



Informatica®

9.6.1 HotFix 3

Guide de sécurité

© Copyright Informatica LLC 1993, 2018

Ce logiciel et sa documentation contiennent des informations appartenant à Informatica Corporation, protégées par la loi sur le droit d'auteur et fournies dans le cadre d'un accord de licence prévoyant des restrictions d'utilisation et de divulgation. Toute ingénierie inverse du logiciel est interdite. Il est interdit de reproduire ou transmettre sous quelque forme et par quelque moyen que ce soit (électronique, photocopie, enregistrement ou autre) tout ou partie de ce document sans le consentement préalable d'Informatica Corporation. Ce logiciel peut être protégé par des brevets américains et/ou internationaux, ainsi que par d'autres brevets en attente.

L'utilisation, la duplication ou la divulgation du Logiciel par le gouvernement américain est sujette aux restrictions décrites dans l'accord de licence applicable du logiciel conformément aux documents DFARS 227.7202-1(a) et 227.7702-3(a) (1995), DFARS 252.227-7013⁽¹⁾⁽ⁱⁱ⁾ (OCT 1988), FAR 12.212(a) (1995), FAR 52.227-19 ou FAR 52.227-14 (ALT III) le cas échéant.

Les informations dans ce produit ou cette documentation sont sujettes à modification sans préavis. Si vous rencontrez des problèmes dans ce produit ou la documentation, veuillez nous en informer par écrit.

Informatica, Informatica Platform, Informatica Data Services, PowerCenter, PowerCenterRT, PowerCenter Connect, PowerCenter Data Analyzer, PowerExchange, PowerMart, Metadata Manager, Informatica Data Quality, Informatica Data Explorer, Informatica B2B Data Transformation, Informatica B2B Data Exchange Informatica On Demand, Informatica Identity Resolution, Informatica Application Information Lifecycle Management, Informatica Complex Event Processing, Ultra Messaging et Informatica Master Data Management sont des marques de commerce ou des marques déposées d'Informatica Corporation aux États-Unis et dans d'autres juridictions du monde. Tous les autres noms de société ou de produit peuvent être des marques de commerce ou des marques déposées de leurs détenteurs respectifs.

Des portions de ce logiciel et/ou de la documentation sont sujettes au copyright détenu par des tierces parties, dont Copyright DataDirect Technologies. Tous droits réservés. Copyright © Sun Microsystems. Tous droits réservés. Copyright © RSA Security Inc. Tous droits réservés. Copyright © Ordinal Technology Corp. Tous droits réservés. Copyright © Aandacht c.v. Tous droits réservés. Copyright Genivia, Inc. Tous droits réservés. Copyright Isomorphic Software. Tous droits réservés. Copyright © Meta Integration Technology, Inc. Tous droits réservés. Copyright © Intalio. Tous droits réservés. Copyright © Oracle. Tous droits réservés. Copyright © Adobe Systems Incorporated. Tous droits réservés. Copyright © DataArt, Inc. Tous droits réservés. Copyright © ComponentSource. Tous droits réservés. Copyright © Microsoft Corporation. Tous droits réservés. Copyright © Rogue Wave Software, Inc. Tous droits réservés. Copyright © Teradata Corporation. Tous droits réservés. Copyright © Yahoo! Inc. Tous droits réservés. Copyright © Glyph & Cog, LLC. Tous droits réservés. Copyright © Thinkmap, Inc. Tous droits réservés. Copyright © Clearpace Software Limited. Tous droits réservés. Copyright © Information Builders, Inc. Tous droits réservés. Copyright © OSS Nokalva, Inc. Tous droits réservés. Copyright Edifecs, Inc. Tous droits réservés. Copyright Cleo Communications, Inc. Tous droits réservés. Copyright © International Organization for Standardization 1986. Tous droits réservés. Copyright © ej-technologies GmbH. Tous droits réservés. Copyright © Jaspersoft Corporation. Tous droits réservés. Copyright © International Business Machines Corporation. Tous droits réservés. Copyright © yWorks GmbH. Tous droits réservés. Copyright © Lucent Technologies. Tous droits réservés. Copyright © Université de Toronto. Tous droits réservés. Copyright © Daniel Veillard. Tous droits réservés. Copyright © Unicon, Inc. Copyright IBM Corp. Tous droits réservés. Copyright © MicroQuill Software Publishing, Inc. Tous droits réservés. Copyright © PassMark Software Pty Ltd. Tous droits réservés. Copyright © LogiXML, Inc. Tous droits réservés. Copyright © 2003-2010 Lorenzi Davide. Tous droits réservés. Copyright © Red Hat, Inc. Tous droits réservés. Copyright © The Board of Trustees of the Leland Stanford Junior University. Tous droits réservés. Copyright © EMC Corporation. Tous droits réservés. Copyright © Flexera Software. Tous droits réservés. Copyright © Jinfonet Software. Tous droits réservés. Copyright © Apple Inc. Tous droits réservés. Copyright © Telerik Inc. Tous droits réservés. Copyright © BEA Systems. Tous droits réservés. Copyright © PDFlib GmbH. Tous droits réservés. Copyright © Orientation in Objects GmbH. Tous droits réservés. Copyright © Tanuki Software, Ltd. Tous droits réservés. Copyright © Ricebridge. Tous droits réservés. Copyright © Sencha, Inc. Tous droits réservés. Copyright © Scalable Systems, Inc. Tous droits réservés. Copyright © jQWidgets. Tous droits réservés. Copyright © Tableau Software, Inc. Tous droits réservés. Copyright © MaxMind, Inc. Tous droits réservés. Copyright © TMate Software s.r.o. Tous droits réservés. Copyright © MapR Technologies Inc. Tous droits réservés.

Ce produit inclut des logiciels développés par Apache Software Foundation (<http://www.apache.org/>), et/ou d'autres logiciels sous licence et sous diverses versions Apache License (la « Licence »). Vous pouvez obtenir une copie de ces licences à l'adresse suivante : <http://www.apache.org/licenses/>. Sauf dispositions contraires de la loi en vigueur ou accord écrit, le logiciel distribué sous cette licence est livré « EN L'ÉTAT », SANS GARANTIE NI CONDITION D'AUCUNE SORTE, expresse ou implicite. Se reporter aux Licences pour la langue spécifique régissant les droits et limitations dans le cadre des Licences.

Ce produit inclut des logiciels développés par Mozilla (<http://www.mozilla.org/>), copyright de logiciel The JBoss Group, LLC, tous droits réservés ; copyright de logiciel © 1999-2006 de Bruno Lowagie et Paulo Soares et d'autres logiciels sous licence et sous diverses versions du GNU Lesser General Public License Agreement, accessible sur <http://www.gnu.org/licenses/lgpl.html>. Les matériaux sont fournis gratuitement par Informatica, « en l'état », sans garantie d'aucune sorte, expresse ou implicite, notamment les garanties implicites de conformité légale et d'usage normal.

Le produit inclut les logiciels ACE(TM) et TAO(TM), copyright Douglas C. Schmidt et son groupe de recherche à Washington University, University of California, Irvine, et Vanderbilt University, Copyright (©) 1993-2006, tous droits réservés.

Ce produit inclut des logiciels développés par OpenSSL Project pour une utilisation dans OpenSSL Toolkit (copyright The OpenSSL Project. Tous droits réservés) et la redistribution de ce logiciel est sujette aux termes publiés sur <http://www.openssl.org> et <http://www.openssl.org/source/license.html>.

Ce produit inclut le logiciel Curl, copyright 1996-2013, Daniel Stenberg, <daniel@haxx.se>. Tous Droits Réservés. Les autorisations et limitations concernant ce logiciel sont sujettes aux conditions publiées sur <http://curl.haxx.se/docs/copyright.html>. L'autorisation d'utiliser, copier, modifier et distribuer ce logiciel à toute fin, avec ou sans rémunération, est accordée par les présentes, à la condition que la notification de copyright ci-dessus et cette notification d'autorisation apparaissent dans toutes les copies.

Le produit inclut des logiciels sous copyright 2001-2005 (©) MetaStuff, Ltd. Tous droits réservés. Les autorisations et limitations concernant ce logiciel sont sujettes aux conditions publiées sur <http://www.dom4j.org/license.html>.

Le produit inclut des logiciels sous copyright © 2004-2007, The Dojo Foundation. Tous Droits Réservés. Les autorisations et limitations concernant ce logiciel sont sujettes aux conditions publiées sur <http://dojotoolkit.org/license>.

Ce produit inclut le logiciel ICU sous copyright de International Business Machines Corporation et autres. Tous Droits Réservés. Les autorisations et limitations concernant ce logiciel sont sujettes aux conditions publiées sur <http://source.icu-project.org/repos/icu/icu/trunk/license.html>.

Ce produit inclut des logiciels sous copyright © 1996-2006 Per Bothner. Tous Droits Réservés. Votre droit à utiliser de tels matériels est défini dans la licence qui peut être consultée sur <http://www.gnu.org/software/kawa/Software-License.html>.

Ce produit inclut le logiciel OSSP UUID sous copyright © 2002 Ralf S. Engelschall, copyright © 2002 The OSSP Project Copyright © 2002 Cable & Wireless Deutschland. Les autorisations et limitations concernant ce logiciel sont sujettes aux conditions publiées sur <http://www.opensource.org/licenses/mit-license.php>.

Ce produit inclut des logiciels développés par Boost (<http://www.boost.org/>) ou sous licence de logiciel Boost. Les autorisations et limitations concernant ce logiciel sont sujettes aux conditions publiées sur http://www.boost.org/LICENSE_1_0.txt.

Ce produit inclut des logiciels sous copyright © 1997-2007 University of Cambridge. Les autorisations et limitations concernant ce logiciel sont sujettes aux conditions publiées sur <http://www.pcre.org/license.txt>.

Ce produit inclut des logiciels sous copyright © 2007 The Eclipse Foundation. Tous Droits Réservés. Les autorisations et limitations concernant ce logiciel sont sujettes aux conditions publiées sur <http://www.eclipse.org/org/documents/epl-v10.php> et <http://www.eclipse.org/org/documents/edl-v10.php>.

Ce produit comprend des logiciels sous licence dont les conditions se trouvent aux adresses : <http://www.tcl.tk/software/tcltk/license.html>, <http://www.bosrup.com/web/overlib/?License>, <http://www.stlport.org/doc/license.html>, <http://asm.ow2.org/license.html>, <http://www.cryptix.org/LICENSE.TXT>, <http://hsqldb.org/web/hsqldbLicense.html>, <http://httpunit.sourceforge.net/doc/license.html>, <http://jung.sourceforge.net/license.txt>, http://www.gzip.org/zlib/zlib_license.html, <http://www.openldap.org/software/release/license.html>, <http://www.libssh2.org>, <http://slf4j.org/license.html>, <http://www.sente.ch/software/OpenSourceLicense.html>, <http://fusesource.com/downloads/license-agreements/fuse-message-broker-v-5-3-license-agreement>, <http://antlr.org/license.html>, <http://aopalliance.sourceforge.net/>, <http://www.bouncycastle.org/licence.html>, <http://www.jgraph.com/jgraphdownload.html>, <http://www.jcraft.com/jsch/LICENSE.txt>, http://jotm.objectweb.org/bsd_license.html, <http://www.w3.org/Consortium/Legal/2002/copyright-software-20021231>, <http://www.slf4j.org/license.html>, <http://nanoxml.sourceforge.net/orig/copyright.html>, <http://www.json.org/license.html>, <http://forge.ow2.org/projects/javaxservice/>, <http://www.postgresql.org/about/license.html>, <http://www.sqlite.org/copyright.html>, <http://www.tcl.tk/software/tcltk/license.html>, <http://www.jaxen.org/faq.html>, <http://www.jdom.org/docs/faq.html>, <http://www.slf4j.org/license.html>, <http://www.iodbc.org/dataspace/iodbc/wiki/IODBC/License>, <http://www.keplerproject.org/md5/license.html>, <http://www.toedter.com/en/jcalendar/license.html>, <http://www.edankert.com/bounce/index.html>, <http://www.net-snmp.org/about/license.html>, <http://www.openmdx.org/#FAQ>, http://www.php.net/license/3_01.txt, <http://srp.stanford.edu/license.txt>, <http://www.schneier.com/blowfish.html>, <http://www.jmock.org/license.html>, <http://xsom.java.net>, <http://benalman.com/about/license/>, <https://github.com/CreateJS/EaselJS/blob/master/src/easeljs/display/Bitmap.js>, <http://www.h2database.com/html/license.html#summary>, <http://jsoncpp.sourceforge.net/LICENSE>, <http://jdbc.postgresql.org/license.html>, <http://protobuf.googlecode.com/svn/trunk/src/google/protobuf/descriptor.proto>, <https://github.com/rantav/hector/blob/master/LICENSE>, <http://web.mit.edu/Kerberos/krb5-current/doc/mitK5license.html>, <http://jibx.sourceforge.net/jibx-license.html>, <https://github.com/lyokato/libgeohash/blob/master/LICENSE>, <https://github.com/hjiang/jsonxx/blob/master/LICENSE>, <https://code.google.com/p/lz4/>, <https://github.com/jedisct1/libsodium/blob/master/LICENSE>, <http://one-jar.sourceforge.net/index.php?page=documents&file=license>, <https://github.com/EsotericSoftware/kryo/blob/master/license.txt>, <http://www.scala-lang.org/license.html>, <https://github.com/tinkerpop/blueprints/blob/master/LICENSE.txt>; et <http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html>.

Ce produit inclut un logiciel sous licence Academic Free License (<http://www.opensource.org/licenses/afl-3.0.php>), licence Common Development Distribution License (<http://www.opensource.org/licenses/cddl1.php>) licence Common Public License (<http://www.opensource.org/licenses/cpl1.0.php>), licence Sun Binary Code License Agreement Supplemental License Terms, licence BSD (<http://www.opensource.org/licenses/bsd-license.php>), le nouvelle licence BSD License (<http://opensource.org/licenses/BSD-3-Clause>), la licence MIT (<http://www.opensource.org/licenses/mit-license.php>), la licence Artistic License (<http://www.opensource.org/licenses/artistic-license-1.0>) et la licence publique du développeur initial Version 1.0 (<http://www.firebirdsql.org/en/initial-developer-s-public-license-version-1-0/>).

Ce produit inclut des logiciels sous copyright © 2003-2006 Joe Walnes, 2006-2007 XStream Committers. Tous Droits Réservés. Les autorisations et limitations concernant ce logiciel sont sujettes aux conditions publiées sur <http://xstream.codehaus.org/license.html>. Ce produit inclut des logiciels développés par Indiana University Extreme! Lab. Pour plus d'informations, veuillez vous rendre sur <http://www.extreme.indiana.edu/>.

Ce produit inclut des logiciels sous copyright © 2013 Frank Balluffi et Markus Moeller. Tous droits réservés. Les autorisations et limitations concernant ce logiciel sont sujettes aux conditions de la licence MIT.

Ce logiciel est protégé par les brevets américains 5 794 246 ; 6 014 670 ; 6 016 501 ; 6 029 178 ; 6 032 158 ; 6 035 307 ; 6 044 374 ; 6 092 086 ; 6 208 990 ; 6 339 775 ; 6 640 226 ; 6 789 096 ; 6 823 373 ; 6 850 947 ; 6 895 471 ; 7 117 215 ; 7 162 643 ; 7 243 110 ; 7 254 590 ; 7 281 001 ; 7 421 458 ; 7 496 588 ; 7 523 121 ; 7 584 422 ; 7 676 516 ; 7 720 842 ; 7 721 270 ; 7 774 791 ; 8 065 266 ; 8 150 803 ; 8 166 048 ; 8 166 071 ; 8 200 622 ; 8 224 873 ; 8 271 477 ; 8 327 419 ; 8 386 435 ; 8 392 460 ; 8 453 159 ; 8 458 230 ; 8 707 336 ; 8 886 617 et RE44 478, par des brevets internationaux et d'autres brevets en instance.

EXCLUSION DE RESPONSABILITÉ : Informatica Corporation fournit cette documentation « en l'état », sans garantie d'aucune sorte, explicite ou implicite, notamment les garanties implicites de non-infraction, de conformité légale ou d'usage normal. Informatica Corporation ne garantit pas que ce logiciel et cette documentation sont exempts d'erreurs. Les informations fournies dans ce logiciel ou cette documentation peuvent inclure des inexactitudes techniques ou des erreurs typographiques. Les informations contenues dans ce logiciel et sa documentation sont sujettes à modification à tout moment sans préavis.

AVIS

Ce produit Informatica (le « Logiciel ») inclut certains pilotes (les « Pilotes DataDirect ») de DataDirect Technologies, une société de Progress Software Corporation (« DataDirect ») qui sont sujets aux conditions suivantes :

1. LES PILOTES DATADIRECT SONT FOURNIS « EN L'ÉTAT », SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, NOTAMMENT LES GARANTIES IMPLICITES DE CONFORMITÉ LÉGALE, D'USAGE NORMAL ET DE NON-INFRACTION.
2. DATADIRECT OU SES FOURNISSEURS TIERS NE POURRONT EN AUCUN CAS ÊTRE TENUS RESPONSABLES ENVERS LE CLIENT UTILISATEUR FINAL DE TOUT DOMMAGE DIRECT, ACCESSOIRE, INDIRECT, SPÉCIAL, CONSÉCUTIF OU AUTRE RÉSULTANT DE L'UTILISATION DES PILOTES ODBC, QU'ILS SOIENT INFORMÉS OU NON À L'AVANCE DE LA POSSIBILITÉ DE TELS DOMMAGES. CES LIMITATIONS S'APPLIQUENT À TOUTES LES CAUSES D'ACTION, NOTAMMENT TOUTE INFRACTION AU CONTRAT, INFRACTION À LA GARANTIE, NÉGLIGENCE, RESPONSABILITÉ STRICTE, REPRÉSENTATION INCORRECTE ET AUTRES TORTS.

Date de publication: 2018-05-16

Sommaire

Préface.....	10
Ressources Informatica.	10
Portail Mon support Informatica.	10
Documentation Informatica.	10
Matrices de disponibilité de produit Informatica.	10
Site Web Informatica.	11
Bibliothèque de procédures Informatica.	11
Base de connaissances Informatica.	11
Canal YouTube du support Informatica.	11
Informatica Marketplace.	11
Informatica Velocity.	11
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.	15
Sécurité opérationnelle.	15
Référentiel de configuration du domaine.	16
Domaine de sécurité.	16
 Chapitre 2: Authentification utilisateur.....	 18
Présentation de l'authentification utilisateur.	18
Authentification utilisateur native.	19
Authentification utilisateur LDAP.	19
Authentification Kerberos.	20
 Chapitre 3: Domaines de sécurité LDAP.....	 21
Présentation des domaines de sécurité LDAP.	21
Configuration d'un domaine de sécurité LDAP.	22
Étape 1. Configurer la connexion au serveur LDAP.	22
Étape 2. Configuration d'un domaine de sécurité.	24
Étape 3. Planifier les heures de synchronisation.	26
Utilisation de groupes imbriqués dans le service d'annuaire LDAP.	27
Utilisation d'un certificat SSL auto-signé.	27
Suppression d'un domaine de sécurité LDAP.	28

Chapitre 4: Configuration de l'authentification Kerberos.....	29
Configuration de l'authentification Kerberos.	29
Étape 1. Créer un domaine de l'utilisateur LDAP avec les utilisateurs de Microsoft Active Directory.	30
Étape 2. Migrer des privilèges et autorisations d'utilisateur natif vers un domaine de sécurité LDAP.	30
Étape 3. Définir le fichier de configuration Kerberos.	34
Étape 4. Générer le nom du principal et le format Keytab.	35
Étape 5. Consulter le fichier texte du format SPN et Keytab.	39
Étape 6. Créer des noms de principal du service et des fichiers Keytab.	41
Étape 7. Configurer l'authentification Kerberos pour le domaine.	44
Étape 8. Mise à jour des nœuds dans le domaine.	46
Étape 9. Mettez à jour les machines du client.	47
Étape 10. Démarrage du domaine Informatica.	47
Après la configuration de l'authentification Kerberos.	48
 Chapitre 5: Sécurité de domaine.....	 49
Présentation de la sécurité de domaine.	49
Communication sécurisée à l'intérieur du domaine.	50
Communication sécurisée pour les services et le gestionnaire de service.	50
Base de données de référentiel de configuration du domaine sécurisée.	56
Base de données de référentiel PowerCenter sécurisée.	59
Base de données du référentiel modèle sécurisée.	59
Communication sécurisée pour les flux de travail et les sessions.	60
Connexions sécurisées à un service d'application Web.	61
Exigences pour les connexions sécurisées aux services d'application Web.	61
Activation des connexions sécurisées sur l'outil Administrator.	62
Services d'applications Web Informatica.	62
Sources et cibles sécurisées.	65
Sources et cibles du service d'intégration de données.	65
Sources et cibles PowerCenter.	66
Stockage de données sécurisé.	66
Répertoire sécurisé sous UNIX.	67
Modification de la clé de cryptage à partir de la ligne de commande.	68
Services et ports d'application.	71
 Chapitre 6: Gestion de la sécurité dans Informatica Administrator.....	 75
Présentation de l'utilisation d'Informatica Administrator.	75
Sécurité utilisateur.	77
Cryptage.	77
Authentification.	78
Autorisation.	78

Onglet Sécurité.	79
Utilisation de la section Rechercher.	80
Utilisation du navigateur de sécurité.	80
Groupes.	81
Utilisateurs.	81
Rôles.	82
Gestion du mot de passe.	83
Modification de votre mot de passe.	83
Gestion de la sécurité de domaine.	83
Gestion de la sécurité des utilisateurs.	84
Chapitre 7: Utilisateurs et groupes.	85
Présentation des utilisateurs et groupesUtilisateurs et groupes.	85
Groupes par défaut.	86
Groupe d'administration.	86
Groupe Tout le monde.	87
Comprendre les comptes utilisateurs.	87
Administrateur par défaut.	87
Administrateur de domaine.	88
Administrateur de client d'application.	88
Utilisateur.	89
Gestion des utilisateurs.	90
Création d'utilisateurs natifsCréation d'utilisateursCréation d'utilisateurs.	90
Modification des propriétés générales d'utilisateurs natifs.	91
Assignation des utilisateurs natifs aux groupes natifs.	91
Assignation des utilisateurs LDAP aux groupes natifs.	92
Activation et désactivation des comptes utilisateurs.	92
Suppression d'utilisateurs natifs.	93
Utilisateurs LDAP.	94
Déverrouillage d'un compte utilisateur.	94
Augmentation de la mémoire système pour un grand nombre d'utilisateurs.	94
Affichage de l'activité utilisateur.	95
Gestion des groupes.	98
Ajout d'un groupe natif.	99
Modification des propriétés d'un groupe natif.	100
Déplacement d'un groupe natif vers un autre groupe natif.	100
Suppression d'un groupe natif.	100
Groupes LDAP.	100
Gestion des profils de systèmes d'exploitation.	100
Créer des profils des systèmes d'exploitation	101
Propriétés des profils de systèmes d'exploitation	101
Création d'un profil de système d'exploitation.	103
Utilisation des profils du système d'exploitation dans un domaine sécurisé.	104

Utilisation des profils du système d'exploitation dans un domaine avec l'authentification Kerberos.	104
Verrouillage de compte.	105
Configuration du verrouillage de compte.	106
Règles et directives de verrouillage de compte.	106

Chapitre 8: Privilèges et rôles. 107

Présentation des privilèges et des rôles.	107
Privilèges.	107
Rôles.	109
Privilèges du domaine.	110
Groupe de privilèges Administration de la sécurité.	110
Groupe de privilèges Administration de domaine.	111
Groupe de privilèges Surveillance.	117
Groupe de privilèges Outils.	118
Groupe de privilèges d'administration Cloud.	119
Privilèges du service Analyst.	119
Privilèges du service de gestion de contenu.	120
Privilèges du service d'intégration de données.	121
Privilèges du Metadata Manager Service.	121
Groupe de privilèges Catalogue.	122
Groupe de privilèges Chargement.	123
Groupe de privilèges du modèle.	125
Groupe de privilèges Sécurité.	125
Privilèges du service de référentiel modèle.	125
Privilèges du PowerCenter Repository Service.	127
Groupe de privilèges Outils.	127
Groupe de privilèges Dossiers.	128
Groupe de privilèges Objets de conception.	130
Groupe de privilèges Sources et cibles.	132
Groupe de privilèges Objets d'exécution.	134
Groupe de privilèges des objets globaux.	138
Privilèges du service d'écoute PowerExchange.	141
Privilèges du service de journalisation PowerExchange.	141
Privilèges du Reporting Service.	142
Groupe de privilèges Administration.	142
Groupe de privilèges Alertes.	143
Groupe de privilèges de communication.	144
Groupe de privilèges Répertoire de contenu.	145
Groupe de privilèges du tableau de bord.	146
Groupe de privilèges d'indicateurs.	147
Groupe de privilèges Gérer les comptes.	147
Groupe de privilèges Rapports.	147

Privilèges du service de reporting et de tableaux de bord.	149
Privilèges du service Test Data Manager.	150
Groupe de privilèges Administration.	151
Groupe de privilèges Connexions.	152
Groupe de privilèges Domaines de données.	152
Groupe de privilèges Masquage des données.	153
Groupe de privilèges Sous-ensemble de données.	154
Groupe de privilèges Stratégies.	155
Groupe de privilèges Projets.	155
Groupe de privilèges Règles.	157
Groupe de privilèges Génération de données.	158
Gestion des rôles.	158
Rôles définis par le système.	159
Rôles personnalisés.	162
Gestion des rôles personnalisés.	162
Attribution de privilèges et de rôles aux utilisateurs et aux groupes.	163
Privilèges hérités.	164
Étapes permettant d'attribuer des privilèges et des rôles aux utilisateurs et groupes.	164
Affichage des utilisateurs avec des privilèges pour un service.	165
Résolution des problèmes de privilèges et de rôles.	166
Chapitre 9: Autorisations.	168
Présentation des autorisations.	168
Types d'autorisations.	169
Filtres de recherche des autorisations.	170
Autorisations d'objets de domaines.	171
Autorisations par objet de domaine.	172
Autorisations par utilisateur ou groupe.	174
Autorisations du profil de système d'exploitation.	175
Autorisations de connexion.	176
Types d'autorisations de connexion.	177
Autorisations de connexion par défaut.	177
Attribution d'autorisations à une connexion.	178
Affichage des détails des autorisations pour une connexion.	178
Modification des autorisations sur une connexion.	178
Autorisations du service de données SQL.	179
Types d'autorisations de service de données SQL.	179
Attribuer des autorisations pour un service de données SQL.	180
Affichage des détails des autorisations pour un service de données SQL.	180
Modification des autorisations pour un service de données SQL.	181
Refus d'autorisations pour un service de données SQL.	182
Sécurité au niveau des colonnes.	182
Autorisations du service web.	184

Types d'autorisations de service Web.	184
Attribution des autorisations pour un service Web.	184
Affichage des détails des autorisations pour un service Web.	185
Modification des autorisations dans un service Web.	185
Chapitre 10: Rapports d'audit.	187
Présentation des rapports d'audit.	187
Informations personnelles de l'utilisateur.	188
Association de groupes d'utilisateurs.	189
Privilèges.	190
Association de rôles.	190
Autorisation d'objet de domaine.	191
Sélection d'utilisateurs pour un rapport d'audit.	191
Sélection des groupes pour un rapport d'audit.	192
Sélection des rôles pour un rapport d'audit.	193
Annexe A: Rôles personnalisés.	194
Rôles personnalisés du PowerCenter Repository Service.	194
Rôles personnalisés du Metadata Manager Service.	196
Rôles personnalisés du Reporting Service.	197
Rôles personnalisés du service Test Data Manager.	204
Rôle personnalisé du service Analyst.	208
Index.	209

Préface

Le Guide de sécurité Informatica contient des informations sur la sécurité dans le domaine Informatica. Il contient les informations nécessaires pour gérer la sécurité du domaine Informatica et des clients Informatica qui se connectent au domaine. Ce guide suppose que vous connaissez le domaine Informatica et Informatica Administrator. Il suppose également que vous êtes familiarisé avec les serveurs d'authentification et les processus de votre réseau.

Ressources Informatica

Portail Mon support Informatica

En tant que client Informatica, vous pouvez accéder au portail Mon support Informatica sur <http://mysupport.informatica.com>.

Ce site contient des informations sur les produits et les groupes d'utilisateurs, des bulletins d'information, un lien vers le système de gestion des dossiers d'assistance à la clientèle d'Informatica (ATLAS), une bibliothèque de procédures Informatica, une base de connaissances Informatica, ainsi que la documentation nécessaire sur les produits Informatica et l'accès à sa communauté d'utilisateurs.

Ce site contient des informations sur les produits et les groupes d'utilisateurs, des bulletins d'information, un lien vers la bibliothèque de procédures Informatica, une base de connaissances Informatica, ainsi que la documentation nécessaire sur les produits Informatica et l'accès à sa communauté d'utilisateurs.

Documentation Informatica

L'équipe Documentation d'Informatica s'efforce de fournir une documentation précise et utilisable. N'hésitez pas à contacter l'équipe Documentation d'Informatica par courriel à l'adresse infa_documentation@informatica.com pour lui faire part de vos questions, commentaires ou suggestions concernant cette documentation. Ces commentaires et suggestions nous permettront d'améliorer notre documentation. Veuillez préciser si vous acceptez d'être contacté au sujet de ces commentaires.

L'équipe Documentation met à jour la documentation chaque fois que nécessaire. Pour obtenir la toute dernière version de la documentation concernant votre produit, consultez la Documentation de produit sur <http://mysupport.informatica.com>.

Matrices de disponibilité de produit Informatica

Les matrices de disponibilité de produit (PAM) indiquent les versions des systèmes d'exploitation, les bases de données et les autres types de sources et cibles de données pris en charge par une version d'un produit.

Vous pouvez consulter les PAM sur le portail Mon Support Informatica à l'adresse <https://mysupport.informatica.com/community/my-support/product-availability-matrices>.

Site Web Informatica

Vous pouvez accéder au site Web d'entreprise Informatica sur <http://www.informatica.com>. Le site contient des informations sur Informatica, son expertise, les événements à venir et les bureaux de vente. Vous y trouverez aussi des informations sur ses produits et ses partenaires. Les rubriques de service du site fournissent des informations importantes sur le support technique, la formation et l'éducation, ainsi que les services d'implémentation.

Bibliothèque de procédures Informatica

En tant que client Informatica, vous avez accès à la bibliothèque de procédures Informatica sur <http://mysupport.informatica.com>. La bibliothèque de procédures Informatica est une collection de ressources destinée à vous familiariser avec les produits Informatica et leurs fonctionnalités. Elle regroupe des articles et des démonstrations interactives qui permettent de résoudre des problèmes courants et de comparer les fonctionnalités et les comportements, et qui vous guident lors de la réalisation de tâches concrètes spécifiques.

Base de connaissances Informatica

En tant que client Informatica, vous avez accès à la base de connaissances Informatica sur <http://mysupport.informatica.com>. Utilisez la base de connaissances pour rechercher des solutions documentées aux problèmes techniques connus concernant les produits Informatica. Vous y trouverez également la réponse aux questions les plus fréquentes, des livres blancs et des conseils techniques. N'hésitez pas à contacter l'équipe Base de connaissances Informatica par courriel à l'adresse KB_Feedback@informatica.com pour lui faire part de vos questions, commentaires et suggestions concernant la base de connaissances.

Canal YouTube du support Informatica

Vous pouvez accéder au canal YouTube du support Informatica sur <http://www.youtube.com/user/INFASupport>. Le canal YouTube du support Informatica contient des vidéos concernant les solutions qui vous guident dans l'exécution de tâches spécifiques. Si vous avez des questions, commentaires ou suggestions concernant le canal YouTube du support Informatica, contactez l'équipe de support YouTube par courriel à l'adresse supportvideos@informatica.com ou envoyez un tweet à @INFASupport.

Informatica Marketplace

Informatica Marketplace est un forum où développeurs et partenaires peuvent partager des solutions qui permettent d'augmenter, d'étendre ou d'améliorer les implémentations d'intégration de données. En tirant profit des centaines de solutions disponibles sur Marketplace, vous pouvez améliorer votre productivité et accélérer le temps d'implémentation de vos projets. Vous pouvez accéder à Informatica Marketplace à l'adresse <http://www.informaticamarketplace.com>.

Informatica Velocity

Vous pouvez accéder à Informatica Velocity à l'adresse <http://mysupport.informatica.com>. Développé à partir de l'expérience concrète de centaines de projets de gestion de données, Informatica Velocity représente le savoir collectif de nos consultants, qui ont travaillé avec des entreprises du monde entier pour

planifier, développer, déployer et tenir à jour des solutions de gestion des données efficaces. Si vous avez des questions, des commentaires et des suggestions sur Informatica Velocity, contactez le support des services professionnels Informatica à l'adresse ips@informatica.com.

Support client international Informatica

Vous pouvez contacter un centre de support client par téléphone ou via l'assistance en ligne.

L'assistance en ligne requiert un nom d'utilisateur et un mot de passe. Vous pouvez demander un nom d'utilisateur et un mot de passe sur <http://mysupport.informatica.com>.

Les numéros de téléphone du support client international Informatica sont disponibles sur le site Web Informatica à l'adresse <http://www.informatica.com/us/services-and-training/support-services/global-support-centers/>.

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, 15](#)
- [Référentiel de configuration du domaine, 16](#)
- [Domaine de sécurité, 16](#)

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.

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 client. 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

Utilisez keytool pour créer un certificat SSL ou une demande de signature de certificat (CSR), ainsi que des keystores et des truststores au format JKS.

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

<http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>

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, 18](#)
- [Authentification utilisateur native, 19](#)
- [Authentification utilisateur LDAP, 19](#)
- [Authentification Kerberos, 20](#)

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

Les comptes utilisateur natifs sont stockés dans le domaine Informatica et peuvent uniquement être utilisés dans ce domaine. Kerberos et les comptes utilisateur LDAP sont stockés dans un service d'annuaire LDAP et sont partagés par des applications de l'entreprise.

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.

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 le domaine Informatica pour permettre aux utilisateurs figurant dans un service d'annuaire LDAP de se connecter aux applications client Informatica. Le domaine Informatica 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.

Informatica ne prend pas en charge l'authentification Kerberos croisée ou multi-domaines. L'hôte du serveur, les machines du client et le serveur d'authentification Kerberos doivent se trouver dans le même domaine.

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.

CHAPITRE 3

Domaines de sécurité LDAP

Ce chapitre comprend les rubriques suivantes :

- [Présentation des domaines de sécurité LDAP, 21](#)
- [Configuration d'un domaine de sécurité LDAP, 22](#)
- [Suppression d'un domaine de sécurité LDAP, 28](#)

Présentation des domaines de sécurité LDAP

Un domaine de sécurité LDAP contient un ensemble d'utilisateurs et de groupes importés à partir d'un service d'annuaire LDAP. Vous pouvez créer un domaine de sécurité LDAP si vous utilisez l'authentification utilisateur LDAP ou l'authentification réseau Kerberos.

Vous pouvez configurer les domaines de sécurité LDAP de manière à stocker la liste des utilisateurs d'un service d'annuaire LDAP que vous voulez autoriser dans les applications client Informatica. Le domaine de sécurité ne stocke pas les justificatifs d'identité du compte d'utilisateur. Lorsqu'un utilisateur se connecte à un client Informatica, le gestionnaire de service vérifie que le compte utilisateur se trouve dans un domaine de sécurité. Si le compte d'utilisateur appartient à un domaine de sécurité LDAP, le gestionnaire de service authentifie l'utilisateur avec le service d'annuaire LDAP.

Lorsque vous installez les services Informatica et que vous n'activez pas l'authentification Kerberos, le programme d'installation Informatica crée le domaine de sécurité natif par défaut. Après l'installation, vous pouvez ajouter des utilisateurs et des groupes au domaine de sécurité natif. Si vous disposez d'utilisateurs dans un service d'annuaire LDAP que vous souhaitez autoriser dans les applications client Informatica, vous pouvez paramétrer les domaines de sécurité LDAP en plus du domaine de sécurité natif. Configurez une connexion au serveur LDAP et importez les utilisateurs et les groupes dans les domaines de sécurité LDAP.

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. Après l'installation, vous pouvez configurer une connexion au serveur LDAP et importer des utilisateurs et des groupes depuis le service d'annuaire LDAP dans le domaine de sécurité LDAP. Si vous utilisez l'authentification Kerberos, vous ne pouvez pas utiliser le domaine de sécurité natif.

Configuration d'un domaine de sécurité LDAP

Vous pouvez créer un domaine de sécurité LDAP pour les comptes utilisateur que vous importez à partir d'un service d'annuaire LDAP. Pour organiser des groupes d'utilisateurs différents, vous pouvez créer plusieurs domaines de sécurité LDAP.

Vous créez et gérez les utilisateurs et les groupes LDAP dans le service d'annuaire LDAP. Définissez une connexion au serveur LDAP et utilisez les filtres de recherche pour spécifier les utilisateurs et les groupes qui peuvent accéder au domaine Informatica. Importez ensuite les comptes utilisateur dans les domaines de sécurité LDAP. Si le serveur LDAP utilise le protocole SSL, vous devez également spécifier l'emplacement du certificat SSL.

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

- Service Microsoft Active Directory

Remarque: Si vous utilisez l'authentification Kerberos, vous pouvez importer des utilisateurs uniquement à partir d'un service d'annuaire Microsoft Active Directory (AD).

- Service Sun Java System Directory
- Service Novell e-Directory
- Service IBM Tivoli Directory
- Service d'annuaire Open LDAP

Lorsque vous importez des utilisateurs dans un domaine de sécurité LDAP, vous pouvez leur attribuer des rôles, des privilèges et des autorisations. Vous pouvez assigner des comptes utilisateur LDAP aux groupes natifs pour les organiser en fonction des rôles dans le domaine Informatica. Vous ne pouvez pas utiliser l'outil Administrator pour créer, modifier ou supprimer des utilisateurs et groupes dans un domaine de sécurité LDAP.

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

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

1. Configurez la connexion au service d'annuaire LDAP.
2. Configurez un domaine de sécurité.
3. Planifiez les heures de synchronisation.

Étape 1. Configurer la connexion au serveur LDAP

Configurez la connexion au serveur LDAP contenant le service d'annuaire à partir duquel vous voulez importer les comptes utilisateur pour le domaine Informatica.

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 vous modifiez les propriétés de la connexion LDAP en vue de la connexion à un autre service d'annuaire LDAP, vérifiez que les filtres d'utilisateur et de groupe dans les domaines de sécurité LDAP sont corrects pour le nouveau service d'annuaire LDAP. Vérifiez que les filtres incluent les utilisateurs et les groupes que vous souhaitez utiliser dans le domaine Informatica.

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 le menu **Actions** et sélectionnez **Configuration LDAP**.
3. Dans la boîte de dialogue **Configuration LDAP**, cliquez sur l'onglet **Connectivité LDAP**.
4. Configurez les propriétés de la connexion pour le serveur LDAP.

Vous devrez peut-être contacter l'administrateur LDAP pour obtenir les informations sur le serveur LDAP.

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

Propriété	Description
Nom du serveur	Nom de la machine hébergeant le service d'annuaire LDAP.
Port	Port d'écoute du serveur LDAP. Numéro de port pour 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 65 535.
Service d'annuaire LDAP	Type de service d'annuaire LDAP. Sélectionnez parmi les services d'annuaire suivants : <ul style="list-style-type: none">- Service Microsoft Active Directory- Service Sun Java System Directory- Service Novell e-Directory- Service IBM Tivoli Directory- Service d'annuaire Open LDAP Remarque: Si vous utilisez l'authentification Kerberos, vous devez sélectionner le service Microsoft Active Directory.
Nom	Nom unique (DN) pour 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. Laissez vide pour une connexion anonyme. Pour plus d'informations, consultez la documentation du service d'annuaire LDAP.
Mot de passe	Mot de passe de l'utilisateur principal. Laissez vide pour une connexion anonyme. Non disponible si vous utilisez l'authentification Kerberos.
Utiliser le certificat SSL	Indique que le serveur LDAP utilise le protocole SSL (Secure Socket Layer).
Certificat LDAP de confiance	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. Pour permettre au gestionnaire de service de reconnaître un certificat auto-signé comme étant valide, indiquez le fichier truststore et le mot de passe à utiliser.
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. Activez cette option.

Propriété	Description
Attribut d'appartenance à un groupe	Nom de l'attribut qui contient les informations d'appartenance au groupe d'un utilisateur. Attribut dans l'objet groupe LDAP qui contient les DN des utilisateurs et groupes membres d'un groupe. Par exemple, <i>member</i> ou <i>memberof</i> .
Taille maximale	<p>Nombre maximum de groupes et de comptes d'utilisateurs à importer dans un domaine de sécurité. Par exemple, si la valeur est définie sur 100, vous pouvez importer un maximum de 100 groupes et de 100 comptes d'utilisateurs dans le domaine de sécurité.</p> <p>Si le nombre d'utilisateurs et de groupes 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 et groupes à importer.</p> <p>Par défaut 1 000.</p>

5. Cliquez sur Tester la connexion pour vérifier que la connexion au serveur LDAP est valide.

Étape 2. Configuration d'un domaine de sécurité

Créez un domaine de sécurité 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. 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 importe les groupes et la liste des utilisateurs qui appartiennent aux groupes. Il importe les groupes inclus dans le filtre de groupes et les comptes d'utilisateurs inclus dans le filtre d'utilisateurs.

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.

Remarque: Contrairement aux noms d'utilisateurs natifs, les noms d'utilisateurs LDAP peuvent être sensibles à la casse.

Lorsque vous configurez le service d'annuaire LDAP, vous pouvez utiliser des attributs différents pour l'ID unique (UID). Le gestionnaire de service exige un UID spécifique pour identifier les utilisateurs dans chaque service d'annuaire LDAP. Avant de configurer le domaine de sécurité, vérifiez que le service d'annuaire LDAP utilise l'UID requis.

Le tableau suivant indique l'UID requis pour chaque service d'annuaire LDAP :

Service d'annuaire LDAP	UID
IBMTivoliDirectory	uid
Microsoft Active Directory	sAMAccountName
NovellE	uid

Service d'annuaire LDAP	UID
OpenLDAP	uid
SunJavaSystemDirectory	uid

Le gestionnaire de service n'importe pas l'attribut LDAP qui indique qu'un compte d'utilisateur est activé ou désactivé. Vous devez activer ou désactiver un compte d'utilisateur LDAP dans l'outil Administrator. L'état du compte d'utilisateur dans le service d'annuaire LDAP affecte l'authentification de l'utilisateur dans les clients de l'application. Par exemple, un compte d'utilisateur est activé dans le domaine Informatica mais désactivé dans le service d'annuaire LDAP. Si le service d'annuaire LDAP permet aux comptes d'utilisateurs désactivés de se connecter, l'utilisateur peut se connecter aux clients de l'application. Si le service d'annuaire LDAP ne permet pas aux comptes d'utilisateurs désactivés de se connecter, l'utilisateur ne peut pas se connecter aux clients de l'application.

Remarque: 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** et sélectionnez **Configuration LDAP**.
3. Dans la boîte de dialogue **Configuration LDAP**, cliquez sur l'onglet **Domaines de sécurité**.
4. Cliquez sur **Ajouter**.
5. Utilisez la syntaxe de requête LDAP pour créer des filtres afin de spécifier les utilisateurs et les groupes à inclure dans le domaine de sécurité que vous créez.

Vous devrez peut-être contacter l'administrateur LDAP pour obtenir les informations sur les utilisateurs et les groupes disponibles dans le service d'annuaire LDAP.

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. Il ne peut pas dépasser 128 caractères ni contenir 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.
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.

Propriété	Description
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>
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	Une chaîne de requête LDAP qui spécifie les critères de recherche pour les groupes dans le service d'annuaire.

6. 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.
7. Pour ajouter un autre domaine de sécurité LDAP, répétez les étapes [4](#) à [6](#).
8. 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.
9. Cliquez sur **OK** pour enregistrer les domaines de sécurité.

Étape 3. Planifier les heures de synchronisation

Vous pouvez configurer une planification pour que le gestionnaire de service synchronise périodiquement la liste des utilisateurs et des groupes du domaine de sécurité LDAP avec celle du service d'annuaire LDAP.

Important: Avant de démarrer le processus de synchronisation, vérifiez que le fichier `/etc/hosts` contient une entrée pour le nom d'hôte du serveur LDAP. Si le gestionnaire de service ne peut pas résoudre le nom d'hôte pour le serveur LDAP, la synchronisation des utilisateurs peut échouer.

Pendant la synchronisation, le gestionnaire de service importe les utilisateurs et groupes depuis le service d'annuaire LDAP. Le gestionnaire de service supprime tous les utilisateurs ou les groupes du domaine de sécurité LDAP qui ne sont plus inclus dans les filtres de recherche utilisée pour l'importation.

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 correcte, vous pouvez planifier les heures auxquelles le gestionnaire de service synchronise les domaines de sécurité 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.

Remarque: Pendant la synchronisation, le gestionnaire de service verrouille le compte d'utilisateur qu'il synchronise. Lorsque le compte d'utilisateur est verrouillé, le gestionnaire de service ne peut pas authentifier le compte d'utilisateur. L'utilisateur ne pourra peut-être pas se connecter aux clients de l'application. Si des utilisateurs sont connectés aux clients de l'application lorsque la synchronisation démarre, ils ne pourront peut-être pas effectuer les tâches. La durée de la synchronisation dépend du nombre d'utilisateurs et de groupes à synchroniser. Pour éviter toute interruption de l'utilisation, synchronisez les domaines de sécurité

à des heures auxquelles la plupart des utilisateurs ne sont pas connectés. Pour synchroniser plus de 100 utilisateurs ou groupes, activez la pagination dans le service d'annuaire LDAP avant d'exécuter la synchronisation. Si vous n'activez pas la pagination dans le service d'annuaire LDAP, la synchronisation peut échouer.

Pour configurer une planification afin de synchroniser 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.

Vous pouvez ajouter autant d'heures de synchronisation dans la journée que nécessaire. Si la liste d'utilisateurs et de groupes dans le service d'annuaire LDAP change souvent, vous pouvez planifier le gestionnaire de service pour qu'il effectue plusieurs synchronisations par jour.

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

Remarque: Si vous redémarrez le domaine Informatica avant que le gestionnaire de service ne se synchronise avec le service d'annuaire LDAP, les heures de synchronisation ajoutées sont perdues.

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. Par défaut, le gestionnaire de service ne se connecte pas à un serveur LDAP qui utilise un certificat auto-signé.

Pour utiliser un certificat auto-signé, importez-le dans un fichier truststore et utilisez la variable d'environnement INFA_JAVA_OPTS pour spécifier le fichier truststore et le mot de passe :

```
setenv INFA_JAVA_OPTS -Djavax.net.ssl.trustStore=<TrustStoreFile>  
-Djavax.net.ssl.trustStorePassword=<TrustStorePassword>
```

Sous Windows, configurez INFA_JAVA_OPTS en tant que variable système.

Redémarrez le nœud pour appliquer la modification. Le gestionnaire de service utilise le fichier truststore pour vérifier le certificat SSL.

`keytool` est un utilitaire de gestion de clés et de certificats qui permet de générer et d'administrer des clés et des certificats à utiliser avec le protocole de sécurité SSL. Vous pouvez utiliser `keytool` pour créer un fichier truststore ou pour importer un certificat vers un fichier truststore existant. L'utilitaire `keytool` est disponible dans le répertoire suivant :

```
<PowerCenterClientDir>\CMD_Uilities\PC\java\bin
```

Pour plus d'informations sur l'utilisation de `keytool`, consultez la documentation sur le site Web de Sun : <http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>.

Le logiciel disponible en téléchargement sur les liens référencés appartient à un tiers ou à des tierces parties et non Informatica Corporation. Les liens de téléchargement peuvent être sujets à des erreurs, omissions ou modifications. Informatica n'assume aucune responsabilité pour ce type de liens et/ou ce type de logiciels, exclut toutes garanties, expresses ou implicites, y compris, mais ne se limitant pas aux garanties de conformité légale, d'usage normal et de non-infraction et exclut toutes responsabilités liées.

Suppression d'un domaine de sécurité LDAP

Pour interdire définitivement l'accès des utilisateurs à des clients d'application dans un domaine de sécurité LDAP, vous pouvez supprimer ce dernier. Lorsque vous supprimez un domaine de sécurité LDAP, le gestionnaire de service supprime tous les comptes utilisateur et groupes du domaine de sécurité de la base de données de configuration du domaine.

1. Dans la boîte de dialogue Configuration de LDAP, cliquez sur l'onglet Domaines de sécurité.
La boîte de dialogue Configuration de LDAP affiche la liste des domaines de sécurité.
2. Pour vérifier que vous supprimez le domaine de sécurité adéquat, cliquez sur le nom de domaine de sécurité afin d'afficher le filtre utilisé pour importer les utilisateurs et groupes et vérifier qu'il s'agit du domaine de sécurité que vous voulez supprimer.
3. Cliquez sur le bouton Supprimer en regard d'un domaine de sécurité pour le supprimer.
4. Cliquez sur OK pour confirmer que vous voulez supprimer le domaine de sécurité.

CHAPITRE 4

Configuration de l'authentification Kerberos

- [Configuration de l'authentification Kerberos, 29](#)

Configuration de l'authentification Kerberos

Lorsque vous créez le domaine Informatica lors de l'installation, vous pouvez sélectionner l'option permettant d'activer l'authentification Kerberos. 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.

Pour configurer l'authentification Kerberos pour le domaine Informatica sur la ligne de commande, procédez comme suit :

1. Créez un domaine de l'utilisateur LDAP avec les utilisateurs de Microsoft Active Directory.
2. Migrez les utilisateurs natifs vers un domaine de sécurité LDAP.
3. Définissez la configuration Kerberos et copiez le fichier de configuration dans le répertoire Informatica.
4. Générez le nom de fichier SPN et Keytab au format requis par le domaine Informatica.
5. Consultez le fichier texte du format de fichier SPN et Keytab.
6. Créez les SPN et les fichiers Keytab.
7. Configurez l'authentification Kerberos pour le domaine Informatica.
8. Mettez à jour les nœuds du domaine Informatica.
9. Mettez à jour les machines du client.
10. Démarrez le domaine Informatica et exécutez l'outil Administrator.

Lorsque vous configurez l'authentification Kerberos et les domaines de sécurité LDAP, vérifiez que les comptes utilisateur ont des autorisations et des privilèges corrects. Vérifiez que les services du domaine fonctionnent comme prévu et que les utilisateurs peuvent se connecter avec l'authentification unique.

Remarque: La procédure indiquée part du principe que vous avez installé les services Informatica sans activer l'authentification Kerberos. Si vous avez activé l'authentification Kerberos lors de l'installation, suivez la procédure indiquée dans les guides d'installation Informatica.

Étape 1. Créer un domaine de l'utilisateur LDAP avec les utilisateurs de Microsoft Active Directory

Avant de configurer le domaine Informatica pour utiliser l'authentification Kerberos, consultez ses comptes utilisateur. Vérifiez qu'ils se trouvent dans des domaines de sécurité LDAP et qu'ils sont importés depuis le service Microsoft Active Directory.

Si le domaine comporte des comptes utilisateur dans un domaine de sécurité LDAP qui n'utilise pas Microsoft Active Directory, migrez les utilisateurs vers un domaine de sécurité LDAP qui utilise Microsoft Active Directory. Pour plus d'informations sur la migration des comptes utilisateur vers Microsoft Active Directory, consultez la documentation de votre implémentation de LDAP.

Si le domaine comporte des comptes utilisateur dans le domaine de sécurité natif, migrez les utilisateurs vers un domaine de sécurité LDAP qui utilise Microsoft Active Directory.

Définissez un domaine de sécurité LDAP et configurez la connexion au service Microsoft Active Directory. Ensuite, configurez les filtres pour les utilisateurs et les groupes, puis synchronisez les comptes utilisateur du domaine.

Pour plus d'informations sur la configuration d'un domaine LDAP et la synchronisation des comptes utilisateur, voir ["Configuration d'un domaine de sécurité LDAP" à la page 22](#).

Étape 2. Migrer des privilèges et autorisations d'utilisateur natif vers un domaine de sécurité LDAP

Lorsque vous configurez le domaine pour utiliser l'authentification Kerberos, vous ne pouvez pas accéder aux comptes utilisateur du domaine de sécurité natif. Migrez les groupes d'utilisateurs natifs, les rôles, les privilèges et les autorisations vers un domaine de sécurité LDAP avant de configurer l'authentification Kerberos.

Si le domaine comporte des comptes utilisateur dans le domaine de sécurité natif, les comptes utilisateur correspondants dans le domaine de sécurité LDAP doivent comporter les mêmes groupes, rôles, privilèges et autorisations. Migrez les groupes, rôles, privilèges et autorisations des utilisateurs natifs vers les utilisateurs Active Directory du domaine de sécurité LDAP. Ensuite, vérifiez que les groupes, rôles, privilèges et autorisations ont correctement migré.

Si le domaine ne comporte pas de comptes utilisateur dans le domaine de sécurité natif, vous pouvez passer à ["Étape 3. Définir le fichier de configuration Kerberos" à la page 34](#).

Pour migrer les groupes, rôles, privilèges et autorisations des utilisateurs natifs vers les utilisateurs du domaine de sécurité LDAP, procédez comme suit :

1. Vérifiez les comptes utilisateur pour l'authentification Kerberos.
2. Créez le fichier de migration d'utilisateur.
3. Exécutez la commande `infacmd isp migrateusers`.
4. Vérifiez les groupes, rôles, privilèges et autorisations pour les comptes d'utilisateur.

Remarque: Pour éviter les problèmes lorsque vous migrez les groupes d'utilisateurs, les rôles, les privilèges et les autorisations, n'exécutez pas de flux de travail ou ne modifiez pas de groupes d'utilisateurs, rôles, privilèges ou autorisations pendant le processus de migration.

Vérifier les comptes utilisateur pour l'authentification Kerberos

Affichez la liste des comptes utilisateur natifs et déterminez les comptes que vous voulez migrer vers un domaine de sécurité LDAP pour l'authentification Kerberos.

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

```
infacmd isp ListAllUsers
```

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

Si les comptes ne se trouvent pas dans le service Microsoft Active Directory, ajoutez-les au service d'annuaire. Pour plus d'informations sur l'ajout de comptes utilisateur au service Microsoft Active Directory, consultez la documentation Microsoft Active Directory.

Remarque: Le nom d'utilisateur des comptes utilisateur du domaine de sécurité LDAP a une longueur maximale de 20 caractères. Lorsque vous ajoutez les comptes utilisateur au service Microsoft Active Directory, vérifiez que le nom d'utilisateur ne comporte pas plus de 20 caractères.

Créer le fichier de migration d'utilisateur

La commande `infacmd isp migrateUsers` utilise un fichier de migration d'utilisateur pour déterminer les groupes, rôles, privilèges et autorisations à attribuer aux utilisateurs LDAP. Le fichier de migration d'utilisateur est un fichier en texte brut qui contient la liste des utilisateurs natifs et des utilisateurs LDAP correspondants qui requièrent les mêmes groupes, rôles, privilèges et autorisations.

Lorsque vous créez le fichier de migration d'utilisateur, vous devez spécifier le domaine de sécurité pour le compte utilisateur. Une barre oblique (/) sépare le domaine de sécurité du nom d'utilisateur. Une virgule (,) sépare l'utilisateur natif de l'utilisateur LDAP correspondant. Les domaines de sécurité sont sensibles à la casse. Les noms d'utilisateur ne sont pas sensibles à la casse.

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

```
Native/<SourceUserName>,LDAP/<TargetUserName>
```

Vous pouvez migrer les groupes, rôles, privilèges et autorisations des utilisateurs natifs vers des utilisateurs de différents domaines de sécurité LDAP. Par exemple, le fichier de migration d'utilisateur contient la liste suivante d'utilisateurs :

```
Native/User1,LDAPSecurityDomain/User1
Native/User2,LDAPSecurityDomain/User2
Native/User3,newLDAPSecDomain/User3
```

La commande `migrateUser` attribue à User1 et User2 dans LDAPSecurityDomain les mêmes groupes, rôles, privilèges et autorisations qu'à User1 et User2 dans le domaine de sécurité natif. La commande attribue à User3 dans newLDAPSecDomain les mêmes groupes, rôles, privilèges et autorisations qu'à User3 dans le domaine de sécurité natif.

La commande `migrateUsers` ignore toute entrée avec un nom d'utilisateur source ou cible dupliqué.

Exécuter la commande `infacmd isp migrateUsers`

Pour migrer des groupes, rôles, privilèges et autorisations d'utilisateurs du domaine de sécurité natif vers des utilisateurs du domaine de sécurité LDAP, exécutez la commande `infacmd migrateUsers` et spécifiez le fichier de migration d'utilisateur à utiliser.

Avant d'exécuter la commande `infacmd isp migrateUsers`, vérifiez que toutes les instances des services suivants du domaine sont en cours d'exécution :

- Service Analyst
- Service de gestion de contenu
- Service de référentiel modèle
- Service Metadata Manager
- Service de référentiel PowerCenter
- Service de rapports

Vérifiez que le service de référentiel PowerCenter est exécuté en mode normal.

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

```
infacmd isp migrateUsers -dn <DomainName> -un <AdministratorUserName> -pd  
<AdministratorPassword> -umf <UserMigrationFile>
```

Par exemple, la commande suivante migre les groupes, rôles, privilèges et autorisations des utilisateurs en fonction du fichier de migration d'utilisateur `um_s.txt` :

```
infacmd isp migrateUsers -dn UMT_Domain -un Administrator -pd Administrator -umf C:\UMT  
\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_uml_date_heure.txt` dans le répertoire d'exécution de la commande.

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

Résolution des problèmes de la commande `migrateUsers`

Comment faire pour améliorer les performances de la migration ?

Pour améliorer les performances de migration, procédez comme suit :

1. Créez plusieurs fichiers de migration d'utilisateur uniques avec un nombre limité d'utilisateurs dans chaque fichier.
2. Exécutez simultanément plusieurs instances de la commande `migrateUsers`.

Par exemple, pour migrer les groupes, rôles, privilèges et autorisations de 150 utilisateurs, créez trois fichiers de migration d'utilisateur contenant chacun 50 utilisateurs. Ensuite, exécutez simultanément trois instances de la commande `migrateUsers`. Spécifiez un fichier de migration d'utilisateur unique pour chaque instance de la commande.

La commande `migrateUsers` échoue.

Si la commande `migrateUsers` échoue, les chemins de récupération suivants sont disponibles :

- Exécutez à nouveau la commande `migrateUsers`.

- Modifiez le fichier de migration d'utilisateur. Ensuite, exécutez la commande `migrateUsers`.

Lorsque vous exécutez à nouveau la commande, spécifiez le même fichier de migration d'utilisateur. 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.

Pour modifier le fichier de migration d'utilisateur, procédez comme suit :

1. Affichez le fichier journal détaillé qui a été créé lorsque vous avez exécuté la commande `migrateUsers`.
2. Supprimez du fichier de migration d'utilisateur les utilisateurs qui ont été correctement migrés.
3. Exécutez la commande `migrateUsers`.

Vérifier les privilèges et autorisations des comptes utilisateur

Avant d'activer l'authentification Kerberos, vérifiez que les utilisateurs du domaine de sécurité LDAP disposent des groupes, rôles, privilèges et autorisations corrects. Vous pouvez utiliser `infacmd` pour vérifier les groupes, rôles, privilèges et autorisations des comptes utilisateur du domaine de sécurité LDAP.

Vérifiez que les objets suivants ont correctement migré :

Utilisateurs et groupes

Pour déterminer les groupes auxquels appartiennent les comptes utilisateur, obtenez la liste des utilisateurs et des groupes associés. Exécutez la commande suivante :

```
infacmd aud getUserGroupAssociation
```

Rôles

Pour obtenir la liste des rôles associés aux utilisateurs et aux groupes du domaine, exécutez la commande suivante :

```
infacmd aud getUserGroupAssociationForRoles
```

Privilèges

Pour obtenir la liste des privilèges attribués aux utilisateurs et aux groupes du domaine, exécutez la commande suivante :

```
infacmd aud getPrivilegeAssociation
```

Autorisations

Pour obtenir la liste des autorisations attribuées aux utilisateurs et aux groupes du domaine, exécutez la commande suivante :

```
infacmd aud getDomainObjectPermissions
```

Autorisations sur les dossiers et les objets globaux

Si le domaine contient un service de référentiel PowerCenter, vérifiez les autorisations sur les dossiers PowerCenter et les objets du référentiel global attribuées aux comptes utilisateur. Le référentiel PowerCenter peut comporter les objets suivants :

- Dossiers
- Groupes de déploiement
- Libellés
- Requêtes
- Connexions

Après avoir configuré le domaine pour utiliser l'authentification Kerberos, vous ne pouvez pas modifier les comptes utilisateur natifs.

Après avoir confirmé que les groupes, rôles, privilèges et autorisations des comptes utilisateur natifs ont été correctement déplacés vers les comptes utilisateur LDAP, supprimez les comptes utilisateur natifs. Utilisez l'outil Administrator pour supprimer les comptes utilisateur. Pour plus d'informations, voir ["Suppression d'utilisateurs natifs" à la page 93](#).

Étape 3. Définir le fichier de configuration Kerberos

Kerberos stocke les informations de configuration dans un fichier nommé *krb5.conf*. Informatica requiert que des propriétés spécifiques du fichier de configuration Kerberos soient définies pour que le domaine Informatica puisse utiliser correctement l'authentification Kerberos. Vous devez définir les propriétés dans le fichier de configuration *krb5.conf*, puis copier le fichier dans le répertoire Informatica.

Le fichier de configuration contient les informations relatives au serveur Kerberos, y compris le domaine Kerberos et l'adresse du KDC. Vous pouvez demander à l'administrateur Kerberos de définir les propriétés dans le fichier de configuration et de vous une copie de ce fichier.

1. Sauvegardez le fichier *krb5.conf* avant d'effectuer des modifications.
2. Modifiez le fichier *krb5.conf*.
3. Dans la section *libdefaults*, définissez ou ajoutez les propriétés requises par Informatica.

Le tableau suivant répertorie les valeurs pour lesquelles vous devez définir des propriétés dans la section *libdefaults* :

Paramètre	Valeur
default_realm	Nom du domaine de service du domaine Informatica.
forwardable	Permet à un service de déléguer les justificatifs d'identité d'un l'utilisateur client à un autre service. Définissez ce paramètre sur True. Le domaine Informatica requiert que les services d'application authentifient les justificatifs d'identité de l'utilisateur client avec d'autres services.
default_tkt_enctypes	Type de cryptage de la clé de session dans le TGT (Ticket-Granting Ticket). Définissez ce paramètre sur <i>rc4-hmac</i> . Informatica prend uniquement en charge le type de cryptage <i>rc4-hmac</i> .
udp_preference_limit	Détermine le protocole utilisé par Kerberos lors de l'envoi d'un message au KDC. Définissez <i>udp_preference_limit</i> = 1 pour toujours utiliser TCP. Le domaine Informatica prend uniquement en charge le protocole TCP. Si <i>udp_preference_limit</i> est défini sur une autre valeur, le domaine Informatica peut s'arrêter inopinément.

4. Dans la section *realms*, incluez le numéro de port dans l'adresse du KDC en le séparant par un point.
Par exemple, si l'adresse du KDC est *kerberos.example.com* et le numéro de port 88, définissez le paramètre *kdc* comme suit :

```
kdc = kerberos.example.com:88
```

5. Enregistrez le fichier *krb5.conf*.
6. Copiez le fichier de configuration dans le répertoire Informatica.

Vous devez copier le fichier *krb5.conf* dans le répertoire suivant : `<INFA_HOME>/services/shared/security`

Si le domaine comporte plusieurs nœuds, copiez le fichier *krb5.conf* dans le même répertoire sur tous les nœuds du domaine.

L'exemple suivant montre le contenu d'un fichier `krb5.conf` dans lequel les propriétés requises ont été définies :

```
[libdefaults]
default_realm = AFNIKRB.AFNIDEV.COM
forwardable = true
default_tkt_enctypes = rc4-hmac
udp_preference_limit = 1

[realms]
AFNIKRB.AFNIDEV.COM = {
    admin_server = SMPLKERDC01.AFNIKRB.AFNIDEV.COM
    kdc = SMPLKERDC01.AFNIKRB.AFNIDEV.COM:88
}

[domain_realm]
afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
.afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
```

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

Étape 4. Générer le nom du principal et le format Keytab

Si vous exécutez le domaine Informatica avec l'authentification Kerberos, vous devez associer les noms de principal du service (SPN) et les fichiers Keytab aux nœuds et processus de ce domaine. Informatica requiert que les fichiers Keytab authentifient les services du réseau sans demander de mot de passe.

Selon les exigences de sécurité du domaine, vous pouvez définir le principal du service selon l'un des niveaux suivants :

Niveau nœud

Si le domaine est utilisé pour le test ou le développement et ne nécessite pas un niveau élevé de sécurité, vous pouvez définir le principal du service au niveau nœud. Vous pouvez utiliser un SPN et un fichier Keytab pour le nœud et tous ses processus de service. Vous devez également configurer un SPN et un fichier Keytab distincts pour les processus HTTP du nœud.

Niveau processus

Si le domaine est utilisé pour la production et requiert un niveau élevé de sécurité, vous pouvez définir le principal du service au niveau processus. Créez un SPN et un fichier Keytab uniques pour chaque nœud et chacun de ses processus. Vous devez également configurer un SPN et un fichier Keytab distincts pour les processus HTTP du nœud.

Le domaine Informatica exige que les noms de principal de service et de fichier keytab respectent un format spécifique. Pour vous assurer que vous respectez le format correct pour les noms de principal de service et de fichier keytab, utilisez Informatica Kerberos SPN Format Generator pour générer une liste des principaux de service et des noms de fichiers keytab dans le format qu'exige le domaine Informatica.

Spécifications du principal du service au niveau nœud

Si le domaine Informatica ne nécessite pas un niveau élevé de sécurité, le nœud et les processus de service peuvent partager les mêmes SPN et fichiers Keytab. Le domaine ne nécessite pas un SPN distinct pour chaque processus de service d'un nœud.

Le domaine Informatica requiert des SPN et des fichiers Keytab pour les composants suivants au niveau nœud :

Le nom unique (DN) du principal pour le service d'annuaire LDAP

Nom de principal du DN de l'utilisateur lié qui est utilisé pour les recherches dans le service d'annuaire LDAP. Le nom du fichier Keytab doit être `infa_ldapuser.keytab`.

Processus de nœud

Nom du principal du nœud Informatica qui lance ou accepte les appels d'authentification. Le même nom de principal est utilisé pour authentifier les services dans le nœud. Chaque nœud de passerelle du domaine requiert un nom de principal spécifique.

Processus HTTP dans le domaine

Nom du principal pour tous les services d'application Web dans le domaine Informatica, y compris Informatica Administrator. Le navigateur utilise ce nom de principal pour s'authentifier auprès de tous les processus HTTP du domaine. Le nom du fichier keytab doit être `webapp_http.keytab`.

Spécifications du principal du service au niveau processus

Si le domaine Informatica nécessite un niveau élevé de sécurité, créez un SPN et un fichier Keytab distincts pour chaque nœud et chacun de ses services.

Le domaine Informatica requiert des SPN et des fichiers Keytab pour les composants suivants au niveau processus :

Le nom unique (DN) du principal pour le service d'annuaire LDAP

Nom de principal du DN de l'utilisateur lié qui est utilisé pour les recherches dans le service d'annuaire LDAP. Le nom du fichier Keytab doit être `infa_ldapuser.keytab`.

Processus de nœud

Nom du principal du nœud Informatica qui lance ou accepte les appels d'authentification.

Service Informatica Administrator

Nom du principal du service Informatica Administrator qui authentifie ce service avec d'autres services dans le domaine Informatica. Le nom du fichier Keytab doit être `_AdminConsole.keytab`.

Processus HTTP dans le domaine

Nom du principal pour tous les services d'application Web dans le domaine Informatica, y compris Informatica Administrator. Le navigateur utilise ce nom de principal pour s'authentifier auprès de tous les processus HTTP du domaine. Le nom du fichier keytab doit être `webapp_http.keytab`.

Processus de service

Nom du principal pour le service d'application exécuté sur un nœud dans le domaine Informatica. Chaque service d'application requiert un nom de principal du service et de fichier Keytab unique.

Exécution d'Informatica Kerberos SPN Format Generator sous Windows

Vous pouvez exécuter Informatica Kerberos SPN Format Generator pour générer un fichier qui affiche le format correct des SPN et des noms de fichier Keytab requis dans le domaine Informatica.

1. Sur une machine qui héberge le nœud Informatica, accédez au répertoire Informatica suivant :
`<InformaticaDirectory>/Tools/Kerberos`
2. Exécutez le fichier `SPNFormatGenerator.bat`.
La page de **bienvenue** d'Informatica Kerberos SPN Format Generator s'affiche.
3. Cliquez sur **Suivant**.
La page **Niveau principal de service** s'affiche.
4. Sélectionnez le niveau auquel définir les principaux du service Kerberos pour le domaine.

Le tableau suivant décrit les niveaux que vous pouvez sélectionner :

Niveau	Description
Niveau processus	Configure le domaine pour utiliser un nom de principal de service (SPN) et un fichier Keytab uniques pour chaque nœud et chaque service d'application sur un nœud. Le nombre de SPN et de fichiers Keytab requis pour chaque nœud dépend du nombre de processus de service d'application exécutés sur le nœud. Utilisez l'option de niveau de processus pour les domaines qui nécessitent un niveau élevé de sécurité, comme par exemple les domaines de production.
Niveau nœud	Configure le domaine pour partager les SPN et les fichiers keytab sur un nœud. Cette option nécessite un SPN et un fichier Keytab pour le nœud et tous les services d'application exécutés sur le nœud. Elle requiert également un autre SPN et un autre fichier keytab pour tous les processus HTTP s'exécutant sur le nœud. Utilisez l'option de niveau de nœud pour les domaines qui n'ont pas besoin d'un niveau élevé de sécurité, tels que les domaines de test et de développement.

5. Cliquez sur **Suivant**.

La page **Paramètres d'authentification - Authentification Kerberos** s'affiche.

6. Entrez les paramètres de domaine et de nœud pour générer le format SPN.

Le tableau suivant décrit les paramètres que vous devez indiquer :

Invite	Description
Nom du domaine	Nom du domaine. Le nom ne doit pas dépasser 128 caractères et doit être en ASCII 7 bits uniquement. Il ne peut pas contenir d'espace ni les caractères spéciaux suivants : ` % * + ; " ? , < > \ /
Nom du nœud	Nom du nœud Informatica.
Nom d'hôte du nœud	Nom d'hôte complet ou adresse IP de la machine sur laquelle créer le 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 la machine.
Nom du domaine du service	Nom du domaine Kerberos pour les services du domaine Informatica. Le nom du domaine doit être en majuscules.

Si vous définissez le principal du service au niveau nœud, l'utilitaire affiche le bouton **+Nœud**. Si vous définissez le principal du service au niveau processus, l'utilitaire affiche les boutons **+Nœud** et **+Service**.

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

Vous pouvez entrer plusieurs nœuds pour un domaine.

8. Pour générer le format SPN pour un service, cliquez sur **+Service** et spécifiez le nom du service dans le champ **Service sur le nœud**.

Le champ **Service sur le nœud** s'affiche uniquement si vous définissez le principal du service au niveau processus et cliquez sur **+Service**. Vous pouvez entrer plusieurs services pour un nœud. Les services s'affichent immédiatement sous le nœud sur lequel ils sont exécutés.

9. Pour supprimer un nœud de la liste, cliquez sur **-Nœud**.
Informatica SPN Format Generator supprime le nœud. Si vous avez ajouté des services au nœud, ils sont supprimés avec celui-ci.
10. Pour supprimer un service d'un nœud, désélectionnez le champ du nom de service.
11. Cliquez sur **Suivant**.
Le générateur de format SPN affiche le chemin et le nom du fichier qui contient la liste des noms de fichier de principal du service et Keytab.
12. Cliquez sur **Terminer** pour quitter le générateur de format SPN.
SPN Format Generator génère un fichier texte qui contient les noms du SPN et du fichier keytab dans le format requis pour le domaine Informatica.

Exécution d'Informatica Kerberos SPN Format Generator sous UNIX

Vous pouvez exécuter Informatica Kerberos SPN Format Generator pour générer un fichier qui affiche le format correct des SPN et des noms de fichier Keytab requis dans le domaine Informatica.

1. Sur une machine qui héberge le nœud Informatica, accédez au répertoire Informatica suivant :
<InformaticaDirectory>/Tools/Kerberos
2. Sur une ligne de commande shell, exécutez le fichier SPNFormatGenerator.sh.
3. Appuyez sur **Entrée** pour continuer.
4. Dans la section **Niveau principal de service**, sélectionnez le niveau auquel définir les principaux du service Kerberos pour le domaine.

Le tableau suivant décrit les niveaux que vous pouvez sélectionner :

Niveau	Description
1->Niveau processus	Configure le domaine pour utiliser un nom de principal de service (SPN) et un fichier Keytab uniques pour chaque nœud et chaque service d'application sur un nœud. Le nombre de SPN et de fichiers Keytab requis pour chaque nœud dépend du nombre de processus de service d'application exécutés sur le nœud. Utilisez l'option de niveau de processus pour les domaines qui nécessitent un niveau élevé de sécurité, comme par exemple les domaines de production.
2->Niveau nœud	Configure le domaine pour partager les SPN et les fichiers keytab sur un nœud. Cette option nécessite un SPN et un fichier Keytab pour le nœud et tous les services d'application exécutés sur le nœud. Elle requiert également un autre SPN et un autre fichier keytab pour tous les processus HTTP s'exécutant sur le nœud. Utilisez l'option de niveau de nœud pour les domaines qui n'ont pas besoin d'un niveau élevé de sécurité, tels que les domaines de test et de développement.

5. Entrez les paramètres de domaine et de nœud requis pour générer le format SPN.

Le tableau suivant décrit les paramètres que vous devez indiquer :

Invite	Description
Nom du domaine	Nom du domaine. Le nom ne doit pas dépasser 128 caractères et doit être en ASCII 7 bits uniquement. Il ne peut pas contenir d'espace ni les caractères spéciaux suivants : ` % * + ; " ? , < > \ /
Nom du nœud	Nom du nœud Informatica.
Nom d'hôte du nœud	Nom d'hôte complet ou adresse IP de la machine sur laquelle créer le 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 la machine.
Nom du domaine du service	Nom du domaine Kerberos pour les services du domaine Informatica. Le nom du domaine doit être en majuscules.

Si vous définissez le principal du service au niveau nœud, l'invite **Ajouter le nœud ?** s'affiche. Si vous définissez le principal du service au niveau processus, l'invite **Ajouter le service ?** s'affiche.

6. À l'invite **Ajouter le nœud ?**, entrez 1 pour générer le format SPN pour un autre nœud. Ensuite, entrez le nom du nœud et le nom d'hôte du nœud.
Pour générer les formats SPN pour plusieurs nœuds, entrez 1 à chaque invite **Ajouter le nœud ?**, puis entrez un nom de nœud et un nom d'hôte de nœud.
 7. À l'invite **Ajouter le service ?**, entrez 1 pour générer le format SPN pour un service qui sera exécuté sur le nœud précédent. Ensuite, entrez le nom du service.
Pour générer les formats SPN pour plusieurs services, entrez 1 à chaque invite **Ajouter le service ?**, puis entrez un nom de service.
 8. Entrez 2 pour mettre fin à l'invite **Ajouter le service ?** ou **Ajouter le nœud ?**.
Le générateur de format SPN affiche le chemin et le nom du fichier qui contient la liste des noms de fichier de principal du service et Keytab.
 9. Appuyez sur Entrée pour quitter le générateur de format SPN.
- SPN Format Generator génère un fichier texte qui contient les noms du SPN et du fichier keytab dans le format requis pour le domaine Informatica.

Étape 5. Consulter le fichier texte du format SPN et Keytab

Kerberos SPN Format Generator génère un fichier texte nommé SPNKeytabFormat.txt qui indique le format des noms de fichier de principal du service et Keytab requis par le domaine Informatica. La liste inclut les noms de fichier SPN et Keytab en fonction du niveau de principal du service que vous sélectionnez.

Consultez le fichier texte et vérifiez qu'il ne contient aucun message d'erreur.

Le fichier texte contient les informations suivantes :

Nom de l'entité

Identifie le nœud ou le service associé au processus.

SPN

Format du SPN dans la base de données de principaux Kerberos. Le SPN est sensible à la casse. Chaque type de SPN possède un format spécifique.

Un SPN peut avoir l'un des formats suivants :

Type de Keytab	Format SPN
NODE_SPN	isp/<NodeName>/<DomainName>@<REALMNAME>
NODE_AC_SPN	_AdminConsole/<NodeName>/<DomainName>@<REALMNAME>
NODE_HTTP_SPN	HTTP/<NodeHostName>@<REALMNAME> 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	<ServiceName>/<NodeName>/<DomainName>@<REALMNAME>

Nom du fichier Keytab

Format du nom du fichier Keytab à créer pour le SPN associé dans la base de données de principaux Kerberos. Le nom de fichier Keytab est sensible à la casse.

Les noms de fichier Keytab utilisent les formats suivants :

Type de Keytab	Nom du fichier Keytab
NODE_SPN	<NodeName>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<ServiceName>.keytab

Type de Keytab

Type de Keytab. Le type de Keytab peut être l'un des suivants :

- NODE_SPN. Fichier Keytab pour un processus de nœud.
- NODE_AC_SPN. Fichier Keytab pour le processus de service Informatica Administrator.
- NODE_HTTP_SPN. Fichier Keytab pour des processus HTTP dans un nœud.
- SERVICE_PROCESS_SPN. Fichier Keytab pour un processus de service.

Principaux du service au niveau nœud

L'exemple suivant 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@MY.SVCREALM.COM	Node01.keytab
NODE_SPN		
Node01	HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab
NODE_HTTP_SPN		
Node02	isp/Node02/Infadomain@MY.SVCREALM.COM	Node02.keytab
NODE_SPN		
Node02	HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM	webapp_http.keytab
NODE_HTTP_SPN		
Node03	isp/Node03/Infadomain@MY.SVCREALM.COM	Node03.keytab
NODE_SPN		


```
Node03          HTTP/NodeHost03.enterprise.com@MY.SVCREALM.COM    webapp_http.keytab
NODE_HTTP_SPN
```

Principaux du service au niveau processus

L'exemple suivant montre le contenu du fichier SPNKeytabFormat.txt généré pour les principaux du service au niveau processus :

```
ENTITY_NAME      SPN
KEY_TAB_NAME     KEY_TAB_TYPE
Node01           isp/Node01/InfaDomain@MY.SVCREALM.COM
Node01.keytab    NODE_SPN
Node01           AdminConsole/Node01/InfaDomain@MY.SVCREALM.COM
_AdminConsole.keytab NODE_AC_SPN
Node01           HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab NODE_HTTP_SPN
Node02           isp/Node02/InfaDomain@MY.SVCREALM.COM
Node02.keytab    NODE_SPN
Node02           AdminConsole/Node02/InfaDomain@MY.SVCREALM.COM
_AdminConsole.keytab NODE_AC_SPN
Node02           HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab NODE_HTTP_SPN
Service10:Node01 Service10/Node01/InfaDomain@MY.SVCREALM.COM
Service10.keytab SERVICE_PROCESS_SPN
Service100:Node02 Service100/Node02/InfaDomain@MY.SVCREALM.COM
Service100.keytab SERVICE_PROCESS_SPN
Service200:Node02 Service200/Node02/InfaDomain@MY.SVCREALM.COM
Service200.keytab SERVICE_PROCESS_SPN
```

Étape 6. Créer des noms de principal du service et des fichiers Keytab

Après avoir généré la liste des noms de fichier SPN et Keytab au format requis par Informatica, envoyez une demande à l'administrateur Kerberos pour ajouter les SPN à la base de données de principaux Kerberos et créer les fichiers Keytab.

Respectez les consignes suivantes lorsque vous créez le SPN et les fichiers Keytab :

Le nom principal de l'utilisateur (UPN) doit être le même que le SPN.

Lorsque vous créez un compte utilisateur pour le principal du service, vous devez affecter à l'UPN le même nom que le SPN. Les services d'application du domaine Informatica peuvent agir en tant que service ou en tant que client, selon l'opération. Vous devez configurer le principal du service de façon qu'il soit identifiable par les mêmes UPN et SPN.

Un compte utilisateur doit être associé à un seul SPN. Ne définissez pas plusieurs SPN pour un même compte utilisateur.

Activez la délégation dans Microsoft Active Directory.

Vous devez activer la délégation pour tous les comptes utilisateur dont les principaux de service sont utilisés dans le domaine Informatica. Dans le service Microsoft Active Directory, définissez l'option **Approuver cet utilisateur pour la délégation à tous les services (Kerberos uniquement)** pour chaque compte utilisateur pour lequel vous définissez un SPN.

L'authentification déléguée intervient quand un utilisateur est authentifié auprès d'un service et que ce service utilise les justificatifs d'identité 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 Microsoft Active Directory.

Par exemple, lorsqu'un client PowerCenter se connecte au service de référentiel PowerCenter, le compte utilisateur du client est authentifié avec le principal du service de référentiel PowerCenter. Lorsque le

service de référentiel PowerCenter se connecte au service d'intégration PowerCenter, le principal du service de référentiel PowerCenter peut utiliser le justificatif d'identité de l'utilisateur du client pour s'authentifier auprès du service d'intégration PowerCenter. Il n'est pas nécessaire que le compte utilisateur du client s'authentifie aussi auprès du service d'intégration PowerCenter.

Utilisez l'utilitaire ktpass pour créer les fichiers keytab du principal du service.

Microsoft Active Directory fournit l'utilitaire ktpass pour créer les fichiers keytab. Informatica ne prend en charge l'authentification Kerberos que sur Microsoft Active Directory et ne certifie que les fichiers keytab créés avec ktpass.

Les fichiers Keytab d'un nœud doivent être disponibles sur la machine qui héberge ce nœud. Par défaut, les fichiers Keytab sont stockés dans le répertoire suivant : `<INFA_HOME>/isp/config/keys`.

Lorsque vous recevez les fichiers Keytab de l'administrateur Kerberos, copiez-les dans le répertoire spécifié pour les fichiers Keytab utilisés dans le domaine Informatica.

Résolution des problèmes de nom de principal du service et de fichier Keytab

Vous pouvez utiliser les utilitaires Kerberos pour vérifier que les noms de principal du service et de fichier Keytab créés par l'administrateur Kerberos correspondent aux noms que vous avez demandés. Vous pouvez également utiliser les utilitaires pour déterminer le statut du centre de distribution de clés (KDC) Kerberos.

Vous pouvez utiliser des utilitaires Kerberos comme *setspn*, *kinit* et *klist* pour afficher et vérifier les SPN et les fichiers Keytab. Pour utiliser les utilitaires, vérifiez que la variable d'environnement `KRB5_CONFIG` contient le chemin et le nom du fichier de configuration Kerberos.

Remarque: Les exemples suivants présentent des moyens d'utiliser les utilitaires Kerberos afin de vérifier la validité des SPN et des fichiers Keytab. Ils peuvent être différents de la façon dont l'administrateur Kerberos utilise les utilitaires pour créer les SPN et les fichiers Keytab requis pour le domaine Informatica. 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 :

klist

Vous pouvez utiliser *klist* pour répertorier les principaux Kerberos et les clés 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 <keytab_file>
```

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

```
Keytab name: FILE:int_srv01.keytab
KVNO Timestamp      Principal
-----
 3 12/31/69 19:00:00 int_srv01/node01_vMPE/Domn96_vMPE@REALM
 3 12/31/69 19:00:00 int_srv01/node01_vMPE/Domn96_vMPE@REALM
 3 12/31/69 19:00:00 int_srv01/node01_vMPE/Domn96_vMPE@REALM
 3 12/31/69 19:00:00 int_srv01/node01_vMPE/Domn96_vMPE@REALM
 3 12/31/69 19:00:00 int_srv01/node01_vMPE/Domn96_vMPE@REALM
```

kinit

Vous pouvez utiliser *kinit* pour demander un TGT (Ticket-Granting Ticket) pour un compte utilisateur afin de vérifier que le KDC est en cours d'exécution et peut attribuer des tickets. Pour demander un TGT pour un compte utilisateur, exécutez la commande suivante :

```
kinit <user_account>
```

Vous pouvez également utiliser *kinit* pour demander un TGT et vérifier que le fichier Keytab peut être utilisé pour établir une connexion Kerberos. Pour demander un TGT pour un SPN, exécutez la commande suivante :

```
kinit -V -k -t <keytab_file> <SPN>
```

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

```
Using default cache: /tmp/krb5cc_10000073
Using principal: int_srvc01/node01_vMPE/Domn96_vMPE@REALM
Using keytab: int_srvc01.keytab
Authenticated to Kerberos v5
```

setspn

Vous pouvez utiliser *setspn* pour afficher, modifier ou supprimer le SPN d'un compte de service Active Directory. Sur la machine qui héberge le service Active Directory, ouvrez une fenêtre de ligne de commande et exécutez la commande.

Pour afficher les SPN associés à un compte utilisateur, exécutez la commande suivante :

```
setspn -L <user_account>
```

L'exemple de sortie suivant montre le SPN associé au compte utilisateur *is96svc* :

```
Registered ServicePrincipalNames for CN=is96svc,OU=AllSvcAccts,OU=People,
DC=ds,DC=intrac0rp,DC=zec0rp:
    int_srvc01/node02_vMPE/Domn96_vMPE
```

Pour afficher les comptes utilisateur associés à un SPN, exécutez la commande suivante :

```
setspn -Q <SPN>
```

L'exemple de sortie suivant montre le compte utilisateur associé au SPN *int_srvc01/node02_vMPE/Domn96_vMPE* :

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
CN=is96svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
    int_srvc01/node02_vMPE/Domn96_vMPE

Existing SPN found!
```

Pour rechercher les SPN en double, exécutez la commande suivante :

```
setspn -X
```

L'exemple de sortie suivant montre plusieurs comptes utilisateur associés à un SPN :

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
Processing entry 1125
HOST/mtb01.REALM is registered on these accounts:
    CN=Team1svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
    CN=MTB1svc,OU=IIS,OU=WPC960K3,OU=WINServers,DC=ds,DC=intrac0rp,DC=zec0rp
```

Remarque: La recherche de SPN en double peut prendre beaucoup de temps et consommer une grande quantité de mémoire.

kdestroy

Vous pouvez utiliser *kdestroy* pour supprimer les tickets d'autorisation Kerberos actifs et le cache des justificatifs d'identité de l'utilisateur qui les contient. Si vous exécutez *kdestroy* sans paramètres, vous supprimez le cache de justificatifs d'identité par défaut.

Étape 7. Configurer l'authentification Kerberos pour le domaine

Exécutez la commande `infasetup` pour changer l'authentification du domaine Informatica en authentification réseau Kerberos.

Remarque: Vérifiez que tous les objets du référentiel sont archivés avant de configurer le domaine pour utiliser l'authentification Kerberos.

Lorsque vous exécutez la commande `infasetup` pour modifier l'authentification du domaine, elle crée les domaines de sécurité LDAP suivants :

- Domaine de sécurité interne : Le domaine de sécurité interne dans un domaine de sécurité LDAP portant le nom `_infalInternalNamespace`. Le domaine de sécurité `_infalInternalNamespace` contient le compte administrateur par défaut créé lors de la configuration de l'authentification Kerberos. Après avoir configuré l'authentification Kerberos, vous ne pouvez pas ajouter d'utilisateurs au domaine de sécurité `_infalInternalNamespace` ni supprimer ce dernier.
- Domaine de sécurité de la zone de l'utilisateur. Le domaine de sécurité de la zone de l'utilisateur est un domaine de sécurité LDAP portant le nom de la zone de l'utilisateur Kerberos. Après avoir configuré l'authentification Kerberos, vous pouvez importer des utilisateurs de la base de données de principaux Kerberos dans le domaine de sécurité du domaine des utilisateurs.

La commande `infasetup` crée également un compte administrateur. Vous pouvez spécifier le nom d'utilisateur de l'administrateur. Une fois l'authentification Kerberos configurée, le domaine de sécurité `_infalInternalNamespace` contient le compte administrateur.

Pour configurer le domaine pour utiliser l'authentification Kerberos, exécutez la commande suivante :

```
infasetup switchToKerberosMode
```

1. Sur le nœud principal de passerelle, exécutez la commande `infasetup` pour modifier l'authentification du domaine.

Lorsque vous y êtes invité, accédez au répertoire dans lequel les programmes de ligne de commande Informatica sont installés. Par défaut, les programmes de ligne de commande sont installés dans le répertoire suivant : `<InformaticaInstallationDir>/isp/bin`

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

Entrez les commandes suivantes :

- Windows : `infasetup switchToKerberosMode`
- UNIX : `infasetup.sh switchToKerberosMode`

Le tableau suivant décrit les options de la commande switchToKerberosMode :

Option	Argument	Description
-administratorName -ad	administrator_name	Nom d'utilisateur du compte administrateur du domaine qui est créé lors de la configuration de l'authentification Kerberos. Le compte utilisateur doit se trouver dans la base de données de principaux Kerberos. Une fois l'authentification Kerberos configurée, cet utilisateur est inclus dans le domaine de sécurité <i>_infalInternalNamespace</i> .
-ServiceRealmName -srn	realm _name_of_node_spn	Nom du domaine Kerberos auquel les services du domaine Informatica appartiennent. Le nom de domaine, sensible à la casse, doit être en majuscules. Le nom du domaine de service et le nom du domaine d'utilisateur doivent être identiques.
-UserRealmName -urn	realm _name_of_user_spn	Nom du domaine Kerberos auquel les utilisateurs du domaine Informatica appartiennent. Le nom de domaine, sensible à la casse, doit être en majuscules. Le nom du domaine de service et le nom du domaine d'utilisateur doivent être identiques.
-SPNShareLevel -spnSL	PROCESS NODE	Niveau du principal du service pour le domaine. Définissez la propriété sur l'un des niveaux suivants : <ul style="list-style-type: none"> - Processus. Le domaine requiert un nom unique de principal du service (SPN) et un fichier Keytab pour chaque nœud et chaque service sur ce nœud. Le nombre de SPN et de fichiers Keytab requis pour chaque nœud dépend du nombre de processus de service exécutés sur le nœud. Utilisez l'option de niveau processus si le domaine requiert un niveau élevé de sécurité, par exemple un domaine de production. - Nœud. Le domaine utilise un SPN et un fichier Keytab pour le nœud et tous les services exécutés sur celui-ci. Il requiert également un SPN et un fichier Keytab distincts pour tous les processus HTTP sur le nœud. Utilisez l'option de niveau nœud si le domaine ne requiert pas un niveau élevé de sécurité, par exemple un domaine de test ou de développement. La valeur par défaut est le processus.

La commande switchToKerberosMode fait passer le mode d'authentification pour le domaine de l'authentification utilisateur LDAP à l'authentification réseau Kerberos.

Étape 8. Mise à jour des nœuds dans le domaine

Exécutez la commande `infasetup` pour mettre à jour tous les autres nœuds du domaine avec les informations du serveur d'authentification Kerberos.

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

Pour mettre à jour les nœuds de passerelle et les nœuds de travail, utilisez les commandes suivantes :

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 chacun d'entre eux.

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 chacun d'entre eux.

1. Sur une machine qui héberge un nœud Informatica, exécutez la commande `infasetup` pour mettre à jour ce nœud.

Lorsque vous y êtes invité, accédez au répertoire dans lequel les programmes de ligne de commande Informatica sont installés. Par défaut, les programmes de ligne de commande sont installés dans le répertoire suivant : `<InformaticaInstallationDir>/isp/bin`

2. 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`

Le tableau suivant décrit les options de mise à jour des informations d'authentification Kerberos pour un nœud :

Option	Argument	Description
<code>-EnableKerberos</code> <code>-krb</code>	<code>enable_kerberos</code>	Configure le domaine Informatica pour utiliser l'authentification Kerberos.
<code>-ServiceRealmName</code> <code>-srn</code>	<code>realm</code> <code>_name_of_node_spn</code>	Nom du domaine Kerberos auquel les services du domaine Informatica appartiennent. Le nom de domaine, sensible à la casse, doit être en majuscules. Le nom du domaine de service et le nom du domaine d'utilisateur doivent être identiques.
<code>-UserRealmName</code> <code>-urn</code>	<code>realm</code> <code>_name_of_user_spn</code>	Nom du domaine Kerberos auquel les utilisateurs du domaine Informatica appartiennent. Le nom de domaine, sensible à la casse, doit être en majuscules. Le nom du domaine de service et le nom du domaine d'utilisateur doivent être identiques.

Étape 9. Mettez à jour les machines du client

Copiez le fichier de configuration Kerberos et définissez la variable d'environnement sur les machines qui hébergent les clients Informatica. Vous devez également configurer le navigateur pour accéder aux applications Web 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 les machines clientes.

Copiez le fichier de configuration sur chaque machine qui héberge un client Informatica. Vous devez copier le fichier `krb5.conf` dans le répertoire suivant : `<Informatica Client Directory>/shared/security`

Définissez les variables d'environnement KRB5_CONFIG avec le fichier de configuration Kerberos.

Utilisez la variable d'environnement KRB5_CONFIG pour stocker le chemin d'accès et le nom du fichier de configuration Kerberos, `krb5.conf`. Vous devez définir la variable d'environnement KRB5_CONFIG sur chaque machine qui héberge un client Informatica.

Configurez le navigateur Web.

Si le domaine Informatica s'exécute sur un réseau avec l'authentification Kerberos, vous devez configurer le navigateur afin d'autoriser l'accès aux applications Web Informatica. Dans Microsoft Internet Explorer et Google Chrome, ajoutez l'URL de l'application Web Informatica à la liste des sites de confiance. Si vous utilisez Chrome version 41 ou ultérieure, vous devez également définir les stratégies `AuthServerWhitelist` et `AuthNegotiateDelegateWhitelist`.

Sous UNIX, créez un fichier cache des justificatifs d'identité pour l'authentification unique

Pour exécuter les programmes de ligne de commande Informatica sous UNIX avec l'authentification unique, vous devez générer un fichier cache des justificatifs d'identité pour authentifier le compte utilisateur exécutant les commandes sur le réseau Kerberos. Utilisez l'utilitaire `kinit` depuis MIT Kerberos pour générer le fichier cache des justificatifs d'identité. Le fichier cache des justificatifs d'identité permet à un utilisateur d'exécuter les commandes sans les options de nom d'utilisateur et de mot de passe.

Si vous utilisez un fichier cache des justificatifs d'identité, vous devez définir le chemin et le nom par défaut du cache des justificatifs d'identité dans la variable d'environnement KRB5CCNAME.

Pour plus d'informations sur l'exécution des programmes de ligne de commande Informatica sous UNIX avec l'authentification unique, consultez le *Guide de référence des commandes d'Informatica*.

Étape 10. Démarrage du domaine Informatica

Après avoir configuré le domaine Informatica pour qu'il utilise l'authentification Kerberos, démarrez le domaine et l'outil Administrator.

1. Sous Windows, vous pouvez démarrer le service Informatica depuis le Panneau de Configuration ou le menu Démarrer.

Pour démarrer Informatica depuis le menu Démarrer de Windows, cliquez sur **Programmes > Informatica [Version] > Serveur**. Cliquez sur **Démarrer les services Informatica** et sélectionnez **Exécuter en tant qu'administrateur**.

Sous UNIX, exécutez la commande suivante pour démarrer le démon Informatica :

```
infaservice.sh startup
```

Par défaut, `infaservice.sh` est installé dans le répertoire suivant : `<INFA_HOME>/tomcat/bin`

2. Démarrez Informatica Administrator.

Utilisez l'URL suivante pour démarrer l'outil Administrator : `http://<nom d'hôte complet>:<port http>`. Si vous avez configuré l'outil Administrator pour utiliser une connexion sécurisée, utilisez le protocole HTTPS : `https://<nom d'hôte complet>:<port http>`

Lorsque vous démarrez l'outil Administrator, vous devez ajouter l'URL à la liste des sites de confiance du navigateur.

3. Sélectionnez le domaine de sécurité pour votre compte utilisateur.

Si vous utilisez l'authentification Kerberos, le réseau utilise l'authentification unique. Vous n'avez pas besoin de vous connecter à l'outil Administrator avec un nom d'utilisateur et un mot de passe.

Après la configuration de l'authentification Kerberos

Si le principal du service du domaine est au niveau processus, un SPN et un fichier Keytab sont nécessaires pour chaque service que vous créez dans le domaine. Avant d'activer un service, vérifiez qu'un SPN et un fichier Keytab sont disponible pour ce service. Kerberos ne peut pas authentifier le service d'application si celui-ci ne dispose pas d'un fichier Keytab dans le répertoire Informatica.

Si aucun SPN ni fichier Keytab n'est disponible pour les services d'application que vous prévoyez de créer sur le domaine, vous devez créer le SPN et le fichier Keytab avant d'activer le service. Vous pouvez utiliser Informatica Kerberos SPN Format Generator pour générer le format du nom de fichier SPN et Keytab pour le service. Pour enregistrer l'heure, choisissez les noms des services que vous voulez créer et les nœuds sur lesquels ils s'exécuteront. Ensuite, exécutez l'utilitaire pour générer le format de nom de fichier SPN et Keytab pour tous les services en même temps.

Pour plus d'informations sur l'exécution d'Informatica Kerberos SPN Format Generator, voir ["Étape 4. Générer le nom du principal et le format Keytab" à la page 35](#).

Envoyez une demande à l'administrateur Kerberos pour ajouter les SPN à la base de données de principaux et créer le fichier Keytab correspondant.

Lorsque vous recevez les fichiers Keytab de l'administrateur Kerberos, copiez-les dans le répertoire spécifié pour ces fichiers. Par défaut, les fichiers Keytab sont stockés dans le répertoire suivant : `<INFA_HOME>/isp/config/keys`

Si le principal du service du domaine est au niveau nœud, vous pouvez créer et activer les services d'application sans créer de SPN et de fichiers Keytab supplémentaires.

CHAPITRE 5

Sécurité de domaine

Ce chapitre comprend les rubriques suivantes :

- [Présentation de la sécurité de domaine, 49](#)
- [Communication sécurisée à l'intérieur du domaine, 50](#)
- [Connexions sécurisées à un service d'application Web, 61](#)
- [Sources et cibles sécurisées, 65](#)
- [Stockage de données sécurisé, 66](#)
- [Services et ports d'application, 71](#)

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 client.

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. Après l'installation, vous pouvez configurer la communication sécurisée dans le domaine à partir de l'outil Administrator 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, telles que le service Analyst, 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.

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 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 un 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`.

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_keystore.pem` et d'un keystore au format JKS nommé `infa_keystore.jks`.

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.

Pour plus d'informations sur la méthode de création d'un keystore et d'un truststore personnalisés, consultez l'article How-To Library Informatica « How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain » : <https://mysupport.informatica.com/docs/DOC-12984>

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 entrepôt de clés et truststore lors de l'exécution de 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. Exécutez la commande de mise à jour du domaine.

Lorsque vous y êtes invité, accédez au répertoire dans lequel les programmes de ligne de commande Informatica sont installés. Par défaut, les programmes de ligne de commande sont installés dans le répertoire suivant : <InformaticaInstallationDir>/isp/bin

3. Exécutez la commande infacmd avec les options et les arguments requis.

Entrez la commande suivante :

- 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

4. Arrêtez le domaine.
Le domaine doit être arrêté avant l'exécution des commandes infasetup.
5. 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 entrepôt de clés aux formats PEM et JKS. Les fichiers entrepôt de clés 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. Obligatoire si vous utilisez votre propre certificat SSL. Répertoire contenant les fichiers truststore. Le domaine Informatica requiert le certificat SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir des fichiers truststore aux formats PEM et JKS. Les fichiers truststore doivent être nommés infa_truststore.jks et infa_truststore.pem. 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. Obligatoire si vous utilisez votre propre certificat SSL. Mot de passe du fichier infa_truststore.jks.

6. 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 entrepôt de clés et truststore pour tous les nœuds du domaine.

7. Redémarrez le domaine.

Après avoir mis à jour tous les nœuds du domaine, vous devez mettre à jour les machines qui hébergent les outils clients Informatica. Définissez l'emplacement des certificats SSL dans les variables d'environnement truststore Informatica.

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 entrepôt de clés et `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` pour mettre à jour les fichiers de configuration Informatica et spécifier les fichiers de certificat SSL.

Lorsque vous y êtes invité, accédez au répertoire dans lequel les programmes de ligne de commande Informatica sont installés. Par défaut, les programmes de ligne de commande sont installés dans le répertoire suivant : `<InformaticaInstallationDir>/isp/bin`

8. 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 entrepôt de clés aux formats PEM et JKS. Les fichiers entrepôt de clés 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. Obligatoire si vous utilisez votre propre certificat SSL. Répertoire contenant les fichiers truststore. Le domaine Informatica requiert le certificat SSL au format PEM et dans des fichiers Java Keystore (JKS). Le répertoire doit contenir des fichiers truststore aux formats PEM et JKS. Les fichiers truststore doivent être nommés infa_truststore.jks et infa_truststore.pem. 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. Obligatoire si vous utilisez votre propre certificat SSL. 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 entrepôt de clés et truststore pour tous les nœuds du domaine.

- Redémarrez le domaine.

Après avoir mis à jour tous les nœuds du domaine, vous devez mettre à jour les machines qui hébergent les outils clients Informatica. Définissez l'emplacement des certificats SSL dans les variables d'environnement truststore Informatica.

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. Spécifiez l'emplacement et le mot de passe des fichiers truststore utilisés pour sécuriser le domaine avec des variables d'environnement.

Si vous utilisez le certificat SSL Informatica par défaut, vous n'avez pas besoin de définir la variable d'environnement `INFA_TRUSTSTORE` ou `INFA_TRUSTSTORE_PASSWORD`. Lorsque vous installez les clients Informatica, le programme d'installation définit les variables d'environnement et installe les fichiers truststore par défaut dans le répertoire suivant : `<Répertoire d'installation Informatica>\clients\shared\security`

Si vous fournissez les certificats SSL à utiliser, copiez les fichiers truststore sur la machine qui héberge le client et définissez dans la variable `INFA_TRUSTSTORE` le répertoire qui contient les fichiers truststore. Vous devez disposer de fichiers truststore en format JKS et PEM nommés `infa_truststore.jks` et `infa_truststore.pem`. Vous devez également définir dans la variable `INFA_TRUSTSTORE_PASSWORD` le mot de passe pour le fichier `infa_truststore.jks`.

Utilisez les variables d'environnement suivantes pour les informations truststore :

INFA_TRUSTSTORE

Définissez dans cette variable le répertoire qui contient les fichiers truststore pour les certificats SSL. Le répertoire doit contenir les fichiers truststore nommés `infa_truststore.jks` et `infa_truststore.pem`.

INFA_TRUSTSTORE_PASSWORD

Définissez dans cette variable le mot de passe du fichier `infa_truststore.jks`. Le mot de passe doit être crypté. Utilisez le programme de ligne de commande `pmpasswd` pour crypter le mot de passe.

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
-DatabaseTlsEnabled -dbtls	database_tls_enabled	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 True.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Obligatoire. Chemin et nom du fichier truststore contenant le certificat SSL pour la base de données.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Obligatoire. Mot de passe du fichier truststore de la base de données sécurisée.

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

EncryptionMethod

Obligatoire. 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 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 par rapport au nom d'hôte figurant dans le certificat SSL.

cryptoProtocolVersion

Requis pour Oracle si le domaine Informatica s'exécute sur AIX et que le niveau de cryptage de la base de données Oracle est défini sur TLS. Définissez le paramètre sur
`cryptoProtocolVersion=TLSv1,TLSv1.1,TLSv1.2.`

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

Restaurer la table suivante :

- ISP_RUN_LOG

- 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 infasetup RestoreDomain 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

Obligatoire. 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 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 par rapport au nom d'hôte figurant dans le certificat SSL.

cryptoProtocolVersion

Requis pour Oracle si le domaine Informatica s'exécute sur AIX et que le niveau de cryptage de la base de données Oracle est défini sur TLS. Définissez le paramètre sur

`cryptoProtocolVersion=TLSv1,TLSv1.1,TLSv1.2`.

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

Vous pouvez sécuriser la connexion entre l'outil Administrator 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 de la console Hub des services Web
- Service Metadata Manager
- Service de l'analyseur de données

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

Lorsque vous créez le service Analyst, vous pouvez configurer les propriétés HTTPS sécurisées de l'outil Analyst.

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 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 entrepôt de clés	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 Analyst utilise le mot de passe par défaut <i>changeit</i> .
Protocole SSL	Laissez ce champ vierge.

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 pour 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 souhaitez configurer le protocole de sécurité SSL 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. Si vous configurez HTTPS, vérifiez que le numéro de port précédant le port HTTPS est également disponible. Par exemple, si vous configurez 10255 pour le numéro de port HTTPS, vous devez vérifier que 10254 est également disponible. Metadata Manager utilise le port 10254 pour le protocole HTTP.
Fichier entrepôt de clés	Fichier keystore contenant les clés et les certificats requis si vous utilisez le protocole de sécurité SSL avec l'application Web Metadata Manager. Remarque: Le service Metadata Manager utilise le cryptage RSA. Par conséquent, Informatica vous recommande d'utiliser un certificat SSL généré avec l'algorithme RSA.
Mot de passe keystore	Mot de passe du fichier keystore.

Sécurité pour l'analyseur de données

Lorsque vous créez le service de rapports, vous pouvez configurer les propriétés HTTPS sécurisées de l'analyseur de données.

Pour sécuriser la connexion entre le navigateur et les services de rapports, configurez la propriété suivante du service de rapports :

Propriété	Description
Activer le protocole HTTPS sur le port	Port SSL utilisé par le service de rapports pour les connexions sécurisées. Vous pouvez modifier la valeur si vous avez configuré le port HTTPS pour le nœud où vous créez le service de rapports. Entrez une valeur comprise entre 1 et 65535 et assurez-vous qu'elle est différente de celle du port HTTP. Si le nœud sur lequel vous créez le service de rapports n'est pas configuré pour le port HTTPS, vous ne pouvez pas configurer le protocole HTTPS pour le service de rapports. La valeur par défaut est 16443.

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, Qualité des données ou Profilage dans l'outil Developer ou Administrator.

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

Obligatoire. 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 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 par rapport au nom d'hôte figurant 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 des 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 `rwx` 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 `rwx` 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 cryptage contient un fichier nommé *sitekey*, Informatica renomme le fichier *siteKey_old*.

migrateEncryptionKey

Modifie la clé de cryptage utilisée pour stocker les données sensibles dans le domaine Informatica.

Remarque: Si le domaine contient un service de rapports, ne modifiez pas la clé de cryptage. La commande `migrateEncryptionKey` échoue si le domaine contient un service de rapports.

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 cryptage pour le domaine, exécutez la commande `infasetup generateEncryptionKey`.

Spécifiez les options suivantes requises pour générer une clé de cryptage :

Option	Argument	Description
-keyword -kw	keyword	Chaîne de texte utilisée comme mot de base à partir duquel générer une clé de cryptage. Le mot clé doit respecter les critères suivants : <ul style="list-style-type: none">- Il comporte entre 8 et 20 caractères.- Il doit inclure au moins une lettre en majuscule.- Il doit inclure au moins une lettre en minuscule.- Il doit inclure au moins un chiffre.- Il ne doit pas contenir d'espaces.
-domainName -dn	domain_name	Nom du domaine Informatica.
-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.

4. Pour modifier la clé de cryptage du domaine, exécutez la commande `infasetup migrateEncryptionKey` et spécifiez l'emplacement de l'ancienne clé de cryptage 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>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 dans le domaine à mettre à jour et crypter les données sensibles dans les référentiels avec la nouvelle clé de cryptage.

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 présente le port par défaut associé au domaine Informatica :

Type	Port par défaut
Configuration du domaine	La valeur par défaut est 6005. Vous pouvez modifier le port par défaut lors de l'installation. Vous pouvez modifier le port après l'installation avec la commande <code>infasetup updateGatewayNode</code> .
Gestionnaire de service	6006
Arrêt du gestionnaire de service	6007
Informatica Administrator (HTTP)	6008
Informatica Administrator (HTTPS)	8443
Arrêt d'Informatica Administrator	6009
Processus de service (minimum)	6013
Processus de service (maximum)	6113

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 Analyst (base de données temporaire)	Aucun port par défaut. Saisissez le numéro de port de la base de données.

Service de gestion du contenu

Le tableau suivant présente le port par défaut associé au service de gestion du contenu :

Type	Port par défaut
Service de gestion du contenu (HTTP)	8105
Service de gestion du contenu (HTTPS)	Aucun port par défaut. Saisissez le numéro de port requis lorsque vous créez le service.

Service Data Director

Le tableau suivant présente le port par défaut associé au service Data Director :

Type	Port par défaut
Service Data Director (HTTP)	Aucun port par défaut. Saisissez le numéro de port requis lorsque vous créez le service.
Service Data Director (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)	8085
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.

Type	Port par défaut
Base de données de l'entrepôt de profilage	Aucun port par défaut. Saisissez le numéro de port de la base de données.
Base de données des tâches humaines	Aucun port par défaut. Saisissez le numéro de port de la base de données.

Service du gestionnaire de métadonnées

Le tableau suivant présente le port par défaut associé au service du gestionnaire de métadonnées :

Type	Port par défaut
Service du gestionnaire de métadonnées (HTTP)	La valeur par défaut est 10250.
Service du gestionnaire de métadonnées (HTTPS)	Aucun port par défaut. Saisissez le numéro de port requis lorsque vous créez le service. Si vous configurez HTTPS, vérifiez que le numéro de port précédant le port HTTPS est également disponible. Par exemple, si vous configurez 10255 pour le numéro de port HTTPS, vous devez vérifier que 10254 est également disponible. Le gestionnaire de métadonnées utilise le port 10254 pour HTTP.

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 de rapports

Le tableau suivant présente le port par défaut associé au service de rapports :

Type	Port par défaut
Service de rapports (HTTP)	16080
Service de rapports (HTTPS)	16443

Service de création de rapports et de tableaux de bord

Le tableau suivant présente le port par défaut associé au service de création de rapports et de tableaux de bord :

Type	Port par défaut
Service de création de rapports et de tableaux de bord (HTTP)	Aucun port par défaut. Saisissez le numéro de port requis lorsque vous créez le service.
Service de création de rapports et de tableaux de bord (HTTPS)	Aucun port par défaut. Saisissez le numéro de port requis lorsque vous créez le service.

Service du hub de services Web

Le tableau suivant présente le port par défaut associé au service du hub de services Web :

Type	Port par défaut
Service du hub de services Web (HTTP)	7333
Service du hub de services Web (HTTPS)	7343

CHAPITRE 6

Gestion de la sécurité dans Informatica Administrator

Ce chapitre comprend les rubriques suivantes :

- [Présentation de l'utilisation d'Informatica Administrator, 75](#)
- [Sécurité utilisateur, 77](#)
- [Onglet Sécurité, 79](#)
- [Gestion du mot de passe, 83](#)
- [Gestion de la sécurité de domaine, 83](#)
- [Gestion de la sécurité des utilisateurs, 84](#)

Présentation de l'utilisation d'Informatica Administrator

Informatica Administrator est l'outil d'administration que vous utilisez pour administrer le domaine Informatica 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 applications exécutées dans le 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 du domaine

Gérer des journaux, objets de domaine et autorisations utilisateur. Surveiller les tâches et applications exécutées dans le service d'intégration de données.

Tâches d'administration du domaine

Gérer des journaux, objets de domaine et autorisations utilisateur.

Tâches d'administration de la sécurité

Gérer les utilisateurs, les groupes, les rôles et les privilèges.

L'outil Administrator comprend les onglets suivants :

Domaine

Afficher et modifier les propriétés du domaine et les objets à l'intérieur du domaine.

Journaux

Afficher les événements du journal pour le domaine et les services à l'intérieur du domaine.

Surveillance

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.

Surveillance

Afficher l'état des tâches de profil, les tâches de fiche d'évaluation, les tâches d'aperçu, les tâches de mappage, les services de données SQL, les services Web et les flux de travail pour chaque service d'intégration de données.

Surveillance

Afficher l'état des tâches de profil, les tâches d'aperçu, les tâches de mappage et les flux de travail pour le service d'intégration de données.

Surveillance

Afficher et surveiller les déploiements Ultra Messaging.

Rapports

Exécuter un rapport des services Web ou un rapport de gestion des licences.

Sécurité

Gérer les utilisateurs, les groupes, les rôles et les privilèges.

Sécurité

Gérer les utilisateurs, les groupes, les rôles et les privilèges. Si vous utilisez PowerCenter Express Personal Edition, vous n'avez pas accès à l'onglet Sécurité.

Sécurité

Gérer les utilisateurs, les groupes, les rôles et les privilèges.

L'outil Administrator possède les éléments d'en-tête suivants :

Se déconnecter

Déconnectez-vous de l'outil Administrator.

Gérer

Gérez votre compte.

Aide

Accédez à l'aide pour l'onglet actuel et déterminez la version d'Informatica.

Aide

Accédez à l'aide pour l'onglet actuel, déterminez la version d'Informatica, et configurez la politique d'utilisation de données.

Aide

Accédez à l'aide pour l'onglet actuel, déterminez la version d'Informatica, et configurez la politique d'utilisation de données.

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 Data Analyzer, Informatica Administrator, Informatica Analyst, Informatica Developer, Metadata Manager et le client PowerCenter. 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 et Informatica Developer. Le gestionnaire de service et certains services d'application contrôlent la sécurité utilisateur dans les clients d'application. Le client d'application inclut Informatica Administrator.

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 du contenu
- Service Metadata Manager
- Service de rapports
- Service de rapports et de tableaux de bord
- Service du hub de services Web

Vous pouvez également utiliser HTTPS pour sécuriser la connexion au domaine et aux services d'application. Les services d'application suivants prennent en charge la connexion HTTPS ainsi que le domaine Informatica :

- Service d'intégration de données
- Service Analyst

Vous pouvez également utiliser HTTPS pour sécuriser la connexion au domaine et aux services d'application.

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.

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.

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.

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 lancez un client d'application à partir d'un autre, le client d'application transmet le jeton d'application au client d'application suivant. Le client d'application suivant envoie le jeton d'authentification au gestionnaire de service pour authentification de l'utilisateur.

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.

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
- Service de rapports

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 de référentiel modèle

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 de Data Analyzer
- Référentiel modèle
- Référentiel PowerCenter
- Référentiel PowerCenter pour Metadata Manager

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 :

- Redémarrage du Service Metadata Manager, du service de référentiel modèle, du service de référentiel PowerCenter ou du Reporting service.
- 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.

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 :

- Vous redémarrez le service de référentiel modèle.
- Vous ajoutez ou supprimez des utilisateurs ou des groupes natifs.

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.

L'onglet Sécurité possède les composants suivants :

- Section Rechercher. Recherche des utilisateurs, groupes ou rôles par nom.
- Navigateur. Le navigateur s'affiche dans le panneau de gauche et affiche les groupes, utilisateurs et rôles.
- Volet 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 profils LDAP et les profils du système d'exploitation. Vous pouvez également afficher les utilisateurs possédant les privilèges pour un service.
- Menu Actions de sécurité. Contient des options pour créer ou supprimer un groupe, un utilisateur ou un rôle.
- Menu Actions de sécurité. Contient des options pour créer ou supprimer un groupe, un utilisateur ou un rôle.

Remarque: Si vous utilisez PowerCenter Express Personnel Edition, vous n'avez pas accès à l'onglet Sécurité

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 volet de contenu de l'onglet Sécurité. Lorsque vous sélectionnez un objet dans le navigateur, le volet de contenu affiche des informations sur l'objet.

Le navigateur dans l'onglet Sécurité comprend les sections suivantes :

- 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.

Le navigateur fournit différents moyens d'effectuer une tâche. Vous pouvez utiliser l'une des méthodes suivantes pour gérer les groupes, utilisateurs et rôles :

- Cliquer sur le menu Actions. Chaque section du navigateur comprend un menu Actions pour gérer les groupes, utilisateurs ou rôles. Sélectionnez un objet dans le navigateur et cliquez sur le menu Actions pour créer, supprimer ou déplacer des groupes, utilisateurs ou rôles.
- Cliquer avec le bouton droit de la souris sur un objet. Cliquez avec le bouton droit de la souris sur un objet dans le navigateur pour afficher les options Créer, Supprimer et Déplacer disponibles dans le menu Actions.
- Faire glisser un objet d'une section à une autre. Sélectionnez un objet et faites-le glisser vers une autre section du navigateur pour affecter l'objet à un autre objet. Par exemple, pour affecter un utilisateur à un

groupe natif, vous pouvez sélectionner un utilisateur dans la section Utilisateurs du navigateur et le faire glisser vers un groupe natif dans la section Groupes.

- Faire glisser plusieurs utilisateurs ou rôles depuis le volet de contenu vers le navigateur. Sélectionnez plusieurs utilisateurs ou rôles dans le volet de contenu et faites-les glisser vers le navigateur pour affecter ces objets à un autre objet. Par exemple, pour affecter plusieurs utilisateurs à un groupe natif, vous pouvez sélectionner le dossier Natif dans la section Utilisateurs du navigateur pour afficher tous les utilisateurs natifs dans le volet de contenu. Utilisez les touches Ctrl ou Maj pour sélectionner plusieurs utilisateurs et faire glisser les utilisateurs sélectionnés vers un groupe natif de la section Groupes du navigateur.
- 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.

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.

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.

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. Cliquez avec le bouton droit de la souris sur un groupe, puis sélectionnez Aller à l'élément pour afficher les détails du groupe dans le volet de contenu.

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.

Utilisateurs

Un utilisateur avec un compte dans le domaine Informatica peut se connecter aux clients d'applications suivants :

- Informatica Administrator
- Client PowerCenter
- Metadata Manager
- Data Analyzer

- Informatica Developer
- Informatica Analyst
- Jaspersoft

Un utilisateur avec un compte dans le domaine Informatica peut se connecter aux clients d'applications suivants :

- Informatica Administrator
- Informatica Developer

Un utilisateur avec un compte dans le domaine Informatica peut se connecter à Informatica Administrator.

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.

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.

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.

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. Cliquez avec le bouton droit de la souris sur un utilisateur et sélectionnez Naviguer dans un élément pour afficher les détails de l'utilisateur dans le volet de contenu.

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.

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. Cliquez avec le bouton droit sur un rôle et sélectionnez Naviguer dans un élément pour afficher les détails du rôle dans le volet de contenu.

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.

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 ou avec l'URL suivante : `http://<host>:<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.

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, 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.

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, le nœud, la licence, les connexions de base de données 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.

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.

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.

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.

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 7

Utilisateurs et groupes

Ce chapitre comprend les rubriques suivantes :

- [Présentation des utilisateurs et groupes](#) [Utilisateurs et groupes, 85](#)
- [Groupes par défaut, 86](#)
- [Comprendre les comptes utilisateurs, 87](#)
- [Gestion des utilisateurs, 90](#)
- [Gestion des groupes, 98](#)
- [Gestion des profils de systèmes d'exploitation, 100](#)
- [Verrouillage de compte, 105](#)

Présentation des utilisateurs et 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. Les tâches que vous pouvez effectuer dépendent du type de compte utilisateur dont vous disposez et du type de licence PowerCenter Express.

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.

Remarque: Si vous installez PowerCenter Express Personal Edition, vous devez utiliser le compte d'administrateur par défaut pour toutes les opérations. Vous ne pouvez pas créer des utilisateurs ou des groupes et gérer les autorisations.

La gestion des comptes d'utilisateurs dans Informatica implique les composants clés suivants :

- **Utilisateurs.** Vous pouvez configurer différents types de comptes d'utilisateurs 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.

- 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.
- 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.
- 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 PowerCenter sous UNIX, vous pouvez le configurer pour utiliser les profils de systèmes d'exploitation lors de l'exécution des flux de travail. 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.
- 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 l'outil Developer. Vous pouvez également déverrouiller un compte utilisateur.
- Verrouillage de compte. Vous pouvez configurer le verrouillage d'un compte pour verrouiller un compte utilisateur lorsque l'utilisateur indique une mauvaise connexion à l'outil Administrator. 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 :

- Tout le monde
- Administrateur

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.

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

Un domaine Informatica peut posséder les types de compte suivants :

- Administrateur par défaut
- Administrateur de domaine
- Administrateur de client d'application
- Utilisateur

Le domaine Informatica possède un compte administrateur par défaut.

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.

L'administrateur par défaut est un compte utilisateur du domaine de sécurité natif. Vous ne pouvez pas créer d'administrateur par défaut. 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.

L'administrateur de domaine peut se connecter à l'outil Administrator et configurer les services d'application dans le 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 Data Analyzer

Dispose de toutes les autorisations et de tous les privilèges dans Data Analyzer. L'administrateur Data Analyzer peut se connecter à Data Analyzer pour créer et gérer des objets Data Analyzer et effectuer toutes les tâches dans le client d'application.

Pour créer un administrateur Data Analyzer, attribuez à un utilisateur le rôle administrateur pour un Reporting service.

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 du gestionnaire de métadonnées.

Administrateur Jaspersoft

Privilèges d'administrateur mappés au rôle ROLE_ADMINISTRATOR dans Jaspersoft.

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 rapports 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 créer, modifier et supprimer des utilisateurs selon le type de licence PowerCenter Express. Vous pouvez attribuer des rôles, autorisations et privilèges à un compte utilisateur. Les rôles, autorisations et privilèges attribués à l'utilisateur déterminent les tâches que l'utilisateur peut effectuer dans le domaine Informatica. Si vous utilisez PowerCenter Express Personnel Edition, vous ne pouvez pas créer d'utilisateurs ou de groupes. Vous devez utiliser l'utilisateur Administrateur par défaut pour effectuer toutes les tâches.

Vous pouvez créer, modifier et supprimer des utilisateurs selon le type de licence. Vous pouvez attribuer des rôles, autorisations et privilèges à un compte utilisateur. Les rôles, autorisations et privilèges attribués à l'utilisateur déterminent les tâches que l'utilisateur peut effectuer dans le domaine Informatica.

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 Création d'utilisateursCréation d'utilisateurs

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	<p>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.</p> <p>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 : , + " \ < > ; / * % ? &</p> <p>Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Tous les autres caractères d'espacement sont interdits.</p> <p>Remarque: Data Analyzer utilise le nom de compte utilisateur et le domaine de sécurité au format <i>UserName@SecurityDomain</i> pour déterminer la longueur du nom de connexion utilisateur. La combinaison du nom utilisateur, du symbole @ et du domaine de sécurité ne peut pas dépasser 128 caractères.</p>
Mot de passe	<p>Mot de passe du compte utilisateur. Le mot de passe peut comprendre de 1 à 80 caractères maximum.</p>
Confirmer le mot de passe	<p>Saisissez une nouvelle fois le mot de passe pour le confirmer. Vous devez saisir une nouvelle fois le mot de passe. Ne faites pas un copier-coller du mot de passe.</p>

Propriété	Description
Nom complet	Nom complet du compte utilisateur. Le nom complet ne peut pas inclure les caractères spéciaux suivants : < > " Remarque: Dans Data Analyzer, la propriété du nom complet équivaut à trois propriétés distinctes que l'on appelle prénom, deuxième prénom et nom de famille.
Description	Description du compte utilisateur. La description ne peut pas dépasser 765 caractères, ni inclure les caractères spéciaux suivants : < > "
E-mail	Adresse email de l'utilisateur. L'adresse e-mail ne peut pas inclure les caractères spéciaux suivants : < > " Saisissez l'adresse e-mail 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 assigner 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 assigner 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 des groupes assignés et cliquez sur Supprimer.
6. Cliquez sur OK pour enregistrer les assignations 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, cliquez sur l'onglet Sécurité.
2. Dans la section Groupes du navigateur, sélectionnez un groupe natif et cliquez sur Modifier.
3. Cliquez sur l'onglet Utilisateurs.
4. Pour assigner un utilisateur LDAP à un groupe, sélectionnez un utilisateur LDAP dans la colonne Tous les utilisateurs et cliquez sur Ajouter.
5. Pour retirer un utilisateur LDAP d'un groupe, sélectionnez un utilisateur LDAP dans la colonne des utilisateurs assignés et cliquez sur Supprimer.
6. Cliquez sur OK pour enregistrer les assignations 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.

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. 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 Data Analyzer

Lorsque vous supprimez un utilisateur, Data Analyzer supprime les alertes, les comptes e-mail d'alerte et les dossiers et tableaux de bord personnels associés à l'utilisateur.

Data Analyzer supprime tous les rapports auxquels l'utilisateur souscrit selon le profil de sécurité du rapport. Data Analyzer conserve un profil de sécurité pour chacun des utilisateurs qui souscrit au rapport. Un rapport qui utilise une sécurité basée sur l'utilisateur se sert du profil de sécurité de l'utilisateur qui accède au rapport. Un rapport qui utilise une sécurité basée sur le fournisseur se sert du profil de sécurité de l'utilisateur qui possède le rapport.

Lorsque vous supprimez un utilisateur, Data Analyzer ne supprime aucun rapport dans le dossier public dont l'utilisateur est le propriétaire. Data Analyzer peut exécuter un rapport avec une sécurité basée sur les utilisateurs même si le propriétaire du rapport n'existe pas. Toutefois, Data Analyzer ne peut pas déterminer le profil de sécurité d'un rapport ayant une sécurité basée sur le fournisseur si le propriétaire du rapport n'existe pas. Avant de supprimer un utilisateur, vérifiez que les rapports avec une sécurité basée sur le fournisseur ont un nouveau propriétaire.

Si par exemple, vous souhaitez supprimer l'utilisateur A qui possède un rapport dans un dossier public ayant une sécurité basée sur le fournisseur. Créez ou sélectionnez un utilisateur ayant le même profil de sécurité que l'utilisateur A. Identifiez tous les rapports ayant une sécurité basée sur le fournisseur dans le dossier public dont l'utilisateur A est le propriétaire. Faites ensuite se connecter l'utilisateur ayant le même profil de sécurité et sauvegardez les rapports dans le dossier public avec une sécurité basée sur le fournisseur et le même nom de rapport. Ceci vous assure qu'après la suppression de l'utilisateur, les rapports restent dans le dossier public avec la même sécurité.

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, ExportObjects, ImportDomainObjects et ImportObjects
- infacmd oie 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. Configure 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 la commande `infacmd isp getUserActivityLog` ou l'onglet Journaux de l'outil Administrator pour afficher les journaux d'activité utilisateur. Utilisez les événements du journal d'activité utilisateur pour déterminer quand un utilisateur a créé, mis à jour ou supprimé des services, nœuds, utilisateurs, groupes ou rôles.

Exécutez la commande suivante pour afficher les événements du journal d'activité utilisateur pour tous les utilisateurs :

```
infacmd isp getUserActivityLog -dn domain_name -un user_name -pd password
```

La commande requiert le rôle Administrateur ou l'appartenance au groupe d'administration.

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 sur la ligne de commande ou les écrire 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 les journaux d'activité utilisateur et l'onglet Journaux de l'outil Administrator, consultez le *Guide d'Informatica Administrator*.

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.

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.

Vous pouvez attribuer des rôles, autorisations et privilèges à un groupe. Les rôles, autorisations et privilèges attribués au groupe déterminent les tâches que les utilisateurs du groupe peuvent effectuer dans le domaine.

Vous pouvez attribuer des rôles, autorisations et privilèges à un groupe. 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.

Un groupe natif peut contenir des comptes d'utilisateurs 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.

Un groupe natif peut contenir des comptes d'utilisateurs 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

Si le PowerCenter Integration Service utilise les profils de système d'exploitation, il exécute les workflows avec les paramètres de profil du système d'exploitation attribués au workflow ou au dossier contenant le workflow.

Vous pouvez créer, modifier, supprimer et attribuer des autorisations aux profils du système d'exploitation dans la boîte de dialogue Configuration des profils de système d'exploitation.

Pour afficher la boîte de dialogue Configuration des profils de système d'exploitation, cliquez sur Configuration des profils de système d'exploitation du menu Actions de sécurité.

Procédez comme suit pour configurer un profil de système d'exploitation :

1. Créez un profil de système d'exploitation.
2. Configurez les variables du processus de service et les variables d'environnement dans les propriétés de profil du système d'exploitation.
3. Attribuez les autorisations aux profils de système d'exploitation.

Créer des profils des systèmes d'exploitation

Créez des profils des systèmes d'exploitation si le service d'intégration PowerCenter en utilise.

Le tableau suivant décrit les propriétés que vous devez configurer pour créer un profil du système d'exploitation :

Propriété	Description
Nom	Nom du profil du 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 d'espaces 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.
Nom d'utilisateur système	Nom d'un utilisateur de système d'exploitation qui existe sur les ordinateurs où le service d'intégration PowerCenter est exécuté. Le service d'intégration PowerCenter exécute des flux de travail en utilisant l'accès système de l'utilisateur du système défini pour le profil du 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.
\$PMRootDir	Répertoire racine accessible par le nœud. Répertoire racine pour d'autres variables de processus de service. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " ,

Vous ne pouvez pas modifier le nom ou le nom de l'utilisateur système après avoir créé un profil du système d'exploitation. Si vous ne voulez pas utiliser l'utilisateur du système d'exploitation spécifié dans le profil de ce dernier, supprimez-le. Après avoir supprimé le profil du système d'exploitation, attribuez-en un autre aux dossiers du référentiel auquel il était assigné.

Propriétés des profils de systèmes d'exploitation

Après avoir créé un profil de système d'exploitation, configurez les propriétés correspondantes. Pour modifier les propriétés d'un profil de système d'exploitation, sélectionnez le profil dans la boîte de dialogue Configuration des profils du système d'exploitation, puis cliquez sur Modifier.

Remarque: Les variables de processus de service qui sont définies dans les propriétés de session et les fichiers de paramètres remplacent les paramètres de profils de systèmes d'exploitation.

Le tableau suivant décrit les propriétés d'un profil de système d'exploitation :

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 où le PowerCenter Integration Service est exécuté. Le PowerCenter Integration Service exécute des workflows à l'aide de l'accès de l'utilisateur du système défini pour le profil de système d'exploitation.
\$PMRootDir	Répertoire racine accessible par le nœud. Répertoire racine pour d'autres variables de processus de service. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " ,
\$PMSessionLogDir	Répertoire pour les journaux de sessions. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/SessLogs.
\$PMBadFileDir	Répertoire pour les fichiers de rejet. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/BadFiles.
\$PMCacheDir	Répertoire pour les 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 PowerCenter Integration Service. N'utilisez pas un 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 pour les fichiers cibles. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/TgtFiles.
\$PMSourceFileDir	Répertoire pour les fichiers sources. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/SrcFiles.
\$PMExtProcDir	Répertoire pour les procédures externes. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/ExtProc.
\$PMTempDir	Répertoire pour les fichiers temporaires. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/Temp.

Propriété	Description
\$PMLookupFileDir	Répertoire pour les fichiers de recherche. Il ne peut pas inclure les caractères spéciaux suivants : * ? < > " , La valeur par défaut est \$PMRootDir/LkpFiles.
\$PMStorageDir	Répertoire pour les fichiers d'exécution. Les fichiers de récupération des workflows sont enregistrés dans le répertoire \$PMStorageDir configuré dans les propriétés du PowerCenter Integration Service. Les fichiers de récupération des workflows 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 des workflows. 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.

Création d'un profil de système d'exploitation

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans le menu Actions de sécurité, cliquez sur Configuration des profils de système d'exploitation.
La boîte de dialogue Configuration des profils de système d'exploitation s'affiche.
3. Cliquez sur Créer un profil.
4. Entrez le nom d'utilisateur, le nom de l'utilisateur système et \$PMRootDir.
5. Cliquez sur OK.
Après avoir créé le profil, vous devez configurer ses propriétés.
6. Cliquez sur le profil de système d'exploitation que vous souhaitez configurer.
7. Sélectionnez l'onglet Propriétés et cliquez sur Modifier.
8. Modifiez les propriétés et cliquez sur OK.
9. Sélectionnez l'onglet Autorisations.
Une liste de tous les utilisateurs possédant une autorisation sur le profil de système d'exploitation s'affiche.
10. Cliquez sur Modifier.
11. Modifiez l'autorisation et cliquez sur OK.

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`.

- Par ailleurs, si le service d'intégration PowerCenter utilise l'option Session ou Grille, vous devez définir les variables d'environnement suivantes pour le 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`.

INFA_KEYSTORE_PASSWORD

Définissez la valeur sur le mot de passe du fichier `infa_keystore.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.

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 systèmes 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 systèmes 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 8

Privilèges et rôles

Ce chapitre comprend les rubriques suivantes :

- [Présentation des privilèges et des rôles, 107](#)
- [Privilèges du domaine, 110](#)
- [Privilèges du service Analyst, 119](#)
- [Privilèges du service de gestion de contenu, 120](#)
- [Privilèges du service d'intégration de données, 121](#)
- [Privilèges du Metadata Manager Service, 121](#)
- [Privilèges du service de référentiel modèle, 125](#)
- [Privilèges du PowerCenter Repository Service, 127](#)
- [Privilèges du service d'écoute PowerExchange, 141](#)
- [Privilèges du service de journalisation PowerExchange, 141](#)
- [Privilèges du Reporting Service, 142](#)
- [Privilèges du service de reporting et de tableaux de bord, 149](#)
- [Privilèges du service Test Data Manager, 150](#)
- [Gestion des rôles, 158](#)
- [Attribution de privilèges et de rôles aux utilisateurs et aux groupes, 163](#)
- [Affichage des utilisateurs avec des privilèges pour un service, 165](#)
- [Résolution des problèmes de privilèges et de rôles, 166](#)

Présentation des privilèges et des rôles

Vous gérez la sécurité utilisateur grâce aux privilèges et aux rôles.

Vous pouvez modifier des privilèges et des rôles selon le type de licence PowerCenter Express.

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 dans le domaine Informatica que l'utilisateur peut effectuer à l'aide de l'outil Administrator et des programmes de ligne de commande infacmd et pmrep.

- Privilèges du domaine. Déterminent les actions dans le domaine Informatica que l'utilisateur peut effectuer à l'aide de l'outil Administrator.
- 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 et Informatica Analyst.
- 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 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'intégration de données. Détermine les actions dans les applications que l'utilisateur peut effectuer à l'aide de l'outil Administrator. Ce privilège détermine également si les utilisateurs peuvent développer et exporter les résultats du profil.
- 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.
- Privilège du service de référentiel modèle. Détermine les actions dans les projets que l'utilisateur peut effectuer à l'aide 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 Reporting Service. Déterminent les actions de rapports que l'utilisateur peut effectuer à l'aide de Data Analyzer.
- Privilèges du service de création de rapports et de tableaux de bord. Déterminent les actions que l'utilisateur peut effectuer à l'aide de Jaspersoft.
- Privilèges du service Test Data Manager. Déterminent les tâches de découverte de données, de masquage des données, de sous-ensemble de données et de génération de données de test que les utilisateurs peuvent effectuer à l'aide de Test Data Manager.

Les privilèges déterminent les actions que les utilisateurs peuvent effectuer dans les clients de l'application. Informatica fournit des privilèges du domaine qui déterminent les actions que les utilisateurs peuvent effectuer à l'aide de l'outil Administrator.

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 assignez des privilèges aux utilisateurs et groupes dans l'onglet Sécurité de l'outil Administrator.

L'outil Administrator 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 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.
- Administration de domaine. Inclut des privilèges pour gérer le domaine, les dossiers et les services d'application.
- 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.
- Outils. Inclut les privilèges de connexion à l'outil Administrator.
- Surveillance. Inclut les privilèges de surveillance des déploiements Ultra Messaging et d'affichage des statistiques.

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 assignez 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 assignez 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 assignez des rôles et autorisations aux groupes, vous pouvez simplifier les tâches d'administration de l'utilisateur. Par exemple, si un utilisateur change de poste au sein d'une organisation, déplacez l'utilisateur vers un autre groupe. Si un nouvel utilisateur rejoint l'organisation, ajoutez l'utilisateur à un groupe. L'utilisateur hérite des rôles et autorisations assignés au groupe. Vous n'avez pas besoin de réassigner les privilèges, rôles et autorisations. Pour plus d'informations, consultez l'article Bibliothèque de procédures Informatica [Using Groups and Roles to Manage Informatica Access Control](#).

Astuce: Si vous organisez des utilisateurs en groupes puis assignez des rôles et autorisations aux groupes, vous pouvez simplifier les tâches d'administration de l'utilisateur. Par exemple, si un utilisateur change de poste au sein d'une organisation, déplacez l'utilisateur vers un autre groupe. Si un nouvel utilisateur rejoint l'organisation, ajoutez l'utilisateur à un groupe. L'utilisateur hérite des rôles et autorisations assignés au groupe. Vous n'avez pas besoin de réassigner les privilèges, rôles et autorisations.

Privilèges du domaine

Les privilèges du domaine déterminent les actions que les utilisateurs peuvent effectuer à l'aide de l'outil Administrator et des programmes de ligne de commande infacmd et pmrep.

Les privilèges du domaine déterminent les actions que les utilisateurs peuvent effectuer à l'aide de l'outil Administrator.

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 les privilèges de gestion du domaine, des dossiers, nœuds, grilles, licences, services d'application et connexions.
Surveillance	Inclut les privilèges de configuration des préférences 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.
Administration Cloud	Inclut les privilèges permettant d'ajouter des organisations Informatica Cloud dans l'outil Administrator et les afficher.

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 de gestion du domaine, des services d'application et des connexions.
Surveillance	Inclut les privilèges de configuration des préférences 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.

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 de gestion du domaine, des services d'application et des connexions.
Surveillance	Inclut des privilèges de surveillance des déploiements UM et d'affichage des statistiques.
Outils	Inclut les privilèges de connexion à l'outil Administrator.

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.

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 assigné le rôle Administrateur sur le domaine peut effectuer les tâches suivantes :

- Créer des profils de système d'exploitation.
- Accorder des autorisations pour les profils de système d'exploitation.
- Supprimer 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.
- 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 assignées 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 : - Afficher les propriétés de domaine et les événements du journal. - Configurer les paramètres globaux.
Dossier	L'utilisateur peut afficher les propriétés du 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 de services Web	L'utilisateur peut exécuter le rapport des services Web.

Autorisation pour	Description
Domaine	L'utilisateur peut effectuer les actions suivantes : - Afficher les propriétés de domaine et les événements du journal. - Configurer les paramètres globaux.
Service d'application	L'utilisateur peut afficher les propriétés du service d'application et les événements du journal.
Nœud	L'utilisateur peut afficher les propriétés du nœud.

Remarque: Pour réaliser des tâches de gestion de domaine dans l'outil Administrator, les utilisateurs doivent également posséder le privilège Accès à Informatica Administrator.

Privlège 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.

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.- 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.

Autorisation pour	Description
Service Metadata Manager	<p>L'utilisateur peut effectuer les actions suivantes :</p> <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 du gestionnaire de métadonnées. <p>Remarque: Pour créer ou restaurer le contenu du référentiel Metadata Manager, l'utilisateur doit faire partie du groupe Administrateur par défaut.</p>
Service Metadata Manager Service de référentiel PowerCenter	L'utilisateur peut restaurer le référentiel PowerCenter pour Metadata Manager.
Service de référentiel modèle	<p>L'utilisateur peut effectuer les actions suivantes :</p> <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.
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 le gestionnaire du référentiel PowerCenter. - 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 le gestionnaire du référentiel PowerCenter. - 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 de rapports	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Sauvegarder, restaurer et mettre à niveau le contenu du référentiel de Data Analyzer. - Créer et supprimer le contenu du référentiel de Data Analyzer.
Service Test Data Manager	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Créer et supprimer le contenu du référentiel Test Data Manager. - Mettre 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.

Autorisation pour	Description
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.

Autorisation pour	Description
Domaine d'exécution du service d'application 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.
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.

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	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Configurer et arrêter des nœuds et des grilles. - Accorder des autorisations sur les nœuds et grilles.
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.

Privlège 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 : <ul style="list-style-type: none">- 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.

Privlège 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.

L'utilisateur ayant le privilège Gérer les connexions peut créer, modifier et supprimer des connexions dans l'outil Administrator, 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.

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.
- Prévisualiser les données ou exécuter un mappage 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.
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.

Groupe de privilèges Surveillance

Les privilèges dans le groupe 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 dans le groupe Surveillance :

Privilège	Autorisation pour	Description
Configurer les paramètres globaux	Domaine	L'utilisateur peut configurer les paramètres globaux.
Configurer les statistiques et les rapports	Domaine	L'utilisateur peut configurer les préférences des statistiques et des rapports de surveillance.
Afficher les tâches d'autres utilisateurs	-	L'utilisateur peut afficher les tâches d'autres utilisateurs.
Afficher les statistiques	-	L'utilisateur peut afficher les statistiques pour les objets du domaine.
Afficher les rapports	-	L'utilisateur peut pour afficher les rapports pour les objets du domaine.
Accéder à partir de l'outil d'analyse	-	L'utilisateur peut accéder à la fonction de surveillance de l'outil Analyst.
Accéder à partir de l'outil Developer	-	L'utilisateur peut accéder à la fonction de surveillance de l'outil Developer.
Accéder à partir de l'outil Administrator	-	L'utilisateur peut accéder à la fonction de surveillance de l'outil Administration.
Autoriser les actions pour les tâches	-	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Abandonner les tâches.- Réexécuter les tâches de mappage.- Afficher les journaux pour une tâche.

Privilège	Autorisation pour	Description
Configurer les paramètres globaux	Domaine	L'utilisateur peut configurer les paramètres globaux.
Configurer les statistiques et les rapports	Domaine	L'utilisateur peut configurer les préférences des statistiques et des rapports de surveillance.
Afficher les tâches d'autres utilisateurs	-	L'utilisateur peut afficher les tâches d'autres utilisateurs.
Afficher les statistiques	-	L'utilisateur peut afficher les statistiques pour les objets du domaine.

Privilège	Autorisation pour	Description
Afficher les rapports	-	L'utilisateur peut pour afficher les rapports pour les objets du domaine.
Accéder à partir de l'outil Developer	-	L'utilisateur peut accéder à la fonction de surveillance de l'outil Developer.
Accéder à partir de l'outil Administrator	-	L'utilisateur peut accéder à la fonction de surveillance de l'outil Administration.
Autoriser les actions pour les tâches	-	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Abandonner les tâches. - Réexécuter les tâches de mappage. - Afficher les journaux pour une tâche.

Pour accéder à l'affichage en lecture seule de l'onglet Surveillance, le privilège Accès à Informatica Administrator n'est pas nécessaire.

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	Autorisation	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.

Pour réaliser des tâches dans l'outil Administrator, les utilisateurs doivent posséder le privilège Accès à Informatica Administrator.

Pour exécuter les commandes infacmd ou pour accéder à l'affichage en lecture seule de l'onglet Surveillance, les utilisateurs n'ont pas besoin du privilège Accès à Informatica Administrator.

Groupe de privilèges d'administration Cloud

Les privilèges du groupe Surveillance déterminent quels utilisateurs 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 dans les projets. Exécuter sur la connexion de la source de données relationnelles.	L'utilisateur peut exécuter des profils et des fiches d'évaluation pour des utilisateurs sous licence dans l'outil Analyst.
Accéder aux spécifications de mappage	Lire dans les projets.	L'utilisateur peut accéder aux spécifications de mappage pour les utilisateurs sous licence dans l'outil Analyst.
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 les glossaires	-	L'utilisateur peut gérer le glossaire métier.

Privilège	Autorisation	Description
Accès à l'espace de travail	-	L'utilisateur peut accéder aux espaces de travail suivants dans l'outil Analyst : - 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.

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 développer et exporter les résultats de profil à l'aide de l'outil Developer.

Le tableau suivant répertorie les autorisations requises et les actions que les utilisateurs peuvent effectuer avec le privilège du groupe de privilèges Administration des applications :

Nom du privilège	Autorisation pour	Description
Gérer les applications	Service d'intégration de données	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
Développer et exporter les résultats	Lire dans 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.

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.	Écriture	L'utilisateur peut partager un dossier contenant un raccourci avec d'autres utilisateurs et d'autres groupes.
Afficher le lignage	S. O.	Lecture	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 métier. - 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.	Lecture	L'utilisateur peut afficher les catalogues associés.
Afficher les rapports	S. O.	Lecture	L'utilisateur peut afficher les rapports Metadata Manager dans l'analyseur de données.
Afficher les résultats de profil	S. O.	Lecture	L'utilisateur peut afficher les informations de profilage pour des objets de métadonnées dans le catalogue depuis une source relationnelle.
Afficher le catalogue	S. O.	Lecture	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Afficher les ressources et les objets de métadonnées dans le catalogue de métadonnées. - Rechercher dans le catalogue de métadonnées.

Privilège	Inclut les privilèges	Autorisation	Description
Afficher les relations	S. O.	Lecture	L'utilisateur peut afficher les relations pour des objets de métadonnées, des catégories et des termes d'entreprise.
Gérer les relations	Afficher les relations	Écriture	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.	Lecture	L'utilisateur peut afficher les commentaires pour des objets de métadonnées, des catégories et des termes d'entreprise.
Publier des commentaires	Afficher les commentaires	Écriture	L'utilisateur peut ajouter les commentaires pour des objets de métadonnées, des catégories et des termes d'entreprise.
Supprimer les commentaires	<ul style="list-style-type: none"> - Publier des commentaires - Afficher les commentaires 	Écriture	L'utilisateur peut supprimer des commentaires pour des objets de métadonnées, des catégories et des termes d'entreprise.
Afficher les liens	S. O.	Lecture	L'utilisateur peut afficher les liens pour des objets de métadonnées, des catégories et des termes d'entreprise.
Gérer les liens	Afficher les liens	Écriture	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.	Lecture	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Affichez les glossaires métier dans la vue Glossaire. - Rechercher des glossaires métier.
Gérer les objets	S. O.	Écriture	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - 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. Ajouter des attributs à des modèles intégrés.
Exporter/Importer des modèles	Afficher le modèle	-	L'utilisateur peut importer et exporter des modèles personnalisés et des modèles intégrés modifiés.

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 privilèges du service de référentiel modèle déterminent les actions que les utilisateurs peuvent effectuer sur les projets à l'aide d'Informatica Developer.

Les privilèges du service de référentiel modèle et les autorisations d'objet de référentiel modèle déterminent les tâches que les utilisateurs peuvent effectuer sur les projets et les objets qu'ils contiennent.

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
-	Lire dans le projet	L'utilisateur peut afficher les projets et les objets qu'ils contiennent.
-	Écrire dans le projet	L'utilisateur peut créer, modifier et supprimer des objets dans les projets.
-	Attribuer sur le projet	L'utilisateur peut attribuer et révoquer des autorisations sur les projets pour les utilisateurs et les groupes.
Accéder à Analyst	-	L'utilisateur peut accéder au référentiel modèle à partir de l'outil Analyst.
Accès à Developer	-	L'utilisateur peut accéder au référentiel modèle à partir de l'outil Developer.
Créer, modifier et supprimer des projets	-	L'utilisateur peut effectuer les actions suivantes : - Créer des projets.
Créer, modifier et supprimer des projets	Écrire dans les projets.	L'utilisateur peut effectuer les actions suivantes : - 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	-	L'utilisateur peut créer, modifier et supprimer des domaines de données dans un glossaire de domaine de données. Affichez ce privilège sous le titre Administration de domaine de données .
Gérer les notifications	-	L'utilisateur peut configurer les notifications de fiche d'évaluation. Affichez ce privilège sous le titre Profilage de l'administration .
Afficher les détails de sécurité	-	L'utilisateur peut afficher les noms des projets pour lesquels les utilisateurs n'ont pas d'autorisation de lecture par erreur et de détails de message d'avertissement.

Privilège	Autorisation	Description
-	Lire dans le projet	L'utilisateur peut afficher les projets et les objets qu'ils contiennent.
-	Écrire dans le projet	L'utilisateur peut créer, modifier et supprimer des objets dans les projets.
-	Attribuer sur le projet	L'utilisateur peut attribuer et révoquer des autorisations sur les projets pour les utilisateurs et les groupes.
Accès à Developer	-	L'utilisateur peut accéder au référentiel modèle à partir de l'outil Developer.

Privilège	Autorisation	Description
Créer, modifier et supprimer des projets	-	L'utilisateur peut effectuer les actions suivantes : - Créer des projets. - Mettre à niveau le service de référentiel modèle.
Créer, modifier et supprimer des projets	Écrire dans le projet	L'utilisateur peut effectuer les actions suivantes : - Modifier des projets. - Supprimez des projets si l'utilisateur les a créés.
Afficher les détails de sécurité	-	L'utilisateur peut afficher les noms des projets pour lesquels les utilisateurs n'ont pas d'autorisation de lecture par erreur et de détails de message 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 : - Se connecter au référentiel PowerCenter à l'aide du Repository Manager. - Exécuter les commandes <i>pmrep</i> .
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 Reporting Service

Les privilèges du Reporting Service déterminent les actions de rapports que l'utilisateur peut effectuer à l'aide de Data Analyzer.

Le tableau suivant décrit chaque groupe de privilèges pour le Reporting Service :

Groupe de privilèges	Description
Administration	Comprend les privilèges pour gérer les objets dans l'onglet Administration de Data Analyzer.
Alertes	Comprend les privilèges pour gérer les objets dans l'onglet Alertes de Data Analyzer.
Communication	Comprend les privilèges pour partager les informations de tableaux de bord ou de reporting avec d'autres utilisateurs.
Répertoire de contenu	Comprend les privilèges pour gérer les objets dans l'onglet Rechercher de Data Analyzer.
Tableaux de bord	Comprend les privilèges pour gérer les tableaux de bord dans Data Analyzer.
Indicateurs	Comprend les privilèges pour gérer les indicateurs dans Data Analyzer.
Gérer le compte	Comprend les privilèges pour gérer les objets dans l'onglet Compte de Data Analyzer.
Rapports	Comprend les privilèges pour gérer les rapports dans Data Analyzer.

Groupe de privilèges Administration

Les privilèges du groupe de privilèges Administration déterminent les tâches que les utilisateurs peuvent effectuer dans l'onglet Administration de l'analyseur de données.

Le tableau suivant répertorie les privilèges et les autorisations du groupe de privilèges Administration :

Privilège	Inclut les privilèges	Autorisation	Description
Gérer le schéma	-	Lire, écrire et exécuter dans : - Le dossier de mesures - Le dossier d'attributs - Le dossier de dimensions du modèle - Métrologie - Attribut - Dimension du modèle	L'utilisateur peut créer, modifier et supprimer des tables de schéma.
Exporter/importer les fichiers XML	-	-	L'utilisateur peut exporter ou importer des métadonnées sous forme de fichiers XML.
Gérer l'accès utilisateur	-	-	L'utilisateur peut gérer des utilisateurs, des groupes et des rôles.
Configurer les plannings et les tâches	-	Lire, écrire et supprimer les plannings basés sur les événements et sur les heures.	L'utilisateur peut créer et gérer des plannings et des tâches.
Gérer les propriétés du système	-	-	L'utilisateur peut gérer les paramètres et les propriétés du système.
Configurer les limites de demande	- Gérer les propriétés du système	-	L'utilisateur peut accéder aux paramètres de gestion des demandes.
Configurer les flux de messages en temps réel	-	-	L'utilisateur peut ajouter, modifier et supprimer des flux de message en temps réel.

Groupe de privilèges Alertes

Les privilèges du groupe de privilèges Alertes déterminent les tâches que les utilisateurs peuvent effectuer dans l'onglet Alertes de l'analyseur de données.

Le tableau suivant répertorie les privilèges et les autorisations du groupe de privilèges Alertes :

Privilège	Inclut les privilèges	Autorisation	Description
Recevoir des alertes	-	-	L'utilisateur peut recevoir et afficher les alertes déclenchées.
Créer des alertes en temps réel	- Recevoir des alertes	-	L'utilisateur peut créer une alerte pour un rapport en temps réel.
Configurer des options de génération	- Recevoir des alertes	-	L'utilisateur peut configurer les options de génération d'alertes.

Groupe de privilèges de communication

Les privilèges dans le groupe de privilèges de communication déterminent les tâches que les utilisateurs peuvent effectuer pour partager des informations de tableau de bord ou de rapports avec d'autres utilisateurs.

Le tableau suivant répertorie les privilèges et les autorisations du groupe de privilèges de communication :

Privilège	Inclut les privilèges	Autorisation	Description
Print	-	Lire dans le rapport Lire dans le tableau de bord	L'utilisateur peut imprimer les rapports et les tableaux de bord.
Envoyer par e-mail les liens de l'objet	-	Lire dans le rapport Lire dans le tableau de bord	L'utilisateur peut envoyer des liens pour les rapports ou les tableaux de bord dans un courriel.
Envoyer par e-mail le contenu de l'objet	- Envoyer par e-mail les liens de l'objet	Lire dans le rapport Lire dans le tableau de bord	L'utilisateur peut envoyer le contenu d'un rapport ou d'un tableau de bord dans un courriel.
Exporter	-	Lire dans le rapport Lire dans le tableau de bord	L'utilisateur peut exporter les rapports et tableaux de bord.
Exporter vers Excel ou au format CSV	- Exporter	Lire dans le rapport Lire dans le tableau de bord	L'utilisateur peut exporter les rapports vers Excel ou vers des fichiers de valeurs séparées par des virgules.
Exporter vers un tableau croisé dynamique	- Exporter - Exporter vers Excel ou au format CSV	Lire dans le rapport Lire dans le tableau de bord	L'utilisateur peut exporter les rapports vers un tableau croisé dynamique Excel.
Afficher les discussions	-	Lire dans le rapport Lire dans le tableau de bord	L'utilisateur peut lire des discussions.
Ajouter les discussions	- Afficher les discussions	Lire dans le rapport Lire dans le tableau de bord	L'utilisateur est capable d'ajouter des messages aux discussions.

Privilège	Inclut les privilèges	Autorisation	Description
Gérer les discussions	- Afficher les discussions	Lire dans le rapport Lire dans le tableau de bord	L'utilisateur peut supprimer les messages et les commentaires des discussions.
Envoyer des commentaires	-	Lire dans le rapport Lire dans le tableau de bord	L'utilisateur peut créer des messages de commentaires.

Groupe de privilèges Répertoire de contenu

Les privilèges du groupe de privilèges Répertoire de contenu déterminent les tâches que les utilisateurs peuvent effectuer dans l'onglet Rechercher de l'analyseur de données.

Le tableau suivant répertorie les privilèges et les autorisations du groupe de privilèges Répertoire de contenu :

privilège	Inclut les privilèges	Autorisation	Description
Accéder au répertoire de contenu	-	Lire dans les dossiers	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Accéder aux dossiers et au contenu de l'onglet Rechercher. - Accéder aux dossiers personnels. - Rechercher les éléments disponibles pour les utilisateurs avec le rôle Client de base. - Rechercher les rapports par nom ou rechercher les rapports que vous utilisez fréquemment. - Afficher les rapports du concepteur PowerCenter ou du gestionnaire de flux de travail.
Accéder à la recherche avancée	- Accéder au répertoire de contenu	Lire dans les dossiers	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Rechercher des éléments avancés. - Rechercher les rapports que vous créez ou les rapports utilisés par un utilisateur spécifique.
Gérer le répertoire de contenu	- Accéder au répertoire de contenu	Lire et écrire dans les dossiers	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none"> - Créer des dossiers. - Copier un dossier. - Couper et coller les dossiers. - Renommer les dossiers.

privilège	Inclut les privilèges	Autorisation	Description
Gérer le répertoire de contenu	- Accéder au répertoire de contenu	Supprimer dans les dossiers	L'utilisateur peut supprimer des dossiers.
Gérer les documents partagés	- Accéder au répertoire de contenu - Gérer le répertoire de contenu	Lire dans les dossiers Écrire dans les dossiers	L'utilisateur peut gérer les documents partagés dans les dossiers.

Groupe de privilèges du tableau de bord

Les privilèges du groupe de privilèges du tableau de bord déterminent les tâches que les utilisateurs peuvent effectuer dans les tableaux de bord de l'analyseur de données.

Le tableau suivant répertorie les privilèges et les autorisations du groupe de privilèges du tableau de bord :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher les tableaux de bord	-	Lire dans les tableaux de bord	L'utilisateur peut afficher le contenu des tableaux de bord personnels et des tableaux de bord publics.
Gérer le tableau de bord personnel	- Afficher les tableaux de bord	Lire et écrire dans les tableaux de bord	L'utilisateur peut gérer le tableau de bord personnel.
Créer, modifier et supprimer des tableaux de bord	- Afficher les tableaux de bord	Lire et écrire dans les tableaux de bord	L'utilisateur peut effectuer les actions suivantes : - Créer des tableaux de bord. - Modifier des tableaux de bord.
Créer, modifier et supprimer des tableaux de bord	- Afficher les tableaux de bord	Supprimer dans les tableaux de bord	L'utilisateur peut supprimer des tableaux de bord.
Accéder à la création de tableaux de bord de base	- Afficher les tableaux de bord - Créer, modifier et supprimer des tableaux de bord	Lire et écrire dans les tableaux de bord	L'utilisateur peut effectuer les actions suivantes : - Utiliser les options de configuration de base du tableau de bord. - Diffuser les tableaux de bord sous forme de liens.
Accéder à la création de tableaux de bord avancés	- Afficher les tableaux de bord - Créer, modifier et supprimer des tableaux de bord - Accéder à la création de tableaux de bord de base	Lire et écrire dans les tableaux de bord	L'utilisateur peut utiliser toutes les options de configuration du tableau de bord.

Groupe de privilèges d'indicateurs

Les privilèges du groupe de privilèges d'indicateurs déterminent les tâches que peuvent effectuer les utilisateurs avec les indicateurs.

Le tableau suivant répertorie les privilèges et les autorisations du groupe de privilèges d'indicateurs :

Privilège	Inclut les privilèges	Autorisation	Description
Interagir avec les indicateurs	-	Lire dans le rapport Écrire dans le tableau de bord	L'utilisateur peut utiliser et interagir avec les indicateurs.
Créer un indicateur en temps réel	-	Lire et écrire dans le rapport Écrire dans le tableau de bord	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Créer un indicateur dans un rapport en temps réel.- Créer un indicateur d'évaluation.
Obtenir des mises à jour automatiques continues d'indicateurs en temps réel	-	Lire dans le rapport	L'utilisateur peut afficher des mises à jour d'indicateurs continues, automatiques et animées en temps réel.

Groupe de privilèges Gérer les comptes

Le privilège du groupe de privilèges Gérer les comptes détermine les tâches que les utilisateurs peuvent effectuer dans l'onglet Gérer les comptes de l'analyseur de données.

Le tableau suivant répertorie les privilèges et autorisations du groupe de privilèges Gérer les comptes :

Privilège	Inclut les privilèges	Autorisation	Description
Gérer les paramètres personnels	-	-	L'utilisateur peut configurer les préférences personnelles du compte.

Groupe de privilèges Rapports

Les privilèges du groupe de privilèges Rapports déterminent les tâches que les utilisateurs peuvent effectuer avec les rapports dans l'analyseur de données.

Le tableau suivant répertorie les privilèges et les autorisations du groupe de privilèges Rapports :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher les rapports	-	Lire dans le rapport	Affichez les rapports et les métadonnées associées.
Analyser les rapports	- Afficher les rapports	Lire dans le rapport	L'utilisateur peut effectuer les actions suivantes : <ul style="list-style-type: none">- Analysez les rapports.- Affichez les données, métadonnées et graphiques de rapports.

Privilège	Inclut les privilèges	Autorisation	Description
Interagir avec les données	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports 	Lire et écrire dans le rapport	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Accédez à la barre d'outils dans l'onglet Analyser et effectuez des tâches au niveau des données dans la table et les graphiques des rapports. - Cliquez avec le bouton droit de la souris sur les éléments de l'onglet Analyser.
Développer n'importe quel point	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports - Interagir avec les données 	Lire dans le rapport	L'utilisateur peut choisir un attribut de développement dans les rapports.
Créer des groupes de filtres	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports - Interagir avec les données 	Lire et écrire dans le rapport	L'utilisateur peut créer et enregistrer des groupes de filtres dans les rapports.
Promouvoir une métrologie personnalisée	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports - Interagir avec les données 	Écrire dans le rapport	L'utilisateur peut promouvoir des scores personnalisés des rapports aux schémas.
Afficher la demande	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports - Interagir avec les données 	Lire dans le rapport	L'utilisateur peut afficher les demandes de rapport.
Afficher les métadonnées du cycle de vie	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports - Interagir avec les données 	Écrire dans le rapport	L'utilisateur peut modifier les touches de temps dans l'onglet Time.
Créer et supprimer des rapports	<ul style="list-style-type: none"> - Afficher les rapports 	Écrire et supprimer dans le rapport	L'utilisateur peut créer ou supprimer des rapports.
Accéder à la création de rapports de base	<ul style="list-style-type: none"> - Afficher les rapports - Créer et supprimer des rapports 	Écrire dans le rapport	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Créez des rapports à l'aide des options de reporting de base. - Diffusez le lien dans un rapport de l'analyseur de données et modifiez la demande SQL pour le rapport.
Accéder à la création de rapports avancés	<ul style="list-style-type: none"> - Afficher les rapports - Créer et supprimer des rapports - Accéder à la création de rapports de base 	Écrire dans le rapport	<p>L'utilisateur peut effectuer les actions suivantes :</p> <ul style="list-style-type: none"> - Créez des rapports à l'aide de toutes les options de rapports disponibles. - Diffusez le contenu du rapport sous forme de pièce jointe et de lien. - Archivez les rapports. - Créez et gérez des modèles Excel. - Définissez la sécurité basée sur le fournisseur d'un rapport.

Privilège	Inclut les privilèges	Autorisation	Description
Enregistrer la copie des rapports	- Afficher les rapports	Écrire dans le rapport	L'utilisateur peut utiliser la fonction Enregistrer sous pour enregistrer le rapport sous un autre nom.
Modifier les rapports	- Afficher les rapports	Écrire dans le rapport	L'utilisateur peut modifier les rapports.

Privilèges du service de reporting et de tableaux de bord

Les privilèges du service de reporting et de tableaux de bord sont mappés aux rôles dans Jaspersoft.

Le groupe de privilèges d'accès contient tous les privilèges du service de reporting et de tableaux de bord.

Le tableau suivant décrit chaque privilège pour le service de reporting et de tableaux de bord :

Nom du privilège	Description
Administrateur	<p>Les utilisateurs assignés au privilège administrateur peuvent effectuer les tâches suivantes dans le serveur JasperReports :</p> <ul style="list-style-type: none"> - Créer des sous-organisations. - Créer, modifier et supprimer des utilisateurs. - Créer, modifier et supprimer des rôles. - Se connecter en tant que n'importe quel utilisateur dans l'entreprise. - Créer, modifier et supprimer des dossiers et des objets de référentiel de tous types. - Assigner des rôles aux utilisateurs, dont le rôle ROLE_ADMINISTRATOR qui accorde les privilèges d'administrateur de l'entreprise. - Définir les autorisations d'accès aux dossiers et objets du référentiel. <p>Ce privilège est mappé au rôle ROLE_ADMINISTRATOR dans Jaspersoft.</p>
Super-utilisateur	<p>Les utilisateurs ayant le privilège de super-utilisateur peuvent effectuer toutes les tâches qu'un utilisateur avec le privilège d'administrateur peut effectuer. En outre, les utilisateurs avec le privilège de super-utilisateur peuvent effectuer les tâches suivantes dans le serveur JasperReports :</p> <ul style="list-style-type: none"> - Créer des organisations de niveau supérieur. - Créer des utilisateurs qui peuvent accéder à toutes les organisations. - Assigner le rôle ROLE_SUPERUSER qui accorde les privilèges d'administrateur système. - Définir les paramètres de configuration au niveau du système. <p>Ce privilège est mappé au rôle ROLE_SUPERUSER dans Jaspersoft.</p>
Utilisateur standard	<p>Les utilisateurs assignés au privilège d'utilisateur standard peuvent afficher des rapports dans le serveur JasperReports.</p> <p>Ce privilège est mappé au rôle ROLE_USER dans Jaspersoft.</p>

Pour plus d'informations sur les privilèges associés à ces rôles dans Jaspersoft, consultez la documentation de Jaspersoft.

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. Un utilisateur ayant le privilège d'effectuer certaines actions a besoin d'autorisations pour effectuer l'action sur un objet spécifique. Configurez les autorisations dans l'onglet Sécurité de l'outil Administrator.

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 et des rôles, affecter 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.
Data Masking	Inclut des privilèges pour afficher et gérer des règles de masquage et des affectations de stratégies dans Test Data Manager.
Sous-ensemble de données	Inclut des privilèges pour afficher et gérer des objets de sous-ensemble, notamment des entités, des groupes et des modèles, 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.
Règles	Inclut des privilèges pour afficher et gérer des règles de masquage et de génération dans Test Data Manager.
Génération des données	Inclut des privilèges pour afficher et gérer la génération de données de test 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 :

Privilège	Inclut les privilèges	Autorisation	Description
Gérer des préférences	-	Écrire	L'utilisateur peut effectuer les actions suivantes dans Informatica Administrator et Test Data Manager : <ul style="list-style-type: none">- Créer des rôles.- Modifier des rôles.- Supprimer des rôles.- Afficher des rôles.- Associer des rôles aux utilisateurs.- Associer des privilèges aux utilisateurs.- Associer des rôles aux groupes d'utilisateurs.- Associer des privilèges aux groupes d'utilisateurs.- Ajouter des licences.- Définir le référentiel TDM.- Définir le référentiel PowerCenter.- Définir les niveaux de sensibilité des domaines de données.- Définir les attributs personnalisés d'un projet.- Définir les attributs de génération de flux de travail.- Activer le profilage des données.- Définir des services de profilage.- Afficher des objets d'administration.- Configurez les options d'indexation de la recherche par mot-clé.
Afficher des connexions	-	Lire	L'utilisateur peut effectuer les actions suivantes sur la page Connexions de Test Data Manager : <ul style="list-style-type: none">- Afficher des connexions.- Tester des connexions.
Gérer des connexions	Afficher des connexions	Écrire	L'utilisateur peut effectuer les actions suivantes sur la page Connexions de Test Data Manager : <ul style="list-style-type: none">- Créer des connexions.- Modifier des connexions.- Supprimer des connexions.- Afficher des connexions.- Tester des connexions.

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 :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher un sous-ensemble de données	-	Lire	L'utilisateur peut effectuer les actions de sous-ensemble de données suivantes dans Test Data Manager : <ul style="list-style-type: none">- Afficher des groupes.- Afficher des modèles- Afficher des entités.- Afficher les objets récents d'un projet.
Gérer un sous-ensemble de données	Afficher un sous-ensemble de données	Écrire	L'utilisateur peut effectuer les actions de sous-ensemble de données suivantes dans Test Data Manager : <ul style="list-style-type: none">- Créer des groupes.- Modifier des groupes.- Supprimer des groupes.- Ajouter des paramètres de groupe.- Créer des modèles.- Modifier des modèles.- Supprimer des modèles.- Ajouter des paramètres de modèle.- Créer une entité.- Modifier une entité.- Supprimer une entité.- Ajouter des critères d'entité.- Activer des relations.- Désactiver des relations.- Modifier des relations- Vérifier et agir sur des modifications.- Marquer la vérification des modifications comme terminée.

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 :

Privilège	Inclut les privilèges	Autorisation	Description
Afficher un projet	-	Lire	L'utilisateur peut effectuer les actions suivantes sur les projets dans Test Data Manager : <ul style="list-style-type: none">- Afficher des projets.- Afficher des plans.- Afficher les rapport détaillés d'un plan.- Afficher les rapport d'audit d'un plan.- Afficher les projets récents
Gérer un projet	Afficher un projet	Écrire	L'utilisateur peut effectuer les actions suivantes sur les projets dans Test Data Manager : <ul style="list-style-type: none">- Créer des projets- Modifier des projets.- Supprimer des projets- Afficher des projets.- Associer des utilisateurs à des projets.- Associer des groupes d'utilisateurs à des projets.- Associer des règles à des projets ou en supprimer.- Associer des stratégies à des projets ou en supprimer.- Créer des plans.- Modifier des plans.- Supprimer des plans.- Générer des plans.

Privilège	Inclut les privilèges	Autorisation	Description
Découvrir un projet	-	Écrire	<p>L'utilisateur peut effectuer les actions de découverte suivantes sur les projets dans Test Data Manager :</p> <ul style="list-style-type: none"> - Classer des tables. - Marquer une découverte comme terminée. - Associer des domaines de données aux colonnes. - Marquer des colonnes comme restreintes. - Marquer des colonnes comme sensibles - Définir une colonne de valeurs similaire - Supprimer des colonnes de valeurs similaires - Ajouter des clés primaires - Supprimer des clés primaires - Créer des contraintes logiques - Afficher des contraintes logiques - Modifier des contraintes logiques - Supprimer des contraintes logiques - Afficher des projets. - Afficher des domaines de données profilés. - Approuver ou rejeter des domaines de données profilés. - Marquer une classification du domaine de données comme terminée. - Afficher des clés primaires profilées. - Approuver ou rejeter des clés primaires profilées. - Marquer une découverte de clé primaire comme terminée. - Afficher des entités profilées. - Approuver ou rejeter des entités profilées. - Marquer une découverte d'entité comme terminée. - Afficher l'analyse de risque d'un projet. - Afficher la distribution récente des données sensibles d'un projet.
Générer un projet	-	Écrire	<p>L'utilisateur peut générer des flux de travail dans Test Data Manager.</p>
Exécuter un projet	-	Écrire	<p>L'utilisateur peut effectuer les actions d'exécution suivantes sur les projets dans Test Data Manager :</p> <ul style="list-style-type: none"> - Exécuter des plans. - Exécuter des flux de travail. - Arrêter des flux de travail. - Abandonner des flux de travail. - Récupérer des flux de travail. - Afficher l'exécution d'un plan.
Surveiller un projet	-	Lire	<p>L'utilisateur peut effectuer les actions de surveillance suivantes sur les projets dans Test Data Manager :</p> <ul style="list-style-type: none"> - Surveiller des tâches de projet. - Afficher les journaux des tâches d'un projet. - Surveiller des tâches dans des projets. - Afficher des journaux dans des projets.
Effectuer l'audit d'un projet	-	Lire	<p>L'utilisateur peut afficher l'activité récente des projets et des plans dans Test Data Manager.</p>
Importer des métadonnées	-	Écrire	<p>L'utilisateur peut effectuer les actions suivantes sur les projets dans Test Data Manager :</p> <ul style="list-style-type: none"> - Importer des sources - Supprimer des sources.

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.
- Affichez les règles de génération de règles depuis le groupe de privilèges Règles. Pour créer un plan avec des composants de génération.

Groupe de privilèges Règles

Les privilèges du groupe de privilèges Règles déterminent les tâches que les utilisateurs peuvent effectuer sur les règles de masquage des données et de génération de données dans Test Data Manager.

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 des règles de masquage	-	Lire	Les utilisateurs peuvent visualiser les règles de masquage dans Test Data Manager.
Gérer des règles de masquage	Afficher des règles de masquage	Écrire	L'utilisateur peut effectuer les actions suivantes sur les règles de masquage des données dans Test Data Manager : <ul style="list-style-type: none"> - Créer des règles de masquage. - Modifier des règles de masquage. - Supprimer des règles de masquage. - Afficher des règles de masquage.
Afficher des règles de génération	-	Lire	L'utilisateur peut afficher les règles de génération dans Test Data Manager.
Gérer des règles de génération	Afficher des règles de génération	Écrire	L'utilisateur peut effectuer les actions suivantes sur les règles de génération dans Test Data Manager : <ul style="list-style-type: none"> - Créer des règles de génération. - Modifier des règles de génération. - Supprimer des règles de génération. - Afficher des règles de génération.

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 données, 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.

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.

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.

UMSM comporte les types de rôles suivants :

- Administrateur. Il s'agit d'un rôle défini par le système qui dispose de privilèges pour gérer l'outil Administrator. Grâce à ce rôle, vous pouvez créer et gérer des comptes utilisateurs, créer et configurer le service Ultra Messaging, configurer des composants UMSM et des déploiements UM.
- Opérateur. Il s'agit d'un rôle personnalisé qui dispose de privilèges pour surveiller les déploiements UM.

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 du gestionnaire, le service de référentiel modèle, le service de référentiel PowerCenter ou le Reporting Service, l'utilisateur ou groupe se voit accorder tous les privilèges du 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.

Lorsque vous attribuez le rôle Administrateur à un utilisateur ou groupe du domaine, le service d'intégration de données ou le service de référentiel modèle, l'utilisateur ou le groupe se voit accorder tous les privilèges du 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.

Lorsque vous assignez le rôle Administrateur à un utilisateur ou à un groupe pour le domaine ou le service Ultra Messaging, l'utilisateur ou le groupe se voit attribuer 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.

Lorsque vous attribuez le rôle administrateur à un utilisateur ou à un groupe du domaine ou du Data Integration Service, l'utilisateur ou le groupe peut effectuer certaines tâches déterminées par le rôle administrateur, et non pas par les privilèges ou les autorisations..

Lorsque vous attribuez le rôle administrateur à un utilisateur ou à un groupe du domaine ou du service Ultra Messaging, l'utilisateur ou le groupe en question 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.

Vous pouvez affecter à un utilisateur ou à un groupe tous les privilèges pour le domaine ou le service d'intégration de données, puis attribuer à l'utilisateur ou au groupe complet toutes les autorisations sur tous les objets du domaine. Toutefois, cet utilisateur ou ce groupe ne peut pas effectuer les tâches déterminées par le rôle administrateur.

Vous pouvez concéder à un utilisateur ou à un groupe tous les privilèges pour le domaine ou le service Ultra Messaging, puis attribuer à ce même utilisateur ou groupe toutes les autorisations sur tous les objets du domaine. 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 et du service de référentiel PowerCenter :

Le tableau suivant donne la liste des tâches déterminées par le rôle administrateur du domaine ou le service d'intégration de données :

Le tableau suivant donne la liste des tâches déterminées par le rôle administrateur du domaine ou du service Ultra Messaging :

Service	Tâches
Domaine	<ul style="list-style-type: none"> - Configurer les propriétés du domaine. - 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 de référentiel PowerCenter	<ul style="list-style-type: none"> - Assigner les profils de systèmes d'exploitation aux dossiers du référentiel si le PowerCenter Integration Service utilise les profils de systèmes d'exploitation.* - 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>

Service	Tâches
Domaine	<ul style="list-style-type: none"> - Configurer les propriétés du domaine. - Accorder des autorisations sur le domaine - Gérer et purger des événements de journaux. - Recevoir des alertes de domaine. - Afficher les événements du journal d'activité utilisateur.

Service	Tâches
Domaine	<ul style="list-style-type: none"> - Configurer les propriétés du domaine. - Accorder des autorisations sur le domaine - Gérer et purger des événements de journaux. - Recevoir des alertes de domaine.

Service	Tâches
	- Afficher les événements du journal d'activité utilisateur.

Rôles personnalisés

Un rôle personnalisé est un rôle que vous pouvez créer, modifier et supprimer. L'outil Administrator inclut des rôles personnalisés pour le Metadata Manager Service, le PowerCenter Repository Service et le Reporting service. Vous pouvez modifier les privilèges appartenant à ces rôles et vous pouvez attribuer ces rôles aux utilisateurs et groupes.

Vous pouvez également créer des rôles personnalisés et les attribuer aux utilisateurs et groupes.

Gestion des rôles personnalisés

Vous pouvez créer, modifier et supprimer des 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 aux groupes pour un Service du gestionnaire de métadonnées, un service de référentiel PowerCenter ou un Reporting service 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 privilèges ou les rôles modifiés prennent effet à 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.

Étapes permettant d'attribuer des privilèges et des rôles aux utilisateurs et groupes

Vous pouvez attribuer des privilèges et des rôles aux utilisateurs et groupes des manières suivantes :

- Accédez à un utilisateur ou groupe et modifiez les attributions de privilège et de rôle.
- Faites glisser un rôle sur un utilisateur ou groupe.

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.

Attribution de rôles à un utilisateur ou un groupe par glisser

1. Dans l'outil Administrator, cliquez sur l'onglet Sécurité.
2. Dans la section Rôles du navigateur, sélectionnez le dossier contenant les rôles que vous voulez attribuer.
3. Dans le panneau d'informations, sélectionnez le rôle que vous voulez attribuer.
Vous pouvez utiliser les touches Ctrl ou Shift pour sélectionner plusieurs rôles.
4. Faites glisser les rôles sélectionnés vers un utilisateur ou un groupe dans les sections Utilisateurs ou Groupes du navigateur.
La boîte de dialogue Attribuer des rôles s'affiche.
5. Sélectionnez le domaine ou les services d'application auxquels vous voulez attribuer le rôle.
6. 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.

Résolution des problèmes de privilèges et de rôles

Je ne peux attribuer ni privilège ni rôle aux utilisateurs pour un service Metadata Manager, un service de référentiel PowerCenter ou un service de rapports existant.

Vous ne pouvez pas attribuer de privilèges et de rôles aux utilisateurs et groupes pour un service Metadata Manager, un service de référentiel PowerCenter ou un service de rapports existant dans les cas suivants :

- Le service d'application est désactivé.
- Le service de référentiel PowerCenter s'exécute en mode exclusif.

Je ne peux pas attribuer de privilèges à un utilisateur pour un service de rapports activé.

L'analyseur de données utilise le nom du compte utilisateur et le nom du domaine de sécurité au format `UserName@SecurityDomain` pour déterminer la longueur du nom de connexion de l'utilisateur. Vous ne pouvez attribuer aucun privilège ou rôle à un utilisateur pour un service de rapports lorsque la combinaison du nom d'utilisateur, du symbole @ et du nom de domaine de sécurité dépasse 128 caractères.

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.

Certaines tâches de l'outil Administrator 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.

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 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, 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 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.

CHAPITRE 9

Autorisations

Ce chapitre comprend les rubriques suivantes :

- [Présentation des autorisations, 168](#)
- [Autorisations d'objets de domaines, 171](#)
- [Autorisations de connexion, 176](#)
- [Autorisations du service de données SQL, 179](#)
- [Autorisations du service web, 184](#)

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 possède le privilège pour effectuer certaines actions, il 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 et l'autorisation pour le service de référentiel PowerCenter en phase de développement mais pas pour 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 pour les objets suivants :

Vous pouvez utiliser différents outils pour configurer les autorisations pour les objets suivants :

Type d'objet	Outil	Description
Objets de connexion	Outil Administrator Outil Analyst Outil Developer	Vous pouvez assigner des autorisations pour les connexions définies dans l'outil Administrator, l'outil Analyst ou dans l'outil Developer. Ces outils partagent les autorisations de connexion.
Objets de Data Analyzer	Data Analyzer	Vous pouvez attribuer des autorisations pour les dossiers, les rapports, les tableaux de bord, les attributs, la métrologie, les dimensions de modèle et les planifications de Data Analyzer.

Type d'objet	Outil	Description
Objets de domaine	Outil Administrator	Vous pouvez attribuer des autorisations pour les objets de domaine suivants : domaine, dossiers, nœuds, grilles, licences, services d'application et profils de systèmes d'exploitation.
Objets du catalogue Metadata Manager	Metadata Manager	Vous pouvez attribuer des autorisations pour les dossiers et objets de catalogue Metadata Manager.
Projets du référentiel modèle	Outil Analyst Outil Developer	Vous pouvez attribuer des autorisations pour les projets définis dans l'outil Analyst et dans l'outil Developer. Ces outils partagent les autorisations de projet.
Objets du référentiel PowerCenter	Client PowerCenter	Vous pouvez attribuer des autorisations pour les dossiers, groupes de déploiement, libellés, demandes et objets de connexion de PowerCenter.
Objets du services de données SQL	Outil Administrator	Vous pouvez attribuer des autorisations pour les objets de données SQL, tels que les services de données SQL, les schémas virtuels, les tables virtuelles et les procédures stockées virtuelles.
Objets de service Web	Outil Administrator	Vous pouvez attribuer des autorisations pour les services Web ou les opérations du service Web.

Type d'objet	Outil	Description
Objets de connexion	Outil Administrator Outil Developer	Vous pouvez attribuer des autorisations pour une connexion définie dans l'outil Administrator ou dans l'outil Developer. Ces outils partagent les autorisations de connexion.
Objets de domaine	Outil Administrator	Vous pouvez attribuer des autorisations sur les objets de domaine suivante : domaine, dossiers, nœud et services d'application.
Projets du référentiel modèle	Outil Developer	Vous pouvez attribuer des autorisations sur les projets définie dans l'outil Developer.

Vous pouvez utiliser l'outil Administrator pour configurer les autorisations pour un objet de domaine. Vous pouvez attribuer des autorisations aux objets de domaine suivants :

- domaine
- nœud
- services d'application

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.

Autorisations dont héritent les utilisateurs. Lorsque des utilisateurs ont l'autorisation sur un domaine, ils héritent de l'autorisation sur tous les objets du domaine. 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.

Autorisations dont héritent les utilisateurs. Lorsque des utilisateurs ont l'autorisation sur un domaine, ils héritent de l'autorisation sur tous les objets du domaine. 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.

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 a l'autorisation pour un nœud, mais n'a pas le 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 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 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 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 qu'il crée une grille.
Grille	Permet aux utilisateurs de l'outil Administrator 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 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 de consulter et de modifier les propriétés de services d'applications.
Profil de système d'exploitation	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.

Type d'objet de domaine	Description de l'autorisation
Domaine	Autorise les utilisateurs de l'outil Administrator 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.
Nœud	Permet aux utilisateurs de l'outil Administrator de consulter et de modifier les propriétés de nœuds.

Type d'objet de domaine	Description de l'autorisation
Service d'application	Permet aux utilisateurs de l'outil Administrator de consulter et de modifier les propriétés de services d'applications.
Licence	Permet aux utilisateurs de l'outil Administrator de consulter et de modifier les propriétés de licences.

Type d'objet de domaine	Description de l'autorisation
Domaine	Autorise les utilisateurs de l'outil Administrator 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.
Nœud	Permet aux utilisateurs de l'outil Administrator de consulter et de modifier les propriétés de nœuds.
Service d'application	Permet aux utilisateurs de l'outil Administrator de consulter et de modifier les propriétés de services d'applications.
Licence	Permet aux utilisateurs de l'outil Administrator de consulter et de modifier les propriétés de licences.

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 Domaine, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez l'objet de domaine.
3. Dans le volet de contenu, sélectionnez 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 **Domaine**, 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 **Domaine**, 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'en-tête d'Infomatica Administrator, cliquez sur **Gérer > Autorisations**.
La boîte de dialogue **Gérer les autorisations** s'affiche.
2. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**.
3. Entrez une chaîne pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
4. Sélectionnez un utilisateur ou un groupe.
5. Sélectionnez un objet de domaine, 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.
6. Cliquez sur **Fermer**.
7. Ou cliquez sur **Modifier les autorisations** pour modifier les autorisations directes.

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.

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'en-tête d'Infomatica Administrator, cliquez sur **Gérer > Autorisations**.
La boîte de dialogue **Gérer les autorisations** s'affiche.
2. Cliquez sur l'onglet **Groupes** ou **Utilisateurs**.
3. Entrez une chaîne pour rechercher les utilisateurs et groupes, puis cliquez sur le bouton **Filtrer**.
4. Sélectionnez un utilisateur ou un groupe.
5. Sélectionnez un objet de domaine, puis cliquez sur le bouton **Modifier les autorisations directes**.
La boîte de dialogue **Modifier les autorisations directes** s'affiche.
6. Pour attribuer une autorisation sur un objet, sélectionnez **Autoriser**.
7. 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**.
8. Cliquez sur **OK**.
9. Cliquez sur **Fermer**.

Autorisations du profil de système d'exploitation

La boîte de dialogue **Configurer les profils du système d'exploitation** permet d'attribuer, d'afficher et de modifier des autorisations sur 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 PowerCenter peuvent exécuter des workflows attribués au profil de système d'exploitation.

1. Dans l'onglet **Sécurité**, cliquez sur **Actions** > **Configurer les profils de systèmes d'exploitation**.
La boîte de dialogue **Configurer les profils de systèmes d'exploitation** s'affiche.
2. Sélectionnez le profil du système d'exploitation, puis cliquez sur l'onglet **Autorisations**.
3. Sélectionnez la vue **Groupes** ou **Utilisateurs** et cliquez sur le bouton **Attribuer l'autorisation**.
La boîte de dialogue **Attribuer des autorisations** affiche tous les utilisateurs ou groupes n'ayant pas d'autorisation sur le profil de système d'exploitation.
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 **Suivant**.
6. Sélectionnez **Autoriser**, puis cliquez sur **Terminer**.

Affichage des détails des autorisations pour 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**, cliquez sur **Actions** > **Configurer les profils de systèmes d'exploitation**.
La boîte de dialogue **Configurer les profils de systèmes d'exploitation** s'affiche.
2. Sélectionnez le profil du 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 **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.
6. Cliquez sur **Fermer**.
7. Ou cliquez sur **Modifier les autorisations** pour modifier les autorisations directes.

Modification des autorisations dans 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**, cliquez sur **Actions > Configurer les profils de systèmes d'exploitation**.
La boîte de dialogue **Configurer les profils de systèmes d'exploitation** s'affiche.
2. Sélectionnez le profil du système d'exploitation, puis cliquez sur l'onglet **Autorisations**.
3. Sélectionnez la vue **Groupe** 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 **Actions > 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.

Vous pouvez configurer les autorisations sur une connexion dans l'outil Developer 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.
- Service d'intégration de données. Applique les autorisations d'exécution lorsqu'un utilisateur tente de prévisualiser des données ou d'exécuter un mappage 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. 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 mappage 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 **Domaine**, 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 **Domaine**, 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, 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.

7. Cliquez sur **Fermer**.
8. 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 **Domaine**, 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 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 assigner des autorisations à des utilisateurs et groupes dans les objets suivants du service de données SQL :

- service de données SQL
- Table virtuelle
- Procédure virtuelle stockée

Lorsque vous assignez des autorisations pour un objet de service de données SQL, l'utilisateur ou le groupe hérite des mêmes autorisations pour tous les objets qui appartiennent à l'objet du service de données SQL. Par exemple, vous assignez l'autorisation de sélection d'un utilisateur pour un service de données SQL. L'utilisateur hérite de l'autorisation de sélection pour toutes les tables virtuelles dans le 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 assigner d'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 **Domaine**, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un Data Integration Service.
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 **Domaine**, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un Data Integration Service.
3. Dans le volet de contenu, cliquez sur la vue **Applications**.

4. Sélectionnez l'objet 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 Domaine, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un Data Integration Service.
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 : <http://communities.informatica.com/docs/DOC-4507>.

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
- Opération du service Web

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

Vous pouvez attribuer les autorisations suivantes aux utilisateurs et groupes :

- Accorder une autorisation. Les utilisateurs peuvent gérer les autorisations sur les objets de service Web à l'aide de l'outil Administrator ou du programme de ligne de commande *infacmd*.
- Exécuter une autorisation. Les utilisateurs peuvent envoyer des demandes de service Web et recevoir des réponses de service Web.

Le tableau suivant décrit les autorisations pour chaque objet de service Web :

Objet	Accorder une autorisation	Exécuter une autorisation
Service Web	Accorder et retirer une autorisation sur le service Web et sur toutes les opérations du service Web.	Envoyer des demandes de service Web et recevoir des réponses de service Web à partir de toutes les opérations au sein du service Web.
Opération de service Web	Accorder, retirer et refuser une autorisation sur l'opération de service Web.	Envoyer des demandes de service Web et recevoir des réponses de service Web à partir de toutes les opérations du service Web.

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 Domaine, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un Data Integration Service.
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 Domaine, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un Data Integration Service.
3. Dans le volet de contenu, cliquez sur la vue **Applications**.
4. Sélectionnez l'objet 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 Domaine, sélectionnez la vue **Services et nœuds**.
2. Dans le navigateur, sélectionnez un Data Integration Service.
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 10

Rapports d'audit

Ce chapitre comprend les rubriques suivantes :

- [Présentation des rapports d'audit, 187](#)
- [Informations personnelles de l'utilisateur, 188](#)
- [Association de groupes d'utilisateurs, 189](#)
- [Privilèges, 190](#)
- [Association de rôles, 190](#)
- [Autorisation d'objet de domaine, 191](#)
- [Sélection d'utilisateurs pour un rapport d'audit, 191](#)
- [Sélection des groupes pour un rapport d'audit , 192](#)
- [Sélection des rôles pour un rapport d'audit, 193](#)

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

Hierarchie 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

Rôles personnalisés

Cette annexe comprend les rubriques suivantes :

- [Rôles personnalisés du PowerCenter Repository Service, 194](#)
- [Rôles personnalisés du Metadata Manager Service, 196](#)
- [Rôles personnalisés du Reporting Service, 197](#)
- [Rôles personnalisés du service Test Data Manager, 204](#)
- [Rôle personnalisé du service Analyst, 208](#)

Rôles personnalisés du PowerCenter Repository Service

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 workflow
Objets globaux	Créer des connexions

Le tableau suivant présente les privilèges par défaut assignés 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 workflow- Accéder au moniteur de workflow
Objets de conception	<ul style="list-style-type: none">- Créer, modifier et supprimer- Gérer les versions

Groupe de privilèges	Nom du privilège
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

Le tableau suivant présente les privilèges par défaut assignés au rôle personnalisé Opérateur PowerCenter :

Groupe de privilèges	Nom du privilège
Outils	Accéder au moniteur de workflow
Objets d'exécution	<ul style="list-style-type: none"> - Exécuter - Gérer l'exécution - Surveiller

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 au 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 Metadata Manager Service

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

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
Chargement	<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	Autorisations Gérer le catalogue

Le tableau suivant présente les privilèges par défaut assignés 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

Le tableau suivant présente les privilèges par défaut assignés 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
Chargement	<ul style="list-style-type: none"> - Afficher la ressource - Charger la ressource
Modèle	Afficher le modèle

Rôles personnalisés du Reporting Service

Le tableau suivant présente les privilèges par défaut attribués au rôle personnalisé Client avancé du Reporting Service :

Groupe de privilèges	Nom du privilège
Administration	<ul style="list-style-type: none"> - Gérer le schéma - Exporter/importer les fichiers XML - Gérer l'accès utilisateur - Configurer les plannings et les tâches - Gérer les propriétés du système - Configurer les limites de requête - Configurer les flux de messages en temps réel
Alertes	<ul style="list-style-type: none"> - Recevoir des alertes - Créer des alertes en temps réel - Configurer des options de remise

Groupe de privilèges	Nom du privilège
Communication	<ul style="list-style-type: none"> - Imprimer - Envoyer par e-mail les liens de l'objet - Envoyer par e-mail le contenu de l'objet - Exporter - Exporter vers Excel ou au format CSV - Exporter vers un tableau croisé dynamique - Afficher les discussions - Ajouter les discussions - Gérer les discussions - Envoyer des commentaires
Répertoire de contenu	<ul style="list-style-type: none"> - Accéder au répertoire de contenu - Accéder à la recherche avancée - Gérer le répertoire de contenu - Gérer la recherche avancée
Tableau de bord	<ul style="list-style-type: none"> - Afficher les tableaux de bord - Gérer les tableaux de bord personnels
Indicateurs	<ul style="list-style-type: none"> - Interagir avec les indicateurs - Créer des indicateurs en temps réel - Obtenir des mises à jour automatiques continues d'indicateurs en temps réel
Gérer des comptes	Gérer les paramètres personnels
Rapports	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports - Interagir avec les données - Zoomer sur n'importe quel point - Créer des groupes de filtres - Promouvoir une métrologie personnalisée - Afficher la requête - Afficher les métadonnées du cycle de vie - Créer et supprimer des rapports - Accéder à la création de rapports de base - Accéder à la création de rapports avancés - Enregistrer la copie des rapports - Éditer les rapports

Le tableau suivant présente les privilèges par défaut assignés au rôle personnalisé Fournisseur avancé du Reporting Service :

Groupe de privilèges	Nom du privilège
Administration	Gérer le schéma
Alertes	<ul style="list-style-type: none"> - Recevoir des alertes - Créer des alertes en temps réel - Configurer des options de remise
Communication	<ul style="list-style-type: none"> - Imprimer - Envoyer par e-mail les liens de l'objet - Envoyer par e-mail le contenu de l'objet - Exporter - Exporter vers Excel ou au format CSV - Exporter vers un tableau croisé dynamique - Afficher les discussions - Ajouter les discussions - Gérer les discussions - Envoyer des commentaires
Répertoire de contenu	<ul style="list-style-type: none"> - Accéder au répertoire de contenu - Accéder à la recherche avancée - Gérer le répertoire de contenu - Gérer la recherche avancée
Tableaux de bord	<ul style="list-style-type: none"> - Afficher les tableaux de bord - Gérer les tableaux de bord personnels - Créer, éditer et supprimer des tableaux de bord - Accéder à la création de tableaux de bord de base - Accéder à la création de tableaux de bord avancés
Indicateurs	<ul style="list-style-type: none"> - Interagir avec les indicateurs - Créer des indicateurs en temps réel - Obtenir des mises à jour automatiques continues d'indicateurs en temps réel

Groupe de privilèges	Nom du privilège
Gérer des comptes	Gérer les paramètres personnels
Rapports	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports - Interagir avec les données - Zoomer sur n'importe quel point - Créer des groupes de filtres - Promouvoir une métrologie personnalisée - Afficher la requête - Afficher les métadonnées du cycle de vie - Créer et supprimer des rapports - Accéder à la création de rapports de base - Accéder à la création de rapports avancés - Enregistrer la copie des rapports - Éditer les rapports

Le tableau suivant présente les privilèges par défaut assignés au rôle personnalisé Client de base du Reporting Service :

Groupe de privilèges	Nom du privilège
Alertes	<ul style="list-style-type: none"> - Recevoir des alertes - Configurer des options de remise
Communication	<ul style="list-style-type: none"> - Imprimer - Envoyer par e-mail les liens de l'objet - Exporter - Afficher les discussions - Ajouter les discussions - Envoyer des commentaires
Répertoire de contenu	Accéder au répertoire de contenu
Tableaux de bord	Afficher les tableaux de bord
Gérer le compte	Gérer les paramètres personnels
Rapports	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports

Le tableau suivant présente les privilèges par défaut assignés au rôle personnalisé Fournisseur de base du Reporting Service :

Groupe de privilèges	Nom du privilège
Administration	Gérer le schéma
Alertes	<ul style="list-style-type: none"> - Recevoir des alertes - Créer des alertes en temps réel - Configurer des options de remise
Communication	<ul style="list-style-type: none"> - Imprimer - Envoyer par e-mail les liens de l'objet - Envoyer par e-mail le contenu de l'objet - Exporter - Exporter vers Excel ou au format CSV - Exporter vers un tableau croisé dynamique - Afficher les discussions - Ajouter les discussions - Gérer les discussions - Envoyer des commentaires
Répertoire de contenu	<ul style="list-style-type: none"> - Accéder au répertoire de contenu - Accéder à la recherche avancée - Gérer le répertoire de contenu - Gérer la recherche avancée
Tableaux de bord	<ul style="list-style-type: none"> - Afficher les tableaux de bord - Gérer les tableaux de bord personnels - Créer, éditer et supprimer des tableaux de bord - Accéder à la création de tableaux de bord de base
Indicateurs	<ul style="list-style-type: none"> - Interagir avec les indicateurs - Créer des indicateurs en temps réel - Obtenir des mises à jour automatiques continues d'indicateurs en temps réel

Groupe de privilèges	Nom du privilège
Gérer des comptes	Gérer les paramètres personnels
Rapports	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports - Interagir avec les données - Zoomer sur n'importe quel point - Créer des groupes de filtres - Promouvoir une métrologie personnalisée - Afficher la requête - Afficher les métadonnées du cycle de vie - Créer et supprimer des rapports - Accéder à la création de rapports de base - Accéder à la création de rapports avancés - Enregistrer la copie des rapports - Éditer les rapports

Le tableau suivant présente les privilèges par défaut assignés au rôle personnalisé Client intermédiaire du Reporting Service :

Groupe de privilèges	Nom du privilège
Alertes	<ul style="list-style-type: none"> - Recevoir des alertes - Configurer des options de remise
Communication	<ul style="list-style-type: none"> - Imprimer - Envoyer par e-mail les liens de l'objet - Exporter - Exporter vers Excel ou au format CSV - Exporter vers un tableau croisé dynamique - Afficher les discussions - Ajouter les discussions - Gérer les discussions - Envoyer des commentaires
Répertoire de contenu	Accéder au répertoire de contenu
Tableaux de bord	<ul style="list-style-type: none"> - Afficher les tableaux de bord - Gérer les tableaux de bord personnels
Indicateurs	<ul style="list-style-type: none"> - Interagir avec les indicateurs - Obtenir des mises à jour automatiques continues d'indicateurs en temps réel

Groupe de privilèges	Nom du privilège
Gérer des comptes	Gérer les paramètres personnels
Rapports	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports - Interagir avec les données - Afficher les métadonnées du cycle de vie - Enregistrer la copie des rapports

Le tableau suivant présente les privilèges par défaut assignés au rôle personnalisé Client en lecture seule du Reporting Service :

Groupe de privilèges	Nom du privilège
Rapports	Afficher les rapports

Le tableau suivant présente les privilèges par défaut attribués au rôle personnalisé Concepteur de schéma du Reporting Service :

Groupe de privilèges	Nom du privilège
Administration	<ul style="list-style-type: none"> - Gérer le schéma - Configurer les plannings et les tâches - Configurer les flux de messages en temps réel
Alertes	<ul style="list-style-type: none"> - Recevoir des alertes - Créer des alertes en temps réel - Configurer des options de remise
Communication	<ul style="list-style-type: none"> - Imprimer - Envoyer par e-mail les liens de l'objet - Envoyer par e-mail le contenu de l'objet - Exporter - Exporter vers Excel ou au format CSV - Exporter vers un tableau croisé dynamique - Afficher les discussions - Ajouter les discussions - Gérer les discussions - Envoyer des commentaires
Répertoire de contenu	<ul style="list-style-type: none"> - Accéder au répertoire de contenu - Accéder à la recherche avancée - Gérer le répertoire de contenu - Gérer la recherche avancée

Groupe de privilèges	Nom du privilège
Tableaux de bord	<ul style="list-style-type: none"> - Afficher les tableaux de bord - Gérer les tableaux de bord personnels - Créer, éditer et supprimer des tableaux de bord
Indicateurs	<ul style="list-style-type: none"> - Interagir avec les indicateurs - Créer des indicateurs en temps réel - Obtenir des mises à jour automatiques continues d'indicateurs en temps réel
Gérer des comptes	Gérer les paramètres personnels
Rapports	<ul style="list-style-type: none"> - Afficher les rapports - Analyser les rapports - Interagir avec les données - Zoomer sur n'importe quel point - Créer des groupes de filtres - Promouvoir une métrologie personnalisée - Afficher la requête - Afficher les métadonnées du cycle de vie - Créer et supprimer des rapports - Accéder à la création de rapports de base - Accéder à la création de rapports avancés - Enregistrer la copie des rapports - Éditer les rapports

Rôles personnalisés du service Test Data Manager

Le tableau suivant répertorie les privilèges par défaut affectés au rôle personnalisé Administrateur des données de test :

Groupe de privilèges	Nom du privilège
Projets	Effectuer l'audit d'un projet
Administration	<ul style="list-style-type: none"> - Afficher des connexions - Gérer des connexions

Le tableau suivant répertorie les privilèges par défaut affectés au rôle personnalisé Développeur des données de test :

Groupe de privilèges	Nom du privilège
Stratégies	<ul style="list-style-type: none"> - Afficher des stratégies - Gérer des stratégies
Règles	<ul style="list-style-type: none"> - Afficher des règles de masquage - Gérer des règles de masquage - Afficher des règles de génération
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

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé de 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 des connexions - Gérer des connexions

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé Développeur du projet des données de test :

Groupe de privilèges	Nom du privilège
Stratégies	Afficher des stratégies
Règles	<ul style="list-style-type: none"> - Afficher des règles de masquage - Afficher des règles de génération
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 un masquage des données - Gérer un masquage des données
Sous-ensemble de données	<ul style="list-style-type: none"> - Afficher un sous-ensemble de données - Gérer un sous-ensemble de données

Groupe de privilèges	Nom du privilège
Génération des données	<ul style="list-style-type: none"> - Afficher une génération des données - Gérer une génération des données
Administration	<ul style="list-style-type: none"> - Afficher des connexions - Gérer des connexions

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé Propriétaire du projet des données de test :

Groupe de privilèges	Nom du privilège
Stratégies	Afficher des stratégies
Règles	<ul style="list-style-type: none"> - Afficher des règles de masquage - Afficher des règles de génération
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 un masquage des données - Gérer un masquage des données
Sous-ensemble de données	<ul style="list-style-type: none"> - Afficher un sous-ensemble de données - Gérer un sous-ensemble de données
Génération des données	<ul style="list-style-type: none"> - Afficher une génération des données - Gérer une génération des données
Administration	<ul style="list-style-type: none"> - Afficher des connexions - Gérer des connexions

Le tableau suivant répertorie les privilèges par défaut attribués au rôle personnalisé Gestionnaire des risques des données de test :

Groupe de privilèges	Nom du privilège
Stratégies	Afficher des stratégies
Règles	<ul style="list-style-type: none"> - Afficher des règles de masquage - Afficher des règles de génération
Domaines de données	Afficher des domaines de données
Projets	Effectuer l'audit d'un projet

Le tableau suivant répertorie les privilèges par défaut affectés au rôle personnalisé Spécialiste des données de test :

Groupe de privilèges	Nom du privilège
Stratégies	Afficher des stratégies
Règles	<ul style="list-style-type: none"> - Afficher des règles de masquage - Gérer des règles de masquage - Afficher des règles de génération - Gérer des règles de génération
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"> - Gérer un projet - 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 un masquage des données - Gérer un masquage des données
Sous-ensemble de données	<ul style="list-style-type: none"> - Afficher un sous-ensemble de données - Gérer un sous-ensemble de données
Génération des données	<ul style="list-style-type: none"> - Afficher une génération des données - Gérer une génération des données
Administration	<ul style="list-style-type: none"> - Afficher des connexions - Gérer des connexions

Remarque: Si votre configuration TDM utilise le service Informatica 9.6.1 ou si vous avez mis à niveau vers le service Informatica 9.6.1 HotFix 1, un utilisateur disposant du rôle Spécialiste de données de test ne peut pas créer ou supprimer de règles de génération des données. Ce rôle n'inclut pas le privilège Gérer une génération des données. Pour permettre aux utilisateurs disposant de ce rôle de créer et de supprimer des règles de génération des données, vous devez modifier manuellement le rôle. Connectez-vous à l'outil Administrator et modifiez le rôle personnalisé du service TDM pour inclure le privilège Gérer les règles de génération à partir du groupe de privilèges Règles.

Rôle personnalisé du service Analyst

L'utilisateur de glossaire métier 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 métier du service Analyst :

Groupe de privilèges	Nom du privilège
Accès à l'espace de travail	Espace de travail Glossaire

INDEX

A

- Administrateur
 - rôle [159](#)
- administrateur de domaine
 - description [88](#)
- administrateur par défaut
 - description [87](#)
 - modification [87](#)
 - mots de passe, changement [87](#)
- administrateurs
 - client d'application [88](#)
 - domaine [88](#)
 - par défaut [87](#)
- authentification
 - Gestionnaire de service [78](#)
 - Kerberos [20](#)
 - LDAP [19](#), [22](#), [78](#)
 - native [19](#), [78](#)
- Authentification Kerberos
 - description [20](#)
- authentification LDAP
 - certificat SSL auto-signé [27](#)
 - configuration [22](#)
 - description [19](#)
 - groupes imbriqués [27](#)
 - heures de synchronisation [26](#)
 - services d'annuaire [22](#)
- Authentification LDAP
 - description [78](#)
- authentification native
 - description [19](#), [78](#)
- authentification unique
 - description [78](#)
- autorisation
 - Gestionnaire de service [78](#)
 - Service d'intégration de données [78](#)
 - Service de rapports [78](#)
 - Service de référentiel modèle [78](#)
 - Service de référentiel PowerCenter [78](#)
 - Service Metadata Manager [78](#)
 - services d'application [78](#)
- autorisation directe
 - description [169](#)
- autorisation effective
 - description [169](#)
- autorisation héritée
 - description [169](#)
- autorisations
 - connexions [176](#)
 - description [168](#)
 - directes [169](#)
 - dossiers [171](#)
 - effectives [169](#)
 - filtres de recherche [170](#)
 - grilles [171](#)

- autorisations (*a continué*)
 - héritées [169](#)
 - licences [171](#)
 - nœuds [171](#)
 - objets de domaine [171](#)
 - opération du service Web [184](#)
 - procédure virtuelle stockée [179](#)
 - profils du système d'exploitation [171](#), [175](#)
 - schéma virtuel [179](#)
 - service de données SQL [179](#)
 - service Web [184](#)
 - services d'application [171](#)
 - table virtuelle [179](#)
 - types [169](#)
 - utilisation des privilèges [168](#)
- autorisations de domaine
 - directes [169](#)
 - effectives [169](#)
 - héritées [169](#)

C

- certificat SSL
 - authentification LDAP [27](#)
 - Authentification utilisateur LDAP [22](#)
- cibles
 - privilèges [132](#)
- Client PowerCenter
 - administrateur [88](#)
- comptes
 - modification du mot de passe [83](#)
- comptes utilisateur
 - modification du mot de passe [83](#)
- comptes utilisateurs
 - activation [92](#)
 - créés lors de l'installation [87](#)
 - par défaut [87](#)
 - présentation [87](#)
- configuration du client
 - domaine sécurisé [56](#)
- connexions
 - autorisations [176](#)
 - autorisations par défaut [177](#)
 - types d'autorisation [177](#)
- convertUserActivityLog
 - journaux d'activité utilisateur [95](#)
- créer des tables de référence
 - privilège [120](#)

D

- Data Analyzer
 - administrateur [88](#)

- demandes d'objets
 - privileges pour PowerCenter [138](#)
- description du groupe
 - caractères non valides [99](#)
- description utilisateur
 - caractères non valides [90](#)
- domaine
 - administrateur [88](#)
 - privileges [110](#)
 - privileges d'administration [111](#)
 - privileges d'administration de la sécurité [110](#)
 - Rôle Administrateur [159](#)
 - sécurité des utilisateurs [84](#)
 - synchronisation utilisateur [78](#)
 - utilisateurs avec des privileges [165](#)
- domaine de sécurité LDAP
 - description [19](#), [20](#)
- domaine de sécurité natif
 - description [19](#)
- domaine Informatica
 - autorisations [84](#)
 - privileges [84](#)
 - sécurité des utilisateurs [84](#)
 - utilisateurs, gestion [90](#)
- domaine sécurisé
 - configuration du client [56](#)
- domaines de sécurité
 - configuration de LDAP [24](#)
 - LDAP [19–21](#)
 - native [19](#)
 - suppression d'un LDAP [28](#)
- domaines de sécurité LDAP
 - configuration [24](#)
 - description [21](#)
 - suppression [28](#)
- dossiers
 - autorisations [171](#)
 - privileges [128](#)

F

- fichiers de migration d'utilisateur
 - migrateUsers [31](#)
- filtres de recherche
 - autorisations [170](#)

G

- Gestionnaire de service
 - authentification [78](#)
 - authentification unique [78](#)
 - autorisation [78](#)
- getUserActivityLog
 - filtres
 - filtres
 - getUserActivityLog [96](#)
 - journaux d'activité utilisateur [95](#)
- grilles
 - autorisations [171](#)
- groupe de privileges Administration de domaine
 - description [111](#)
- Groupe de privileges Administration de la sécurité
 - description [110](#)
- Groupe de privileges Chargement
 - description [124](#)

- groupe de privileges d'administration Cloud
 - domaine [119](#)
- Groupe de privileges des objets globaux
 - description [138](#)
- groupe de privileges Dossiers
 - description [128](#)
- Groupe de privileges du modèle
 - description [125](#)
- Groupe de privileges Objets d'exécution
 - description [134](#)
- groupe de privileges Objets de conception
 - description [130](#)
- groupe de privileges Outils
 - Service de référentiel PowerCenter [127](#)
- Groupe de privileges Outils
 - domaine [118](#)
- Groupe de privileges Sécurité
 - description [125](#)
- Groupe de privileges Sources et cibles
 - description [132](#)
- groupe de privileges Surveillance
 - domaine [117](#)
- groupe Tout le monde
 - description [87](#)
- groupes
 - caractères non valides [99](#)
 - gestion [98](#)
 - groupe parent [99](#)
 - nom valide [99](#)
 - présentation [81](#)
 - privileges, attribution [163](#)
 - rôles, attribution [163](#)
 - synchronisation [78](#)
 - Tout le monde par défaut [87](#)
- groupes de déploiement
 - privileges pour PowerCenter [138](#)
- groupes de privileges
 - Administration [142](#)
 - administration d'Informatica Cloud [119](#)
 - Administration de domaine [111](#)
 - Administration de la sécurité [110](#)
 - Alertes [143](#)
 - Chargement [124](#)
 - Communication [144](#)
 - description [109](#)
 - Dossiers [128](#)
 - Gérer les comptes [147](#)
 - Indicateurs [147](#)
 - Modèle [125](#)
 - Objets d'exécution [134](#)
 - Objets de conception [130](#)
 - Objets globaux [138](#)
 - Outils [118](#), [127](#)
 - Parcourir [122](#)
 - Rapports [147](#)
 - Répertoire de contenu [145](#)
 - Sécurité [125](#)
 - Sources et cibles [132](#)
 - Surveillance [117](#)
 - Tableau de bord [146](#)
- groupes imbriqués
 - authentification LDAP [27](#)
 - service d'annuaire LDAP [27](#)
- groupes LDAP
 - gestion [98](#)
 - importation [22](#)
- groupes natifs
 - ajout [99](#)

groupes natifs (*a continué*)
déplacement vers un autre groupe [100](#)
gestion [98](#)
modification [100](#)
suppression [100](#)
utilisateurs, assignation [91](#)
groupes parents
description [99](#)

I

infacmd isp
migrateUsers [32](#)
Informatica Administrator
Navigateur [80](#)
onglets, affichage [75](#)
Page Sécurité [79](#)
présentation [75](#)
recherche [80](#)
Informatica Analyst
administrateur [88](#)
Informatica Developer
administrateur [88](#)

J

journaux d'activité utilisateur
convertUserActivityLog [95](#)
formats de sortie [95](#)
getUserActivityLog [95](#)

L

libellés
privileges pour PowerCenter [138](#)
licences
autorisations [171](#)

M

mémoire système
augmentation [94](#)
Metadata Manager
administrateur [88](#)
Metadata Manager Service
privileges [121](#)
rôles personnalisés [196](#)
métrologie personnalisée
privilege pour promouvoir [142](#), [147](#)
migrateUsers
fichiers de migration d'utilisateur [31](#)
infacmd isp [32](#)
modification
mot de passe du compte utilisateur [83](#)
modifier les métadonnées de la table de référence
privilege [120](#)
mot de passe
modification d'un compte utilisateur [83](#)
mots de passe
changement pour l'administrateur par défaut [87](#)
configuration requise [90](#)
utilisateurs natifs [90](#)

N

Navigateur
Page Sécurité [80](#)
nœuds
autorisations [171](#)
nom valide
compte utilisateur [90](#)
groupes [99](#)

O

objets d'exécution
description [134](#)
privileges [134](#)
objets de conception
description [130](#)
privileges [130](#)
objets de connexion
privileges pour PowerCenter [138](#)
objets de domaine
autorisations [171](#)
objets globaux
privileges pour PowerCenter [138](#)
opération du service Web
autorisations [184](#)

P

Page Sécurité
Informatica Administrator [79](#)
Navigateur [80](#)
Parcourir les groupes de privileges
description [122](#)
PowerCenter Repository Service
privileges [127](#)
rôles personnalisés [194](#)
privileges
Administration [142](#)
administration d'Informatica Cloud [119](#)
administration de domaine [111](#)
administration de la sécurité [110](#)
Alertes [143](#)
attribution [163](#)
cibles [132](#)
Communication [144](#)
description [107](#)
domaine [110](#)
dossiers [128](#)
Gérer les comptes [147](#)
hérités [164](#)
Indicateurs [147](#)
Metadata Manager Service [121](#)
objets d'exécution [134](#)
objets de conception [130](#)
Objets globaux PowerCenter [138](#)
outils de domaine [118](#)
outils du service de référentiel PowerCenter [127](#)
PowerCenter Repository Service [127](#)
Rapports [147](#)
Répertoire de contenu [145](#)
Reporting Service [142](#)
résolution des problèmes [166](#)
Service Analyst [119](#)
Service d'écoute PowerExchange [141](#)
Service d'intégration de données [121](#)

- privilèges (*a continué*)
 - service de gestion de contenu [120](#)
 - Service de journalisation PowerExchange [141](#)
 - Service de référentiel modèle [125](#)
 - sources [132](#)
 - surveillance [117](#)
 - Tableau de bord [146](#)
 - utilisation des autorisations [168](#)
- privilèges du service de rapports
 - Groupe de privilèges Administration [142](#)
 - groupe de privilèges Tableau de bord [146](#)
- Privilèges du service de rapports
 - Groupe de privilèges Alertes [143](#)
 - Groupe de privilèges d'indicateurs [147](#)
 - Groupe de privilèges de communication [144](#)
 - Groupe de privilèges Gérer les comptes [147](#)
 - Groupe de privilèges Rapports [147](#)
 - groupe de privilèges Répertoire de contenu [145](#)
- Privilèges du service Metadata Manager
 - Groupe de privilèges Chargement [124](#)
 - Groupe de privilèges du modèle [125](#)
 - Groupe de privilèges Sécurité [125](#)
 - Parcourir les groupes de privilèges [122](#)
- privilèges hérités
 - description [164](#)
- procédure virtuelle stockée
 - autorisations [179](#)
 - autorisations héritées [179](#)
- profil de système d'exploitation
 - modification [101](#)
 - propriétés [101](#)
 - suppression [100](#)
- profil du système d'exploitation
 - création [101](#)
- profils du système d'exploitation
 - autorisations [171](#), [175](#)

R

- rapports d'audit
 - description [187](#)
 - pour les groupes [192](#)
 - pour les utilisateurs [191](#), [193](#)
- Reporting Service
 - privilèges [142](#)
 - rôles personnalisés [197](#)
- rôles
 - Administrateur [159](#)
 - attribution [163](#)
 - description [109](#)
 - gestion [158](#)
 - personnalisé [162](#)
 - présentation [82](#)
 - résolution des problèmes [166](#)
- rôles définis par le système
 - Administrateur [159](#)
 - attribution à des utilisateurs et à des groupes [163](#)
 - description [158](#)
- rôles personnalisés
 - attribution à des utilisateurs et à des groupes [163](#)
 - création [162](#)
 - description [158](#), [162](#)
 - Metadata Manager Service [196](#)
 - modification [162](#)
 - PowerCenter Repository Service [194](#)
 - privilèges, attribution [163](#)
 - Reporting Service [197](#)

- rôles personnalisés (*a continué*)
 - Service Analyst [208](#)
 - suppression [163](#)

S

- schéma virtuel
 - autorisations [179](#)
 - autorisations héritées [179](#)
- Section Rechercher
 - Informatica Administrator [80](#)
- sécurité
 - autorisations [84](#)
 - mots de passe [90](#)
 - privilèges [84](#), [107](#), [110](#)
 - rôles [109](#)
- sécurité au niveau des colonnes
 - restriction des colonnes [182](#)
- sécurité basée sur le fournisseur
 - utilisateurs, suppression [93](#)
- sécurité basée sur les utilisateurs
 - utilisateurs, suppression [93](#)
- Sécurité PowerCenter
 - gestion [79](#)
- sécurité utilisateur
 - description [77](#)
- Service Analyst
 - privilèges [119](#)
 - rôles personnalisés [208](#)
- service d'annuaire LDAP
 - connexion à [22](#)
 - groupes imbriqués [27](#)
- Service d'annuaire Open LDAP
 - authentification LDAP [22](#)
- Service d'écoute PowerExchange
 - privilèges [141](#)
- Service d'intégration de données
 - autorisation [78](#)
 - privilèges [121](#)
- service de données SQL
 - autorisations [179](#)
 - autorisations héritées [179](#)
 - types d'autorisation [179](#)
- service de gestion de contenu
 - privilèges [120](#)
- Service de journalisation PowerExchange
 - privilèges [141](#)
- Service de rapports
 - autorisation [78](#)
 - synchronisation utilisateur [78](#)
 - utilisateurs avec des privilèges [165](#)
- Service de référentiel modèle
 - autorisation [78](#)
 - privilèges [125](#)
 - synchronisation utilisateur [78](#)
 - utilisateurs avec des privilèges [165](#)
- Service de référentiel PowerCenter
 - autorisation [78](#)
 - Rôle Administrateur [159](#)
 - synchronisation utilisateur [78](#)
 - utilisateurs avec des privilèges [165](#)
- Service du gestionnaire de métadonnées
 - utilisateurs avec des privilèges [165](#)
- Service IBM Tivoli Directory
 - authentification LDAP [22](#)
- Service Metadata Manager
 - autorisation [78](#)

- Service Metadata Manager (*a continué*)
 - synchronisation utilisateur [78](#)
- Service Microsoft Active Directory
 - authentification LDAP [22](#)
- Service Novell e-Directory
 - authentification LDAP [22](#)
- Service Sun Java System Directory
 - authentification LDAP [22](#)
- service web
 - types d'autorisation [184](#)
- service Web
 - autorisations [184](#)
- services d'application
 - autorisation [78](#)
 - autorisations [171](#)
 - synchronisation utilisateur [78](#)
- sources
 - privileges [132](#)
- synchronisation
 - heures du service d'annuaire LDAP [26](#)
 - utilisateurs [78](#)
 - utilisateurs LDAP [22](#)

T

- table virtuelle
 - autorisations [179](#)
 - autorisations héritées [179](#)
- Test Data Manager
 - administrateur [88](#)

U

- UpdateColumnOptions
 - substitution des valeurs de colonnes [182](#)
- utilisateurs
 - assignation aux groupes [91](#)

- utilisateurs (*a continué*)
 - caractères non valides [90](#)
 - gestion [90](#)
 - grand nombre d' [94](#)
 - mémoire système [94](#)
 - nom valide [90](#)
 - présentation [81](#)
 - privileges, attribution [163](#)
 - rôles, attribution [163](#)
 - sécurité basée sur le fournisseur [93](#)
 - sécurité basée sur les utilisateurs [93](#)
 - synchronisation [78](#)
- utilisateurs LDAP
 - activation [92](#)
 - assignation aux groupes [92](#)
 - gestion [90](#)
 - importation [22](#)
- utilisateurs natifs
 - activation [92](#)
 - ajout [90](#)
 - assignation aux groupes [91](#)
 - gestion [90](#)
 - modification [91](#)
 - mots de passe [90](#)
 - suppression [93](#)

V

- variables d'environnement
 - INFA_TRUSTSTORE [56](#)
 - INFA_TRUSTSTORE_PASSWORD [56](#)