans le dossier de destination
Exécuter	-	-	-
ShowConnectionInfo	-	-	-
SwitchConnection	Objets d'exécution	Créer, modifier et supprimer	Lire et écrire dans le dossier. Lire dans l'objet de connexion
JournalTroncation	Objets d'exécution	Gérer l'exécution	Lire et exécuter dans le dossier
UndoCheckout (pour vos propres extractions)	Objets de conception	Créer, modifier et supprimer	Lire et écrire dans le dossier.

Commandes pmrep	Groupe de privilèges	Nom du privilège	Autorisation
UndoCheckout (pour vos propres extractions)	Sources et cibles	Créer, modifier et supprimer	Lire et écrire dans le dossier.
UndoCheckout (pour vos propres extractions)	Objets d'exécution	Créer, modifier et supprimer	Lire et écrire dans le dossier.
UndoCheckout (pour les extractions des autres)	Objets de conception	Gérer les versions	Lire et écrire dans le dossier.
UndoCheckout (pour les extractions des autres)	Sources et cibles	Gérer les versions	Lire et écrire dans le dossier.
UndoCheckout (pour les extractions des autres)	Objets d'exécution	Gérer les versions	Lire et écrire dans le dossier.
Désinscrire	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
UnregisterPlugin	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
UpdateConnection	-	-	Lire et écrire dans l'objet de connexion
UpdateEmailAddr	Objets d'exécution	Créer, modifier et supprimer	Lire et écrire dans le dossier.
UpdateSeqGenVals	Objets de conception	Créer, modifier et supprimer	Lire et écrire dans le dossier.
UpdateSrcPrefix	Objets d'exécution	Créer, modifier et supprimer	Lire et écrire dans le dossier.
UpdateStatistics	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
UpdateTargPrefix	Objets d'exécution	Créer, modifier et supprimer	Lire et écrire dans le dossier.
Mettre à niveau	Administration de domaine	Gérer les services	Autorisation pour le PowerCenter Repository Service
Valider	Objets de conception	Créer, modifier et supprimer	Lire et écrire dans le dossier.
Valider	Objets d'exécution	Créer, modifier et supprimer	Lire et écrire dans le dossier.
Version	-	-	-

ANNEXE B

Rôles personnalisés

Cette annexe comprend les rubriques suivantes :

- [Rôle personnalisé du service Analyst, 249](#)
- [Rôles personnalisés du service Metadata Manager, 250](#)
- [Rôle personnalisé de l'opérateur, 251](#)
- [Rôles personnalisés du service de référentiel PowerCenter, 252](#)
- [Rôles personnalisés du Test Data Manager, 254](#)

Rôle personnalisé du service Analyst

L'utilisateur de glossaire d'entreprise du service Analyst est un rôle de service Analyst personnalisé.

Le tableau suivant présente les privilèges par défaut attribués au rôle personnalisé d'utilisateur de glossaire d'entreprise du service Analyst :

Groupe de privilèges	Nom du privilège
Accès à l'espace de travail	Espace de travail Glossaire

Rôles personnalisés du service Metadata Manager

Les rôles personnalisés du service Metadata Manager comprennent l'utilisateur avancé Metadata Manager, l'utilisateur de base Metadata Manager et l'utilisateur intermédiaire Metadata Manager

Utilisateur avancé de Metadata Manager

Le tableau suivant présente les privilèges par défaut assignés au rôle personnalisé Utilisateur avancé de Metadata Manager :

Groupe de privilèges	Nom du privilège
Catalogue	<ul style="list-style-type: none">- Partager des raccourcis- Afficher le lignage- Afficher les catalogues apparentés- Afficher les rapports- Afficher les résultats de profil- Afficher le catalogue- Afficher les relations- Gérer les relations- Afficher les commentaires- Publier des commentaires- Supprimer les commentaires- Afficher les liens- Gérer les liens- Afficher le glossaire- Gérer les objets
Charger	<ul style="list-style-type: none">- Afficher la ressource- Charger la ressource- Gérer les planifications.- Purger les métadonnées- Gérer la ressource
Modèle	<ul style="list-style-type: none">- Afficher le modèle- Gérer le modèle- Exporter/Importer des modèles
Sécurité	Gérer les autorisations du catalogue

Utilisateur de base de Metadata Manager

Le tableau suivant présente les privilèges par défaut attribués au rôle personnalisé Utilisateur de base de Metadata Manager :

Groupe de privilèges	Nom du privilège
Catalogue	<ul style="list-style-type: none">- Afficher le lignage- Afficher les catalogues apparentés- Afficher le catalogue- Afficher les relations- Afficher les commentaires- Afficher les liens
Modèle	Afficher le modèle

Utilisateur intermédiaire de Metadata Manager

Le tableau suivant présente les privilèges par défaut attribués au rôle personnalisé Utilisateur intermédiaire de Metadata Manager :

Groupe de privilèges	Nom du privilège
Catalogue	<ul style="list-style-type: none">- Afficher le lignage- Afficher les catalogues apparentés- Afficher les rapports- Afficher les résultats de profil- Afficher le catalogue- Afficher les relations- Afficher les commentaires- Publier des commentaires- Supprimer les commentaires- Afficher les liens- Gérer les liens- Afficher le glossaire
Charger	<ul style="list-style-type: none">- Afficher la ressource- Charger la ressource
Modèle	Afficher le modèle

Rôle personnalisé de l'opérateur

Le rôle personnalisé de l'opérateur inclut les privilèges de gestion, de planification et de surveillance des services d'application.

Le tableau suivant présente les privilèges par défaut attribués au rôle personnalisé de l'opérateur :

Groupe de privilèges	Nom du privilège
Administration des applications	Gérer les applications
Administration de domaine	Gérer l'exécution des services
Administration du service de référentiel modèle	Gérer le développement basé sur l'équipe

Groupe de privilèges	Nom du privilège
Surveillance	<p>Le groupe de privilèges Surveillance comprend les privilèges suivants :</p> <ul style="list-style-type: none"> - Vue : Afficher les tâches d'autres utilisateurs - Vue : Afficher les statistiques - Vue : Afficher les rapports - Accès à la surveillance : accéder à partir de l'outil Analyst tool - Accès à la surveillance : accéder à partir de l'outil Developer tool - Accès à la surveillance : accéder à partir de l'outil Administrator tool - Exécuter des actions sur des tâches <p>Remarque: Dans un domaine qui utilise l'authentification Kerberos, les utilisateurs doivent avoir le rôle d'administrateur pour le service de référentiel modèle qui est configuré pour la surveillance.</p>
Planificateur	<p>Le groupe de privilèges Planificateur comprend les privilèges suivants :</p> <ul style="list-style-type: none"> - Gestion des tâches planifiées : Créer la planification - Gestion des tâches planifiées : Supprimer la planification - Gestion des tâches planifiées : Modifier la planification - Gestion des tâches planifiées : Afficher les planifications
Outils	Accès à Informatica Administrator

Rôles personnalisés du service de référentiel PowerCenter

Les rôles personnalisés du service de référentiel PowerCenter comprennent : Administrateur de connexion PowerCenter, Développeur PowerCenter, Opérateur PowerCenter et Administrateur de dossier de référentiel PowerCenter.

Administrateur de connexion PowerCenter

Le tableau suivant présente les privilèges par défaut assignés au rôle personnalisé Administrateur de connexion PowerCenter :

Groupe de privilèges	Nom du privilège
Outils	Accéder au gestionnaire de flux de travail
Objets globaux	Créer des connexions

Développeur PowerCenter

Le tableau suivant présente les privilèges par défaut attribués au rôle personnalisé Développeur PowerCenter :

Groupe de privilèges	Nom du privilège
Outils	<ul style="list-style-type: none">- Accéder au Concepteur- Accéder au gestionnaire de flux de travail- Accéder au moniteur de flux de travail
Objets de conception	<ul style="list-style-type: none">- Créer, modifier et supprimer- Gérer les versions
Sources et cibles	<ul style="list-style-type: none">- Créer, modifier et supprimer- Gérer les versions
Objets d'exécution	<ul style="list-style-type: none">- Créer, modifier et supprimer- Exécuter- Gérer les versions- Surveiller

Opérateur PowerCenter

Le tableau suivant présente les privilèges par défaut attribués au rôle personnalisé Opérateur PowerCenter :

Groupe de privilèges	Nom du privilège
Outils	Accéder au moniteur de flux de travail
Objets d'exécution	<ul style="list-style-type: none">- Exécuter- Gérer l'exécution- Surveiller

Administrateur de dossier de référentiel PowerCenter

Le tableau suivant présente les privilèges par défaut assignés au rôle personnalisé Administrateur de dossier du référentiel PowerCenter :

Groupe de privilèges	Nom du privilège
Outils	Accéder à Repository Manager
Dossiers	<ul style="list-style-type: none">- Copier- Créer- Gérer les versions
Objets globaux	<ul style="list-style-type: none">- Gérer les groupes de déploiement- Exécuter les groupes de déploiement- Créer des libellés- Créer des requêtes

Rôles personnalisés du Test Data Manager

Les rôles personnalisés du Test Data Manager incluent l'administrateur de données de test, le développeur de données de test, le DBA du projet de données de test, le développeur du projet de données de test, le propriétaire du projet de données de test, le gestionnaire des risques de données de test, le spécialiste de données de test et l'ingénieur de test.

Administrateur de données de test

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé Administrateur de données de test :

Groupe de privilèges	Nom du privilège
Projets	Effectuer l'audit d'un projet
Administration	<ul style="list-style-type: none">- Afficher les connexions- Gérer les connexions- Gérer les préférences

Développeur de données de test

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé Développeur de données de test :

Groupe de privilèges	Nom du privilège
Stratégies	<ul style="list-style-type: none">- Afficher des stratégies- Gérer des stratégies
Domaines de données	<ul style="list-style-type: none">- Afficher des domaines de données- Gérer des domaines de données
Projets	Effectuer l'audit d'un projet

DBA du projet de données de test

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé DBA du projet des données de test :

Groupe de privilèges	Nom du privilège
Projets	<ul style="list-style-type: none">- Afficher un projet- Exécuter un projet- Surveiller un projet- Effectuer l'audit d'un projet
Administration	<ul style="list-style-type: none">- Afficher les connexions- Gérer les connexions

Développeur du projet de données de test

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé Développeur du projet de données de test :

Groupe de privilèges	Nom du privilège
Stratégies	Afficher des stratégies
Domaines de données	Afficher des domaines de données
Projets	<ul style="list-style-type: none">- Afficher un projet- Découvrir un projet- Exécuter un projet- Surveiller un projet- Effectuer l'audit d'un projet- Importer des métadonnées
Masquage des données	<ul style="list-style-type: none">- Afficher le masquage de données- Gérer le masquage de données
Sous-ensemble de données	<ul style="list-style-type: none">- Afficher un sous-ensemble de données- Gérer un sous-ensemble de données
Administration	<ul style="list-style-type: none">- Afficher les connexions- Gérer les connexions

Propriétaire du projet de données de test

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé Propriétaire du projet de données de test :

Groupe de privilèges	Nom du privilège
Stratégies	Afficher des stratégies
Domaines de données	Afficher des domaines de données
Projets	<ul style="list-style-type: none">- Afficher un projet- Gérer un projet- Découvrir un projet- Exécuter un projet- Surveiller un projet- Effectuer l'audit d'un projet- Importer des métadonnées
Masquage des données	<ul style="list-style-type: none">- Afficher le masquage de données- Gérer le masquage de données
Sous-ensemble de données	<ul style="list-style-type: none">- Afficher un sous-ensemble de données- Gérer un sous-ensemble de données
Administration	<ul style="list-style-type: none">- Afficher les connexions- Gérer les connexions

Gestionnaire des risques de données de test

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé Gestionnaire des risques de données de test :

Groupe de privilèges	Nom du privilège
Stratégies	Afficher des stratégies
Domaines de données	Afficher des domaines de données
Projets	Effectuer l'audit d'un projet

Spécialiste de données de test

Le tableau suivant répertorie les privilèges par défaut affectés au rôle personnalisé Spécialiste de données de test :

Groupe de privilèges	Nom du privilège
Stratégies	Afficher des stratégies
Domaines de données	<ul style="list-style-type: none">- Afficher des domaines de données- Gérer des domaines de données
Projets	<ul style="list-style-type: none">- Afficher un projet- Gérer un projet- Découvrir un projet- Exécuter un projet- Surveiller un projet- Effectuer l'audit d'un projet- Importer des métadonnées
Masquage des données	<ul style="list-style-type: none">- Afficher le masquage de données- Gérer le masquage de données
Sous-ensemble de données	<ul style="list-style-type: none">- Afficher un sous-ensemble de données- Gérer un sous-ensemble de données
Administration	<ul style="list-style-type: none">- Afficher les connexions- Gérer les connexions

Ingénieur de test

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé Ingénieur de test :

Groupe de privilèges	Nom du privilège
Projets	<ul style="list-style-type: none">- Afficher un projet- Surveiller un projet

INDEX

A

activité de connexion

affichage [128](#)

Administrateur

rôle [183](#)

administrateur de domaine

description [121](#)

administrateur par défaut

description [121](#)

modification [121](#)

mots de passe, changement [121](#)

administrateurs

client d'application [122](#)

domaine [121](#)

par défaut [121](#)

application

autorisations [200](#)

as

autorisations par commande [218](#)

privilèges par commande [218](#)

authentification

Gestionnaire de service [111](#)

Kerberos [21](#)

LDAP [20](#), [26](#), [111](#)

native [20](#), [111](#)

authentification Kerberos

authentification inter-domaines [36](#)

Authentification Kerberos

comptes de principaux de service [41](#)

description [21](#)

Fichier de format SPN Keytab [46](#)

keytab [43](#)

niveau du nœud [37](#)

niveau du processus [37](#)

nom de principal du service [43](#)

Synchronisation LDAP [60](#)

authentification LDAP

Azure Active Directory [25](#)

certificat SSL auto-signé [31](#)

configuration [26](#)

description [20](#)

groupes imbriqués [31](#)

services d'annuaire [26](#)

services d'annuaire pris en charge [24](#)

Authentification LDAP

description [111](#)

authentification native

description [20](#), [111](#)

authentification unique

configuration [69](#)

description [111](#)

présentation [66](#)

autorisation

Gestionnaire de service [111](#)

Service d'intégration de données [111](#)

autorisation (*a continué*)

Service de référentiel modèle [111](#)

Service de référentiel PowerCenter [111](#)

Service Metadata Manager [111](#)

services d'application [111](#)

autorisation directe

description [192](#)

autorisation effective

description [192](#)

autorisation héritée

description [192](#)

autorisations

application [200](#)

commandes as [218](#)

commandes d'outils [236](#)

commandes de grappe [219](#)

commandes dis [220](#)

commandes es [222](#)

commandes ipc [222](#)

commandes isp [223](#)

commandes mas [233](#)

commandes mrs [233](#)

commandes ms [236](#)

commandes pmcmd [241](#)

commandes pmrep [244](#)

commandes ps [236](#)

commandes pwx [237](#)

commandes rms [238](#)

commandes rtm [239](#)

commandes sch [239](#)

commandes sql [240](#)

Commandes wfs [241](#)

connexions [197](#)

description [191](#)

directes [192](#)

dossiers [193](#)

effectives [192](#)

filtres de recherche [193](#)

flux de travail [200](#)

grilles [193](#)

héritées [192](#)

licences [193](#)

mappage [200](#)

nœuds [193](#)

objets de domaine [193](#)

opération du service Web [207](#)

procédure virtuelle stockée [203](#)

profils de système d'exploitation [193](#), [196](#)

schéma virtuel [203](#)

service de données SQL [203](#)

service Web [207](#)

services d'application [193](#)

table virtuelle [203](#)

types [192](#)

utilisation des privilèges [191](#)

- autorisations de domaine
 - directes [192](#)
 - effectives [192](#)
 - héritées [192](#)

C

- certificat SSL
 - authentification LDAP [31](#)
- cibles
 - privileges [168](#)
- Client PowerCenter
 - administrateur [122](#)
- comptes
 - modification du mot de passe [117](#)
- comptes utilisateur
 - modification du mot de passe [117](#)
- comptes utilisateurs
 - activation [125](#)
 - créés lors de l'installation [121](#)
 - par défaut [121](#)
 - présentation [121](#)
- configuration du client
 - domaine sécurisé [86](#)
- Configurations LDAP
 - suppression [31](#)
- connexions
 - autorisations [197](#)
 - autorisations par défaut [198](#)
 - types d'autorisation [198](#)
- convertUserActivityLog
 - journaux d'activité utilisateur [128](#)
- créer des tables de référence
 - privilege [156](#)

D

- demandes d'objets
 - privileges pour PowerCenter [174](#)
- description du groupe
 - caractères non valides [132](#)
- description utilisateur
 - caractères non valides [123](#)
- dis
 - autorisations par commande [220](#)
 - privileges par commande [220](#)
- domaine
 - administrateur [121](#)
 - privileges [147](#)
 - privileges d'administration [148](#)
 - privileges d'administration de la sécurité [147](#)
 - Rôle Administrateur [183](#)
 - sécurité des utilisateurs [118](#)
 - synchronisation utilisateur [111](#)
 - utilisateurs avec des privileges [188](#)
- domaine de sécurité LDAP
 - description [20, 21](#)
- domaine de sécurité natif
 - description [20](#)
- domaine Informatica
 - autorisations [118](#)
 - privileges [118](#)
 - sécurité des utilisateurs [118](#)
 - utilisateurs, gestion [123](#)
- domaine sécurisé
 - configuration du client [86](#)

- domaines de sécurité
 - LDAP [20, 21](#)
 - native [20](#)
 - suppression de LDAP [31](#)
- dossiers
 - autorisations [193](#)
 - privileges [164](#)

E

- es
 - autorisations par commande [222](#)
 - privileges par commande [222](#)

F

- fichier truststore cacerts [31](#)
- filtres
 - getUserActivityLog [129](#)
- filtres de recherche
 - autorisations [193](#)
- flux de travail
 - autorisations [200](#)
 - autorisations héritées [200](#)
- fournisseur d'identité
 - configuration pour l'authentification unique [70](#)

G

- gestion des comptes
 - présentation [115](#)
- Gestionnaire de service
 - authentification [111](#)
 - authentification unique [111](#)
 - autorisation [111](#)
- getUserActivityLog
 - filtres [129](#)
 - journaux d'activité utilisateur [128](#)
- grappe
 - autorisations par commande [219](#)
 - privileges par commande [219](#)
- grilles
 - autorisations [193](#)
- groupe de privileges Administration de domaine
 - description [148](#)
- Groupe de privileges Administration de la sécurité
 - description [147](#)
- Groupe de privileges Chargement
 - description [160](#)
- groupe de privileges d'administration Cloud
 - domaine [155](#)
- Groupe de privileges des objets globaux
 - description [174](#)
- groupe de privileges Dossiers
 - description [164](#)
- Groupe de privileges du modèle
 - description [161](#)
- Groupe de privileges Objets d'exécution
 - description [170](#)
- groupe de privileges Objets de conception
 - description [166](#)
- groupe de privileges Outils
 - Service de référentiel PowerCenter [163](#)
- Groupe de privileges Outils
 - domaine [154](#)

- Groupe de privilèges Sécurité
 - description [161](#)
- Groupe de privilèges Sources et cibles
 - description [168](#)
- groupe de privilèges Surveillance
 - domaine [153](#)
- groupe Tout le monde
 - description [120](#)
- groupes
 - caractères non valides [132](#)
 - gestion [132](#)
 - groupe parent [132](#)
 - nom valide [132](#)
 - présentation [113](#)
 - privilèges, attribution [186](#)
 - rôles, attribution [186](#)
 - synchronisation [111](#)
 - Tout le monde par défaut [120](#)
- groupes de déploiement
 - privilèges pour PowerCenter [174](#)
- groupes de privilèges
 - administration d'Informatica Cloud [155](#)
 - Administration de domaine [148](#)
 - Administration de la sécurité [147](#)
 - Chargement [160](#)
 - description [146](#)
 - Dossiers [164](#)
 - Modèle [161](#)
 - Objets d'exécution [170](#)
 - Objets de conception [166](#)
 - Objets globaux [174](#)
 - Outils [154](#), [163](#)
 - Parcourir [158](#)
 - Sécurité [161](#)
 - Sources et cibles [168](#)
 - Surveillance [153](#)
- groupes imbriqués
 - authentification LDAP [31](#)
 - service d'annuaire LDAP [31](#)
- groupes LDAP
 - gestion [132](#)
 - importation [26](#)
- groupes natifs
 - ajout [132](#)
 - déplacement vers un autre groupe [133](#)
 - gestion [132](#)
 - modification [132](#)
 - suppression [133](#)
 - utilisateurs, assignation [124](#)
- groupes parents
 - description [132](#)

I

- Informatica Administrator
 - Navigateur [113](#)
 - onglets, affichage [109](#)
 - Page Sécurité [112](#)
 - présentation [109](#)
 - recherche [112](#)
- Informatica Analyst
 - administrateur [122](#)
- Informatica Developer
 - administrateur [122](#)
- ipc
 - autorisations par commande [222](#)
 - privilèges par commande [222](#)

- isp
 - autorisations par commande [223](#)
 - privilèges par commande [223](#)

J

- journaux d'activité utilisateur
 - codes d'activité [129](#)
 - convertUserActivityLog [128](#)
 - formats de sortie [128](#)
 - getUserActivityLog [128](#)

L

- libellés
 - privilèges pour PowerCenter [174](#)
- licences
 - autorisations [193](#)

M

- mappage
 - autorisations [200](#)
 - autorisations héritées [200](#)
- mas
 - autorisations par commande [233](#)
 - privilèges par commande [233](#)
- mémoire système
 - augmentation [127](#)
- Metadata Manager
 - administrateur [122](#)
- Metadata Manager Service
 - privilèges [158](#)
- modification
 - mot de passe du compte utilisateur [117](#)
- modifier les métadonnées de la table de référence
 - privilège [156](#)
- mot de passe
 - modification d'un compte utilisateur [117](#)
- mots de passe
 - changement pour l'administrateur par défaut [121](#)
 - configuration requise [123](#)
 - utilisateurs natifs [123](#)
- mrs
 - autorisations par commande [233](#)
 - privilèges par commande [233](#)
- ms
 - autorisations par commande [236](#)
 - privilèges par commande [236](#)

N

- Navigateur
 - Page Sécurité [113](#)
- noeuds
 - autorisations [193](#)
- nom valide
 - compte utilisateur [123](#)
 - groupes [132](#)

O

- objets d'exécution
 - description [170](#)
 - privilèges [170](#)
- objets de conception
 - description [166](#)
 - privilèges [166](#)
- objets de connexion
 - privilèges pour PowerCenter [174](#)
- objets de domaine
 - autorisations [193](#)
- objets globaux
 - privilèges pour PowerCenter [174](#)
- opération du service Web
 - autorisations [207](#)
- Operator)
 - rôles personnalisés [251](#)
- outils
 - autorisations par commande [236](#)
 - privilèges par commande [236](#)

P

- Page Sécurité
 - Informatica Administrator [112](#)
 - Navigateur [113](#)
- Parcourir les groupes de privilèges
 - description [158](#)
- pmcmd
 - autorisations par commande [241](#)
 - privilèges par commande [241](#)
- pmrep
 - autorisations par commande [244](#)
 - privilèges par commande [244](#)
- PowerCenter Repository Service
 - privilèges [163](#)
- Présentation de l'authentification
 - Kerberos [33](#), [34](#)
- privilèges
 - administration d'Informatica Cloud [155](#)
 - administration de domaine [148](#)
 - administration de la sécurité [147](#)
 - attribution [186](#)
 - cibles [168](#)
 - commandes as [218](#)
 - commandes d'outils [236](#)
 - commandes de grappe [219](#)
 - commandes dis [220](#)
 - commandes es [222](#)
 - commandes ipc [222](#)
 - commandes isp [223](#)
 - commandes mas [233](#)
 - commandes mrs [233](#)
 - commandes ms [236](#)
 - commandes pmcmd [241](#)
 - commandes pmrep [244](#)
 - commandes ps [236](#)
 - commandes pwx [237](#)
 - commandes rms [238](#)
 - commandes rtm [239](#)
 - commandes sch [239](#)
 - commandes sql [240](#)
 - Commandes wfs [241](#)
 - dépannage [188](#)
 - description [145](#)
 - domaine [147](#)

- privilèges (*a continué*)
 - dossiers [164](#)
 - hérités [186](#)
 - Metadata Manager Service [158](#)
 - objets d'exécution [170](#)
 - objets de conception [166](#)
 - Objets globaux PowerCenter [174](#)
 - outils de domaine [154](#)
 - outils du service de référentiel PowerCenter [163](#)
 - PowerCenter Repository Service [163](#)
 - programmes de ligne de commande [218](#)
 - Service Analyst [155](#)
 - Service d'écoute PowerExchange [177](#)
 - Service d'intégration de données [157](#)
 - service de gestion de contenu [156](#)
 - Service de journalisation PowerExchange [177](#)
 - Service de planificateur [178](#)
 - Service de référentiel modèle [161](#)
 - sources [168](#)
 - surveillance [153](#)
 - utilisation des autorisations [191](#)
- Privilèges du service Metadata Manager
 - Groupe de privilèges Chargement [160](#)
 - Groupe de privilèges du modèle [161](#)
 - Groupe de privilèges Sécurité [161](#)
 - Parcourir les groupes de privilèges [158](#)
- privilèges hérités
 - description [186](#)
- procédure virtuelle stockée
 - autorisations [203](#)
 - autorisations héritées [203](#)
- profil de système d'exploitation
 - création [138](#)
 - gestion [133](#)
 - modification [134](#)
 - par défaut [140](#)
 - propriétés, service d'intégration de données [134](#), [136](#)
 - propriétés, service d'intégration PowerCenter [134](#)
 - suppression [141](#)
- profil du système d'exploitation
 - propriétés, Service d'accès aux métadonnées [138](#)
- profils de système d'exploitation
 - autorisations [193](#), [196](#)
 - présentation [115](#)
- programmes de ligne de commande
 - privilèges [218](#)
- ps
 - autorisations par commande [236](#)
 - privilèges par commande [236](#)
- pwx
 - autorisations par commande [237](#)
 - privilèges par commande [237](#)

R

- rapports d'audit
 - description [211](#)
 - pour les groupes [216](#)
 - pour les utilisateurs [215](#), [217](#)
 - présentation [116](#)
- ressource du service Web
 - autorisations [207](#)
- rms
 - autorisations par commande [238](#)
 - privilèges par commande [238](#)
- rôles
 - Administrateur [183](#)

- rôles (*a continué*)
 - attribution [186](#)
 - dépannage [188](#)
 - description [147](#)
 - gestion [183](#)
 - personnalisé [184](#)
 - présentation [114](#)
- rôles définis par le système
 - Administrateur [183](#)
 - attribution à des utilisateurs et à des groupes [186](#)
 - description [183](#)
- rôles personnalisés
 - attribution à des utilisateurs et à des groupes [186](#)
 - création [185](#)
 - description [183](#), [184](#)
 - modification [185](#)
 - Opérateur [251](#)
 - privileges, attribution [185](#)
 - Service Analyst [249](#)
 - Service de référentiel PowerCenter [252](#)
 - Service Metadata Manager [250](#)
 - suppression [186](#)
- rtm
 - autorisations par commande [239](#)
 - privileges par commande [239](#)

S

- SAML (Security Assertion Markup Language)
 - réponse signée [73](#)
- sch
 - autorisations par commande [239](#)
 - privileges par commande [239](#)
- schéma virtuel
 - autorisations [203](#)
 - autorisations héritées [203](#)
- Section Rechercher
 - Informatica Administrator [112](#)
- sécurité
 - autorisations [118](#)
 - mots de passe [123](#)
 - privileges [118](#), [145](#), [147](#)
 - rôles [147](#)
- sécurité au niveau des colonnes
 - restriction des colonnes [206](#)
- Sécurité PowerCenter
 - gestion [112](#)
- sécurité utilisateur
 - description [110](#)
- Security Assertion Markup Language (SAML)
 - activation sur le domaine [70](#)
 - activation sur les nœuds de passerelle [71](#)
 - assertion chiffrée [74](#)
 - assertion, signée ou chiffrée [71](#)
 - prise en charge [66](#)
 - réponse signée [71](#)
 - signature de demande [71](#), [72](#)
- Service Analyst
 - privileges [155](#)
 - rôles personnalisés [249](#)
- service d'annuaire LDAP
 - groupes imbriqués [31](#)
- Service d'écoute PowerExchange
 - privileges [177](#)
- Service d'intégration de données
 - autorisation [111](#)
 - privileges [157](#)

- service de données SQL
 - autorisations [203](#)
 - autorisations héritées [203](#)
 - types d'autorisation [203](#)
- service de gestion de contenu
 - privileges [156](#)
- Service de journalisation PowerExchange
 - privileges [177](#)
- Service de planificateur
 - privileges [178](#)
- Service de référentiel modèle
 - autorisation [111](#)
 - privileges [161](#)
 - synchronisation utilisateur [111](#)
 - utilisateurs avec des privileges [188](#)
- Service de référentiel PowerCenter
 - autorisation [111](#)
 - Rôle Administrateur [183](#)
 - rôles personnalisés [252](#)
 - synchronisation utilisateur [111](#)
 - utilisateurs avec des privileges [188](#)
- Service du gestionnaire de métadonnées
 - utilisateurs avec des privileges [188](#)
- Service Metadata Manager
 - autorisation [111](#)
 - rôles personnalisés [250](#)
 - synchronisation utilisateur [111](#)
- service Web
 - autorisations [207](#)
 - types d'autorisation [207](#)
- services d'application
 - autorisation [111](#)
 - autorisations [193](#)
 - synchronisation utilisateur [111](#)
- sources
 - privileges [168](#)
- sql
 - autorisations par commande [240](#)
 - privileges par commande [240](#)
- suites de chiffres
 - configuration [97](#)
- synchronisation
 - utilisateurs [111](#)
 - utilisateurs LDAP [26](#)

T

- table virtuelle
 - autorisations [203](#)
 - autorisations héritées [203](#)
- Test Data Manager
 - administrateur [122](#)

U

- UpdateColumnOptions
 - substitution des valeurs de colonnes [206](#)
- utilisateurs
 - assignation aux groupes [124](#)
 - caractères non valides [123](#)
 - gestion [123](#)
 - grand nombre d' [127](#)
 - mémoire système [127](#)
 - nom valide [123](#)
 - présentation [114](#)
 - privileges, attribution [186](#)

utilisateurs (*a continué*)

rôles, attribution [186](#)

synchronisation [111](#)

utilisateurs LDAP

activation [125](#)

assignation aux groupes [125](#)

gestion [123](#)

importation [26](#)

utilisateurs natifs

activation [125](#)

ajout [123](#)

assignation aux groupes [124](#)

gestion [123](#)

modification [124](#)

mots de passe [123](#)

suppression [125](#)

utilitaire keytool [31](#)

V

variables d'environnement

INFA_TRUSTSTORE [86](#)

INFA_TRUSTSTORE_PASSWORD [86](#)

W

wfs

autorisations par commande [241](#)

privilèges par commande [241](#)