



Informatica® Enterprise Data Catalog
10.5.3

Mise à niveau à partir des
versions 10.4.0 et ultérieures

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

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

Soumis à vos droits de retrait, le logiciel transmettra automatiquement certaines informations à Informatica (aux États-Unis) concernant l'environnement informatique et réseau dans lequel le Logiciel est déployé et les statistiques du système et d'utilisation des données du déploiement. Cette transmission est considérée comme faisant partie des Services selon la politique de confidentialité d'Informatica et Informatica utilisera et traitera par ailleurs ces informations conformément à la politique de confidentialité d'Informatica disponible sur <https://www.informatica.com/in/privacy-policy.html>. Il est possible de désactiver la collecte d'utilisation dans l'outil Administrator tool.

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 © University of Toronto. Tous droits réservés. Copyright © Daniel Veillard. Tous droits réservés. Copyright © Unicode, 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. Copyright © Amazon Corporate LLC. Tous droits réservés. Copyright © Highsoft. Tous droits réservés. Copyright © Python Software Foundation. Tous droits réservés. Copyright © BeOpen.com. Tous droits réservés. Copyright © CNRI. 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 soumise 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://www.cryptix.org/LICENSE.TXT>.

hsqldb.org/web/hsqLicense.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-5-3-1-license-agreement> ; <http://antlr.org/license.html> ; <http://aopalliance.sourceforge.net/> ; <http://www.bouncycastle.org/license.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/jaservice/> ; <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> ; <http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html> ; <https://aws.amazon.com/asl/> ; <https://github.com/twbs/bootstrap/blob/master/LICENSE> ; <https://sourceforge.net/p/xmlunit/code/HEAD/tree/trunk/LICENSE.txt> ; <https://github.com/documentcloud/underscore-contrib/blob/master/LICENSE>, and <https://github.com/apache/hbase/blob/master/LICENSE.txt>.

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.

Consultez les brevets applicables à l'adresse <https://www.informatica.com/legal/patents.html>.

EXCLUSION DE RESPONSABILITÉ : Informatica LLC 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 LLC 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.

Consultez les brevets applicables à l'adresse <https://www.informatica.com/legal/patents.html>.

Les renseignements contenus dans cette documentation sont sujets à modification sans préavis. Si vous constatez des problèmes liés à la documentation, merci de les signaler par courriel à l'adresse info_documentation@Informatica.com.

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

Date de publication: 2022-12-08

Sommaire

Préface.....	9
Ressources Informatica.	9
Informatica Network.	9
Base de connaissances Informatica.	9
Documentation Informatica.	10
Matrices de disponibilité des produits Informatica.	10
Informatica Velocity.	10
Informatica Marketplace.	10
Support client international Informatica.	10
 Chapitre 1: Mise à niveau du catalogue de données d'entreprise.....	 11
Présentation de la mise à niveau d'Enterprise Data Catalog.	11
Chemins de mise à niveau.	12
Planification du déploiement.	13
Service de cluster Informatica et services associés.	13
 Chapitre 2: Appliquer le HotFix.....	 15
Présentation de l'installation et de la restauration du HotFix.	15
Application du HotFix des services.	17
Avant l'application du HotFix.	17
Appliquer le HotFix des services en mode console.	19
Appliquer le HotFix des services en mode silencieux.	21
Après l'application du HotFix.	24
Restauration du HotFix des services.	26
Avant la restauration du HotFix.	26
Restaurer le HotFix des services en mode console.	27
Restaurer le HotFix des services en mode silencieux.	28
Après la restauration du HotFix.	29
Application du HotFix client.	30
Appliquer le HotFix client en mode graphique.	30
Appliquer le HotFix client en mode silencieux.	31
Restauration du HotFix client.	32
Restauration du HotFix client en mode graphique.	32
Restauration du HotFix client en mode silencieux.	33
 Chapitre 3: Mettre à niveau Enterprise Data Catalog dans un cluster interne. 34	
Présentation de la mise à niveau d'Enterprise Data Catalog dans un cluster interne.	35
Étape 1. Vérifier les prérequis de la mise à niveau.	36
Configurer les certificats SSL personnalisésPrésentation.	39
Vérifier la somme de contrôle du package d'installation sur	46

Obtenir les clés de licence et copier les fichiers binaires.	46
Effectuer les tâches prérequis	47
Sauvegarder les enrichissements de clé primaire-clé étrangère à l'aide de l'utilitaire de migration.	47
Remplir les prérequis de l'analyse des actifs de données.	47
Étape 2. Sauvegarder les référentiels et les détails de configuration	49
Sauvegarder le domaine Informatica.	49
Sauvegarder le référentiel modèle.	50
Sauvegarder les données du catalogue à l'aide de l'utilitaire export.	50
Sauvegarder le catalogue Données utilisant la commande Idm backupContents.	51
Sauvegarder la configuration SSL.	52
Sauvegarder les informations du domaine.	52
Sauvegarder le schéma de base de données de l'analyse des actifs de données.	52
Sauvegarder MetaDex.	53
Sauvegarder les enrichissements de la ressource Tableau à l'aide de l'utilitaire de migration	53
Sauvegarder les enrichissements de la ressource Qlik Sense à l'aide de l'utilitaire de migration	53
Sauvegarder les enrichissements de la ressource Salesforce à l'aide de l'utilitaire de migration	54
Sauvegarder les enrichissements de la ressource Erwin à l'aide de l'utilitaire de migration	54
Étape 3. Préparer la mise à niveau.	54
Désactivation du service de catalogue.	54
Désactiver les services d'application Informatica.	55
Nettoyer le cluster.	55
Désactiver et désinstaller le service PostgreSQL.	56
Arrêter le domaine Informatica.. . . .	56
Étape 4. Présentation de la mise à niveau du domaine.	57
Exécuter l'utilitaire de validation de cluster	57
Mettre à niveau en mode console.	58
Appliquer le dernier Service Pack ou correctif cumulatif	62
Configurer le référentiel MetaDex (facultatif).	62
Copier les pilotes de ressources tiers.	64
Activer et mettre à niveau les services d'application.	64
Ajouter la licence du domaine Informatica.	65
Mettre à jour la licence du service de cluster Informatica.	66
Étape 5. Effectuer la mise à niveau du domaine Informatica.	66
Vérifier les prérequis de l'utilisateur de la passerelle.	66
Configurer les privilèges Sudo pour l'utilisateur de la passerelle (facultatif).	66
Effectuer la configuration SSL par défaut.	67
Étape 6. Activer et mettre à niveau les services Enterprise Data Catalog.	68
Activer le service de cluster Informatica.	68
Activer et mettre à niveau le service de catalogue.	68
Étape 7. Migrer et vérifier les données du catalogue	68

Migrer les données du catalogue	68
Vérifier les données de catalogue migrées.	70

Chapitre 4: Mettre à niveau Enterprise Data Catalog dans un cluster externe..... 71

Mettre à niveau Enterprise Data Catalog dans un cluster externe.	72
Étape 1. Vérifier les prérequis de la mise à niveau	73
Configurer les certificats SSL personnalisésPrésentation.	76
Vérifier la somme de contrôle du package d'installation sur	83
Obtenir les clés de licence et copier les fichiers binaires.	84
Effectuer les tâches prérequis.	84
Sauvegarder les enrichissements de clé à l'aide de l'utilitaire de migration.	85
Remplir les prérequis de l'analyse des actifs de données.	85
Étape 2. Sauvegarder les référentiels et les détails de configuration.	86
Sauvegarder le domaine.	86
Sauvegarder le référentiel modèle.	87
Sauvegarder les données du catalogue à l'aide de l'utilitaire export.	88
Sauvegarder le catalogueDonnées utilisant la commande Idm backupContents	89
Sauvegarder la configuration SSL.	90
Sauvegarder les informations du domaine.	90
Sauvegarder le schéma de base de données de l'analyse des actifs de données.	90
Sauvegarder MetaDex.	90
Sauvegarder les enrichissements de la ressource Tableau à l'aide de l'utilitaire de migration	91
Étape 3. Préparer la mise à niveau.	91
Désactivation du service de catalogue.	91
Désactiver les services d'application.	91
Arrêter le domaine Informatica.. . . .	91
Étape 4. Mettre à niveau le domaine Informatica.	91
Exécuter l'utilitaire de validation de cluster	92
Mettre à niveau en mode console.	93
Appliquer le dernier Service Pack ou correctif cumulatif	97
Configurer le référentiel MetaDex (facultatif)	97
Copier les pilotes de ressources tiers.	99
Activer et mettre à niveau les services d'application.	99
Ajouter la licence du domaine Informatica.	100
Étape 5. Effectuer la mise à niveau du domaine Informatica.	101
Vérifier les prérequis de l'utilisateur de la passerelle.	101
Configurer les privilèges Sudo pour l'utilisateur de la passerelle (facultatif).	101
Effectuer la configuration SSL par défaut(Facultatif)	102
Étape 6. Activer et mettre à niveau les services Enterprise Data Catalog	102
Créer et activer le service de cluster Informatica.	102
Associer le service de cluster Informatica au service de catalogue.	107
Activer et mettre à niveau le service de catalogue.	107

Étape 7. Migrer et vérifier les données du catalogue	108
Migrer les données du catalogue	108
Vérifier les données de catalogue migrées	109

Chapitre 5: Après la mise à niveau Catalogue de données d'entreprise..... 110

Tâches générales postérieures à la mise à niveau.	110
Importer les transports SAP.	111
Mettre à jour les fichiers binaires pour les ressources Informatica Platform.	112
Restaurer les enrichissements de ressources pour Tableau.	112
Restaurer les enrichissements de ressources pour Erwin.	112
Sauvegarder et restaurer des enrichissements de ressources pour SAP Business Objects.	113
Tâches postérieures à la mise à niveau pour la ressource Qlik Sense.	114
Tâches postérieures à la mise à niveau pour la ressource Salesforce.	114
Afficher les résultats de similarité des colonnes.	114
Synchroniser les événements d'actifs de données pour l'analyse des actifs de données.	115
Restaurer les enrichissements de clé.	115
Exécuter ou créer des ressources.	116
Purger et réexécuter les ressources de référence.	117
Tâches postérieures à la mise à niveau pour MetaDex.	118
Mettre à jour les fichiers du pilote pour les ressources.	119
Supprimer les ressources effacées migrées par l'utilitaire d'exportation.	120
Tâche postérieure à la mise à niveau pour atténuer la vulnérabilité Log4j.	120
Observations postérieures à la mise à niveau.	120

Chapitre 6: Dépannage de la mise à niveau..... 122

Présentation du dépannage de la mise à niveau.	122
Dépannage des problèmes de mise à niveau	122

Annexe A: Mettre à niveau en mode silencieux 125

Configuration du fichier de propriétés	125
Exécution du programme d'installation silencieuse	129

Annexe B: Installation et suppression des distributions tierces..... 130

Présentation de l'installation et de la suppression des distributions tierces.	130
Présentation d'Integration Package Manager.	131
Avant de commencer.	131
Installer ou supprimer des distributions en mode console.	132
Installer ou supprimer des distributions en mode silencieux.	132
Configurer les variables d'environnement pour utiliser les distributions installées.	133
Configurer Informatica Developer.	134
Configurer le service d'intégration de données.	134
Configurer le service d'accès aux métadonnées.	134

Index..... 136

Préface

Pour mettre à niveau Enterprise Data Catalog, suivez les instructions du guide *Mise à niveau d'Informatica®* à partir des versions 10.4.0 et ultérieures. Ce guide inclut des informations sur la mise à niveau d'Enterprise Data Catalog sur un cluster interne et externe. Il comprend également des informations complémentaires sur les tâches requises préalables et postérieures que vous devez effectuer pour terminer la mise à niveau, ainsi que des conseils de dépannage. Sauf indication contraire, le chemin de mise à niveau comprend des HotFix et des Service Packs.

Ressources Informatica

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

Informatica Network

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

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

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

Base de connaissances Informatica

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

Pour effectuer des recherches dans la base de connaissances, visitez le site <https://search.informatica.com>. N'hésitez pas à contacter l'équipe de la base de connaissances Informatica à l'adresse KB_Feedback@informatica.com pour lui faire part de vos questions, commentaires et suggestions concernant la base de connaissances.

Documentation Informatica

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

N'hésitez pas à contacter l'équipe Documentation Informatica à l'adresse info_documentation@informatica.com pour lui faire part de vos questions, commentaires ou suggestions concernant la documentation des produits.

Matrices de disponibilité des produits Informatica

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

Informatica Velocity

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

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

Informatica Marketplace

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

Support client international Informatica

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

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

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

CHAPITRE 1

Mise à niveau du catalogue de données d'entreprise

Ce chapitre comprend les rubriques suivantes :

- [Présentation de la mise à niveau d'Enterprise Data Catalog, 11](#)
- [Planification du déploiement, 13](#)

Présentation de la mise à niveau d'Enterprise Data Catalog

Le programme d'installation fournit un assistant de mise à niveau du domaine pour vous guider à travers le processus de mise à niveau. L'assistant de mise à niveau installe Informatica dans le répertoire que vous indiquez. Il ne modifie pas les fichiers du répertoire de la version précédente.

Vous pouvez mettre à niveau Enterprise Data Catalog déployé sur un cluster externe ou interne vers la version 10.5.3. Le processus de mise à niveau crée un cluster non Hadoop que vous utiliserez à la place du cluster Hadoop interne ou externe précédent. Le cluster non-Hadoop peut être appelé *cluster de catalogue*.

Chemins de mise à niveau

Le chemin de mise à niveau que vous utilisez dépend des produits que vous mettez à niveau. Si vous utilisez une version qui ne prend pas en charge une mise à niveau directe, vous devez d'abord effectuer une mise à niveau vers une version prise en charge.

Le tableau suivant répertorie les chemins de mise à niveau pour chaque produit pris en charge par le programme d'installation.

Produit	Versions
PowerCenter	<p>Vous pouvez appliquer le HotFix 10.5.3 aux versions 10.5, 10.5.1 et 10.5.2, y compris tout Service Pack ou correctif cumulatif.</p> <p>Vous pouvez effectuer une mise à niveau vers la version 10.5.3 à partir des versions précédentes suivantes :</p> <ul style="list-style-type: none"> - 10.2, y compris tout HotFix, Service Pack ou correctif cumulatif - 10.4, y compris tout Service Pack ou correctif cumulatif - 10.4.1, y compris tout Service Pack ou correctif cumulatif
Informatica Data Quality	<p>Vous pouvez effectuer une mise à niveau vers la version 10.5.3 à partir des versions précédentes suivantes :</p> <ul style="list-style-type: none"> - 10.2, y compris tout HotFix, Service Pack ou correctif cumulatif - 10.4, y compris tout Service Pack ou correctif cumulatif - 10.4.1, y compris tout Service Pack ou correctif cumulatif
Data Engineering Integration Data Engineering Quality	<p>Vous pouvez appliquer le HotFix 10.5.3 aux versions 10.5, 10.5.1 et 10.5.2, y compris tout Service Pack ou correctif cumulatif.</p> <p>Vous pouvez effectuer une mise à niveau vers la version 10.5.3 à partir des versions précédentes suivantes :</p> <ul style="list-style-type: none"> - 10.2, y compris tout HotFix, Service Pack ou correctif cumulatif - 10.2.1, y compris tout HotFix, Service Pack ou correctif cumulatif - 10.2.2, y compris tout HotFix, Service Pack ou correctif cumulatif - 10.4, y compris tout Service Pack ou correctif cumulatif - 10.4.1, y compris tout Service Pack ou correctif cumulatif <p>Important: Si Data Engineering se trouve dans le même domaine que tout autre produit pris en charge par le programme d'installation Informatica, vérifiez que tous les produits sont mis à niveau vers la même version de mise à niveau prise en charge avant de passer à la version 10.5.3.</p>
Data Engineering Streaming	<p>Vous pouvez appliquer le HotFix 10.5.3 aux versions 10.5, 10.5.1 et 10.5.2, y compris tout Service Pack ou correctif cumulatif.</p> <p>Vous pouvez effectuer une mise à niveau vers la version 10.5.3 à partir des versions précédentes suivantes :</p> <ul style="list-style-type: none"> - 10.2.2, y compris tout HotFix, Service Pack ou correctif cumulatif - 10.4, y compris tout Service Pack ou correctif cumulatif - 10.4.1, y compris tout Service Pack ou correctif cumulatif
Data Privacy Management	<p>Vous pouvez appliquer le HotFix 10.5.3 aux versions 10.5, 10.5.1 et 10.5.2, y compris tout Service Pack ou correctif cumulatif.</p>
Enterprise Data Catalog	<p>Vous pouvez appliquer le HotFix 10.5.3 aux versions 10.5, 10.5.1 et 10.5.2, y compris tout Service Pack ou correctif cumulatif.</p> <p>Vous pouvez effectuer une mise à niveau vers la version 10.5.3 à partir des versions précédentes suivantes :</p> <ul style="list-style-type: none"> - 10.4, y compris tout Service Pack ou correctif cumulatif - 10.4.1, y compris tout Service Pack ou correctif cumulatif <p>Important: Si Enterprise Data Catalog et Data Engineering se trouvent dans le même domaine d'une version antérieure à 10.4, mettez-les tous deux à niveau vers la version 10.4 ou 10.4.1 avant de passer à la version 10.5.3.</p>

Produit	Versions
Enterprise Data Preparation	<p>Vous pouvez appliquer le HotFix 10.5.3 aux versions 10.5, 10.5.1 et 10.5.2, y compris tout Service Pack ou correctif cumulatif.</p> <p>Vous pouvez effectuer une mise à niveau vers la version 10.5.3 à partir des versions précédentes suivantes :</p> <ul style="list-style-type: none"> - 10.4, y compris tout Service Pack ou correctif cumulatif - 10.4.1, y compris tout Service Pack ou correctif cumulatif <p>Important: Si Data Engineering, Enterprise Data Catalog et Enterprise Data Preparation se trouvent dans le même domaine d'une version antérieure à 10.4, mettez-les tous à niveau vers la version 10.4 ou 10.4.1 avant de passer à la version 10.5.3.</p>
Test Data Management	Vous pouvez appliquer le HotFix 10.5.3 aux versions 10.5, 10.5.1 et 10.5.2, y compris tout Service Pack ou correctif cumulatif.

Planification du déploiement

Vous pouvez prévoir de déployer Enterprise Data Catalog sur un, trois ou six nœuds.

Le déploiement d'Enterprise Data Catalog implique la création et la configuration du service de cluster Informatica. Le service de cluster Informatica exécute et gère le déploiement d'Enterprise Data Catalog. Si vous prévoyez de déployer Enterprise Data Catalog sur plusieurs nœuds, la haute disponibilité est activée par défaut pour fournir la résilience et le basculement pour le service de cluster Informatica.

Le service de cluster Informatica utilise un ensemble d'applications et de services associés fournis avec le programme d'installation pour gérer et exécuter Enterprise Data Catalog.

Lorsque vous configurez le service de cluster Informatica, vous pouvez spécifier un, trois ou six nœuds sur lesquels les applications et les services associés peuvent s'exécuter. Ces nœuds sont appelés nœuds de données dans le cluster. Les nœuds sur lesquels vous souhaitez exécuter des travaux de profilage ou des travaux d'analyse de métadonnées sont appelés nœuds de traitement dans le cluster. Il n'existe aucune restriction sur le nombre de nœuds de traitement que vous pouvez configurer.

Important: Pour les services d'application associés, vous ne pouvez pas configurer plus de trois instances de service pour un déploiement.

Service de cluster Informatica et services associés

Le service de cluster Informatica utilise les services suivants pour exécuter et gérer Enterprise Data Catalog :

Service	Description
MongoDB	Service de gestion de la base de données MongoDB utilisée comme magasin de métadonnées. Enterprise Data Catalog stocke les métadonnées extraites de sources externes dans la base de données MongoDB.
Nomad	Service permettant de gérer le service d'orchestration Nomad utilisé pour planifier les travaux d'analyse des ressources.
Apache Solr	Service de gestion d'Apache Solr utilisé pour indexer et rechercher les actifs du catalogue.

Service	Description
Apache ZooKeeper	Service de gestion d'Apache ZooKeeper utilisé comme application de coordination de services
PostgreSQL	Service de gestion de la base de données PostgreSQL utilisée comme magasin pour les données de profilage de similarité.

CHAPITRE 2

Appliquer le HotFix

Ce chapitre comprend les rubriques suivantes :

- [Présentation de l'installation et de la restauration du HotFix, 15](#)
- [Application du HotFix des services, 17](#)
- [Restauration du HotFix des services, 26](#)
- [Application du HotFix client, 30](#)
- [Restauration du HotFix client, 32](#)

Présentation de l'installation et de la restauration du HotFix

Lorsque vous appliquez le HotFix, le programme d'installation sauvegarde les répertoires existants, applique la nouvelle version du produit et restaure ou met à jour les fichiers de configuration et d'exécution requis. Lorsque vous restaurez un HotFix, le programme d'installation rétablit la version précédemment installée d'Informatica.

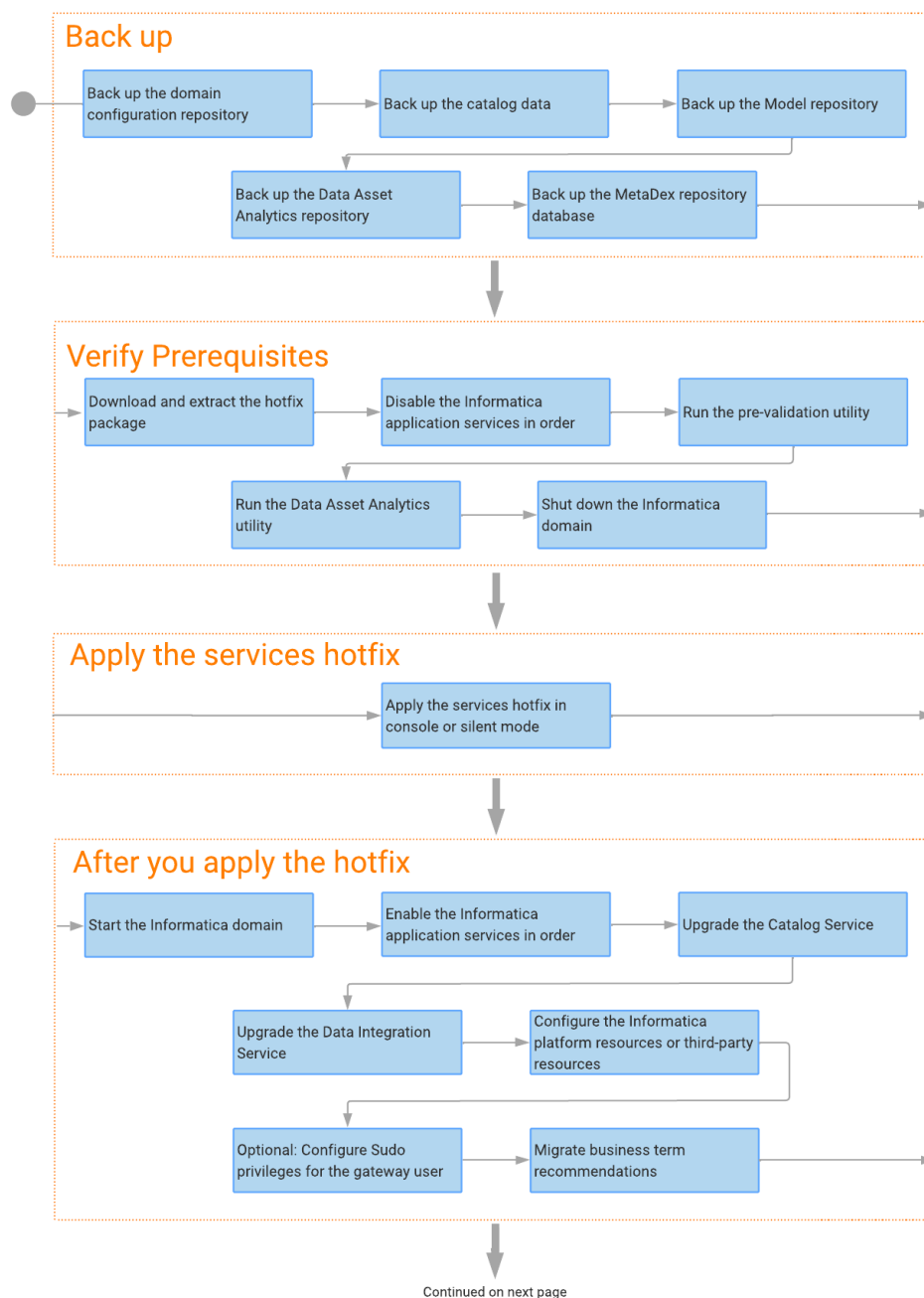
Informatica fournit des programmes d'installation pour appliquer des HotFixes aux services Informatica.

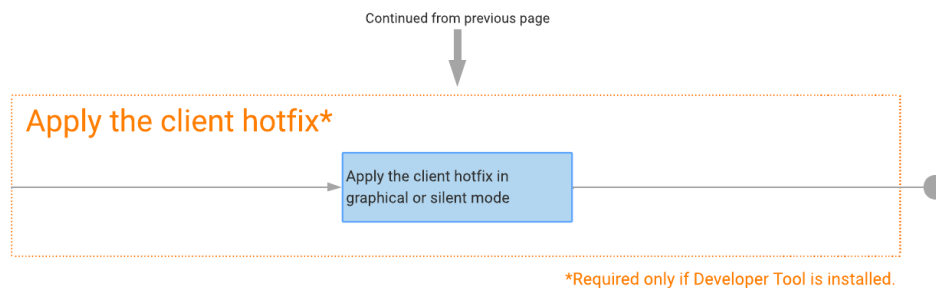
Pour appliquer le HotFix, suivez la procédure suivante :

1. Sauvegardez les données du catalogue, le référentiel modèle et les autres composants.
2. Désactivez le service de catalogue et les autres services d'application Informatica.
3. Arrêtez le service de cluster Informatica et le domaine Informatica.
4. Appliquez le HotFix aux services Informatica en mode console ou silencieux.
5. Démarrez le domaine Informatica et effectuez les tâches postérieures à la mise à niveau.

Si vous souhaitez restaurer le HotFix, vous pouvez exécuter le programme d'installation en mode console ou silencieux.

L'image suivante montre les étapes que vous devez effectuer pour appliquer le HotFix :





Application du HotFix des services

Lorsque vous appliquez le HotFix, le programme d'installation sauvegarde les répertoires existants, applique la nouvelle version du produit et restaure ou met à jour les fichiers de configuration et d'exécution requis.

Vous pouvez exécuter les programmes d'installation pour appliquer des HotFixes aux clients et aux services Informatica.

Veillez à sauvegarder les données du catalogue et le référentiel modèle avant d'appliquer le HotFix. Sans sauvegarde valide, vous ne pouvez pas réussir une restauration du HotFix. Après avoir appliqué le HotFix, le programme d'installation crée le répertoire `BACK_FROM_HF`. Les fichiers du répertoire sont requis pour la restauration. Si vous supprimez le répertoire, vous ne pouvez pas restaurer le HotFix.

Avant l'application du HotFix

Avant d'exécuter le programme d'installation pour appliquer le HotFix, effectuez les tâches prérequis suivantes :

1. Téléchargez et extrayez le package HotFix.
2. Pour installer des packages d'intégration, téléchargez les fichiers du programme d'installation des packages. Le programme d'installation d'Informatica ne télécharge pas les packages d'intégration tiers par défaut.
3. Extrayez les packages d'intégration dans le répertoire : `<Informatica installer files>/source`
4. Arrêtez tous les processus qui accèdent au répertoire et aux sous-répertoires d'installation, y compris les invites de commandes et les programmes en ligne de commande.
5. Fermez les clients Informatica sur toutes les machines sur lesquelles vous souhaitez appliquer le HotFix.
6. Effectuez les étapes suivantes pour sauvegarder les métadonnées de configuration du domaine Informatica :
 - a. Exécutez la commande `infasetup backupDomain` pour sauvegarder les tables de la base de données de configuration du domaine dans un fichier.
 - b. Sauvegardez les fichiers de configuration des métadonnées dans tout répertoire accessible par les machines sur lesquelles vous installez Informatica.

`infasetup` se trouve dans le répertoire suivant : `<Informatica installation directory>/isp/bin`

7. Sauvegardez les fichiers binaires à partir du répertoire d'installation d'Informatica. Sauvegardez également les fichiers suivants du domaine Informatica :

- `<Informatica installation directory>/isp/config/keys/siteKey`
- `<Informatica installation directory>/domains.infa`
- `<Informatica installation directory>/tomcat/conf/server.xml`
- `<Informatica installation directory>/isp/config/nodemeta.xml`

Le fichier `nodemeta.xml` contient les métadonnées d'un nœud. Il est stocké dans le répertoire suivant sur chaque nœud du domaine : `isp/config`. Si vous utilisez le même nom de répertoire de sauvegarde sur tous les nœuds, renommez le fichier avant de le copier vers l'emplacement de la sauvegarde. Par exemple, vous sauvegardez `nodemeta.xml` dans le répertoire `/nodebak` sur `nodeA` et `nodeB`. Renommez les fichiers de configuration de sorte que, sur `nodeA`, le fichier soit sauvegardé sous `/nodebak/nodemeta_A.xml` et, sur `nodeB`, il soit sauvegardé sous `/nodebak/nodemeta_B.xml`.

Le fichier `domains.infa` contient des informations de connectivité pour les nœuds de passerelle. Il est stocké dans le répertoire d'installation d'Informatica ou à l'emplacement configuré via la variable d'environnement `INFA_DOMAINS_FILE`.

8. Sauvegardez les données du catalogue à l'aide de la commande `infacmd ldm backupContents`.

Remarque: Vérifiez que vous avez effectué une sauvegarde complète des données du catalogue. Si vous avez déployé le service de cluster Informatica sur plusieurs nœuds, vérifiez que vous avez configuré le chemin du système de fichiers partagés du cluster pour le service de cluster Informatica. Si vous ne configurez pas le système de fichiers partagés, le magasin SEARCH n'est pas sauvegardé et un message d'avertissement s'affiche dans le journal de la console. Si le magasin SEARCH n'est pas sauvegardé, la validation de la sauvegarde échoue lorsque vous appliquez ou restaurez le HotFix.

9. Sauvegardez le référentiel modèle à l'aide de la commande `infacmd mrs backupContents`.

10. Sauvegardez le référentiel d'analyse des actifs de données.

11. Sauvegardez le référentiel MetaDex.

12. Sauvegardez les fichiers de configuration SSL suivants :

- Fichiers `truststore` et `keystore` du domaine.
- Fichiers `keystore` par défaut.
- Fichiers `keystore` et `truststore` utilisés par les services d'application.

Par défaut, les fichiers de configuration SSL sont stockés dans le répertoire suivant : `<Informatica installation directory>/services/shared/security`

13. Désactivez les services d'applications Informatica suivants :

- a. Service de catalogue
- b. Service de gestion de contenu
- c. Service d'intégration de données
- d. Service de référentiel modèle
- e. Service Analyst
- f. Service de messagerie électronique

14. Arrêtez le service de cluster Informatica à l'aide de la commande `infacmd ics shutdowncluster` ou à partir d'Informatica Administrator.

15. Exécutez l'utilitaire de pré-validation pour valider les prérequis à l'application du HotFix. L'utilitaire se trouve dans le répertoire suivant : `<Installer directory>/properties/utls/prevalidation/InformaticaClusterValidationUtility.jar`

Pour plus d'informations sur l'exécution de l'utilitaire de pré-validation, reportez-vous à l'[Knowledge Base article](#).

Remarque: Si un message d'erreur de validation d'autorisation pour le répertoire personnalisé du cluster s'affiche, vous pouvez ignorer l'erreur.

16. Exécutez l'utilitaire d'analyse des actifs de données. Pour plus d'informations sur l'exécution de l'utilitaire, reportez-vous à la section ["Exécuter l'utilitaire d'analyse des actifs de données" à la page 48](#).
17. Arrêtez le domaine Informatica à l'aide de la commande `infaservice shutdown`. Par défaut, le fichier exécutable `infaservice` se trouve dans le répertoire suivant : `<Informatica installation directory>/tomcat/bin`.
18. Si la machine utilise le protocole HTTPS pour se connecter à Informatica Administrator, vérifiez que le fichier `keystore` se trouve dans l'emplacement par défaut et qu'il utilise le nom de fichier par défaut. L'emplacement par défaut du fichier `keystore` est `<Informatica installation directory>/tomcat/conf`. Le nom de fichier par défaut pour le fichier `keystore` est `Default.keystore`.
19. Définissez la variable d'environnement `SKIP_VENDOR_CHECK` sur `true` pour supprimer l'invite `sudo` de l'installation du HotFix sous UNIX.

Remarque: Si vous ne disposez pas des privilèges `sudo`, définissez la variable d'environnement sur `true` avant d'appliquer ou de restaurer un HotFix. Si vous disposez de privilèges `sudo`, vous n'avez pas besoin de définir la variable d'environnement.

Appliquer le HotFix des services en mode console

Exécutez le programme d'installation 10.5.3 pour appliquer le HotFix à la version 10.5 ou 10.5.x.

Lorsque vous appliquez le HotFix en mode console, les mots Aide, Quitter et Retour sont des mots réservés. Ne les utilisez pas comme texte d'entrée.

Important: Vous ne pouvez pas revenir à la version précédente de MetaDex lorsque vous appliquez le HotFix.

Vous ne pouvez pas restaurer automatiquement le HotFix à l'aide du programme d'installation. Vous devez effectuer les étapes répertoriées dans la section ["Restaurer le HotFix des services en mode console" à la page 27](#) pour restaurer le HotFix.

1. Exécutez le programme d'installation à l'aide de la commande `./install.sh`.
2. Appuyez sur **Y** pour confirmer que vous souhaitez procéder à l'installation.
3. Appuyez sur **5** pour choisir l'option d'application du HotFix.
4. Appuyez sur **1** pour appliquer le HotFix.
5. Appuyez sur **2** pour accepter les conditions générales et appliquer la licence.
6. Vérifiez que toutes les exigences d'installation sont remplies avant de continuer à appliquer le HotFix.
7. Appuyez sur **Entrée**.
8. Entrez le répertoire d'installation d'Informatica 10.5 ou 10.5.x.
Les noms de répertoire dans le chemin ne doivent pas contenir d'espaces ni les caractères spéciaux suivants : `@|* $ # ! % () { } [] , ; ' "`
9. Appuyez sur **2** pour confirmer que vous avez configuré le service de catalogue sur le nœud.
Remarque: Si vous confirmez que vous avez configuré le service de catalogue sur le nœud, vous devez valider la sauvegarde.
10. Appuyez sur **2** pour confirmer que vous aviez sauvegardé les données du catalogue à l'aide de la commande `infacmd Idm backupContents`.
Appuyez sur **1** pour ignorer la validation de la sauvegarde et continuer.

Vous devez ignorer la validation dans les scénarios suivants :

- Vous avez configuré plusieurs nœuds pour le service de catalogue et vous ne souhaitez pas valider la sauvegarde sur chaque nœud.
- Vous n'avez pas configuré le chemin du système de fichiers partagés du cluster pour le service de cluster Informatica sur une configuration à plusieurs nœuds.
- Vous avez activé le service de référentiel modèle et le service d'intégration de données, mais vous n'avez pas créé le service de catalogue et le service de cluster Informatica.

11. Entrez l'emplacement du fichier de sauvegarde. Par exemple, `/data/Informatica/LDM_BACKUP1050SAML12.zip`.

Remarque: Si le magasin SEARCH n'est pas compris dans la sauvegarde, la validation échoue avec une erreur. Vous pouvez ignorer la validation de la sauvegarde si celle-ci ne comprend pas le magasin SEARCH.

12. Sélectionnez l'une des options suivantes selon le type d'installation :

- Appuyez sur **1** afin de définir l'environnement Sandbox pour un environnement de base utilisé comme preuve de concept avec un minimum d'utilisateurs.
- Appuyez sur **2** afin de définir l'environnement de développement pour l'environnement de conception.
- Appuyez sur **3** afin de définir l'environnement de test pour un traitement de gros volumes plus proche de celui d'un environnement de production.
- Appuyez sur **4** afin de définir l'environnement de production pour un traitement de gros volumes avec des niveaux élevés d'accès concurrentiel destinés aux utilisateurs finaux. Les environnements de production avancés sont généralement des configurations à plusieurs nœuds.

La valeur par défaut est **1** pour Sandbox.

13. Choisissez si vous souhaitez installer des packages d'intégration tiers avec le programme d'installation d'Informatica.

Remarque: Vous devez installer un package d'intégration si vous configurez les services Informatica pour effectuer les tâches suivantes :

- Transférez le traitement vers l'environnement Hadoop ou Databricks.
- Traitez des fichiers complexes dans le domaine Informatica.
- Connectez-vous à l'environnement Hadoop, mais effectuez un traitement dans le domaine Informatica.

Vous pouvez choisir d'installer les packages maintenant ou ultérieurement via Integration Package Manager.

- Appuyez sur **1** pour installer le domaine Informatica sans packages d'intégration.
- Appuyez sur **2** pour installer le domaine Informatica avec des packages d'intégration.

La valeur par défaut est **1**.

14. Si vous choisissez d'installer des packages d'intégration, sélectionnez-en un ou plusieurs que vous souhaitez installer dans la liste. Séparez plusieurs packages par une virgule.
La valeur par défaut est **1**.

Remarque: Les fichiers du programme d'installation des packages sélectionnés doivent être disponibles dans le répertoire : `<Informatica installer files>/source`

15. Appuyez sur **Entrée**.

16. Dans Récapitulatif de post-installation, vérifiez les informations d'installation et appuyez sur **Entrer** pour appliquer le HotFix.

Le programme d'installation copie les fichiers Informatica dans le répertoire d'installation.

17. Dans Récapitulatif de post-installation, vérifiez que l'application du HotFix est terminée et appuyez sur **Entrer** pour quitter le programme d'installation.

Appliquer le HotFix des services en mode silencieux

Pour appliquer le HotFix en mode silencieux, créez le fichier SilentInput.properties, puis exécutez le programme d'installation.

Informatica fournit un exemple de fichier de propriétés appelé SilentInput_hotFix.properties, qui inclut les paramètres requis par le programme d'installation.

Important: Vous ne pouvez pas revenir à la version précédente de MetaDex lorsque vous appliquez le HotFix.

1. Placez-vous dans le répertoire racine qui contient les fichiers d'installation.
2. Recherchez le fichier `SilentInput_HotFix.properties`.
3. Sauvegardez le fichier avant de le modifier.
4. Utilisez un éditeur de texte pour ouvrir le fichier et modifier les valeurs. Le tableau suivant décrit les propriétés de l'installation que vous pouvez modifier :

Nom de la propriété	Description
INSTALL_TYPE	Indique s'il faut appliquer ou restaurer le HotFix. Si la valeur est 0, le programme d'installation applique le Hotfix à l'installation Informatica actuelle. Si la valeur est 1, le programme d'installation restaure le HotFix actuel. Définissez la propriété sur 0 pour appliquer le HotFix.
USER_INSTALL_DIR	Répertoire de l'installation Informatica sur laquelle appliquer ou restaurer le HotFix. Pour appliquer le HotFix aux services Informatica, entrez le chemin d'accès absolu du répertoire dans lequel la version actuelle des services Informatica est installée.
ENABLE_USAGE_COLLECTION	Permet au logiciel de transmettre automatiquement certaines informations à Informatica (aux États-Unis) concernant l'environnement informatique et réseau dans lequel le Logiciel est déployé et les statistiques du système et d'utilisation des données du déploiement. Cette transmission est considérée comme faisant partie des Services selon la politique de confidentialité d'Informatica et Informatica utilisera et traitera par ailleurs ces informations conformément à la politique de confidentialité d'Informatica disponible sur https://www.informatica.com/in/privacy-policy.html . Il est possible de désactiver la collecte d'utilisation dans l'outil Administrator tool. Pour en savoir plus sur la désactivation de l'envoi de statistiques d'utilisation, consultez le <i>Guide d'Informatica Administrator</i> . Vous devez définir la valeur sur 1 pour appliquer le HotFix.

Nom de la propriété	Description
INSTALLATION_ENVIRONMENT	<p>Si vous appliquez le HotFix, spécifiez le type d'environnement associé à l'installation des services Informatica.</p> <ul style="list-style-type: none"> Appuyez sur 1 afin de définir l'environnement Sandbox pour un environnement de base utilisé comme preuve de concept avec un minimum d'utilisateurs. Appuyez sur 2 afin de définir l'environnement de développement pour l'environnement de conception. Appuyez sur 3 afin de définir l'environnement de test pour un traitement de gros volumes plus proche de celui d'un environnement de production. Appuyez sur 4 afin de définir l'environnement de production pour un traitement de gros volumes avec des niveaux élevés d'accès concurrentiel destinés aux utilisateurs finaux. Les environnements de production avancés sont généralement des configurations à plusieurs nœuds. <p>La valeur par défaut est 1 pour Sandbox.</p>
EDC_CATALOG_INST	Requis pour les installations d'Enterprise Data Catalog, de Data Privacy Management et d'Enterprise Data Preparation. Définissez la propriété sur true si le service de catalogue s'exécute sur le nœud sur lequel vous souhaitez appliquer le HotFix.
EDC_HF_BACKUP	Requis pour les installations d'Enterprise Data Catalog, de Data Privacy Management et d'Enterprise Data Preparation si vous avez défini EDC_CATALOG_INST=true. Définissez la propriété sur true si vous avez effectué une sauvegarde du catalogue.
EDC_BACK_UP_DIR	Requis pour les installations d'Enterprise Data Catalog, de Data Privacy Management et d'Enterprise Data Preparation si vous avez défini les propriétés EDC_CATALOG_INST et EDC_HF_BACKUP sur true. Entrez l'emplacement du fichier de sauvegarde des données du catalogue.
INSTALL_HADOOP_LIBRARIES	<p>Détermine s'il faut installer des packages pour intégrer le domaine à l'environnement Hadoop ou Databricks.</p> <p>Le domaine et le client Informatica nécessitent les packages d'intégration pour transférer le traitement vers Hadoop ou Databricks, pour traiter des fichiers complexes dans le domaine Informatica ou pour se connecter à Hadoop ou à Databricks lorsque vous les traitez dans le domaine Informatica.</p> <p>Si vous n'installez pas les packages d'intégration maintenant, vous pouvez le faire ultérieurement via Integration Package Manager.</p> <p>Définissez la valeur sur true si vous souhaitez installer les packages d'intégration.</p>
SELECTED_HADOOP_LIBRARIES	<p>Détermine les packages d'intégration que vous souhaitez installer à partir de la liste des packages pris en charge.</p> <p>Entrez les packages à installer. Séparez plusieurs packages par une virgule.</p> <p>Remarque: Les fichiers du programme d'installation des packages sélectionnés doivent être disponibles dans le répertoire : <code><Informatica installer files>/source</code></p>

- Enregistrez le fichier de propriétés sous le nom SilentInput.properties dans le même dossier.
- Accédez à la racine du répertoire du programme d'installation des services.
- Vérifiez que le répertoire contient le fichier SilentInput.properties que vous avez modifié et enregistré.
- Pour appliquer le HotFix, sur une ligne de commande shell, entrez la commande suivante pour exécuter le programme d'installation en mode : `./silentInstallHotFix.sh`.

Le programme d'installation copie les fichiers Informatica dans le répertoire d'installation.

9. Effectuez les tâches de post-installation. Pour vérifier que le HotFix est terminé, consultez le fichier journal ou la page **Récapitulatif de post-installation**.

Exemple de propriétés d'entrée en mode silencieux

L'exemple suivant montre le contenu du fichier `SilentInput.properties` lorsque vous appliquez ou restaurez le HotFix en mode silencieux.

```
#####
# Informatica Installer Build Details
# Copyright (c) 1993-2021 Informatica LLC
# This software contains confidential and proprietary
# information of Informatica LLC.
# All Rights Reserved.
#####

# Use the following guidelines when editing this file
# * Use this file to install without user interaction.
# * After you create the properties file, save the file with the name
SilentInput.properties
# * Any error condition that leads to failure, such as an invalid
# installation directory, generates a log file in the user home directory.
# For example: c:\silentErrorLog<time_stamp>.log

#####

# Set ENABLE_USAGE_COLLECTION to 1 to accept the product usage toolkit end user license
# agreement.
# You must set the value as 1 to install the Informatica platform.
# The product usage toolkit end user license agreement is available at: http://
www.informatica.com/us/eula/en-support-eula.aspx.
# As further described in the EULA, your use of the Informatica platform will enable the
# product usage toolkit
# to collect certain product usage and failure information. You may disable this feature
# at any time.
# For more information on how to disable this feature refer the Informatica
Administrator Guide.

ENABLE_USAGE_COLLECTION=0

## *INSTALL_TYPE - Set this value to '0' to apply the hotfix. Set this value to '1' to
roll back the hotfix.

INSTALL_TYPE=0

# * The USER_INSTALL_DIR variable must point to a valid directory with write
# permissions enabled.

USER_INSTALL_DIR=c:\Informatica\10.5

#The INSTALLATION_ENVIRONMENT property represents the installation environment
# Set the property to one of the following installation environment types: Sandbox,
Development, Test, or Production. Values are case-sensitive.
# Set to Sandbox for a basic environment used for proof of concept with minimal
users.
# Set to Development for the design environment.
# Set to Test for high volume processing that is closest to a production environment.
# Set to Production for high volume processing with high levels of concurrency meant for
end users. Advanced production environments are typically multi-node setups.

INSTALLATION_ENVIRONMENT=
```

```

# Required only for EDC installation.
# Set EDC_CATALOG_INST=true if the Catalog Service is running on the node on which you
want to apply or roll back the hotfix.EDC_CATALOG_INST=true

# Required only for EDC installation.
# Set EDC_HF_BACKUP=true if you have set EDC_CATALOG_INST=true and you have taken a
backup of the catalog.
# Run the infacmd ldm backupContents command before you apply the hotfix (INSTALL_TYPE=0)
# Run the infacmd ldm restoreContents command before you rollback the hotfix
(INSTALL_TYPE=1
EDC_HF_BACKUP=true

# Enter the location of the backup file.
# Required for Enterprise Data Catalog installation when the EDC_CATALOG_INST and
EDC_HF_BACKUP parameters are set to true
EDC_BACK_UP_DIR=/home/ilmsatsqe/CSBackup/export.zip

# The INSTALL_HADOOP_LIBRARIES property determines whether to install packages to
integrate the domain with Hadoop or Databricks.
# Set INSTALL_HADOOP_LIBRARIES=true if you want to install integration packages along
with Informatica domain services.
# Set INSTALL_HADOOP_LIBRARIES property only if INSTALL_TYPE=0
# If you don't install the integration packages now, you can install them later through
Integration Package Manager.
INSTALL_HADOOP_LIBRARIES=false

# The SELECTED_HADOOP_LIBRARIES property determines the integration packages that you
want to install.
# Lists the supported integration packages and their versions.
# Set SELECTED_HADOOP_LIBRARIES property only if INSTALL_TYPE=0
# Enter the integration package that you want to install. Separate multiple packages
with a comma.
# You can choose from the following options:
# 1->Azure HDInsight 4.0
# 2->Cloudera 6.3
# 3->Cloudera 7.1
# 4->Cloudera 7.2
# 5->Databricks 7.2
# 6->Databricks 9.1
# 7->Dataproc 2.0
# 8->Elastic MapReduce 5.29
# 9->Elastic MapReduce 6.0
# 10->Elastic MapReduce 6.4
# 11->MapR 6.1
# 12->Select all
SELECTED_HADOOP_LIBRARIES=3

```

Après l'application du HotFix

Après avoir exécuté le programme d'installation pour appliquer le HotFix, démarrez le domaine et effectuez les tâches post-requises pour terminer l'application du HotFix.

Activer et mettre à niveau les services d'application Informatica.

Les tâches postérieures à la mise à niveau pour effectuer l'application du HotFix impliquent le démarrage du domaine Informatica, l'activation des services d'application Informatica et la mise à niveau des services.

1. Exécutez la commande `./infaservice.sh startup` pour démarrer le domaine Informatica. Par défaut, `infaservice.sh` se trouve dans le répertoire suivant : `<Informatica installation directory>/tomcat/bin`
2. Activez les services d'application Informatica suivants dans l'outil Administrator tool :
 - a. Service de référentiel modèle

- b. Service d'intégration de données
 - c. Service de gestion de contenu
 - d. Service Analyst
 - e. Service de cluster Informatica
3. Activez le service de catalogue et mettez-le à niveau.

Remarque:

- Si vous avez activé l'analyse des actifs de données, le démarrage du service de catalogue prend plus de temps. Le service ne sera pas disponible avant la fin de la mise à niveau du référentiel d'analyse des actifs de données.
- Pour connaître l'état de la mise à niveau du référentiel de l'analyse des actifs de données, reportez-vous au fichier `daa_upgrade.log` à partir du répertoire d'installation.

La mise à niveau d'Enterprise Data Catalog 10.5.3 est terminée.

4. Mettre à niveau le service d'intégration de données.

Configurer les ressources Informatica Platform ou des ressources tierces

Si vous n'avez pas configuré des ressources Informatica Platform ou des ressources tierces, téléchargez les fichiers binaires du scanner et les pilotes de ressources depuis l'emplacement de téléchargement d'Akamai mentionné dans l'e-mail de confirmation.

Copiez les fichiers binaires du scanner dans le répertoire suivant : `<Informatica installation directory>/services/CatalogService/ScannerBinaries`

Remarque: Le fichier `ScannerBinaries.zip` comprend les fichiers binaires de ressources Informatica Platform pour la version 10.5.3 et le fichier `ExtendedScannerBinaries.zip` comprend les fichiers binaires de ressources Informatica Platform des versions précédentes.

Configurer les privilèges Sudo pour l'utilisateur de la passerelle (facultatif)

Si vous prévoyez de modifier les propriétés du service de cluster Informatica ou de remplacer les certificats SSL configurés pour le service de cluster Informatica, attribuez des privilèges sudo à l'utilisateur de la passerelle.

Les commandes suivantes nécessitent des privilèges sudo pour l'utilisateur de la passerelle lorsque vous activez le service de cluster Informatica pour la première fois :

- `mkdir`
- `chown`
- `chmod`
- `echo`
- `systemctl`
- `cp`
- `mv`
- `sysctl`
- `rm`
- `tee`
- `sed`
- `sshd`

Pour configurer les privilèges sudo pour les commandes, vous devez ajouter les commandes au fichier `/etc/sudoers`, comme illustré dans l'exemple suivant : `/bin/mkdir, /bin/chown, /bin/chmod, /bin/echo, /bin/systemctl, /bin/cp, /bin/mv, /usr/sbin/sysctl, /bin/rm, /usr/bin/tee, /usr/bin/sed, /usr/sbin/sshd`.

Remarque: Les commandes `tee` et `sed` ne nécessitent aucun privilège sudo dans les versions 10.5.1.1 et ultérieures.

Vous pouvez déterminer le répertoire où se trouve chaque commande à l'aide de la commande `which <command name>`.

Après avoir activé le service de cluster Informatica pour la première fois, vous pouvez choisir de désactiver la validation des autorisations sudo pour le service de cluster Informatica. Pour désactiver la validation, configurez la propriété personnalisée suivante pour le service de cluster Informatica :

`IcsCustomOptions.IcsGatewayUserSudoEnabled` et définissez la valeur sur `false`. Après la désactivation de la validation, les privilèges sudo ne sont pas requis lorsque vous redémarrez le service de cluster Informatica. Pour arrêter cependant le service de cluster Informatica, l'autorisation sudo est toujours requise pour la commande `systemctl`.

Pour exécuter la commande `infacmd ics cleanCluster` afin de nettoyer le service de cluster Informatica, l'autorisation sudo doit être configurée pour les commandes `systemctl` et `rm`.

Remarque: Les services associés au service de cluster Informatica, tels qu'Apache Solr, PostgreSQL et Nomad nécessitent un utilisateur non racine disposant de privilèges sudo pour exécuter les services. Sudo permet à un utilisateur d'exécuter des programmes ou des commandes avec des privilèges élevés pendant une période spécifique. Enterprise Data Catalog nécessite un utilisateur non-racine avec des autorisations sudo pour exécuter certaines commandes lors de l'exécution de tâches administratives telles que l'installation, la mise à niveau et la surveillance du statut des services. Pour plus d'informations sur les commandes utilisées et le rôle de chaque commande lors de la mise à niveau, reportez-vous à l'article de la base de connaissances [Enable sudo privileges for a non-root user in Enterprise Data Catalog](#).

Migrer les recommandations de termes d'entreprise

Pour migrer les recommandations de termes d'entreprise, exécutez la commande `infacmd ldm upgradePropagationStageFrom105` à partir du répertoire suivant : `<Informatica installation directory>/isp/bin`

Une fois la commande exécutée, les recommandations de Business Glossary s'affichent dans l'outil Enterprise Data Catalog. Pour plus d'informations sur la commande, reportez-vous à la *Référence des commandes d'Informatica*.

Restauration du HotFix des services

Vous pouvez restaurer le HotFix si nécessaire. Pour restaurer le HotFix, effectuez les tâches préalables requises, puis exécutez le programme d'installation.

Avant la restauration du HotFix

Avant de restaurer le HotFix, effectuez les tâches prérequis suivantes :

1. Sauvegardez les données du catalogue à l'aide de la commande `infacmd ldm backupContents`. Pour plus d'informations sur la commande, reportez-vous à la *Référence des commandes Informatica*.

2. Sauvegardez le référentiel modèle à l'aide de la commande `infacmd mrs BackupContents`. Pour plus d'informations sur la commande, reportez-vous à la *Référence des commandes Informatica*.
3. Désactivez les services d'applications Informatica suivants :
 - a. Service de catalogue
 - b. Service Analyst
 - c. Service de gestion de contenu
 - d. Service d'intégration de données
 - e. Service de référentiel modèle
 - f. Service de cluster Informatica
 - g. Service de messagerie électronique

Remarque: Pour désactiver un service, dans Informatica Administrator, sélectionnez-le, puis cliquez sur **Actions > Désactiver le service**.
4. Arrêtez le service de cluster Informatica à l'aide de la commande `infacmd ics shutdowncluster` ou à partir d'Informatica Administrator.
5. Nettoyez le service de cluster Informatica à l'aide de la commande `infacmd ics cleancluster`.
6. Pour le service de référentiel modèle associé au service de catalogue, vous devez supprimer le contenu du service.
7. Arrêtez le domaine Informatica à l'aide de la commande `infaservice shutdown`. La commande se trouve par défaut dans le répertoire suivant : `<Informatica installation directory>/tomcat/bin`.

Restaurer le HotFix des services en mode console

Vous pouvez restaurer le HotFix que vous avez appliqué. Pour restaurer le HotFix en mode console, exécutez le programme d'installation.

1. Exécutez le programme d'installation à l'aide de la commande `./install.sh`.
2. Appuyez sur **Y** pour confirmer que vous souhaitez procéder à l'installation.
3. Appuyez sur **5** pour restaurer le HotFix.
4. Appuyez sur **2** pour restaurer le HotFix.
5. Appuyez sur **2** pour accepter la licence.
6. Vérifiez les prérequis et appuyez sur **Entrée**.
7. Entrez le répertoire d'installation d'Informatica et appuyez sur **Entrée**.
8. Appuyez sur **2** pour confirmer que vous avez configuré le service de catalogue sur le nœud.

Remarque: Si vous confirmez que vous avez configuré le service de catalogue sur le nœud sur lequel vous prévoyez de restaurer le HotFix, vous devez valider la sauvegarde sur le nœud. Appuyez sur **1** pour ignorer la validation de la sauvegarde et passer à l'étape 11.

Vous devez ignorer la validation dans les scénarios suivants :

- Vous n'avez pas configuré le chemin du système de fichiers partagés du cluster pour le service de cluster Informatica sur une configuration à plusieurs nœuds.
- Vous avez configuré plusieurs nœuds pour le service de catalogue et vous ne souhaitez pas valider la sauvegarde sur chaque nœud.
- Vous avez activé le service de référentiel modèle et le service d'intégration de données, mais vous n'avez pas créé le service de catalogue et le service de cluster Informatica.

9. Appuyez sur **2** pour confirmer que vous aviez sauvegardé les données du catalogue à l'aide de la commande `infacmd ldm backupContents`.
10. Entrez l'emplacement du fichier de sauvegarde. Par exemple, `/data/Informatica/LDM_BACKUP1050SAML12.zip`.
Remarque: Si le magasin SEARCH n'est pas compris dans la sauvegarde, la validation échoue avec une erreur. Vous pouvez ignorer la validation de la sauvegarde si celle-ci ne comprend pas le magasin SEARCH.
11. Appuyez sur **Entrée** pour démarrer la restauration.
12. Dans Récapitulatif de pré-installation, appuyez sur **Entrer** pour continuer.
13. Appuyez sur **Entrer** pour quitter le programme d'installation à la fin de la restauration.

Restaurer le HotFix des services en mode silencieux

Pour restaurer le HotFix en mode silencieux, mettez à jour le fichier `SilentInput.properties`, puis exécutez le programme d'installation en mode silencieux.

Informatica fournit un exemple de fichier de propriétés, nommé `SilentInput_hotFix.properties`, qui contient les paramètres requis par le programme d'installation.

1. Placez-vous dans le répertoire racine qui contient les fichiers d'installation.
2. Recherchez le fichier `SilentInput_HotFix.properties`.
3. Sauvegardez le fichier avant de le modifier.
4. Utilisez un éditeur de texte pour ouvrir le fichier et modifier les valeurs. Le tableau suivant décrit les propriétés de l'installation que vous pouvez modifier :

Nom de la propriété	Description
INSTALL_TYPE	Indique s'il faut appliquer ou restaurer le HotFix. Définissez la valeur sur 1 pour restaurer le HotFix actuel.
USER_INSTALL_DIR	Répertoire de l'installation Informatica sur laquelle restaurer le HotFix. Répertoire de l'installation Informatica sur laquelle restaurer le HotFix.
ENABLE_USAGE_COLLECTION	Permet au logiciel de transmettre automatiquement certaines informations à Informatica (aux États-Unis) concernant l'environnement informatique et réseau dans lequel le Logiciel est déployé et les statistiques du système et d'utilisation des données du déploiement. Cette transmission est considérée comme faisant partie des Services selon la politique de confidentialité d'Informatica et Informatica utilisera et traitera par ailleurs ces informations conformément à la politique de confidentialité d'Informatica disponible sur https://www.informatica.com/in/privacy-policy.html . Il est possible de désactiver la collecte d'utilisation dans l'outil Administrator tool. Pour en savoir plus sur la désactivation de l'envoi de statistiques d'utilisation, consultez le <i>Guide d'Informatica Administrator</i> . Vous devez définir la valeur sur 1 pour restaurer le HotFix.
INSTALLATION_ENVIRONMENT	Vous pouvez ignorer la propriété lors de la restauration.

Nom de la propriété	Description
EDC_CATALOG_INST	Requis pour les installations d'Enterprise Data Catalog, de Data Privacy Management et d'Enterprise Data Preparation. Définissez la propriété sur true si le service de catalogue s'exécute sur le nœud sur lequel vous souhaitez appliquer le HotFix.
EDC_HF_BACKUP	Requis pour les installations d'Enterprise Data Catalog, de Data Privacy Management et d'Enterprise Data Preparation si vous avez défini EDC_CATALOG_INST=true. Définissez la propriété sur true si vous avez effectué une sauvegarde du catalogue.
EDC_BACK_UP_DIR	Requis pour les installations d'Enterprise Data Catalog, de Data Privacy Management et d'Enterprise Data Preparation si vous avez défini les propriétés EDC_CATALOG_INST et EDC_HF_BACKUP sur true. Entrez l'emplacement du fichier de sauvegarde des données du catalogue.

- Enregistrez le fichier de propriétés sous le nom SilentInput.properties.
- Accédez à la racine du répertoire du programme d'installation des services Informatica.
- Vérifiez que le répertoire contient le fichier SilentInput.properties que vous avez modifié et enregistré.
- Sur une ligne de commande shell, entrez la commande suivante pour exécuter le programme d'installation en mode silencieux :

```
./silentInstallHotFix.sh.
```

Le programme d'installation supprime le dernier HotFix et restaure la version précédente d'Informatica.

- Effectuez les tâches postérieures à la restauration. Pour vérifier que la restauration est terminée, consultez le fichier journal ou la page **Récapitulatif de post-installation**.

Après la restauration du HotFix

Après avoir exécuté le programme d'installation pour restaurer le HotFix, démarrez le domaine Informatica et effectuez les tâches post-requises pour terminer la restauration.

- Démarrez le domaine Informatica.
- Utilisez la commande `infacmd mrs deleteContents` pour supprimer le contenu du référentiel modèle pour la version 10.5.3.
- Activez le service de référentiel modèle.
- Utilisez la commande `infacmd mrs RestoreContents` pour restaurer le contenu du référentiel modèle.
- Activez le service d'intégration de données.
- Activez le service de gestion de contenu.
- Activez le service Analyst.
- Activez le service de messagerie électronique.
- Activez le service de cluster Informatica.
- Exécutez la commande `infacmd Idm restoreContents` pour restaurer les données du catalogue.
- À partir d'Informatica Administrator, supprimez les propriétés personnalisées que vous aviez configurées pour le service de catalogue après la mise à niveau vers la version 10.5.3.
- Activez le service de catalogue.

Remarque: Le programme d'installation conserve les propriétés de configuration de l'analyse des actifs de données sur la page du service de catalogue lorsque vous affichez celui-ci dans Informatica Administrator.

Application du HotFix client

Lorsque vous appliquez le HotFix, le programme d'installation sauvegarde les répertoires existants, applique la nouvelle version du client et restaure ou met à jour les fichiers de configuration et d'exécution requis.

Vous pouvez exécuter le programme d'installation du client pour appliquer un HotFix aux clients Informatica que vous utilisez.

Appliquer le HotFix client en mode graphique

Quand vous exécutez le programme d'installation en mode graphique, une fenêtre de console s'ouvre et s'exécute en arrière-plan. L'installation s'arrête si vous fermez cette fenêtre.

1. Connectez-vous à la machine à l'aide d'un compte d'utilisateur système. Le compte utilisateur doit être le même compte utilisé pour installer la version précédente des services Informatica.
2. Fermez toutes les autres applications.
3. Pour commencer l'installation, exécutez le fichier `install.bat` depuis le répertoire racine où vous avez décompressé ou désarchivé le package d'installation du HotFix client.
4. Sur la page Informatica 10.5.3, sélectionnez **Appliquer le HotFix à la version 10.5, 10.5.1 ou 10.5.2 ou restaurez le HotFix.**, puis cliquez sur **Démarrer**.

La page **Type d'installation** s'affiche.

5. Sélectionnez **Appliquer le HotFix** pour choisir d'appliquer le HotFix.
6. Vérifiez que toutes les exigences sont remplies avant de continuer le HotFix, puis cliquez sur **Suivant**.
La page **Répertoire d'installation** s'affiche.
7. Entrez le chemin d'accès absolu du répertoire dans lequel la version actuelle du client Informatica est installée et spécifiez l'environnement d'installation.

8. Cochez la case si vous souhaitez installer des packages d'intégration tiers avec le programme d'installation d'Informatica.

Remarque: Vous devez installer un module d'intégration pour traiter des fichiers complexes dans le domaine ou pour vous connecter à un environnement Hadoop ou Databricks, mais les traiter dans le domaine. Vous pouvez choisir d'installer les packages maintenant ou ultérieurement via Integration Package Manager.

9. Si vous choisissez d'installer des packages d'intégration, sélectionnez-en un ou plusieurs que vous souhaitez installer dans la liste.

Remarque: Les fichiers du programme d'installation des packages sélectionnés doivent être disponibles dans le répertoire : `<Informatica installer files>/source`

10. Cliquez sur **Suivant**.

La page **Récapitulatif de pré-installation** s'affiche.

11. Vérifiez les informations d'installation, puis cliquez sur **Installer** pour appliquer le HotFix.

Le programme d'installation copie les fichiers Informatica dans le répertoire d'installation.

12. Effectuez les tâches de post-installation. Pour vérifier que le HotFix est terminé, consultez le fichier journal ou la page **Récapitulatif de post-installation**.

Appliquer le HotFix client en mode silencieux

Pour appliquer le HotFix en mode silencieux, créez le fichier `SilentInput.properties`, puis exécutez le programme d'installation.

Informatica fournit un exemple de fichier de propriétés appelé `SilentInput_hotFix.properties` qui inclut les paramètres requis par le programme d'installation.

1. Accédez au répertoire racine qui contient les fichiers d'installation du client.
2. Recherchez le fichier `SilentInput_HotFix.properties`.
3. Sauvegardez le fichier avant de le modifier.
4. Utilisez un éditeur de texte pour ouvrir le fichier et modifier les valeurs. Le tableau suivant décrit les propriétés de l'installation que vous pouvez modifier :

Nom de la propriété	Description
INSTALL_TYPE	Indique s'il faut appliquer ou restaurer le HotFix. Si la valeur est 0, le programme d'installation applique le HotFix à l'installation du client Informatica actuelle. Si la valeur est 1, le programme d'installation restaure le HotFix actuel. Définissez la propriété sur 0 pour appliquer le HotFix.
USER_INSTALL_DIR	Répertoire de l'installation du client Informatica sur laquelle appliquer ou restaurer le HotFix. Pour appliquer le HotFix, entrez le chemin d'accès absolu du répertoire dans lequel la version actuelle des clients Informatica est installée.
INSTALL_HADOOP_LIBRARIES	Détermine s'il faut installer des packages pour intégrer le domaine à l'environnement Hadoop ou Databricks. Le domaine et le client Informatica nécessitent les packages d'intégration pour transférer le traitement vers Hadoop ou Databricks, pour traiter des fichiers complexes dans le domaine Informatica ou pour se connecter à Hadoop ou à Databricks lorsque vous les traitez dans le domaine Informatica. Si vous n'installez pas les packages d'intégration maintenant, vous pouvez le faire ultérieurement via Integration Package Manager. Définissez la valeur sur true si vous souhaitez installer les packages d'intégration.
SELECTED_HADOOP_LIBRARIES	Détermine les packages d'intégration que vous souhaitez installer à partir de la liste des packages pris en charge. Entrez les packages à installer. Séparez plusieurs packages par une virgule. Remarque: Les fichiers du programme d'installation des packages sélectionnés doivent être disponibles dans le répertoire : <code><Informatica installer files>/source</code>

5. Enregistrez le fichier de propriétés sous le nom `SilentInput.properties` dans le même dossier.
6. Double-cliquez sur `silentInstallHotFix.bat` pour appliquer le HotFix.
Le programme d'installation copie les fichiers clients Informatica dans le répertoire d'installation.
7. Effectuez les tâches de post-installation. Pour vérifier que le HotFix est terminé, consultez le fichier journal ou la page **Récapitulatif de post-installation**.

Exemple de propriétés d'entrée en mode silencieux

L'exemple suivant montre le contenu du fichier `SilentInput.properties` lorsque vous appliquez ou restaurez le client HotFix en mode silencieux.

```
#####
# Informatica Installer Build Details
# Copyright (c) 1993-2021 Informatica LLC
# This software contains confidential and proprietary
# information of Informatica LLC.
# All Rights Reserved.
#####

# Use the following guidelines when editing this file
# * Use this file to install without user interaction.
# * After you create the properties file, save the file with the name
SilentInput.properties
# * Any error condition that leads to failure, such as an invalid
# installation directory, generates a log file in the user home directory.
# For example: c:\silentErrorLog<time_stamp>.log

#####

#####
## *INSTALL_TYPE - Set this value to '0' to apply the hotfix. Set this value to '1' to
roll back the hotfix.

INSTALL_TYPE=0

# * The USER_INSTALL_DIR variable must point to a valid directory with write
# permissions enabled.

USER_INSTALL_DIR=c:\Informatica\10.5

#####
# After you create the properties file, save the file with the name
SilentInput.properties and
# run the silent installer to perform the Informatica client installation.
#####
```

Restauration du HotFix client

Vous pouvez restaurer le HotFix si nécessaire. Pour restaurer le HotFix, effectuez les tâches préalables requises, puis exécutez le programme d'installation.

Restauration du HotFix client en mode graphique

Quand vous exécutez le programme d'installation en mode graphique, une fenêtre de console s'ouvre et s'exécute en arrière-plan. La restauration s'arrête si vous fermez cette fenêtre.

1. Connectez-vous à la machine à l'aide d'un compte d'utilisateur système. Le compte utilisateur doit être le même compte utilisé pour installer la version précédente des services Informatica.
2. Fermez toutes les autres applications.
3. Pour commencer l'installation, exécutez le fichier `install.bat` depuis le répertoire racine où vous avez décompressé ou désarchivé le package d'installation du HotFix client.
4. Sur la page Informatica 10.5.3, sélectionnez **Appliquer le HotFix à la version 10.5, 10.5.1 ou 10.5.2 ou restaurez le HotFix.**, puis cliquez sur **Démarrer**.

La page **Type d'installation** s'affiche.

5. Sélectionnez **Restaurer le HotFix** pour choisir de restaurer le HotFix.
6. Vérifiez que toutes les exigences sont remplies avant de continuer la restauration, puis cliquez sur **Suivant**.

La page **Répertoire d'installation** s'affiche.

7. Entrez le chemin d'accès absolu pour le répertoire dans lequel la version actuelle des clients Informatica est installée, puis cliquez sur **Suivant**.

La page **Récapitulatif de pré-installation** s'affiche.

8. Vérifiez les informations d'installation, puis cliquez sur **Installer** pour restaurer le HotFix.

Le programme d'installation supprime le dernier HotFix et rétablit la version précédente des clients Informatica.

9. Effectuez les tâches de post-installation. Pour vérifier que la restauration est terminée, consultez le fichier journal ou la page **Récapitulatif de post-installation**.

Restauration du HotFix client en mode silencieux

Pour restaurer le HotFix en mode silencieux, créez le fichier `SilentInput.properties`, puis exécutez le programme d'installation avec le fichier.

Informatica fournit un exemple de fichier de propriétés appelé `SilentInput_hotFix.properties` qui inclut les paramètres requis par le programme d'installation.

1. Accédez au répertoire racine qui contient les fichiers d'installation du client.
2. Recherchez le fichier `SilentInput_HotFix.properties`.
3. Sauvegardez le fichier avant de le modifier.
4. Utilisez un éditeur de texte pour ouvrir le fichier et modifier les valeurs. Le tableau suivant décrit les propriétés de l'installation que vous pouvez modifier :

Nom de la propriété	Description
INSTALL_TYPE	Indique s'il faut appliquer ou restaurer le HotFix. Si la valeur est 0, le programme d'installation applique le HotFix à l'installation du client Informatica actuelle. Si la valeur est 1, le programme d'installation restaure le HotFix actuel. Définissez la valeur sur 1 pour restaurer le HotFix.
USER_INSTALL_DIR	Répertoire de l'installation du client Informatica sur laquelle restaurer le HotFix. Entrez le chemin d'accès absolu du répertoire dans lequel la version actuelle des clients Informatica est installée.

5. Enregistrez le fichier de propriétés sous le nom `SilentInput.properties` dans le même dossier.
6. Pour restaurer le HotFix sous Windows, double-cliquez sur `silentInstallHotFix.bat`.

Le programme d'installation supprime le dernier HotFix et restaure la version précédente des clients Informatica.

7. Effectuez les tâches de post-installation. Pour vérifier que la restauration est terminée, consultez le fichier journal ou la page **Récapitulatif de post-installation**.

CHAPITRE 3

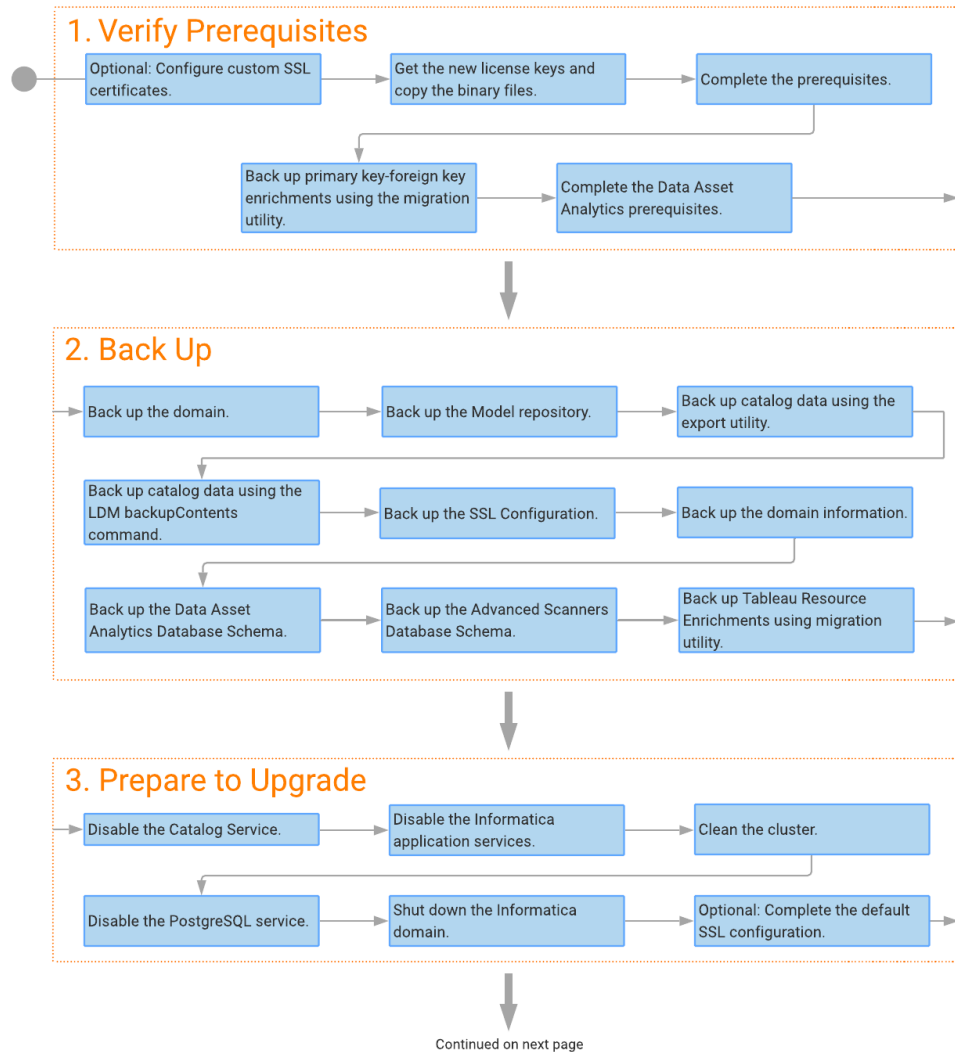
Mettre à niveau Enterprise Data Catalog dans un cluster interne

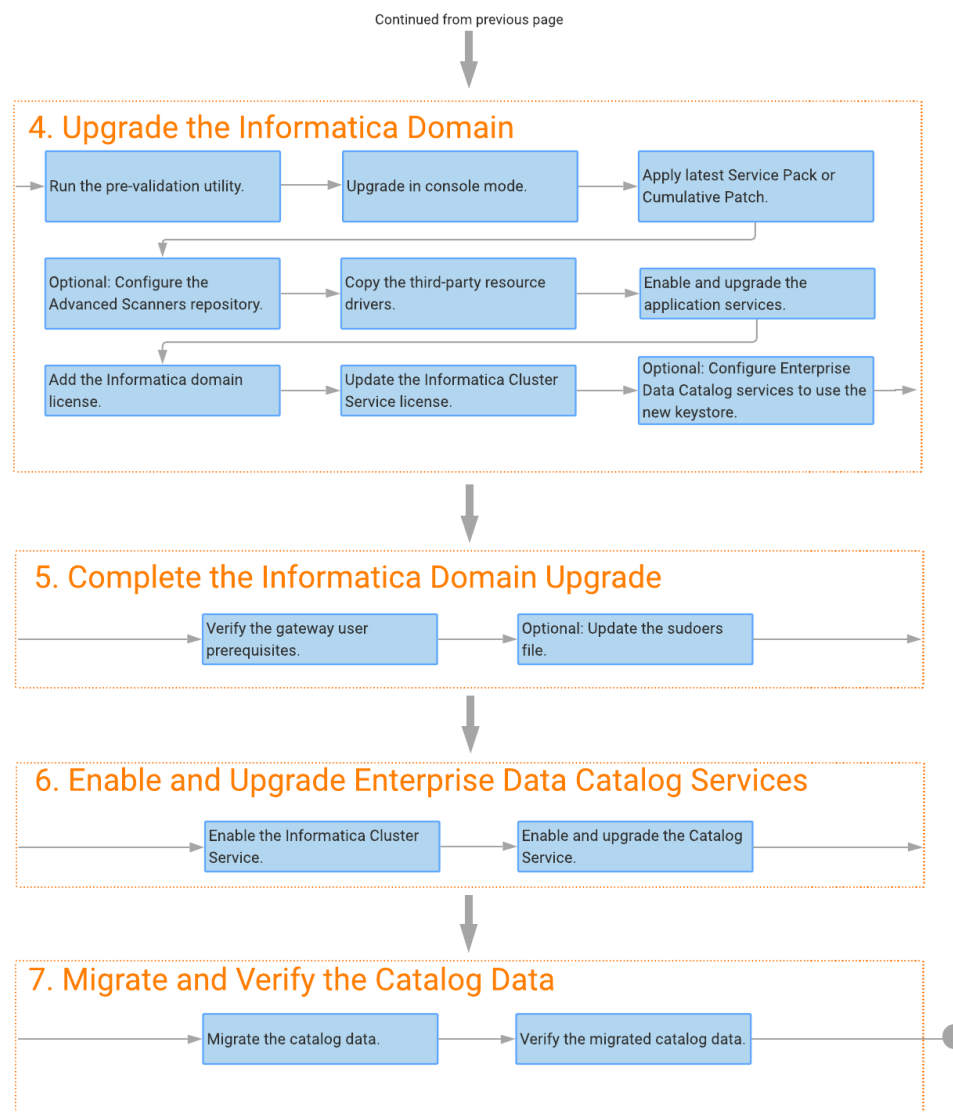
Ce chapitre comprend les rubriques suivantes :

- [Présentation de la mise à niveau d'Enterprise Data Catalog dans un cluster interne, 35](#)
- [Étape 1. Vérifier les prérequis de la mise à niveau, 36](#)
- [Étape 2. Sauvegarder les référentiels et les détails de configuration , 49](#)
- [Étape 3. Préparer la mise à niveau, 54](#)
- [Étape 4. Présentation de la mise à niveau du domaine, 57](#)
- [Étape 5. Effectuer la mise à niveau du domaine Informatica, 66](#)
- [Étape 6. Activer et mettre à niveau les services Enterprise Data Catalog, 68](#)
- [Étape 7. Migrer et vérifier les données du catalogue , 68](#)

Présentation de la mise à niveau d'Enterprise Data Catalog dans un cluster interne

L'image suivante montre les étapes que vous devez effectuer pour mettre à niveau Enterprise Data Catalog :





Étape 1. Vérifier les prérequis de la mise à niveau

Avant de démarrer la mise à niveau en tant qu'utilisateur non-racine avec des privilèges sudo, validez les prérequis suivants :

- Vérifiez qu'au moins 100 Go d'espace disque libre sont disponibles sur la machine sur laquelle le domaine Informatica s'exécute.
- Vérifiez que Java Development Kit (JDK) 1.8 est installé.
- Si le cluster est activé pour Kerberos et SSL, sauvegardez les fichiers truststore et keystore par défaut du domaine Informatica.
- Vérifiez si le référentiel de configuration de domaine est connecté lors de la mise à niveau.
- Vérifiez que ntpd est synchronisé entre le nœud de domaine Informatica et les nœuds de cluster.

- Installez les applications et les packages suivants sur tous les nœuds avant de mettre à niveau Enterprise Data Catalog :

- Bash Shell
- rsync
- libcurl
- xz-libs
- systemctl
- zip
- unzip
- tar
- wget
- scp
- rpm
- curl
- nslookup
- md5sum
- netstat
- ping
- ifconfig
- cksum
- dnsdomainname
- libncurses5
- OpenSSL version 1.0.1e-30.el6_6.5.x86_64 ou versions ultérieures.

OpenSSL 3.0 n'est pas pris en charge.

Vérifiez que la variable \$PATH pointe vers le répertoire `/usr/bin` pour utiliser la version correcte de Linux OpenSSL.

Dans les versions 10.5.1.0.1 et ultérieures, rsync est utilisé à la place de scp pour les transferts de fichiers.

Dans les versions 10.5.1.0.2 et ultérieures, le paramètre MaxStartups dans le fichier de configuration du serveur SSH est validé. Le nombre maximal de connexions SSH simultanées non authentifiées doit être défini sur une valeur supérieure ou égale à 30. Pour définir la valeur de ce paramètre sur 30, ouvrez le fichier `/etc/ssh/sshd_config`, passez la valeur du paramètre MaxStartups à 30:30:100, puis redémarrez le démon sshd.

Remarque: Les connexions SSH non authentifiées sont des connexions de socket au démon SSH qui sont établies sans authentification de l'utilisateur.

- Le tableau suivant répertorie les ports par défaut qui doivent être disponibles pour le service de cluster Informatica :

Service	Port par défaut
HTTP/HTTPS	9075
Serf Nomad	4648
HTTP Nomad	4646
RPC Nomad	4647
ZooKeeper	2181
Homologue ZooKeeper	2888
Leader ZooKeeper	3888
Solr	8983
MongoDB	27017
PostgreSQL	5432

- Si vous avez configuré le référentiel de MetaDex, sauvegardez la base de données du référentiel MetaDex.
- Remarque:** La mémoire par défaut du serveur MetaDex est de 4 Go.
- Supprimez les valeurs configurées pour les variables d'environnement suivantes à l'aide de la commande `unset` :
 - INFA_HOME
 - INFA_DOMAINS_FILE
 - DISPLAY
 - JRE_HOME
 - INFA_TRUSTSTORE
 - INFA_TRUSTSTORE_PASSWORD
- Vérifiez que les variables d'environnement `LD_LIBRARY_PATH` et `PATH` ne contiennent pas de versions précédentes d'Informatica.
- Supprimez le fichier JAR suivant des nœuds sur lesquels le service de catalogue s'exécute : `<Informatica Installation Directory>/logs/<NodeName> /services/CatalogService/<CatalogServiceName>/migrate/restore.jar`.
- À partir de la version 10.5, le framework de connectivité universelle (UCF, Universal Connectivity Framework) est déconseillé. Pour utiliser les ressources UCF que vous aviez configurées dans les versions antérieures, copiez les fichiers jar de l'UCF de l'emplacement d'installation existant vers le nouvel emplacement de mise à niveau : `<$INFA_HOME>/services/CatalogService/ScannerJars/bin`.

Remarque: Les fichiers JAR d'UCF comprennent le modèle du fichier `com.infa.ldm.extended.*.jar`.

Après avoir mis à niveau le service de catalogue, les ressources UCF existantes sont répertoriées dans la boîte de dialogue **Sélectionner le type de ressource** de Catalog Administrator.

Remarque: Conservez un enregistrement du nombre d'actifs du catalogue, de Catalog Administrator et du tableau de bord de l'analyse des actifs de données pour référence. Vous pouvez utiliser l'API REST `/data/`

search pour afficher le nombre d'actifs au format JSON, comme indiqué dans l'exemple suivant : `http://<CatalogAdmin>:<port>/access/2/catalog/data/search?defaultFacets=false&disableSemanticSearch=true&enableLegacySearch=false&facet=true&facetId=core.classType&facetId=core.resourceName&facetId=core.resourceType&highlight=false&includeRefObjects=false&offset=0&pageSize=1&q=* &tabId=all`.

Pour plus d'informations, reportez-vous à la [Référence des API REST d'Enterprise Data Catalog](#).

Si vous utilisez Axon Data Governance avec Enterprise Data Catalog, assurez-vous qu'Axon SuperAdmin a désactivé le travail d'intégration des actifs et le travail de récupération des liens de référence avant la mise à niveau. Pour plus d'informations, reportez-vous à l'[Informatica Knowledge Base article](#).

Configurer les certificats SSL personnalisésPrésentation

Lors d'une installation ou d'une mise à niveau, vous pouvez utiliser les certificats SSL de votre choix, appelés certificats SSL personnalisés, pour sécuriser les composants associés au service de cluster Informatica. Vous pouvez choisir d'utiliser des certificats SSL personnalisés signés par une autorité de certification ou des certificats SSL personnalisés auto-signés comme certificats de client et de cluster.

Si vous choisissez d'utiliser des certificats SSL personnalisés signés par une autorité de certification, utilisez les scripts `generate_csr.sh` et `generate_certs.sh` pour générer les certificats requis.

Si vous choisissez d'utiliser des certificats SSL personnalisés auto-signés, utilisez l'utilitaire SSL personnalisé fourni avec le programme d'installation pour générer les certificats requis.

Exigences d'activation des certificats SSL personnalisés

Avant d'activer SSL personnalisé pour Enterprise Data Catalog, sécurisez le domaine Informatica à l'aide de certificats SSL personnalisés.

Vérifiez les prérequis suivants pour le domaine Informatica :

- Les fichiers `truststore` et `keystore` personnalisés sont placés dans un répertoire personnalisé. Le nom du fichier `truststore` doit être `infa_truststore.jks`.
- Le répertoire qui stocke les fichiers `keystore` et `truststore` est accessible aux programmes de ligne de commande.

Important: Le programme d'installation place les fichiers par défaut `infa_truststore.jks` et `keystore` dans le répertoire `<Informatica installation directory>/services/shared/security` sur chaque nœud. Ne remplacez pas les fichiers `truststore` et `keystore` par défaut, ne les supprimez pas, ni ne les déplacez. Ne placez pas les fichiers `truststore` et `keystore` personnalisés dans le répertoire.

Pour savoir comment convertir un domaine Informatica non-SSL en un domaine Informatica compatible SSL, reportez-vous à l'article de la base de connaissances

[Convert a non-SSL Informatica domain to an SSL-enabled Informatica domain](#).

Générer des certificats SSL personnalisés signés par une autorité de certification (CA)

Vous disposez d'un certificat SSL personnalisé pour le domaine Informatica, et vous souhaitez utiliser les certificats SSL signés par l'autorité de certification en tant que certificats clients et de cluster pour le service de cluster Informatica.

Utilisez les scripts `generate_csr.sh` et `generate_certs.sh` pour générer la demande de signature de certificat (CSR, Certificate Signing Request) à envoyer à une autorité de certification (CA) et générer les certificats SSL requis. Vous pouvez télécharger les scripts à partir d'Akamai Download Manager.

Effectuez les étapes suivantes pour utiliser les scripts afin de générer les certificats :

1. Extrayez les scripts `generate_csr.sh` et `generate_certs.sh` de l'emplacement suivant : `<Location of installer files>/properties/utils/CustomSSLScriptsUtil_ExternalCA`.
2. Définissez la variable d'environnement `JAVA_HOME` pour qu'elle pointe vers JDK 8.
3. Dans le fichier `gen_csr.properties`, indiquez les valeurs des paramètres suivants :

Paramètre	Description
<code>Infadomainkeystorepassword</code>	Mot de passe du keystore de domaine Informatica en texte brut.
<code>ServerHosts</code>	Hôtes du service de cluster Informatica qui incluent les nœuds de données, les nœuds de traitement et le nœud de passerelle. Entrez une liste de noms de domaine complets (FQDN) séparée par des virgules de nœuds de cluster.
<code>ClientHosts</code>	Liste des noms d'hôtes uniques séparée par des virgules des nœuds de domaine et des nœuds de cluster.
<code>Infadomainname</code>	Nom de domaine Informatica.
<code>ICSServiceName</code>	Nom du service de cluster Informatica.
<code>KeysOutputDir</code>	Répertoire de stockage des clés générées. Spécifiez le répertoire <code>\$CUSTOM KEYSTORE LOC</code> pour éviter les étapes supplémentaires de copie des clés générées. Les répertoires <code>\$ICS SERVICENAME/client_certs</code> et <code>\$ICS SERVICENAME/cluster_certs</code> sont créés sous le répertoire <code>\$CUSTOM KEYSTORE LOC</code> . <code>\$CUSTOM KEYSTORE LOC</code> est le répertoire où se trouve le keystore personnalisé pour le domaine Informatica (<code>infa_keystore.jks</code>). <code>\$ICS SERVICENAME</code> est le nom du service de cluster Informatica.
<code>CertsOutputDir</code>	Répertoire <code>\$CUSTOM TRUSTSTORE LOC</code> de stockage des fichiers truststore générés. Les répertoires <code>\$ICS SERVICENAME/client_certs</code> et <code>\$ICS SERVICENAME/cluster_certs</code> sont créés sous le répertoire <code>\$CUSTOM TRUSTSTORE LOC</code> . <code>\$CUSTOM TRUSTSTORE LOC</code> est le répertoire dans lequel se trouve le truststore personnalisé pour le domaine Informatica (<code>infa_truststore.jks</code>).
<code>DNSDomainName</code>	Nom de domaine DNS pour les nœuds de cluster.
<code>ClusterCert_OrganizationUnit</code>	Facultatif. Valeur du paramètre <code>OrganizationUnit</code> pour le certificat des nœuds de cluster.
<code>ClusterCert_Organization</code>	Valeur du paramètre <code>Organisation</code> pour le certificat des nœuds de cluster. Remarque: Vérifiez que la combinaison des paramètres <code>Organisation (O)</code> et <code>Unité d'organisation (OU)</code> dans l'objet du certificat est distincte pour les certificats clients et de cluster
<code>ClusterCert_Location</code>	Valeur du paramètre <code>Emplacement</code> pour le certificat des nœuds de cluster.
<code>ClusterCert_State</code>	Valeur du paramètre <code>État</code> pour le certificat des nœuds de cluster.
<code>ClusterCert_CountryCode</code>	Valeur du paramètre <code>Code de pays</code> pour le certificat des nœuds de cluster.

Paramètre	Description
DomainCert_OrganizationUnit	Facultatif. Valeur du paramètre Unité d'organisation pour le certificat des nœuds de domaine.
DomainCert_Organization	Valeur du paramètre Organisation pour le certificat des nœuds de domaine. Remarque: Vérifiez que la combinaison des paramètres Organisation (O) et Unité d'organisation (OU) dans l'objet du certificat est distincte pour les certificats clients et de cluster
DomainCert_Location	Facultatif. Valeur du paramètre Emplacement pour le certificat des nœuds de domaine. La valeur par défaut est le paramètre ClusterCert_Location.
DomainCert_State	Facultatif. Valeur du paramètre État pour le certificat des nœuds de domaine. La valeur par défaut est le paramètre ClusterCert_State.
DomainCert_CountryCode	Facultatif. Valeur du paramètre Code de pays pour le certificat des nœuds de domaine. La valeur par défaut est le paramètre ClusterCert_CountryCode.
Custom_Server_Certificate_CN	Facultatif. Valeur du paramètre Nom commun dans le certificat des nœuds de cluster qui peut être utilisée à la place de l'élément \$InfaDomainName-\$ICSServiceName par défaut. Valeur \$DNSDomainName. Remarque: Vous devez entrer des valeurs conformes à RFC2253. Les caractères spéciaux suivants ne sont pas pris en charge : , + " \ < > ;. Les guillemets (") doivent être utilisés par paires. Les caractères \ et " ne doivent pas être utilisés conjointement. La valeur ne peut contenir aucun espace.
Custom_Client_Certificate_CN	Facultatif. Valeur du paramètre Nom commun dans le certificat des nœuds de domaine qui peut être utilisée à la place de l'élément \$InfaDomainName-\$ICSServiceName par défaut. Valeur \$DNSDomainName. La valeur par défaut est le paramètre Custom_Server_Certificate_CN. Remarque: Vous devez entrer des valeurs conformes à RFC2253. Les caractères spéciaux suivants ne sont pas pris en charge : , + " \ < > ;. Les guillemets (") doivent être utilisés par paires. Les caractères \ et " ne doivent pas être utilisés conjointement. La valeur ne peut contenir aucun espace.

Remarque: Si les valeurs contiennent des espaces ou des caractères spéciaux, vous devez placer les valeurs entre guillemets doubles.

- Exécutez le script `generate_csr.sh` à l'aide de la commande suivante pour générer les fichiers `.csr` à envoyer à une autorité de certification (CA) externe : `./generate_csr.sh gen_csr.properties`
Les fichiers suivants sont générés pour le cluster :

```
infa_nodecert.csr
infa_privkey.key
infa_privkey.pem
keystore.jks
```

Les fichiers suivants sont générés pour le client :

```
infa_nodecert.csr
infa_privkey.key
infa_privkey.pem
```

```

keystore.jks
browser_cert.csr
browser_keystore.jks
browser_privkey.key
browser_privkey.pem

```

5. Validez le contenu des fichiers .csr. Exécutez la commande suivante pour afficher le contenu : `keytool -printcertreq -file $PATH TO CSR`

6. Envoyez les fichiers .csr suivants à une autorité de certification (CA) à des fins de signature :

- `<CertsOutputDir>/<ICSServiceName>/client_certs/infa_nodecert.csr`
- `<CertsOutputDir>/<ICSServiceName>/cluster_certs/infa_nodecert.csr`
- `<CertsOutputDir>/<ICSServiceName>/client_certs/browser_cert.csr`

Remarque: Le fichier browser_cert.csr est requis si vous souhaitez créer les certificats de navigateur pour afficher les journaux du travail d'analyse sur Nomad.

7. Après avoir reçu les certificats ou les chaînes de certificats de l'autorité de certification (CA) au format .pem, "[Valider les certificats signés par une autorité de certification \(CA\)](#)" à la page 43 et stockez-les dans un emplacement sous le répertoire \$INFA_HOME sur votre machine.

Remarque: Si vous recevez les certificats ou les chaînes de certificats de l'autorité de certification (CA) au format .cer, exécutez la commande suivante pour convertir les fichiers au format pem : `openssl x509 -inform der -in <certificate file name>.cer -outform pem -out <certificate file name>.pem`.

Si vous recevez une chaîne de certificats de l'autorité de certification (CA), vous devez extraire le certificat racine, les certificats intermédiaires et le certificat d'utilisateur final.

8. Dans le fichier gen_csr.properties, indiquez les valeurs des paramètres suivants :

Paramètre	Description
InfaDomainKeystorePassword	Mot de passe du keystore de domaine Informatica en texte brut.
InfaDomainTruststorePassword	Mot de passe du truststore de domaine Informatica en texte brut.
ClusterCertificate	Chemin d'accès au certificat de cluster signé par l'autorité de certification (CA) au format .pem. Il s'agit d'un certificat d'utilisateur final.
ClientCertificate	Chemin d'accès au certificat client signé par l'autorité de certification (CA) au format .pem. Il s'agit d'un certificat d'utilisateur final.
BrowserCertificate	Chemin d'accès au certificat de navigateur signé par l'autorité de certification (CA) au format .pem.
ICSServiceName	Nom du service de cluster Informatica.
IsCACertificateChainAvailable	Spécifiez si la chaîne de certificats de l'autorité de certification (CA) est disponible sous forme de fichier .pem unique. Entrez true ou false. Remarque: La chaîne de certificats doit contenir uniquement les certificats racine et intermédiaires.

Paramètre	Description
SingleCACertificateChain	Chemin d'accès à la chaîne de certificats de l'autorité de certification (CA) au format .pem.
IndividualCertificatesFromCACHain	Facultatif. Uniquement nécessaire si le paramètre IsCACertificateChainAvailable est défini sur false. Chemins séparés par des virgules vers les certificats publics dans la chaîne de certificats de l'autorité de certification (CA) au format .pem si la chaîne de certificats CA complète est disponible sous forme de fichiers .pem individuels.
KeysOutputDir	Répertoire \$CUSTOM KEYSTORE LOC de stockage des clés générés. Les répertoires \$ICS SERVICENAME/client_certs et \$ICS SERVICENAME/cluster_certs sont créés sous le répertoire \$CUSTOM KEYSTORE LOC. \$CUSTOM KEYSTORE LOC est le répertoire où se trouve le keystore personnalisé pour le domaine Informatica (infa_keystore.jks). \$ICS SERVICENAME est le nom du service de cluster Informatica
CertsOutputDir	Répertoire \$CUSTOM TRUSTSTORE LOC de stockage des fichiers truststore générés. Les répertoires \$ICS SERVICENAME/client_certs et \$ICS SERVICENAME/cluster_certs sont créés sous le répertoire \$CUSTOM TRUSTSTORE LOC. \$CUSTOM TRUSTSTORE LOC est le répertoire dans lequel se trouve le truststore personnalisé pour le domaine Informatica (infa_truststore.jks).

9. Exécutez le script generate_certs.sh à l'aide de la commande suivante pour générer les certificats : `./generate_certs.sh gen_certs.properties`
Le keystore keystore.jks et les clés privées infa_privkey.pem sont stockés dans les répertoires \$CUSTOM KEYSTORE LOC/\$ICSServiceName/client_certs et \$CUSTOM KEYSTORE LOC/\$ICSServiceName/cluster_certs.
Le truststore truststore.jks truststore et les clés publiques infa_nodecert.pem, infa_nodecertkey.pem et infa_pubcert.pem sont stockés dans les répertoires \$CUSTOM TRUSTSTORE LOC/\$ICSServiceName/client_certs et \$CUSTOM TRUSTSTORE LOC/\$ICSServiceName/cluster_certs.
10. Facultatif. Les répertoires \$CUSTOM KEYSTORE LOC et \$CUSTOM TRUSTSTORE LOC sont généralement les mêmes. Si l'emplacement <KeysOutputDir> est différent de \$CUSTOM KEYSTORE LOC et que l'emplacement <CertsOutputDir> est différent de \$CUSTOM TRUSTSTORE LOC, déplacez les clés et les certificats vers les répertoires correspondants.
Remarque: Vérifiez que les répertoires \$CUSTOM KEYSTORE LOC et \$CUSTOM TRUSTSTORE LOC disposent des privilèges d'utilisateur requis. Vérifiez également que l'utilisateur dispose des autorisations chmod 700 minimales configurées pour les répertoires et des autorisations chmod 600 configurées pour les fichiers copiés dans les répertoires.

Pour accéder à l'interface utilisateur (IU) Web Nomad et à l'IU d'administration Solr lorsque le service de cluster Informatica est activé pour SSL, vous devez importer les certificats du navigateur. Pour en savoir plus sur l'importation des certificats de navigateur, reportez-vous à l'article de la base de connaissances [Access Nomad Web UI and Solr Admin UI when Informatica Cluster Service is SSL enabled in Enterprise Data Catalog](#).

Valider les certificats signés par une autorité de certification (CA)

Vous devez utiliser une seule autorité de certification (CA) pour les certificats clients et de cluster. Après avoir reçu les certificats signés de l'autorité de certification (CA), vous devez vérifier que chaque certificat est un certificat X.509 au format .pem.

Exécutez la commande suivante pour afficher le contenu des certificats clients et de cluster signés : `keytool -printcert -file $PATH TO CERTIFICATE PEM FILE.`

Validez les conditions requises suivantes pour les certificats clients et de cluster :

Prérequis	Configuration requise du certificat
Champs obligatoires	<p>Pour le certificat de cluster, tenez compte de la configuration requise de l'utilisation de clé suivante :</p> <p><code>keyUsage = digitalSignature,keyEncipherment</code> <code>extendedKeyUsage = serverAuth,clientAuth</code></p> <p>Pour le certificat client, tenez compte de la configuration requise de l'utilisation de clé suivante :</p> <p><code>keyUsage = digitalSignature</code> <code>extendedKeyUsage = clientAuth</code></p>
Autre nom du sujet (SAN, Subject Alternate Name)	<p>Pour le certificat de cluster, le SAN doit comprendre la liste des nœuds de cluster au format suivant : <code>SAN=DNS:\$CLUSTER HOST1 FQDN,DNS:\$CLUSTER HOST2 FQDN,DNS:\$CLUSTER HOST3 FQDN</code></p> <p>Le certificat client doit contenir les noms de domaine complets (FQDN) pour les nœuds de cluster.</p> <p>Pour le certificat client, le SAN doit comprendre la liste de tous les nœuds Informatica au format suivant : <code>SAN=DNS:\$INFA DOMAIN HOST1 FQDN,DNS:\$INFA DOMAIN HOST2 FQDN</code></p> <p>Le certificat client doit contenir les noms de domaine complets (FQDN) pour les nœuds de domaine et de cluster.</p>

CLUSTER HOST FQDN représente le nom de domaine complet pour l'hôte de passerelle de cluster, les nœuds de traitement et les nœuds de données dans le cluster.

INFA DOMAIN HOST FQDN représente le nom de domaine complet de l'hôte de passerelle de domaine Informatica, des nœuds de domaine, de l'hôte de passerelle de cluster, des nœuds de traitement et des nœuds de données dans le cluster.

Remarque: Vérifiez que l'emplacement du certificat personnalisé pour les nœuds de domaine contient le fichier `infa_truststore.pem`. Vérifiez également que tous les certificats de la chaîne de certificats d'autorité de certification (CA) sont présents dans les fichiers `truststore.jks` et `infa_pubcert.pem`.

Générer des certificats SSL personnalisés auto-signés

Vous disposez d'un certificat SSL personnalisé pour le domaine Informatica, et vous souhaitez utiliser les certificats SSL personnalisés auto-signés en tant que certificats clients et de cluster pour le service de cluster Informatica.

Utilisez l'utilitaire SSL personnalisé fourni avec le programme d'installation pour générer les certificats SSL requis.

Effectuez les étapes suivantes pour utiliser l'utilitaire SSL personnalisé afin de générer les certificats :

1. Extrayez `GenerateCustomSslUtility.zip` de l'emplacement suivant : `<Location of installer files>/properties/Utils/CustomSslCertsUtility/`.
2. Définissez la variable d'environnement `JAVA_HOME` pour qu'elle pointe vers JDK 8.

3. Configurez les paramètres suivants dans le fichier `input.properties` que vous avez extrait du fichier `GenerateCustomSslUtility.zip` :

Paramètre	Description
KeystoreFile	Chemin d'accès au fichier keystore personnalisé avec le nom du fichier. Le type de keystore doit être au format JKS. Format X509. Le fichier doit contenir une seule entrée de clé privée avec la chaîne de certificats complète. Vérifiez que le fichier dispose de la capacité de signature.
-KeystorePassword	Mot de passe du fichier keystore personnalisé au format texte brut.
TruststoreFile	Chemin d'accès au fichier truststore personnalisé avec le nom du fichier. Le type de truststore doit être au format JKS. Format X509. Le fichier doit contenir les certificats publics correspondant à l'entrée de clé privée dans le fichier keystore.
TruststorePassword	Mot de passe du fichier truststore personnalisé au format texte brut.
ISPDomainKeystorePassword	Mot de passe du keystore du domaine Informatica au format texte brut. L'utilitaire utilise le mot de passe du cluster et le fichier keystore.jks du client.
ISPDomainTruststorePassword	Mot de passe du truststore du domaine Informatica au format texte brut. L'utilitaire utilise le mot de passe du cluster et le fichier truststore.jks du client.
KeystoreOutputDir	Représente l'emplacement du keystore personnalisé du domaine Informatica que vous avez fourni lors de l'installation d'Enterprise Data Catalog.
TruststoreOutputDir	Représente l'emplacement du truststore personnalisé du domaine Informatica que vous avez fourni lors de l'installation d'Enterprise Data Catalog. Remarque: Vérifiez que les paramètres KeystoreOutputDir et TruststoreOutputDir pointent vers le même répertoire.
ServerNodes	Liste des noms de domaine complets séparée par des virgules des nœuds à configurer en tant que nœuds de données, nœuds de traitement, hôtes de service et nœud de passerelle lors de la configuration du service de cluster Informatica.
IcsServiceName	Nom du service de cluster Informatica.
ClientNodes	Liste des noms de domaine complets séparée par des virgules des nœuds à configurer en tant qu'hôtes de domaine Informatica, nœuds de données, nœuds de traitement, hôtes de service et nœud de passerelle.
IspDomainName	Nom de domaine Informatica.
ClusterNodeDNSDomain	Nom de domaine de l'hôte de passerelle à configurer pour le service de cluster Informatica.

4. Exécutez l'utilitaire à l'aide de la commande suivante : `java -jar GenerateCustomSslUtility.jar -in input.properties`. L'utilitaire génère les clés et les certificats clients et de cluster suivants :

- Clés :
 - keystore.jks

- infa_privkey.pem

Remarque: Les clés de cluster sont générées dans le répertoire suivant : <Keystore output directory>/<IcsServiceName>/cluster_certs. Les clés de client sont générées dans le répertoire suivant : <Keystore output directory>/<IcsServiceName>/client_certs

- Certificats :

- truststore.jks
- infa_pubcert.pem
- infa_nodecert.pem
- infa_nodecertkey.pem

Remarque: Les certificats de cluster sont générés dans le répertoire suivant : <Truststore output directory>/<IcsServiceName>/cluster_certs. Les certificats clients sont générés dans le répertoire suivant : <Truststore output directory>/<IcsServiceName>/client_certs

5. Copier les certificats générés dans les dossiers requis.
6. Attribuez la propriété des répertoires suivants à l'utilisateur du domaine Informatica :
 - <Keystore output directory>/<IcsServiceName>/cluster_certs
 - <Truststore output directory>/<IcsServiceName>/cluster_certs
 - <Keystore output directory>/<IcsServiceName>/client_certs
 - <Truststore output directory>/<IcsServiceName>/client_certs

Remarque: Vérifiez que tous les certificats clients sont inclus dans un seul répertoire. Vérifiez également que tous les certificats de cluster sont inclus dans un seul répertoire. Vous devez également vérifier que les répertoires disposent de l'autorisation `chmod 700` et que l'autorisation `chmod 600` est configurée dans les fichiers sous les répertoires.

Vérifier la somme de contrôle du package d'installation sur

Avant d'exécuter le programme d'installation des services, vérifiez l'intégrité du package d'installation via la commande `cksum`. La commande `cksum` calcule la valeur de la somme de contrôle pour les programmes d'installation.

Vérifiez la somme de contrôle des fichiers du programme d'installation spécifiques par rapport à celle des fichiers d'installation téléchargés depuis Akamai.

Le tableau suivant répertorie la somme de contrôle et la taille de fichier des services Informatica pour UNIX :

Fichier	Valeur de la somme de contrôle	Taille du fichier
informatica_1053_server_linux-x64.tar	2154528627	11639828480

Une incompatibilité de somme de contrôle peut se produire en cas d'erreurs de données pendant le téléchargement en raison de problèmes de réseau ou en cas de corruption des données dans le fichier sur le disque. Pour plus d'informations sur les propriétés de la somme de contrôle, reportez-vous à la section [HOW TO: Identify file errors after downloading Informatica installation files](#).

Obtenir les clés de licence et copier les fichiers binaires

Avant de démarrer la mise à niveau, procédez comme suit :

- Obtenez les nouvelles clés de licence pour le domaine Informatica et le service de cluster Informatica.

- Copiez les fichiers binaires du programme d'installation à partir de l'emplacement de téléchargement d'Akamai mentionné dans l'e-mail de confirmation et extrayez les fichiers dans un répertoire de la machine sur laquelle vous prévoyez de mettre à niveau Enterprise Data Catalog. Vous devez disposer des autorisations de lecture et d'écriture sur le répertoire des fichiers du programme d'installation et des autorisations d'exécution sur le fichier exécutable.
- Copiez les fichiers binaires du scanner à partir de l'emplacement de téléchargement d'Akamai et placez-les dans le répertoire suivant : `<Location where you extracted the installer binary files>/source`

Effectuer les tâches prérequis

Effectuez les prérequis suivants avant de mettre à niveau le domaine Informatica :

- Effacez les valeurs configurées des variables d'environnement `INFA_TRUSTSTORE` et `INFA_TRUSTSTORE_PASSWORD` si le domaine est activé pour SSL (Secure Sockets Layer).
- Téléchargez et installez la bibliothèque `libidn.so.11` si vous utilisez RHEL 8.3.

Sauvegarder les enrichissements de clé primaire-clé étrangère à l'aide de l'utilitaire de migration

Pour utiliser les améliorations ajoutées aux enrichissements de clé primaire-clé étrangère dans Enterprise Data Catalog, sauvegardez les enrichissements à l'aide de l'utilitaire de migration avant d'effectuer une mise à niveau vers Enterprise Data Catalog version 10.5.3.

Effectuez les étapes suivantes pour exécuter l'utilitaire :

1. Depuis Akamai Download Manager, téléchargez et extrayez le fichier `Informatica_1053_PkFkEnrichmentMigrationUtility.zip` sur la machine du domaine.
2. Exécutez la commande suivante :


```
java -jar PKFkEnrichmentsRestoreUtility.jar export <Catalog Service hostname>
<Catalog Service admin port number> <username> <password> <location to download
enrichments json> <comma separated resource type IDs> <SSL Enabled true false>
```

Remarque : Vérifiez que la longueur du nom de la ressource ne dépasse pas la longueur maximale du nom de fichier prise en charge par le système d'exploitation.

Remplir les prérequis de l'analyse des actifs de données

Si vous avez configuré l'analyse des actifs de données pour Enterprise Data Catalog, vous devez configurer le délai d'expiration de l'arrêt du processus avant d'arrêter le domaine Informatica pour une mise à niveau. Vous devez exécuter l'utilitaire d'analyse des actifs de données avant d'effectuer une mise à niveau vers Enterprise Data Catalog 10.5.3.

Configurer le délai d'expiration du processus

1. Dans l'outil Administrator tool, accédez à la section des propriétés personnalisées du domaine.
2. Ajoutez la propriété personnalisée suivante : `ProcessTerminationTimeout=900`
3. Arrêtez les services Informatica à l'aide de la commande `infaservice.sh shutdown`.
4. Démarrez les services Informatica à l'aide de la commande `infaservice.sh startup`.

Vérifiez que la taille de fichier de la transaction ou des fichiers journaux de rétablissement pour la base de données du référentiel de l'analyse des actifs de données est suffisamment grande. Pour une base de données Oracle, assurez-vous que la base de données contient au moins trois fichiers journaux de rétablissement de 2 Go chacun.

Exécuter l'utilitaire d'analyse des actifs de données

L'analyse des actifs de données affiche des mesures clés et des graphiques clés dans les onglets du tableau de bord en fonction de données analytiques précalculées. Avant d'effectuer la mise à niveau, vous devez remplir les tables de base de données précalculées à l'aide de données analytiques.

Effectuez les étapes suivantes pour exécuter l'utilitaire d'analyse des actifs de données :

1. Sauvegardez le schéma de base de données de l'analyse des actifs de données.
2. Vérifiez le fichier journal daa.log et assurez-vous qu'il n'existe aucun d'événement d'actif de données non traité pour éviter de perdre des données d'événements telles que les connexions utilisateur, les recherches et l'utilisation des actifs.
3. Depuis Akamai Download Manager, téléchargez et extrayez le fichier `informatica_1053_daa_utility.zip` sur le domaine Informatica.

Remarque: Si vous avez appliqué un Service Pack, vous devez télécharger l'utilitaire correspondant à la version du Service Pack.

4. Accédez au répertoire d'extraction des fichiers et au répertoire `config`.
5. Ouvrez le fichier `input.properties` et configurez les paramètres de connexion suivants pour le référentiel d'analyse des actifs de données.

Propriété	Description
<code>databaseType</code>	Type de base de données de l'outil Analyse des actifs de données. Entrez ORACLE, POSTGRESQL ou SQLSERVER.
<code>databaseHostName</code>	Nom d'hôte complet de la machine sur laquelle la base de données est hébergée. Remarque: Si la valeur contient un caractère spécial, vous devez placer la valeur entre guillemets simples (').
<code>databasePort</code>	Numéro de port du service de moteur de base de données.
<code>databaseServiceName</code>	Nom de service de la base de données Oracle.
<code>databaseName</code>	Nom de base de données pour la base de données PostgreSQL ou SQL Server.
<code>databaseUserName</code>	Nom du compte d'utilisateur pour se connecter à la base de données.
<code>databaseAdvanceParameter</code>	Facultatif. Entrez les paramètres de connexion JDBC avancés utilisés pour vous connecter au référentiel Analyse des actifs de données. Remarque: Vous devez placer les paramètres entre guillemets simples (').

6. Sur une ligne de commande shell, entrez la commande suivante pour exécuter l'utilitaire à partir du répertoire d'extraction des fichiers : `./daautil.sh`.
7. Appuyez sur **1** pour sélectionner le mode de mise à niveau.
8. Entrez le mot de passe utilisé pour vous connecter à la base de données.

Remarque: Pour connaître le statut d'exécution, reportez-vous au fichier `daautil.log` du répertoire d'exécution de l'utilitaire.

Étape 2. Sauvegarder les référentiels et les détails de configuration

Sauvegarder le domaine Informatica

Avant de mettre à niveau le domaine, sauvegardez les métadonnées de configuration pour le domaine Informatica.

Effectuez les étapes suivantes pour sauvegarder le domaine Informatica :

- Exécutez la commande `infasetup BackupDomain` pour sauvegarder les tables de la base de données de configuration du domaine dans un fichier.
- Sauvegardez les fichiers de configuration des métadonnées dans tout répertoire accessible par les machines sur lesquelles vous installez Informatica.

Informatica inclut des programmes de ligne de commande pour sauvegarder et restaurer le domaine. `infasetup` est situé dans le répertoire suivant :

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

Pour sauvegarder le domaine avec `infasetup`, utilisez la syntaxe suivante :

```
BackupDomain
<<-DatabaseAddress|-da> database_hostname:database_port|
<-DatabaseConnectionString|-cs> database_connection_string>
<-DatabaseUserName|-du> database_user_name
<-DatabasePassword|-dp> database_password
<-DatabaseType|-dt> database_type
[<-DatabaseServiceName|-ds> database_service_name]
<-BackupFile|-bf> backup_file_name
[<-Force|-f>]
<-DomainName|-dn> domain_name
[<-Tablespace|-ts> tablespace_name (used for IBM DB2 only)]
[<-SchemaName|-sc> schema_name (used for Microsoft SQL Server only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-TrustedConnection|-tc> trusted_connection (used for Microsoft SQL Server only)]
[<-EncryptionKeyLocation|-kl> encryption_key_location]
```

Le tableau suivant décrit les fichiers de métadonnées et les emplacements des fichiers :

Fichier de métadonnées	Description	Emplacement
nodemeta.xml	Contient les métadonnées d'un nœud.	Stocké dans le répertoire <code>isp/config</code> sur chaque nœud du domaine. Si vous utilisez le même nom de répertoire de sauvegarde sur tous les nœuds, renommez <code>nodemeta.xml</code> avant de le copier vers l'emplacement de la sauvegarde. Par exemple, vous sauvegardez <code>nodemeta.xml</code> dans le répertoire <code>/nodebak</code> sur <code>nodeA</code> et <code>nodeB</code> . Renommez les fichiers de configuration de sorte que, sur <code>nodeA</code> , le fichier soit sauvegardé sous <code>/nodebak/nodemeta_A.xml</code> et, sur <code>nodeB</code> , il soit sauvegardé sous <code>/nodebak/nodemeta_B.xml</code> .
domains.infra	Contient les informations de connectivité pour les nœuds passerelle.	Stocké dans un des emplacements suivants : <ul style="list-style-type: none">- Répertoire d'installation d'Informatica.- Emplacement configuré via la variable d'environnement <code>INFA_DOMAINS_FILE</code>.

Sauvegarder le référentiel modèle

Sauvegardez le contenu du référentiel modèle à l'aide de l'outil Administrator tool.

Pour sauvegarder le référentiel modèle, sélectionnez le service de référentiel modèle dans l'outil Administrator tool. Dans le menu **Actions du domaine**, cliquez sur **Contenu de référentiel > Sauvegarder**.

Sauvegarder les données du catalogue à l'aide de l'utilitaire export

Sauvegardez les données du catalogue à l'aide de l'utilitaire `export.jar` afin de pouvoir restaurer les données du catalogue après la mise à niveau.

Utilisez l'utilitaire export si vous avez effectué une mise à niveau d'une version de cluster Hadoop vers un cluster non-Hadoop et que vous souhaitez migrer les données de catalogue existantes vers la version 10.5.3. Contactez le support client international pour télécharger l'utilitaire.

Avant d'exécuter l'utilitaire, vérifiez les prérequis suivants :

- Le service de cluster Informatica est en cours d'exécution.
- Aucun travail n'est en cours d'exécution dans Enterprise Data Catalog. Pour vérifier, consultez l'onglet **Surveillance** dans Catalog Administrator.
- Le service de catalogue est en cours d'exécution.
- Si la sauvegarde contient des données de profil de similarité volumineuses, assurez-vous que le processus `infacmd` inclut une taille de segment de mémoire de 4 Go. Vous pouvez définir la valeur de la taille du segment de mémoire JAVA avec la propriété suivante dans le fichier `Infacmd.sh` :

```
export ICMJava_OPTS=-Xmx4096m
```
- Activez le mode lecture seule pour le catalogue de service. Pour activer le service en mode lecture seule, consultez les exemples de commandes `curl` suivantes :
 - Si le service de catalogue est activé pour SSL, utilisez la commande `curl -k -u <DomainUserName>:<DomainPassword> -X POST "https://<host name>:<Catalog Service port>/access/1/catalog/catalogMode/READONLYMODE" -H "accept: */*"`.
 - Si le service de catalogue n'est pas activé pour SSL, utilisez la commande `curl -k -u <DomainUserName>:<DomainPassword> -X POST "http://<host name>:<Catalog Service port>/access/1/catalog/catalogMode/READONLYMODE" -H "accept: */*"`.

- À partir de votre installation existante, copiez le fichier `application.properties` de `<$INFA_HOME>/logs/<NODE_NAME>/services/CatalogService/<SERVICE_NAME>/<SCN_NAME>/spark/` vers le répertoire de copie du fichier `export.jar`.
- Si le service de catalogue est activé pour SSL, définissez les variables d'environnement suivantes :
 - `INFA_TRUSTSTORE`. Définissez la variable sur l'emplacement du fichier truststore Informatica. L'emplacement par défaut est `$INFA_HOME/services/shared/security`.
 - `INFA_TRUSTSTORE_PASSWORD`. Chiffrez le mot de passe que vous avez défini. Consultez l'exemple de commande pour définir le mot de passe chiffré : `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA=="`

Remarque: Reportez-vous à l'exemple de commande suivant pour chiffrer le mot de passe : `$INFA_HOME/server/bin/pmpasswd <password>`
- Si les données du catalogue sont volumineuses, exécutez l'utilitaire `export.jar` avec une taille de segment de mémoire de 20 Go. Par exemple, `java -Xmx20960m -jar export.jar export`. Pour plus d'informations sur le dimensionnement des performances, reportez-vous au *Guide de réglage des performances d'Enterprise Data Catalog*.
- Définissez l'option d'intervalle de validation sur 48 heures lorsque vous exécutez l'utilitaire `export`. Par exemple, `java -Dexport.commit.interval.ms=172800000 -jar export.jar export`

Exécutez l'utilitaire à l'aide de la commande suivante : `- java -jar export.jar export`

Vous pouvez vérifier le fichier `export.log` généré à l'emplacement d'exécution de l'utilitaire.

Sauvegarder le catalogueDonnées utilisant la commande `ldm backupContents`

Sauvegardez les données du catalogue avant de mettre à niveau Enterprise Data Catalog. La sauvegarde du catalogue garantit la disponibilité des métadonnées, attributs, associations, valeurs, planifications et tâches existants en cas d'échec de la mise à niveau. Sauvegardez les données du catalogue pour les conserver à partir de l'environnement Hadoop en cas d'échec de la restauration ou de la mise à niveau. Vous devez disposer du rôle Informatica Administrator pour effectuer la sauvegarde.

Avant d'exécuter la commande `infacmd ldm backupContents`, vérifiez les prérequis suivants :

- Définissez les variables d'environnement suivantes si le service de catalogue est activé pour SSL :
 - `INFA_TRUSTSTORE`. Reportez-vous à l'exemple de commande suivant pour définir la variable `export INFA_TRUSTSTORE= <Location of the Informatica truststore file>`. L'emplacement par défaut est `<Informatica installation directory>/services/shared/security`.
 - `INFA_KEYSTORE`. Reportez-vous à l'exemple de commande suivant pour définir la variable : `export INFA_KEYSTORE=<Location of the keystore file>`. L'emplacement par défaut est `<Informatica installation directory>/services/shared/security`. Cette variable est requise uniquement si vous avez utilisé une configuration SSL personnalisée. Pour les configurations SSL et non-SSL par défaut, vous devez désactiver la variable.
 - `INFA_TRUSTSTORE_PASSWORD`. Chiffrez le mot de passe que vous avez défini. Reportez-vous à l'exemple de commande suivant pour définir le mot de passe chiffré : `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA=="`.
 - `INFA_KEYSTORE_PASSWORD`. Chiffrez le mot de passe que vous avez défini. Reportez-vous à l'exemple de commande suivant pour définir le mot de passe chiffré : `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI=="`. Cette variable est requise uniquement si vous avez utilisé une configuration SSL personnalisée. Pour les configurations SSL et non-SSL par défaut, vous devez désactiver la variable.

Vous pouvez contacter le support client international Informatica pour obtenir les mots de passe par défaut du truststore et du keystore.

Remarque: Reportez-vous à l'exemple de commande suivant pour chiffrer le mot de passe : `<Informatica installation directory>/server/bin/pmpasswd <password>`

- Estimez la consommation d'espace disque HDFS des données du catalogue. Exécutez la commande suivante pour afficher la taille du répertoire : `hdfs -du /Informatica/LDM/<SCN>`.
- Assurez-vous qu'un espace disque suffisant est disponible dans un hôte de domaine afin que l'espace disque de la sauvegarde soit suffisant.

La commande `infacmd Idm BackupContents`, telle qu'elle s'affiche dans l'exemple suivant, crée un fichier `.zip` du répertoire sur la machine locale : `./infacmd.sh LDM backupContents -dn <name of the Informatica domain> -un <username to connect to the Informatica domain> -pd <password for the username> -sn <name of the Catalog Service> -of <name of the backup ZIP file>`

Pour plus d'informations sur la syntaxe, les paramètres et la description de la commande, consultez le guide *Référence des commandes d'Informatica*.

Remarque: Si la sauvegarde échoue avec un problème de mémoire insuffisante, vous devez augmenter la taille du segment de mémoire JAVA pour la propriété `ICMD_JAVA_OPTS` dans le fichier `infacmd.sh` suivant. Par exemple, `ICMD_JAVA_OPTS=-Xmx20g`.

Sauvegarder la configuration SSL

Sauvegardez les fichiers de configuration SSL suivants à partir de l'emplacement par défaut : `<Informatica installation directory>/services/shared/security`.

- Sauvegardez les fichiers keystore et truststore de domaine.
- Sauvegardez les fichiers keystore par défaut.
- Sauvegardez tous les fichiers keystore et truststore que les services d'application utilisent.

Sauvegarder les informations du domaine

Sauvegardez les fichiers de configuration :

- `<Informatica installation directory>/isp/config/keys/siteKey`
- `<Informatica installation directory>/domains.infa`
- `<Informatica installation directory>/tomcat/conf/server.xml`
- `<Informatica installation directory>/isp/config/nodemeta.xml`

Remarque: Vous devez sauvegarder les fichiers binaires à partir du répertoire d'installation d'Informatica.

Sauvegarder le schéma de base de données de l'analyse des actifs de données

Si vous avez configuré le référentiel de l'analyse des actifs de données, effectuez une sauvegarde du schéma de base de données de l'analyse des actifs de données.

Remarque: Utilisez un outil de base de données pour effectuer une sauvegarde.

Sauvegarder MetaDex

Si vous avez configuré le référentiel de MetaDex, sauvegardez le référentiel MetaDex.

Remarque: Dans la version 10.4, le planificateur de travaux de MetaDex était désactivé par défaut. À partir de la version 10.5, par défaut, le planificateur de travaux supprime les travaux toutes les six heures, ne laissant que les trois derniers travaux. Vous pouvez modifier ce comportement en modifiant les paramètres dans le fichier `repository.properties`. Pour plus d'informations, reportez-vous à la section « Suppression des travaux » du *Guide de l'administrateur de MetaDex*.

1. Utilisez un outil de base de données pour effectuer une sauvegarde du schéma de base de données MetaDex.
Remarque: Veillez à créer une sauvegarde de l'intégralité de la base de données, pas seulement du contenu des données.
2. Créez une sauvegarde des fichiers de configuration suivants :
 - `<workspace>/etc`
 - `<workspace>/setup.env`
3. Créez une sauvegarde du registre de connexion.
4. Dans l'outil MetaDex, exportez vos configurations et projets.
Reportez-vous aux sections « Page de projets » et « Page de configuration » du *Guide de l'administrateur de MetaDex*.

Sauvegarder les enrichissements de la ressource Tableau à l'aide de l'utilitaire de migration

Si le catalogue contient des ressources Tableau, vous devez sauvegarder les enrichissements des ressources Tableau à l'aide de l'utilitaire de migration avant d'effectuer une mise à niveau vers Enterprise Data Catalog version 10.5.3.

1. Depuis Akamai Download Manager, téléchargez et extrayez le fichier `Informatica_1053_TableauEnrichmentMigrationUtility.zip` sur la machine du domaine.
2. Exécutez la commande suivante pour sauvegarder les enrichissements des ressources Tableau :

```
java -jar EnrichmentUtility.jar export <Catalog Service hostname> <Catalog Service admin port number> <username> <password> <location to download enrichments json> <resourceName> <SSL Enabled true/false>
```

Sauvegarder les enrichissements de la ressource Qlik Sense à l'aide de l'utilitaire de migration

Si le catalogue contient des ressources Qlik Sense et que vous utilisez MITI version 11.x, vous devez sauvegarder les enrichissements de ressources Qlik Sense à l'aide de l'utilitaire de migration avant d'effectuer une mise à niveau vers Enterprise Data Catalog version 10.5.3.

1. Téléchargez et extrayez le fichier `QlikSenseEnrichmentsCLIMigrator.jar` sur la machine du domaine, à partir de l'emplacement suivant : `<INFA_HOME>/services/CatalogService/ScannerBinaries/qliksense-utility/lib/`
2. Exécutez la commande suivante pour sauvegarder les enrichissements de la ressource Qlik Sense :

```
java -jar QlikSenseEnrichmentsCLIMigrator.jar export <Catalog Service hostname> <Catalog Service admin port number> <username> <password> <location to download enrichments json> <resourceName> <SSL Enabled true/false>
```

Remarque: Le délai d'exécution de l'utilitaire dépend du nombre d'actifs dans la ressource. Si la ressource comporte de nombreux actifs, vous pouvez configurer la mémoire Java pour sauvegarder les enrichissements.

Sauvegarder les enrichissements de la ressource Salesforce à l'aide de l'utilitaire de migration

Si le catalogue contient des ressources Salesforce, vous devez sauvegarder les enrichissements des ressources Salesforce à l'aide de l'utilitaire de migration avant d'effectuer une mise à niveau vers Enterprise Data Catalog version 10.5.3.

1. Téléchargez et extrayez le fichier `SalesforceEnrichmentcliMigrationUtility.zip` sur la machine du domaine, à partir de l'emplacement suivant : `<INFA_HOME>/services/CatalogService/ScannerBinaries/`
2. Exécutez la commande suivante pour sauvegarder les enrichissements de la ressource Salesforce :

```
java -jar EnrichmentUtility.jar export <Catalog Service hostname> <Catalog Service
admin port number> <username> <password> <location to download enrichments json>
<resourceName> <SSL Enabled true/false>
```

Remarque: Le délai d'exécution de l'utilitaire dépend du nombre d'actifs dans la ressource. Si la ressource comporte de nombreux actifs, vous pouvez configurer la mémoire Java pour sauvegarder les enrichissements.

Sauvegarder les enrichissements de la ressource Erwin à l'aide de l'utilitaire de migration

Si le catalogue contient des ressources Erwin, vous devez sauvegarder les enrichissements des ressources Erwin à l'aide de l'utilitaire de migration avant d'effectuer une mise à niveau vers Enterprise Data Catalog version 10.5.3.

1. Copiez et extrayez le fichier `ErwinEnrichmentsCLIMigrator.jar` à partir de l'emplacement suivant sur la machine du domaine Informatica :
`<Informatica installation directory>/services/CatalogService/ScannerBinaries/erwin-utility/lib`
2. Exécutez la commande suivante pour sauvegarder les enrichissements des ressources Erwin :

```
java -jar ErwinEnrichmentsCLIMigrator.jar export <Catalog Service hostname> <Catalog
Service port number> <Catalog administrator user name> <Catalog administrator
password> <location to download enrichments json> <resourceName> <SSL Enabled true/
false>
```

Étape 3. Préparer la mise à niveau

Désactivation du service de catalogue

Pour désactiver le service, sélectionnez le service de catalogue dans Informatica Administrator et cliquez sur **Actions > Désactiver le service**.

Désactiver les services d'application Informatica

Désactivez les services d'applications Informatica suivants :

1. Service de cluster Informatica
2. Service de gestion de contenu
3. Service d'intégration de données
4. Service de référentiel modèle

Pour désactiver un service d'application, sélectionnez-le dans Informatica Administrator et cliquez sur **Actions > Désactiver le service**.

Nettoyer le cluster

Nettoyez le cluster à l'aide de la commande `infacmd` `ihc cleanCluster`. Après avoir exécuté la commande `infacmd` `ihc cleanCluster`, connectez-vous à chaque nœud de cluster en tant qu'utilisateur non-racine avec des privilèges `sudo` et supprimez le contenu du répertoire `/tmp` que possède l'utilisateur `yarn`. Pour supprimer le contenu, exécutez la commande suivante en tant qu'utilisateur non-racine avec des privilèges `sudo` :

```
find /tmp/ -user yarn -exec rm -fr {} \;.
```

Syntaxe et description de la commande `ihc cleanCluster`

La syntaxe de la commande `infacmd` `ihc cleanCluster` est la suivante :

```
cleanCluster  
  
<-DomainName|-dn> domain_name  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
<-ServiceName|-sn> service_name  
  
[<-SecurityDomain|-sdn> security_domain]  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Le tableau suivant décrit les options et les arguments de la commande `infacmd` `ihc cleanCluster` :

Option	Argument	Description
-DomainName -dn	domain_name	Requis. Nom du domaine Informatica. Vous pouvez définir le nom de domaine avec l'option <code>-dn</code> ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN</code> . Si vous définissez un nom de domaine avec les deux méthodes, l'option <code>-dn</code> est prioritaire.
-UserName -un	user_name	Obligatoire si le domaine utilise l'authentification native ou LDAP. Nom d'utilisateur pour se connecter au domaine. Vous pouvez définir le nom d'utilisateur avec l'option <code>-un</code> ou la variable d'environnement <code>INFA_DEFAULT_DOMAIN_USER</code> . Si vous définissez un nom d'utilisateur avec les deux méthodes, l'option <code>-un</code> est prioritaire. Facultatif si le domaine utilise l'authentification Kerberos. Pour exécuter la commande avec l'authentification unique, ne définissez pas le nom d'utilisateur. Si vous définissez le nom d'utilisateur, la commande s'exécute sans l'authentification unique.

Option	Argument	Description
-Password -pd	password	Obligatoire si vous spécifiez le nom d'utilisateur. Mot de passe pour le nom d'utilisateur. Le mot de passe est sensible à la casse. Vous pouvez définir un mot de passe avec l'option -pd ou la variable d'environnement INFA_DEFAULT_DOMAIN_PASSWORD. Si vous définissez un mot de passe avec les deux méthodes, le mot de passe défini avec l'option -pd est prioritaire.
-ServiceName -sn	service_name	Requis. Nom du service de cluster Informatica.
-SecurityDomain -sdn	security_domain	Obligatoire si le domaine utilise l'authentification LDAP. Facultatif si le domaine utilise l'authentification native ou l'authentification Kerberos. Nom du domaine de sécurité auquel l'utilisateur du domaine est rattaché. Vous pouvez définir un domaine de sécurité avec l'option -sdn ou la variable d'environnement INFA_DEFAULT_SECURITY_DOMAIN. Si vous définissez un nom de domaine de sécurité avec les deux méthodes, l'option -sdn est prioritaire. Le nom du domaine de sécurité est sensible à la casse. Si le domaine utilise l'authentification native ou LDAP, la valeur par défaut est l'authentification Native. Si le domaine utilise l'authentification Kerberos, la valeur par défaut est le domaine de sécurité LDAP créé lors de l'installation. Le nom du domaine de sécurité est le même que le domaine de l'utilisateur indiqué lors de l'installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Facultatif. Temps en secondes pendant lequel infacmd tente d'établir ou de rétablir une connexion au domaine. Vous pouvez définir le délai de résilience avec l'option -re ou la variable d'environnement INFA_CLIENT_RESILIENCE_TIMEOUT. Si vous définissez le délai de résilience avec les deux méthodes, l'option -re est prioritaire.

Désactiver et désinstaller le service PostgreSQL

Vous devez désactiver PostgreSQL avant de procéder à la mise à niveau.

Désactiver le service PostgreSQL

Utilisez la commande suivante sur la machine sur laquelle Informatica Administrator s'exécute pour désactiver le service PostgreSQL : `service postgresql-<PostgreSQL version> stop`. Par exemple, si vous utilisez PostgreSQL version 9.6, utilisez la commande `service postgresql-9.6 stop` ou `systemctl disable postgresql-9.6` or `systemctl disable postgresql-x.x`. suivante

Désinstaller le service PostgreSQL

Utilisez la commande suivante sur la machine sur laquelle Informatica Administrator s'exécute pour désinstaller le service PostgreSQL : `sudo yum remove postgres*` et `sudo rm -rf /var/lib/pgsql/*`.

Remarque: Pour vérifier que le service postgresql est arrêté, exécutez la commande suivante : `systemctl postgresql-<PostgreSQL version> status`.

Arrêter le domaine Informatica.

Depuis Informatica Administrator, arrêtez le domaine Informatica.

Étape 4. Présentation de la mise à niveau du domaine

L'assistant de mise à niveau lit les informations sur le domaine à partir des fichiers de la version précédente et utilise les mêmes paramètres pour configurer les fichiers pour la mise à niveau. Il met à niveau les tables du référentiel de configuration de domaine dans la même base de données que la version précédente. Vous pouvez mettre à niveau le domaine Informatica en mode console ou silencieux.

Effectuez les tâches de préparation à la mise à niveau avant de commencer. Exécutez le programme d'installation sur toutes les machines qui hébergent des versions précédentes d'Informatica que vous souhaitez mettre à niveau.

Remarque: Dans un domaine à plusieurs nœuds, mettez à niveau le nœud de passerelle avant les autres nœuds et mettez à niveau tous les nœuds de travail en parallèle.

Vous pouvez effectuer la mise à niveau depuis le répertoire dans lequel vous avez téléchargé les fichiers d'installation.

Une fois le domaine mis à niveau, mettez à niveau l'outil client Informatica vers la même version Informatica.

Avant d'effectuer la mise à niveau, vérifiez que le fichier truststore du domaine Informatica contient uniquement TrustedCertEntry. Vous devez supprimer toutes les entrées PrivateKeyEntry du fichier.

Exécuter l'utilitaire de validation de cluster

Exécutez l'utilitaire de validation du scanner pour valider les prérequis de la mise à niveau d'Enterprise Data Catalog.

Effectuez les étapes suivantes pour exécuter l'utilitaire :

1. Vérifiez que chaque nœud de cluster dispose d'au moins quatre cœurs de processeur, 16 Go de mémoire et 60 Go d'espace disque libre.

Remarque: La configuration matérielle requise répertoriée ici correspond aux valeurs minimales recommandées pour installer le produit et démarrer les services. Elle varie en fonction de la taille du déploiement. Pour plus d'informations sur la configuration matérielle requise en fonction des tailles de déploiement, reportez-vous au Guide de réglage des performances d'Enterprise Data Catalog.

2. Vérifiez que le répertoire racine () dispose d'un minimum de 10 Go d'espace disque libre.
3. Téléchargez l'utilitaire de validation de cluster Informatica pour la version 10.5.3 d'Akamai Download Manager.

Remarque: Si vous avez appliqué un Service Pack, vous devez télécharger l'utilitaire correspondant à la version du Service Pack.

4. Extrayez le fichier ZIP sur le domaine Informatica que vous prévoyez de mettre à niveau.
5. Accédez au répertoire d'extraction des fichiers et ouvrez les fichiers input.properties.

Remarque: Vous devez disposer des autorisations de lecture et d'écriture sur le répertoire et des autorisations d'exécution sur les fichiers exécutables.

6. Dans le fichier input.properties, configurez les propriétés requises.
7. Désactivez le pare-feu sur chaque hôte du cluster.
8. Activez SSH sans mot de passe entre les nœuds suivants :
 - Nœud qui héberge le domaine Informatica et le nœud qui héberge la passerelle.
 - Hôte de passerelle et nœuds de données.

- Hôte de passerelle et nœuds de traitement.
- Nœuds de sauvegarde et nœud de passerelle.
- Tous les nœuds du cluster et les nœuds de données.

Remarque: Si vous avez activé la configuration avancée pour le service de cluster Informatica et que les services MongoDB, PostgreSQL, Solr et Nomad s'exécutent sur des hôtes différents, activez l'accès sans mot de passe de l'hôte de passerelle aux hôtes qui exécutent ces services.

9. Sur une ligne de commande shell, accédez au répertoire d'extraction des fichiers utilitaires et exécutez la commande suivante : `java -jar InformaticaClusterValidationUtility.jar -in <Location of the input.properties file>`.

L'utilitaire propose les options suivantes :

Option	Description
-hp	Affichez le contenu de l'aide.
-in	Spécifiez l'emplacement du fichier input.properties.
-lf	Facultatif. Spécifiez le répertoire de stockage des fichiers journaux générés par l'utilitaire.
-v	Facultatif. Activez le journal de débogage.
-vf	Facultatif. Si vous avez déplacé les scripts de validation vers un répertoire différent, spécifiez l'emplacement de stockage des scripts de validation.

Remarque: Si un message d'erreur de validation d'autorisation pour le répertoire personnalisé du cluster s'affiche, vous pouvez ignorer l'erreur.

10. Vérifiez l'état de validation à partir des fichiers journaux suivants situés dans le répertoire d'exécution de l'utilitaire :
 - clusterPrevalidation.log
 - clusterPrevalidation.err

Mettre à niveau en mode console

Vous pouvez effectuer une mise à niveau en mode console sous UNIX ou Linux.

Lorsque vous exécutez le programme d'installation en mode console, les mots Quitter, Retour et Aide sont des mots réservés. Ne les utilisez pas comme texte d'entrée.

1. Connectez-vous à la machine avec le même compte d'utilisateur que vous avez utilisé pour installer la version précédente.
2. Arrêtez tous les processus qui accèdent au répertoire et aux sous-répertoires du produit Informatica à mettre à niveau, y compris les invites de commande et suivis d'audit.
3. Sur une ligne de commande shell, exécutez le fichier d'installation.

Le programme d'installation affiche un message vous invitant à vérifier que les variables d'environnement régionales sont définies.

4. Si les variables d'environnement ne sont pas définies, appuyez sur la touche **n** pour quitter le programme d'installation et définissez-les de façon appropriée.

Si les variables d'environnement sont définies, appuyez sur **y** pour continuer.

5. Appuyez sur **2** pour mettre à niveau Informatica.

6. Appuyez sur **2** pour ignorer l'exécution d'Informatica Upgrade Advisor.

Informatica fournit des utilitaires pour faciliter le processus d'installation des services Informatica. Vous pouvez exécuter l'utilitaire avant de mettre à niveau les services Informatica. Informatica Upgrade Advisor valide les services et vérifie la présence de services obsolètes dans le domaine avant d'effectuer une mise à niveau.

Le programme d'installation affiche un avertissement vous demandant d'arrêter le domaine Informatica que vous souhaitez mettre à niveau avant de poursuivre la mise à niveau.

7. Lisez les conditions du kit d'utilisation du produit Informatica et sélectionnez **2** pour poursuivre la mise à niveau.

Soumis à vos droits de retrait décrits ci-dessous, le logiciel transmettra automatiquement certaines informations à Informatica (aux États-Unis) concernant l'environnement informatique et réseau dans lequel le Logiciel est déployé et les statistiques du système et d'utilisation des données du déploiement. Cette transmission est considérée comme faisant partie des Services selon la politique de confidentialité d'Informatica et Informatica utilisera et traitera par ailleurs ces informations conformément à la politique de confidentialité d'Informatica disponible sur <https://www.informatica.com/in/privacy-policy.html>. Vous pouvez désactiver la collecte d'utilisation dans l'outil Administrator tool.

8. La page **Prérequis de mise à niveau** affiche les spécifications système pour la mise à niveau.

Vérifiez les spécifications avant de poursuivre la mise à niveau.

9. Vérifiez les informations de mise à niveau et appuyez sur **Entrée** pour continuer.

Le panneau **Répertoire de mise à niveau** s'affiche.

10. Lorsque vous y êtes invité, entrez le répertoire de la version d'Informatica à mettre à niveau et le répertoire dans lequel vous souhaitez effectuer la mise à niveau vers Informatica 10.5.3.

Le tableau suivant décrit les répertoires que vous devez indiquer :

Répertoire	Description
Répertoire du produit Informatica à mettre à niveau	Répertoire qui contient la version des services Informatica que vous souhaitez mettre à niveau.
Répertoire pour Informatica 10.5.3	<p>Répertoire d'installation d'Informatica 10.5.3.</p> <p>Entrez le chemin absolu du répertoire d'installation. Ce répertoire ne peut pas être le même que celui qui contient la version précédente des services Informatica.</p> <p>Les noms de répertoires dans le chemin ne doivent pas contenir d'espaces ni les caractères spéciaux suivants : @ * \$ # ! % () { } [] , ; '.</p> <p>Remarque: Si vous utilisez un caractère spécial comme á ou €, des résultats inattendus peuvent se produire lors de l'exécution.</p>

11. Parmi les options d'installation suivantes, sélectionnez l'environnement de mise à niveau en fonction de vos besoins :

- Sandbox. Utilisé pour la preuve de concepts ou comme sandbox avec un minimum d'utilisateurs.
- Développement. Utilisé pour un environnement de conception.
- Test. Utilisé pour un environnement de traitement de gros volumes qui ressemble à un environnement de production.
- Production. Utilisé pour les environnements de production pour un traitement de gros volumes avec des niveaux élevés d'accès concurrentiel destinés aux utilisateurs finaux.

12. Choisissez si vous souhaitez modifier le nom d'hôte de nœud, les numéros de port ou le référentiel de configuration du domaine. Appuyez sur **1** pour utiliser la même configuration de nœud que dans la version précédente. Appuyez sur **2** pour modifier la configuration du nœud.
Le panneau **Sélection des composants** s'affiche.
13. Appuyez sur **1** pour mettre à niveau les services Informatica.
14. Si vous avez configuré un service de catalogue sur le nœud, vous devez valider la sauvegarde du catalogue avant d'effectuer une mise à niveau. Appuyez sur **1** si le nœud ne comporte aucun service de catalogue ou sur **2** s'il en comporte un, puis appuyez sur **Entrée** pour continuer.
15. Appuyez sur **2** pour confirmer que vous avez sauvegardé le catalogue à l'aide de l'utilitaire export et de la commande `infacmd LDM backupContents`.
16. Spécifiez l'emplacement du répertoire contenant la sauvegarde du catalogue.
La sauvegarde du catalogue est validée.
17. Appuyez sur **1** si vous voulez configurer le référentiel MetaDex et fournissez les détails suivants :

Propriété	Description
Type de base de données	Spécifiez la base de données à configurer comme référentiel pour MetaDex. Vous pouvez sélectionner l'une des options suivantes : - Oracle - SQLServer
Nom d'utilisateur de la base de données	Nom d'utilisateur configuré pour accéder à la base de données avant la mise à niveau.
Mot de passe de la base de données	Mot de passe configuré pour le nom d'utilisateur.
Nom du schéma	Non applicable si vous avez sélectionné Oracle comme base de données. Spécifiez le schéma à utiliser.
La base de données est-elle sécurisée ?	Spécifiez si la base de données est activée pour SSL.
Chemin d'accès au fichier truststore de la base de données	S'applique si vous avez spécifié que la base de données est activée pour SSL. Fournissez le chemin d'accès complet au fichier truststore de la base de données.
Mot de passe du truststore	S'applique si vous avez spécifié que la base de données est activée pour le mot de passe SSL pour accéder au fichier truststore.
Paramètres JDBC sécurisés	S'applique si vous avez spécifié que la base de données est activée pour SSL. Spécifiez les paramètres de base de données sécurisés, comme indiqué dans l'exemple suivant : <code>EncryptionMethod=SSL;HostNameInCertificate=ORATLS.informatica.com;</code> <code>ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;</code> Enterprise Data Catalog 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 aucun paramètre dans le champ Paramètres JDBC sécurisés.

Propriété	Description
Chaîne de connexion JDBC	<p>Chaîne de connexion JDBC pour la connexion à la base de données.</p> <p>Utilisez les formats suivants pour spécifier les chaînes de connexion :</p> <ul style="list-style-type: none"> - Oracle. jdbc:Informatica:oracle://<host name>:<port number>;ServiceName= - SQLServer. jdbc:Informatica:sqlserver://<host name>:<portnumber>;SelectMethod=cursor;DatabaseName=
MetaDex	Port unique du serveur de référentiel MetaDex. La valeur par défaut est de 48 090.
Activer la communication sécurisée pour le référentiel MetaDex ?	Spécifiez si TLS est activé pour la communication avec le référentiel MetaDex.
Certificats SSL pour sécuriser le référentiel MetaDex ?	<p>Indiquez si vous souhaitez utiliser les certificats SSL par défaut ou les certificats SSL personnalisés pour sécuriser le référentiel MetaDex.</p> <p>Spécifiez les propriétés suivantes si vous souhaitez utiliser les certificats SSL personnalisés :</p> <ul style="list-style-type: none"> - Type de keystore. Spécifiez le type de keystore. - Alias du keystore. Alias unique permettant d'accéder à l'entrée du keystore. - Fichier keystore. Spécifiez le fichier keystore qui contient les clés et les certificats requis. - Mot de passe du keystore. Mot de passe pour accéder au fichier keystore.

Si vous n'aviez pas choisi de configurer le référentiel MetaDex lors de l'installation, vous pouvez le configurer une fois celle-ci terminée. Effectuez les étapes répertoriées dans la section [“Configurer le référentiel MetaDex \(facultatif\)” à la page 62.](#)

Remarque: Assurez-vous que l'utilisateur dispose des autorisations d'écriture sur le fichier de configuration de nœud `nodemeta.xml` situé dans `<Informatica installation directory>/isp/config`.

- Choisissez si vous souhaitez installer des packages d'intégration tiers avec le programme d'installation d'Informatica.

Remarque: Vous devez installer un package d'intégration si vous configurez les services Informatica pour effectuer les tâches suivantes :

- Transférez le traitement vers l'environnement Hadoop ou Databricks.
- Traitez des fichiers complexes dans le domaine Informatica.
- Connectez-vous à l'environnement Hadoop, mais effectuez un traitement dans le domaine Informatica.

Vous pouvez choisir d'installer les packages maintenant ou ultérieurement via Integration Package Manager.

- Appuyez sur **1** pour installer le domaine Informatica sans packages d'intégration.
- Appuyez sur **2** pour installer le domaine Informatica avec des packages d'intégration.

La valeur par défaut est 1.

- Si vous choisissez d'installer des packages d'intégration, sélectionnez-en un ou plusieurs que vous souhaitez installer dans la liste. Séparez plusieurs packages par une virgule.

La valeur par défaut est 1.

Remarque: Les fichiers du programme d'installation des packages sélectionnés doivent être disponibles dans le répertoire : `<Informatica installer files>/source`

20. Appuyez sur **Entrée**.
Le panneau **Sécurité du domaine - Clé de chiffrement** s'affiche.
21. Entrez le nom d'utilisateur et le mot de passe du domaine Informatica.
La page **Récapitulatif de pré-installation** s'affiche.
22. Vérifiez les informations de mise à niveau et appuyez sur **Entrée** pour continuer.
Une fois la mise à niveau du domaine terminée, le panneau **Référentiel de configuration de domaine** s'affiche.
23. Appuyez sur **Entrée** pour continuer la mise à niveau.
Le programme d'installation copie les fichiers de serveur dans le répertoire d'installation d'Informatica 10.5.3.
Le programme d'installation affiche les informations de la base de données et du compte d'utilisateur pour le référentiel de configuration du domaine à mettre à niveau. Il affiche la chaîne de connexion à la base de données pour le référentiel de configuration du domaine en se basant sur la manière dont la chaîne de connexion de la version précédente a été créée lors de l'installation :
 - Si la version précédente utilisait une URL JDBC lors de l'installation, le programme d'installation affiche les propriétés de connexion JDBC, y compris l'adresse et le nom de service de la base de données.
 - Si la version précédente utilisait une chaîne de connexion JDBC personnalisée lors de l'installation, le programme d'installation affiche la chaîne de connexion personnalisée.
24. Si vous utilisez une URL JDBC, vous pouvez spécifier des paramètres supplémentaires à inclure dans la chaîne de connexion.
Si vous utilisez une chaîne de connexion personnalisée, vous ne pouvez pas spécifier de paramètres supplémentaires.
25. Vérifiez les informations et appuyez sur **Entrée**.
La mise à niveau se termine et le panneau **Résumé de post-installation** s'affiche.
26. Appuyez sur **Entrée** pour terminer la procédure d'installation et quitter le programme d'installation.
Vérifiez le fichier `upgrade.log` pour obtenir plus d'informations sur les tâches effectuées par l'assistant de mise à niveau et pour afficher la configuration des composants installés.

Appliquer le dernier Service Pack ou correctif cumulatif

Appliquez le dernier Service Pack ou correctif cumulatif disponible après la mise à niveau du domaine.

Configurer le référentiel MetaDex (facultatif)

Si vous n'aviez pas configuré le référentiel MetaDex lors de la mise à niveau, vous pouvez le faire après avoir mis à niveau Enterprise Data Catalog.

Effectuez les étapes suivantes pour configurer le référentiel :

1. Accédez au répertoire d'extraction des fichiers du programme d'installation et accédez au sous-répertoire suivant : `\properties\MetaDex\`.

2. Ouvrez le fichier `MetaDex.properties` et configurez les propriétés suivantes :

Propriété	Description
USER_INSTALL_DIR	Répertoire d'installation d'Informatica.
MDX_DB_UNAME	Nom d'utilisateur configuré pour accéder à la base de données avant la mise à niveau.
MDX_DB_PASSWD	Mot de passe pour accéder à la base de données.
MDX_DB_TYPE	Type de base de données à configurer. Spécifiez <code>Oracle</code> ou <code>MSSQLServer</code> .
MDX_SQLSERVER_SCHEMA_NAME	S'applique si <code>MDX_DB_TYPE=MSSQLServer</code> . Spécifiez le nom du schéma à utiliser. Si vous ne spécifiez aucun schéma, Enterprise Data Catalog utilise celui par défaut.
MDX_DB_CUSTOM_STRING	Chaîne de connexion JDBC pour la connexion à la base de données. Utilisez les formats suivants pour spécifier les chaînes de connexion : <ul style="list-style-type: none"> - Oracle. jdbc:informatica:oracle: <code>//<host name>:<port number>;ServiceName=</code> - SQLServer. jdbc:informatica:sqlserver: <code>//<host name>:<portnumber>;SelectMethod=cursor;DatabaseName=</code>
MDX_SERVER_PORT	Port unique du serveur de référentiel MetaDex. La valeur par défaut est de 48 090.
MDX_SSL_ENABLED	Spécifiez <code>true</code> si la base de données est activée pour SSL, sinon <code>false</code> . La valeur par défaut est <code>false</code> .
MDX_DB_TRUSTSTORE_FILE	S'applique si vous avez spécifié que la base de données est activée pour SSL. Fournissez le chemin d'accès complet au fichier truststore de la base de données.
MDX_DB_TRUSTSTORE_PASSWD	S'applique si vous avez spécifié que la base de données est activée pour le mot de passe SSL pour accéder au fichier truststore.
MDX_SSL_DEFAULT_STRING	S'applique si vous avez spécifié que la base de données est activée pour SSL. Spécifiez les paramètres de base de données sécurisés, comme indiqué dans l'exemple suivant : <pre>EncryptionMethod=SSL;HostNameInCertificate= ORATLS.informatica.com; ValidateServerCertificate=true; CryptoProtocolVersion=TLSv1.2;</pre> Enterprise Data Catalog 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 aucun paramètre dans le champ Paramètres JDBC sécurisés.

Propriété	Description
MDX_CUSTOM_SELECTION	S'applique si vous avez spécifié que la base de données est activée pour SSL. Indiquez si vous souhaitez utiliser les certificats SSL par défaut ou les certificats SSL personnalisés pour sécuriser le référentiel. Définissez la propriété sur <code>true</code> pour utiliser des certificats SSL personnalisés. Définissez la propriété sur <code>false</code> pour utiliser le certificat SSL par défaut.
MDX_KEYSTORE_FILE	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Spécifiez le fichier keystore qui contient les clés et les certificats requis.
MDX_KEYSTORE_PASSWD	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Mot de passe pour accéder au fichier keystore.
MDX_KEYSTORE_TYPE	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Spécifiez le type de keystore.
MDX_KEYSTORE_ALIAS	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Alias unique permettant d'accéder à l'entrée du keystore.

- Entrez la commande suivante : `./configureMetaDex.sh`

Remarque: Installez MetaDex sur le même nœud sur lequel réside le service de catalogue.

- Si le service de catalogue est en cours d'exécution, recyclez le service.

Copier les pilotes de ressources tiers

Effectuez les postrequis suivants après avoir mis à niveau le domaine Informatica :

- Copiez les fichiers JAR ou ZIP tiers que vous aviez configurés pour des ressources telles que Teradata, JDBC et IBM Netezza de l'emplacement suivant `<Informatica installation directory>services/CatalogService/ScannerBinaries` vers le même emplacement de la machine qui héberge le domaine Informatica mis à niveau.

Activer et mettre à niveau les services d'application

Pour activer un service d'application, sélectionnez-le dans Informatica Administrator et cliquez sur **Actions > Activer le service**. Mettez à niveau les services d'application après avoir mis à niveau tous les nœuds.

Activez les services d'application Informatica suivants :

- Service de référentiel modèle
- Service d'intégration de données
- Service de gestion de contenu

Après avoir activé les services d'application Informatica, exécutez l'assistant de mise à niveau des services pour mettre à niveau ceux-ci.

Remarque: Vous devez désactiver l'analyse des actifs de données avant de mettre à niveau le service de cluster Informatica. Pour désactiver l'analyse des actifs de données, sélectionnez le service de catalogue dans Informatica Administrator. Modifiez les propriétés de configuration de l'analyse des actifs de données et décochez la case **Activer l'analyse des actifs de données**.

Exécuter l'assistant de mise à niveau

Utilisez l'assistant de mise à niveau des services pour mettre à niveau les services d'application et le contenu des bases de données qui leur sont associées. L'assistant de mise à niveau des services affiche les services mis à niveau dans une liste contenant également les services et les bases de données associées qui nécessitent une mise à niveau. Vous pouvez également enregistrer le rapport de mise à niveau actuel ou le précédent.

1. Dans la zone d'en-tête Informatica Administrator, cliquez sur **Gérer > Mettre à niveau**.
2. Sélectionnez les services d'application et les bases de données associées à mettre à niveau.
3. Vous pouvez éventuellement sélectionner l'option **Recycler automatiquement les services après une mise à niveau**.

Si vous choisissez de redémarrer automatiquement les services d'application après la mise à niveau, l'assistant de mise à niveau redémarre les services après leur mise à niveau.

4. Cliquez sur **Suivant**.
5. En cas d'erreurs de dépendance, la boîte de dialogue **Erreurs de dépendance** s'affiche. Examinez les erreurs de dépendance et cliquez sur **OK**. Ensuite, résolvez les erreurs de dépendance et cliquez sur **Suivant**.
6. Entrez les informations de connexion au référentiel.
7. Cliquez sur **Suivant**.

L'assistant de mise à niveau des services met à niveau chaque service d'application et chaque base de données associée, puis affiche le statut et les détails du traitement.

8. Une fois la mise à niveau terminée, la section **Résumé** affiche la liste des services d'application et leur statut de mise à niveau. Cliquez sur chaque service pour afficher les détails dans la section **Détails du service**.
9. Vous pouvez éventuellement cliquer sur **Enregistrer le rapport** pour enregistrer les détails de la mise à niveau dans un fichier.
Si vous choisissez de ne pas enregistrer le rapport, vous pouvez cliquer sur **Enregistrer le rapport précédent** au prochain lancement de l'assistant de mise à niveau des services.
10. Cliquez sur **Fermer**.
11. Si vous n'avez pas choisi de redémarrer automatiquement les services d'application après la mise à niveau, redémarrez les services mis à niveau.

Vous pouvez afficher le rapport de mise à niveau et l'enregistrer. Lors de la deuxième exécution de l'assistant de mise à niveau des services, l'option Enregistrer le rapport précédent s'affiche. Si vous n'avez pas enregistré le rapport de mise à niveau après la mise à niveau des services, vous pouvez sélectionner cette option pour afficher ou enregistrer le rapport de mise à niveau précédent.

Ajouter la licence du domaine Informatica

Effectuez les étapes suivantes pour ajouter la nouvelle licence pour le domaine Informatica :

1. Connectez-vous à Informatica Administrator.
2. Sélectionnez le domaine Informatica.
3. Cliquez sur **Nouveau > Licence**.
4. Donnez un nom à la nouvelle licence.
5. Sélectionnez la nouvelle clé de licence dans la liste déroulante **Licence**.

Mettre à jour la licence du service de cluster Informatica

Effectuez les étapes suivantes pour mettre à jour la licence du service de cluster Informatica :

1. Connectez-vous à Informatica Administrator.
2. Sélectionnez le domaine.
3. Sélectionnez la licence existante et cliquez sur **Services attribués**.
4. Cliquez sur **Modifier**.
5. Sélectionnez le service de cluster Informatica et cliquez sur **Supprimer**.
6. Cliquez sur **OK** pour confirmer.
7. Sélectionnez la nouvelle licence et cliquez sur **Services attribués**.
8. Cliquez sur **Modifier**.
9. Sélectionnez le service de cluster Informatica et cliquez sur **Ajouter**.
10. Cliquez sur **OK** pour confirmer.

Étape 5. Effectuer la mise à niveau du domaine Informatica

Vérifier les prérequis de l'utilisateur de la passerelle

L'utilisateur de la passerelle doit être un utilisateur non-racine avec un accès sudo. Vous devez activer une connexion SSH sans mot de passe entre le domaine Informatica et l'hôte de passerelle pour l'utilisateur de la passerelle. L'utilisateur de la passerelle doit disposer des privilèges requis pour exécuter la commande ping.

Configurer les privilèges Sudo pour l'utilisateur de la passerelle (facultatif)

Si vous prévoyez de modifier les propriétés du service de cluster Informatica ou de remplacer les certificats SSL configurés pour le service de cluster Informatica, attribuez des privilèges sudo à l'utilisateur de la passerelle.

Les commandes suivantes nécessitent des privilèges sudo pour l'utilisateur de la passerelle lorsque vous activez le service de cluster Informatica pour la première fois :

- mkdir
- chown
- chmod
- echo
- systemctl
- cp
- mv
- sysctl
- rm

- tee
- sed
- sshd

Pour configurer les privilèges sudo pour les commandes, vous devez ajouter les commandes au fichier `/etc/sudoers`, comme illustré dans l'exemple suivant : `/bin/mkdir, /bin/chown, /bin/chmod, /bin/echo, /bin/systemctl, /bin/cp, /bin/mv, /usr/sbin/sysctl, /bin/rm, /usr/bin/tee, /usr/bin/sed, /usr/sbin/sshd`.

Remarque: Les commandes `tee` et `sed` ne nécessitent aucun privilège sudo dans les versions 10.5.1.1 et ultérieures.

Vous pouvez déterminer le répertoire où se trouve chaque commande à l'aide de la commande `which <command name>`.

Après avoir activé le service de cluster Informatica pour la première fois, vous pouvez choisir de désactiver la validation des autorisations sudo pour le service de cluster Informatica. Pour désactiver la validation, configurez la propriété personnalisée suivante pour le service de cluster Informatica :

`IcsCustomOptions.IcsGatewayUserSudoEnabled` et définissez la valeur sur `false`. Après la désactivation de la validation, les privilèges sudo ne sont pas requis lorsque vous redémarrez le service de cluster Informatica. Pour arrêter cependant le service de cluster Informatica, l'autorisation sudo est toujours requise pour la commande `systemctl`.

Pour exécuter la commande `infacmd ics cleanCluster` afin de nettoyer le service de cluster Informatica, l'autorisation sudo doit être configurée pour les commandes `systemctl` et `rm`.

Remarque: Les services associés au service de cluster Informatica, tels qu'Apache Solr, PostgreSQL et Nomad nécessitent un utilisateur non racine disposant de privilèges sudo pour exécuter les services. Sudo permet à un utilisateur d'exécuter des programmes ou des commandes avec des privilèges élevés pendant une période spécifique. Enterprise Data Catalog nécessite un utilisateur non-racine avec des autorisations sudo pour exécuter certaines commandes lors de l'exécution de tâches administratives telles que l'installation, la mise à niveau et la surveillance du statut des services. Pour plus d'informations sur les commandes utilisées et le rôle de chaque commande lors de la mise à niveau, reportez-vous à l'article de la base de connaissances "[Configurer les privilèges Sudo pour l'utilisateur de la passerelle \(facultatif\)](#)" à la [page 66](#).

Effectuer la configuration SSL par défaut

Si le domaine Informatica est activé pour SSL à l'aide des certificats SSL par défaut, vous pouvez configurer le service de cluster Informatica et le service de catalogue pour utiliser le nouveau keystore.

Pour configurer les services afin d'utiliser le keystore 10.5.3, procédez comme suit :

1. Désactivez le service de cluster Informatica et le service de catalogue.
2. Modifiez les options de processus pour le service de cluster Informatica et le service de catalogue, et indiquez l'emplacement du fichier `Default.keystore` de la version 10.5.3. Le chemin d'accès par défaut au fichier est `<Informatica installation directory>/tomcat/conf/Default.keystore`.
3. À partir du fichier 10.5.3 `<Informatica installation directory>/services/shared/security/infactruststore.jks`, supprimez la valeur existante configurée pour l'alias `infactruststore` et importez le fichier `<Informatica installation directory>/tomcat/conf/Default.keystore`.
4. Activez le service de cluster Informatica et le service de catalogue.

Étape 6. Activer et mettre à niveau les services Enterprise Data Catalog

Activer le service de cluster Informatica

Pour activer le service d'application, sélectionnez-le dans Informatica Administrator et cliquez sur **Actions > Activer le service**.

Activer et mettre à niveau le service de catalogue

Pour activer et mettre à niveau le service de catalogue, sélectionnez celui-ci, puis cliquez sur **Activer le service** depuis le menu **Actions** dans Informatica Administrator.

Après avoir démarré le service de catalogue, Informatica Administrator vous invite à mettre à niveau le service de catalogue.

Effectuez les étapes suivantes :

1. Mettez à niveau le service de catalogue.
2. Activez le service de messagerie si vous aviez configuré le service pour le service de catalogue.

Remarque:

- Le programme d'installation inclut Azul JDK. Après la mise à niveau, Enterprise Data Catalog utilise Azul JDK sur tous les nœuds du cluster.
- Si vous avez activé l'analyse des actifs de données, le démarrage du service de catalogue prend plus de temps. Le service ne sera pas disponible avant la fin de la mise à niveau du référentiel d'analyse des actifs de données.
- Pour connaître l'état de la mise à niveau du référentiel de l'analyse des actifs de données, consultez le fichier `daa_upgrade.log` à partir du répertoire d'installation.
- Si vous avez activé l'analyse des actifs de données, exécutez [“Remplir les prérequis de l'analyse des actifs de données” à la page 47](#).

Étape 7. Migrer et vérifier les données du catalogue

Migrer les données du catalogue

Utilisez la commande `infacmd.sh LDM migrateContents` pour migrer les données que vous avez sauvegardées à l'aide de l'utilitaire `export`.

Effectuez les étapes suivantes pour migrer les données de catalogue :

1. Définissez les variables d'environnement suivantes :
 - `INFA_TRUSTSTORE`. Reportez-vous à l'exemple de commande suivant pour définir la variable `export`
`INFA_TRUSTSTORE= <Location of the Informatica truststore file>`. L'emplacement par défaut est `<Informatica installation directory>/services/shared/security`.

- **INFA_KEYSTORE.** Reportez-vous à l'exemple de commande suivant pour définir la variable : `export INFA_KEYSTORE=<Location of the keystore file>`. L'emplacement par défaut est `<Informatica installation directory>/services/shared/security`. Cette variable est requise uniquement si vous avez utilisé une configuration SSL personnalisée pour le domaine Informatica. Pour les configurations SSL et non-SSL par défaut, vous devez désactiver la variable.
- **INFA_TRUSTSTORE_PASSWORD.** Chiffrez le mot de passe que vous avez défini. Reportez-vous à l'exemple de commande suivant pour définir le mot de passe chiffré : `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA=="`.
- **INFA_KEYSTORE_PASSWORD.** Chiffrez le mot de passe que vous avez défini. Reportez-vous à l'exemple de commande suivant pour définir le mot de passe chiffré : `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI=="`. Cette variable est requise uniquement si vous avez utilisé une configuration SSL personnalisée pour le domaine Informatica. Pour les configurations SSL et non-SSL par défaut, vous devez désactiver la variable.

Vous pouvez contacter le support client international Informatica pour obtenir les mots de passe par défaut du truststore et du keystore.

Remarque: Reportez-vous à l'exemple de commande suivant pour chiffrer le mot de passe :

`<Informatica installation directory>/server/bin/pmpasswd <password>`

2. Si les données de catalogue exportées sont volumineuses, mettez à jour la propriété `xdocs.content.systemProperties=-Xmx20G` dans le fichier `<Informatica installation directory>/services/CatalogService/Binaries/MigrationModuleConfigurations.properties`, puis réinitialisez la propriété `ICMD_JAVA_OPTS=-Xmx20g` dans le fichier `<Informatica installation directory>/isp/bin/infacmd.sh`. Pour plus d'informations sur le dimensionnement des performances, reportez-vous au *Guide de réglage des performances d'Enterprise Data Catalog*.
3. Exécutez la commande `infacmd ldm migrateContents` comme indiqué : `./infacmd.sh ldm migrateContents -un <Informatica Domain User Name> -pd <Informatica Domain Password> -dn <Informatica Domain Name> -sn <Name of the Catalog Service> -id <Export Directory>`

Remarque: L'élément `<Export Directory>` signifie le répertoire dans lequel le contenu sauvegardé est disponible.

Pour régler les paramètres de performances pour migrer les données ou ignorer des ressources ayant échoué, modifiez les paramètres spécifiés dans le fichier `MigrationModuleConfigurations.properties` disponible à l'emplacement suivant : `<Informatica installation directory>/services/CatalogService/Binaries`

Pour plus d'informations sur les paramètres de performances, reportez-vous au tableau suivant :

Propriété	Description
<code>enableModule=</code>	Définissez la valeur sur <code>true</code> si vous souhaitez activer un module spécifique, sinon définissez la propriété sur <code>false</code> . Par exemple, <code>similarity.content.enableModule=true</code> permet la migration des données de profilage de similarité.
<code>Dblacklist =</code>	Répertoriez les ressources à ignorer au format suivant : <code>-Dblacklist=<resource name1>,<resource name2></code>
<code>DmaxParallelRestores=</code>	Spécifiez le nombre de threads à exécuter en parallèle lorsque vous migrez des données.
<code>systemProperties=</code>	Utilisez la propriété pour spécifier les ressources système à utiliser. Par exemple, <code>xdocs.content.systemProperties=-Xmx6G -XX:+HeapDumpOnOutOfMemoryError</code>

Vérifier les données de catalogue migrées

Vous pouvez utiliser la commande `infacmd migrateContents -verify` comme indiqué dans l'exemple suivant pour vérifier le contenu migré : `./infacmd.sh LDM migrateContents -un Administrator -pd Administrator -dn Domain -sn CS -id /data/Installer1050/properties/utils/upgrade/EDC/export -verify`.

Pour plus d'informations sur la syntaxe, les paramètres et la description de la commande, consultez le *Guide de référence des commandes d'Informatica*.

Après avoir exécuté la commande `infacmd migrateContents -verify`, celle-ci génère un fichier nommé `results.txt`.

Le tableau suivant décrit les messages qui s'affichent dans le fichier `results.txt` :

Message d'erreur	Description
missing from backup	Indique que certaines ressources ont été analysées avant de vérifier les données de catalogue migrées.
missing from warehouse	Indique que les actifs n'étaient pas compris dans la version 10.5.3.

Remarque: Assurez-vous que la ressource n'est pas purgée ou rechargée avant de vérifier les données de catalogue migrées.

CHAPITRE 4

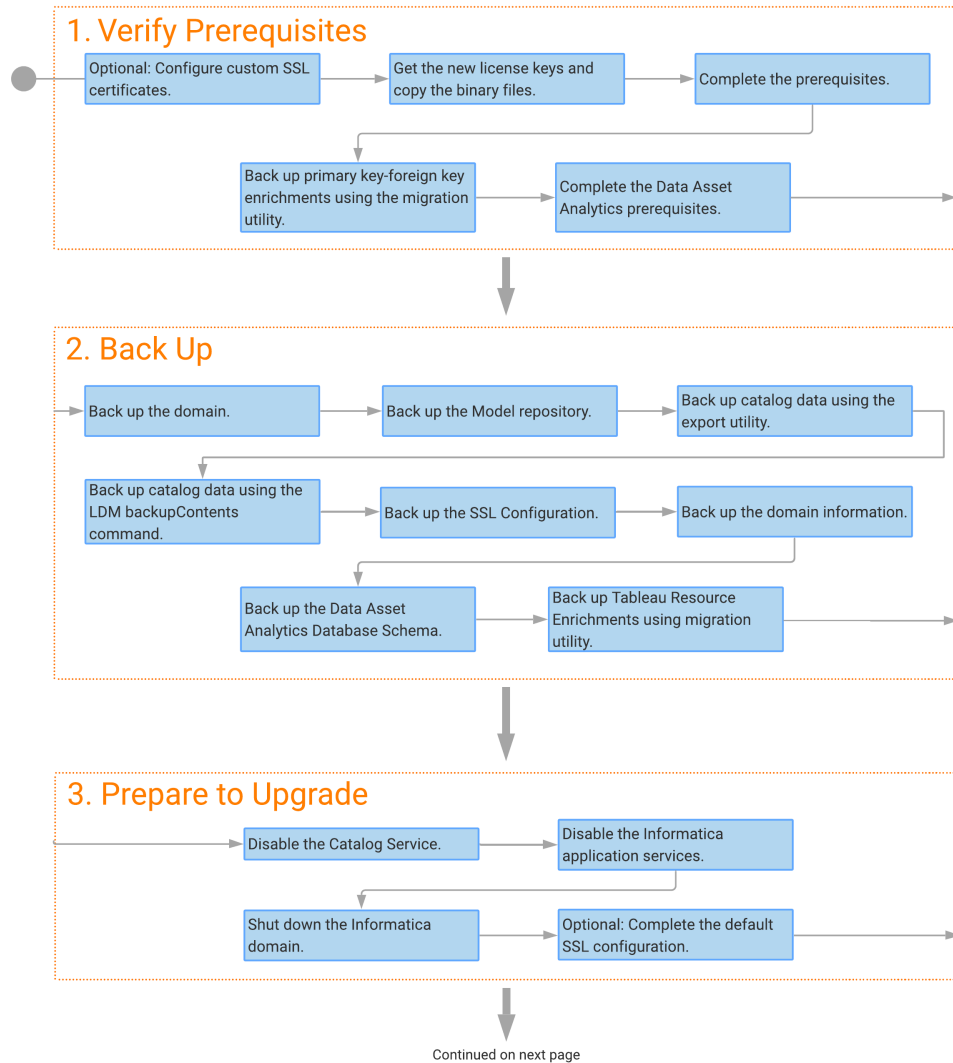
Mettre à niveau Enterprise Data Catalog dans un cluster externe

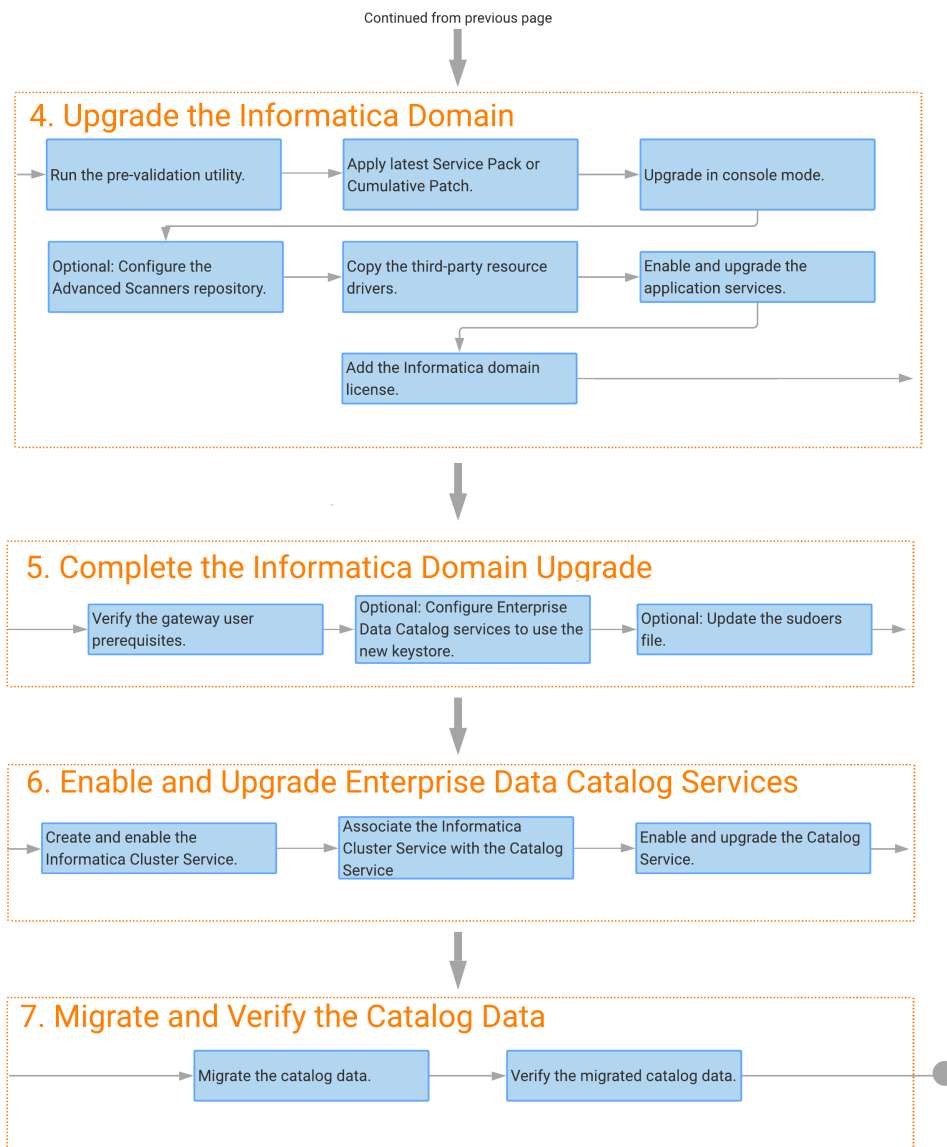
Ce chapitre comprend les rubriques suivantes :

- [Mettre à niveau Enterprise Data Catalog dans un cluster externe, 72](#)
- [Étape 1. Vérifier les prérequis de la mise à niveau , 73](#)
- [Étape 2. Sauvegarder les référentiels et les détails de configuration, 86](#)
- [Étape 3. Préparer la mise à niveau, 91](#)
- [Étape 4. Mettre à niveau le domaine Informatica, 91](#)
- [Étape 5. Effectuer la mise à niveau du domaine Informatica, 101](#)
- [Étape 6. Activer et mettre à niveau les services Enterprise Data Catalog , 102](#)
- [Étape 7. Migrer et vérifier les données du catalogue , 108](#)

Mettre à niveau Enterprise Data Catalog dans un cluster externe

L'image suivante montre les étapes que vous devez effectuer pour mettre à niveau Enterprise Data Catalog :





Étape 1. Vérifier les prérequis de la mise à niveau

Avant de démarrer la mise à niveau en tant qu'utilisateur non-racine avec des privilèges sudo, validez les prérequis suivants :

- Vérifiez qu'au moins 100 Go d'espace disque libre sont disponibles sur la machine sur laquelle le domaine Informatica s'exécute.
- Vérifiez que Java Development Kit (JDK) 1.8 est installé.
- Si le cluster est activé pour Kerberos et SSL, sauvegardez les fichiers truststore et keystore par défaut du domaine Informatica.

- Vérifiez que la connexion au référentiel de configuration du domaine est disponible pendant la mise à niveau.
- Vérifiez que ntpd est synchronisé entre le nœud de domaine Informatica et les nœuds de cluster.
- Si vous effectuez une mise à niveau à partir d'un cluster activé pour Kerberos et SSL, effectuez une sauvegarde du truststore de domaine Informatica et des fichiers keystore par défaut.
- Installez les applications et les packages suivants sur tous les nœuds avant de mettre à niveau Enterprise Data Catalog :
 - Bash Shell
 - rsync
 - libcurl
 - xz-libs
 - systemctl
 - zip
 - unzip
 - tar
 - wget
 - scp
 - rpm
 - curl
 - nslookup
 - md5sum
 - netstat
 - ping
 - ifconfig
 - cksum
 - dnsdomainname
 - libncurses5
 - OpenSSL version 1.0.1e-30.el6_6.5.x86_64 ou versions ultérieures.

OpenSSL 3.0 n'est pas pris en charge.

Vérifiez que la variable \$PATH pointe vers le répertoire `/usr/bin` pour utiliser la version correcte de Linux OpenSSL.

Dans les versions 10.5.1.0.1 et ultérieures, rsync est utilisé à la place de scp pour les transferts de fichiers.

Dans les versions 10.5.1.0.2 et ultérieures, le paramètre MaxStartups dans le fichier de configuration du serveur SSH est validé. Le nombre maximal de connexions SSH simultanées non authentifiées doit être défini sur une valeur supérieure ou égale à 30. Pour définir la valeur de ce paramètre sur 30, ouvrez le fichier `/etc/ssh/sshd_config`, passez la valeur du paramètre MaxStartups à 30:30:100, puis redémarrez le démon sshd.

Remarque: Les connexions SSH non authentifiées sont des connexions de socket au démon SSH qui sont établies sans authentification de l'utilisateur.

- Le tableau suivant répertorie les ports par défaut qui doivent être disponibles pour le service de cluster Informatica :

Service	Port par défaut
HTTP/HTTPS	9075
Serf Nomad	4648
HTTP Nomad	4646
RPC Nomad	4647
ZooKeeper	2181
Homologue ZooKeeper	2888
Leader ZooKeeper	3888
Solr	8983
MongoDB	27017
PostgreSQL	5432

- Si vous avez configuré le référentiel de MetaDex, sauvegardez la base de données du référentiel MetaDex.

Remarque: Si vous effectuez une mise à niveau à partir de la version 10.4.1.3.3 ou antérieure vers la version 10.5.3 et si vous avez utilisé la propriété `scanners.executions.max` dans le fichier `server.properties`, renommez-la en `scanners.server.execution.slots`.

La mémoire par défaut du serveur MetaDex est de 4 Go.

- Supprimez les valeurs configurées pour les variables d'environnement suivantes à l'aide de la commande `unset` :
 - INFA_HOME
 - INFA_DOMAINS_FILE
 - DISPLAY
 - JRE_HOME
 - INFA_TRUSTSTORE
 - INFA_TRUSTSTORE_PASSWORD
- Vérifiez que les variables d'environnement `LD_LIBRARY_PATH` et `PATH` ne contiennent pas de versions précédentes d'Informatica.
- Supprimez le fichier JAR suivant des nœuds sur lesquels le service de catalogue s'exécute : `<Informatica Installation Directory>/logs/<NodeName> /services/CatalogService/<CatalogServiceName>/migrate/restore.jar`.

- À partir de la version 10.5, le framework de connectivité universelle (UCF, Universal Connectivity Framework) est déconseillé. Pour utiliser les ressources UCF que vous aviez configurées dans les versions antérieures, copiez les fichiers JAR de l'UCF de l'emplacement d'installation existant vers le nouvel emplacement de mise à niveau : `<$INFA_HOME>/services/CatalogService/ScannerJars/bin`.

Remarque: Les fichiers JAR d'UCF comprennent le modèle du fichier `com.infa.ldm.extended.*.jar`.

Après avoir mis à niveau le service de catalogue, les ressources UCF existantes sont répertoriées dans la boîte de dialogue **Sélectionner le type de ressource** de Catalog Administrator.

Remarque: Conservez un enregistrement du nombre d'actifs du catalogue, de Catalog Administrator et du tableau de bord de l'analyse des actifs de données pour référence. Vous pouvez utiliser l'API REST `/data/search` pour afficher le nombre d'actifs au format JSON, comme indiqué dans l'exemple suivant : `http://<CatalogAdmin>:<port>/access/2/catalog/data/search?defaultFacets=false&disableSemanticSearch=true&enableLegacySearch=false&facet=true&facetId=core.classType&facetId=core.resourceName&facetId=core.resourceType&highlight=false&includeRefObjects=false&offset=0&pageSize=1&q=* &tabId=all`.

Pour plus d'informations, reportez-vous à la *Référence des API REST d'Enterprise Data Catalog*.

Si vous utilisez Axon Data Governance avec Enterprise Data Catalog, assurez-vous qu'Axon SuperAdmin a désactivé le travail d'intégration des actifs et le travail de récupération des liens de référence avant la mise à niveau. Pour plus d'informations, reportez-vous à l'[Informatica Knowledge Base article](#).

Configurer les certificats SSL personnalisésPrésentation

Lors d'une installation ou d'une mise à niveau, vous pouvez utiliser les certificats SSL de votre choix, appelés certificats SSL personnalisés, pour sécuriser les composants associés au service de cluster Informatica. Vous pouvez choisir d'utiliser des certificats SSL personnalisés signés par une autorité de certification ou des certificats SSL personnalisés auto-signés comme certificats de client et de cluster.

Si vous choisissez d'utiliser des certificats SSL personnalisés signés par une autorité de certification, utilisez les scripts `generate_csr.sh` et `generate_certs.sh` pour générer les certificats requis.

Si vous choisissez d'utiliser des certificats SSL personnalisés auto-signés, utilisez l'utilitaire SSL personnalisé fourni avec le programme d'installation pour générer les certificats requis.

Exigences d'activation des certificats SSL personnalisés

Avant d'activer SSL personnalisé pour Enterprise Data Catalog, sécurisez le domaine Informatica à l'aide de certificats SSL personnalisés.

Vérifiez les prérequis suivants pour le domaine Informatica :

- Les fichiers `truststore` et `keystore` personnalisés sont placés dans un répertoire personnalisé. Le nom du fichier `truststore` doit être `infa_truststore.jks`.
- Le répertoire qui stocke les fichiers `keystore` et `truststore` est accessible aux programmes de ligne de commande.

Important: Le programme d'installation place les fichiers par défaut `infa_truststore.jks` et `keystore` dans le répertoire `<Informatica installation directory>/services/shared/security` sur chaque nœud. Ne remplacez pas les fichiers `truststore` et `keystore` par défaut, ne les supprimez pas, ni ne les déplacez. Ne placez pas les fichiers `truststore` et `keystore` personnalisés dans le répertoire.

Pour savoir comment convertir un domaine Informatica non-SSL en un domaine Informatica compatible SSL, reportez-vous à l'article de la base de connaissances

[Convert a non-SSL Informatica domain to an SSL-enabled Informatica domain](#).

Générer des certificats SSL personnalisés signés par une autorité de certification (CA)

Vous disposez d'un certificat SSL personnalisé pour le domaine Informatica, et vous souhaitez utiliser les certificats SSL signés par l'autorité de certification en tant que certificats clients et de cluster pour le service de cluster Informatica.

Utilisez les scripts `generate_csr.sh` et `generate_certs.sh` pour générer la demande de signature de certificat (CSR, Certificate Signing Request) à envoyer à une autorité de certification (CA) et générer les certificats SSL requis. Vous pouvez télécharger les scripts à partir d'Akamai Download Manager.

Effectuez les étapes suivantes pour utiliser les scripts afin de générer les certificats :

1. Extrayez les scripts `generate_csr.sh` et `generate_certs.sh` de l'emplacement suivant : `<Location of installer files>/properties/utils/CustomSSLScriptsUtil_ExternalCA`.
2. Définissez la variable d'environnement `JAVA_HOME` pour qu'elle pointe vers JDK 8.
3. Dans le fichier `gen_csr.properties`, indiquez les valeurs des paramètres suivants :

Paramètre	Description
<code>Infadomainkeystorepassword</code>	Mot de passe du keystore de domaine Informatica en texte brut.
<code>ServerHosts</code>	Hôtes du service de cluster Informatica qui incluent les nœuds de données, les nœuds de traitement et le nœud de passerelle. Entrez une liste de noms de domaine complets (FQDN) séparée par des virgules de nœuds de cluster.
<code>ClientHosts</code>	Liste des noms d'hôtes uniques séparée par des virgules des nœuds de domaine et des nœuds de cluster.
<code>Infadomainname</code>	Nom de domaine Informatica.
<code>ICSServiceName</code>	Nom du service de cluster Informatica.
<code>KeysOutputDir</code>	Répertoire de stockage des clés générées. Spécifiez le répertoire <code>\$CUSTOM KEYSTORE LOC</code> pour éviter les étapes supplémentaires de copie des clés générées. Les répertoires <code>\$ICS SERVICENAME/client_certs</code> et <code>\$ICS SERVICENAME/cluster_certs</code> sont créés sous le répertoire <code>\$CUSTOM KEYSTORE LOC</code> . <code>\$CUSTOM KEYSTORE LOC</code> est le répertoire où se trouve le keystore personnalisé pour le domaine Informatica (<code>infa_keystore.jks</code>). <code>\$ICS SERVICENAME</code> est le nom du service de cluster Informatica.
<code>CertsOutputDir</code>	Répertoire <code>\$CUSTOM TRUSTSTORE LOC</code> de stockage des fichiers truststore générés. Les répertoires <code>\$ICS SERVICENAME/client_certs</code> et <code>\$ICS SERVICENAME/cluster_certs</code> sont créés sous le répertoire <code>\$CUSTOM TRUSTSTORE LOC</code> . <code>\$CUSTOM TRUSTSTORE LOC</code> est le répertoire dans lequel se trouve le truststore personnalisé pour le domaine Informatica (<code>infa_truststore.jks</code>).
<code>DNSDomainName</code>	Nom de domaine DNS pour les nœuds de cluster.
<code>ClusterCert_OrganizationUnit</code>	Facultatif. Valeur du paramètre <code>OrganizationUnit</code> pour le certificat des nœuds de cluster.

Paramètre	Description
ClusterCert_Organization	Valeur du paramètre Organisation pour le certificat des nœuds de cluster. Remarque: Vérifiez que la combinaison des paramètres Organisation (O) et Unité d'organisation (OU) dans l'objet du certificat est distincte pour les certificats clients et de cluster
ClusterCert_Location	Valeur du paramètre Emplacement pour le certificat des nœuds de cluster.
ClusterCert_State	Valeur du paramètre État pour le certificat des nœuds de cluster.
ClusterCert_CountryCode	Valeur du paramètre Code de pays pour le certificat des nœuds de cluster.
DomainCert_OrganizationUnit	Facultatif. Valeur du paramètre Unité d'organisation pour le certificat des nœuds de domaine.
DomainCert_Organization	Valeur du paramètre Organisation pour le certificat des nœuds de domaine. Remarque: Vérifiez que la combinaison des paramètres Organisation (O) et Unité d'organisation (OU) dans l'objet du certificat est distincte pour les certificats clients et de cluster
DomainCert_Location	Facultatif. Valeur du paramètre Emplacement pour le certificat des nœuds de domaine. La valeur par défaut est le paramètre ClusterCert_Location.
DomainCert_State	Facultatif. Valeur du paramètre État pour le certificat des nœuds de domaine. La valeur par défaut est le paramètre ClusterCert_State.
DomainCert_CountryCode	Facultatif. Valeur du paramètre Code de pays pour le certificat des nœuds de domaine. La valeur par défaut est le paramètre ClusterCert_CountryCode.
Custom_Server_Certificate_CN	Facultatif. Valeur du paramètre Nom commun dans le certificat des nœuds de cluster qui peut être utilisée à la place de l'élément \$InfaDomainName-\$ICSServiceName par défaut. Valeur \$DNSDomainName. Remarque: Vous devez entrer des valeurs conformes à RFC2253. Les caractères spéciaux suivants ne sont pas pris en charge : , + " \ < > ;. Les guillemets (") doivent être utilisés par paires. Les caractères \ et " ne doivent pas être utilisés conjointement. La valeur ne peut contenir aucun espace.
Custom_Client_Certificate_CN	Facultatif. Valeur du paramètre Nom commun dans le certificat des nœuds de domaine qui peut être utilisée à la place de l'élément \$InfaDomainName-\$ICSServiceName par défaut. Valeur \$DNSDomainName. La valeur par défaut est le paramètre Custom_Server_Certificate_CN. Remarque: Vous devez entrer des valeurs conformes à RFC2253. Les caractères spéciaux suivants ne sont pas pris en charge : , + " \ < > ;. Les guillemets (") doivent être utilisés par paires. Les caractères \ et " ne doivent pas être utilisés conjointement. La valeur ne peut contenir aucun espace.

Remarque: Si les valeurs contiennent des espaces ou des caractères spéciaux, vous devez placer les valeurs entre guillemets doubles.

- Exécutez le script `generate_csr.sh` à l'aide de la commande suivante pour générer les fichiers `.csr` à envoyer à une autorité de certification (CA) externe : `./generate_csr.sh gen_csr.properties`
Les fichiers suivants sont générés pour le cluster :

infa_nodecert.csr
infa_privkey.key
infa_privkey.pem
keystore.jks

Les fichiers suivants sont générés pour le client :

infa_nodecert.csr
infa_privkey.key
infa_privkey.pem
keystore.jks
browser_cert.csr
browser_keystore.jks
browser_privkey.key
browser_privkey.pem

5. Validez le contenu des fichiers .csr. Exécutez la commande suivante pour afficher le contenu : `keytool -printcertreq -file $PATH TO CSR`

6. Envoyez les fichiers .csr suivants à une autorité de certification (CA) à des fins de signature :

- `<CertsOutputDir>/<ICSServiceName>/client_certs/infa_nodecert.csr`
- `<CertsOutputDir>/<ICSServiceName>/cluster_certs/infa_nodecert.csr`
- `<CertsOutputDir>/<ICSServiceName>/client_certs/browser_cert.csr`

Remarque: Le fichier browser_cert.csr est requis si vous souhaitez créer les certificats de navigateur pour afficher les journaux du travail d'analyse sur Nomad.

7. Après avoir reçu les certificats ou les chaînes de certificats de l'autorité de certification (CA) au format .pem, "[Valider les certificats signés par une autorité de certification \(CA\)](#)" à la page 43 et stockez-les dans un emplacement sous le répertoire \$INFA_HOME sur votre machine.

Remarque: Si vous recevez les certificats ou les chaînes de certificats de l'autorité de certification (CA) au format .cer, exécutez la commande suivante pour convertir les fichiers au format pem : `openssl x509 -inform der -in <certificate file name>.cer -outform pem -out <certificate file name>.pem`.

Si vous recevez une chaîne de certificats de l'autorité de certification (CA), vous devez extraire le certificat racine, les certificats intermédiaires et le certificat d'utilisateur final.

8. Dans le fichier gen_csr.properties, indiquez les valeurs des paramètres suivants :

Paramètre	Description
InfaDomainKeystorePassword	Mot de passe du keystore de domaine Informatica en texte brut.
InfaDomainTruststorePassword	Mot de passe du truststore de domaine Informatica en texte brut.
ClusterCertificate	Chemin d'accès au certificat de cluster signé par l'autorité de certification (CA) au format .pem. Il s'agit d'un certificat d'utilisateur final.

Paramètre	Description
ClientCertificate	Chemin d'accès au certificat client signé par l'autorité de certification (CA) au format .pem. Il s'agit d'un certificat d'utilisateur final.
BrowserCertificate	Chemin d'accès au certificat de navigateur signé par l'autorité de certification (CA) au format .pem.
ICSServiceName	Nom du service de cluster Informatica.
IsCACertificateChainAvailable	Spécifiez si la chaîne de certificats de l'autorité de certification (CA) est disponible sous forme de fichier .pem unique. Entrez true ou false. Remarque: La chaîne de certificats doit contenir uniquement les certificats racine et intermédiaires.
SingleCACertificateChain	Chemin d'accès à la chaîne de certificats de l'autorité de certification (CA) au format .pem.
IndividualCertificatesFromCACHain	Facultatif. Uniquement nécessaire si le paramètre IsCACertificateChainAvailable est défini sur false. Chemins séparés par des virgules vers les certificats publics dans la chaîne de certificats de l'autorité de certification (CA) au format .pem si la chaîne de certificats CA complète est disponible sous forme de fichiers .pem individuels.
KeysOutputDir	Répertoire \$CUSTOM KEYSTORE LOC de stockage des clés générés. Les répertoires \$ICS SERVICENAME/client_certs et \$ICS SERVICENAME/cluster_certs sont créés sous le répertoire \$CUSTOM KEYSTORE LOC. \$CUSTOM KEYSTORE LOC est le répertoire où se trouve le keystore personnalisé pour le domaine Informatica (infa_keystore.jks). \$ICS SERVICENAME est le nom du service de cluster Informatica
CertsOutputDir	Répertoire \$CUSTOM TRUSTSTORE LOC de stockage des fichiers truststore générés. Les répertoires \$ICS SERVICENAME/client_certs et \$ICS SERVICENAME/cluster_certs sont créés sous le répertoire \$CUSTOM TRUSTSTORE LOC. \$CUSTOM TRUSTSTORE LOC est le répertoire dans lequel se trouve le truststore personnalisé pour le domaine Informatica (infa_truststore.jks).

9. Exécutez le script generate_certs.sh à l'aide de la commande suivante pour générer les certificats : `./generate_certs.sh gen_certs.properties`
Le keystore keystore.jks et les clés privées infa_privkey.pem sont stockés dans les répertoires \$CUSTOM KEYSTORE LOC/\$ICSServiceName/client_certs et \$CUSTOM KEYSTORE LOC/\$ICSServiceName/cluster_certs.
Le truststore truststore.jks truststore et les clés publiques infa_nodecert.pem, infa_nodecertkey.pem et infa_pubcert.pem sont stockés dans les répertoires \$CUSTOM TRUSTSTORE LOC/\$ICSServiceName/client_certs et \$CUSTOM TRUSTSTORE LOC/\$ICSServiceName/cluster_certs.

10. Facultatif. Les répertoires \$CUSTOM KEYSTORE LOC et \$CUSTOM TRUSTSTORE LOC sont généralement les mêmes. Si l'emplacement <KeysOutputDir> est différent de \$CUSTOM KEYSTORE LOC et que l'emplacement <CertsOutputDir> est différent de \$CUSTOM TRUSTSTORE LOC, déplacez les clés et les certificats vers les répertoires correspondants.

Remarque: Vérifiez que les répertoires \$CUSTOM KEYSTORE LOC et \$CUSTOM TRUSTSTORE LOC disposent des privilèges d'utilisateur requis. Vérifiez également que l'utilisateur dispose des autorisations chmod 700 minimales configurées pour les répertoires et des autorisations chmod 600 configurées pour les fichiers copiés dans les répertoires.

Pour accéder à l'interface utilisateur (IU) Web Nomad et à l'IU d'administration Solr lorsque le service de cluster Informatica est activé pour SSL, vous devez importer les certificats du navigateur. Pour en savoir plus sur l'importation des certificats de navigateur, reportez-vous à l'article de la base de connaissances ["Générer des certificats SSL personnalisés signés par une autorité de certification \(CA\)" à la page 77](#).

Valider les certificats signés par une autorité de certification (CA)

Vous devez utiliser une seule autorité de certification (CA) pour les certificats clients et de cluster. Après avoir reçu les certificats signés de l'autorité de certification (CA), vous devez vérifier que chaque certificat est un certificat X.509 au format .pem.

Exécutez la commande suivante pour afficher le contenu des certificats clients et de cluster signés : `keytool -printcert -file $PATH TO CERTIFICATE PEM FILE`.

Validez les conditions requises suivantes pour les certificats clients et de cluster :

Prérequis	Configuration requise du certificat
Champs obligatoires	<p>Pour le certificat de cluster, tenez compte de la configuration requise de l'utilisation de clé suivante :</p> <p>keyUsage = digitalSignature,keyEncipherment extendedKeyUsage = serverAuth,clientAuth</p> <p>Pour le certificat client, tenez compte de la configuration requise de l'utilisation de clé suivante :</p> <p>keyUsage = digitalSignature extendedKeyUsage = clientAuth</p>
Autre nom du sujet (SAN, Subject Alternate Name)	<p>Pour le certificat de cluster, le SAN doit comprendre la liste des nœuds de cluster au format suivant : SAN=DNS:\$CLUSTER HOST1 FQDN,DNS:\$CLUSTER HOST2 FQDN,DNS:\$CLUSTER HOST3 FQDN</p> <p>Le certificat client doit contenir les noms de domaine complets (FQDN) pour les nœuds de cluster.</p> <p>Pour le certificat client, le SAN doit comprendre la liste de tous les nœuds Informatica au format suivant : SAN=DNS:\$INFA DOMAIN HOST1 FQDN,DNS:\$INFA DOMAIN HOST2 FQDN</p> <p>Le certificat client doit contenir les noms de domaine complets (FQDN) pour les nœuds de domaine et de cluster.</p>

CLUSTER HOST FQDN représente le nom de domaine complet pour l'hôte de passerelle de cluster, les nœuds de traitement et les nœuds de données dans le cluster.

INFA DOMAIN HOST FQDN représente le nom de domaine complet de l'hôte de passerelle de domaine Informatica, des nœuds de domaine, de l'hôte de passerelle de cluster, des nœuds de traitement et des nœuds de données dans le cluster.

Remarque: Vérifiez que l'emplacement du certificat personnalisé pour les nœuds de domaine contient le fichier infa_truststore.pem. Vérifiez également que tous les certificats de la chaîne de certificats d'autorité de certification (CA) sont présents dans les fichiers truststore.jks et infa_pubcert.pem.

Générer des certificats SSL personnalisés auto-signés

Vous disposez d'un certificat SSL personnalisé pour le domaine Informatica, et vous souhaitez utiliser les certificats SSL personnalisés auto-signés en tant que certificats clients et de cluster pour le service de cluster Informatica.

Utilisez l'utilitaire SSL personnalisé fourni avec le programme d'installation pour générer les certificats SSL requis.

Effectuez les étapes suivantes pour utiliser l'utilitaire SSL personnalisé afin de générer les certificats :

1. Extrayez `GenerateCustomSslUtility.zip` de l'emplacement suivant : `<Location of installer files>/properties/Utils/CustomSslCertsUtility/`.
2. Définissez la variable d'environnement `JAVA_HOME` pour qu'elle pointe vers JDK 8.
3. Configurez les paramètres suivants dans le fichier `input.properties` que vous avez extrait du fichier `GenerateCustomSslUtility.zip` :

Paramètre	Description
KeystoreFile	Chemin d'accès au fichier keystore personnalisé avec le nom du fichier. Le type de keystore doit être au format JKS. Format X509. Le fichier doit contenir une seule entrée de clé privée avec la chaîne de certificats complète. Vérifiez que le fichier dispose de la capacité de signature.
-KeystorePassword	Mot de passe du fichier keystore personnalisé au format texte brut.
TruststoreFile	Chemin d'accès au fichier truststore personnalisé avec le nom du fichier. Le type de truststore doit être au format JKS. Format X509. Le fichier doit contenir les certificats publics correspondant à l'entrée de clé privée dans le fichier keystore.
TruststorePassword	Mot de passe du fichier truststore personnalisé au format texte brut.
ISPDomainKeystorePassword	Mot de passe du keystore du domaine Informatica au format texte brut. L'utilitaire utilise le mot de passe du cluster et le fichier <code>keystore.jks</code> du client.
ISPDomainTruststorePassword	Mot de passe du truststore du domaine Informatica au format texte brut. L'utilitaire utilise le mot de passe du cluster et le fichier <code>truststore.jks</code> du client.
KeystoreOutputDir	Représente l'emplacement du keystore personnalisé du domaine Informatica que vous avez fourni lors de l'installation d'Enterprise Data Catalog.
TruststoreOutputDir	Représente l'emplacement du truststore personnalisé du domaine Informatica que vous avez fourni lors de l'installation d'Enterprise Data Catalog. Remarque: Vérifiez que les paramètres <code>KeystoreOutputDir</code> et <code>TruststoreOutputDir</code> pointent vers le même répertoire.
ServerNodes	Liste des noms de domaine complets séparée par des virgules des nœuds à configurer en tant que nœuds de données, nœuds de traitement, hôtes de service et nœud de passerelle lors de la configuration du service de cluster Informatica.
IcsServiceName	Nom du service de cluster Informatica.

Paramètre	Description
ClientNodes	Liste des noms de domaine complets séparée par des virgules des nœuds à configurer en tant qu'hôtes de domaine Informatica, nœuds de données, nœuds de traitement, hôtes de service et nœud de passerelle.
IspDomainName	Nom de domaine Informatica.
ClusterNodeDNSDomain	Nom de domaine de l'hôte de passerelle à configurer pour le service de cluster Informatica.

4. Exécutez l'utilitaire à l'aide de la commande suivante : `java -jar GenerateCustomSslUtility.jar -in input.properties`. L'utilitaire génère les clés et les certificats clients et de cluster suivants :

- Clés :

- keystore.jks
- infa_privkey.pem

Remarque: Les clés de cluster sont générées dans le répertoire suivant : `<Keystore output directory>/<IcsServiceName>/cluster_certs`. Les clés de client sont générées dans le répertoire suivant : `<Keystore output directory>/<IcsServiceName>/client_certs`

- Certificats :

- truststore.jks
- infa_pubcert.pem
- infa_nodecert.pem
- infa_nodecertkey.pem

Remarque: Les certificats de cluster sont générés dans le répertoire suivant : `<Truststore output directory>/<IcsServiceName>/cluster_certs`. Les certificats clients sont générés dans le répertoire suivant : `<Truststore output directory>/<IcsServiceName>/client_certs`

5. Copier les certificats générés dans les dossiers requis.

6. Attribuez la propriété des répertoires suivants à l'utilisateur du domaine Informatica :

- `<Keystore output directory>/<IcsServiceName>/cluster_certs`
- `<Truststore output directory>/<IcsServiceName>/cluster_certs`
- `<Keystore output directory>/<IcsServiceName>/client_certs`
- `<Truststore output directory>/<IcsServiceName>/client_certs`

Remarque: Vérifiez que tous les certificats clients sont inclus dans un seul répertoire. Vérifiez également que tous les certificats de cluster sont inclus dans un seul répertoire. Vous devez également vérifier que les répertoires disposent de l'autorisation `chmod 700` et que l'autorisation `chmod 600` est configurée dans les fichiers sous les répertoires.

Vérifier la somme de contrôle du package d'installation sur

Avant d'exécuter le programme d'installation des services, vérifiez l'intégrité du package d'installation via la commande `cksum`. La commande `cksum` calcule la valeur de la somme de contrôle pour les programmes d'installation.

Vérifiez la somme de contrôle des fichiers du programme d'installation spécifiques par rapport à celle des fichiers d'installation téléchargés depuis Akamai.

Le tableau suivant répertorie la somme de contrôle et la taille de fichier des services Informatica pour UNIX :

Fichier	Valeur de la somme de contrôle	Taille du fichier
informatica_1053_server_linux-x64.tar	2154528627	11639828480

Une incompatibilité de somme de contrôle peut se produire en cas d'erreurs de données pendant le téléchargement en raison de problèmes de réseau ou en cas de corruption des données dans le fichier sur le disque. Pour plus d'informations sur les propriétés de la somme de contrôle, reportez-vous à la section [HOW TO: Identify file errors after downloading Informatica installation files](#).

Obtenir les clés de licence et copier les fichiers binaires

Avant de démarrer la mise à niveau, procédez comme suit :

- Obtenez les nouvelles clés de licence pour le domaine Informatica et le service de cluster Informatica.
- Copiez les fichiers binaires du programme d'installation à partir de l'emplacement de téléchargement d'Akamai mentionné dans l'e-mail de confirmation et extrayez les fichiers dans un répertoire de la machine sur laquelle vous prévoyez de mettre à niveau Enterprise Data Catalog. Vous devez disposer des autorisations de lecture et d'écriture sur le répertoire des fichiers du programme d'installation et des autorisations d'exécution sur le fichier exécutable.
- Copiez les fichiers binaires du scanner à partir de l'emplacement de téléchargement d'Akamai et placez-les dans le répertoire suivant : `<Location where you extracted the installer binary files>/source`

Effectuer les tâches prérequis

Avant de mettre à niveau le domaine Informatica, effectuez les prérequis tels que le téléchargement des fichiers du programme d'installation et la copie des fichiers binaires requis.

- Téléchargez le fichier d'installation à partir du lien FTP que contient votre e-mail de commande. Téléchargez le fichier TAR d'installation d'Informatica sur le site Informatica Electronic Software Download vers un répertoire sur votre machine, puis extrayez les fichiers du programme d'installation. Extrayez les fichiers du programme d'installation dans un répertoire situé sur votre machine. L'utilisateur qui exécute le programme d'installation doit disposer d'autorisations de lecture et d'écriture sur le répertoire qui contient les fichiers du programme d'installation et d'autorisations d'exécution sur le fichier exécutable.
- Copiez les nouveaux fichiers binaires du scanner d'Akamai Download Manager sur votre répertoire d'installation.
- Effacez les valeurs configurées des variables d'environnement `INFA_TRUSTSTORE` et `INFA_TRUSTSTORE_PASSWORD` si le domaine est activé pour SSL (Secure Sockets Layer).
- Téléchargez et installez la bibliothèque `libidn.so. 11` si vous utilisez RHEL 8.3.

Sauvegarder les enrichissements de clé à l'aide de l'utilitaire de migration

Pour utiliser les améliorations ajoutées aux enrichissements de clé primaire-clé étrangère dans Enterprise Data Catalog version 10.5.3, sauvegardez les enrichissements à l'aide de l'utilitaire de migration avant d'effectuer une mise à niveau.

Effectuez les étapes suivantes pour exécuter l'utilitaire :

1. Depuis Akamai Download Manager, téléchargez et extrayez le fichier `Informatica_1053_PkFkEnrichmentMigrationUtility.zip` sur la machine du domaine.
2. Exécutez la commande suivante :

```
java -jar PKFkEnrichmentsRestoreUtility.jar export <Catalog Service hostname>  
<Catalog Service admin port number> <username> <password> <location to download  
enrichments json> <comma separated resource type IDs> <SSL Enabled true false>
```

Remarque: Vérifiez que la longueur du nom de la ressource ne dépasse pas la longueur maximale du nom de fichier prise en charge par le système d'exploitation.

Remplir les prérequis de l'analyse des actifs de données

Si vous avez configuré l'analyse des actifs de données pour Enterprise Data Catalog, vous devez configurer le délai d'expiration de l'arrêt du processus avant d'arrêter le domaine Informatica pour une mise à niveau. Vous devez exécuter l'utilitaire d'analyse des actifs de données avant d'effectuer une mise à niveau vers Enterprise Data Catalog 10.5.3.

Configurer le délai d'expiration du processus

1. Dans l'outil Administrator tool, accédez à la section des propriétés personnalisées du domaine.
2. Ajoutez la propriété personnalisée suivante :
`ProcessTerminationTimeout=900`
3. Arrêtez les services Informatica à l'aide de la commande `infaservice.sh shutdown`.
4. Démarrez les services Informatica à l'aide de la commande `infaservice.sh startup`.

Vérifiez que la taille de fichier de la transaction ou des fichiers journaux de rétablissement pour la base de données du référentiel de l'analyse des actifs de données est suffisamment grande. Pour une base de données Oracle, assurez-vous que la base de données contient au moins trois fichiers journaux de rétablissement de 2 Go chacun.

Exécuter l'utilitaire d'analyse des actifs de données

L'analyse des actifs de données affiche des mesures clés et des graphiques clés dans les onglets du tableau de bord en fonction de données analytiques précalculées. Avant d'effectuer la mise à niveau, vous devez remplir les tables de base de données précalculées à l'aide de données analytiques.

Effectuez les étapes suivantes pour exécuter l'utilitaire d'analyse des actifs de données :

1. Sauvegardez le schéma de base de données de l'analyse des actifs de données.
2. Vérifiez le fichier journal `daa.log` et assurez-vous qu'il n'existe aucun d'événement d'actif de données non traité pour éviter de perdre des données d'événements telles que les connexions utilisateur, les recherches et l'utilisation des actifs.
3. Depuis Akamai Download Manager, téléchargez et extrayez le fichier `informatica_1053_daa_utility.zip` sur le domaine Informatica.

Remarque: Si vous avez appliqué un Service Pack, vous devez télécharger l'utilitaire correspondant à la version du Service Pack.

4. Accédez au répertoire d'extraction des fichiers et au répertoire `config`.

- Ouvrez le fichier `input.properties` et configurez les paramètres de connexion suivants pour le référentiel d'analyse des actifs de données.

Propriété	Description
<code>databaseType</code>	Type de base de données de l'outil Analyse des actifs de données. Entrez ORACLE, POSTGRESQL ou SQLSERVER.
<code>databaseHostName</code>	Nom d'hôte complet de la machine sur laquelle la base de données est hébergée. Remarque: Si la valeur contient un caractère spécial, vous devez placer la valeur entre guillemets simples (').
<code>databasePort</code>	Numéro de port du service de moteur de base de données.
<code>databaseServiceName</code>	Nom de service de la base de données Oracle.
<code>databaseName</code>	Nom de base de données pour la base de données PostgreSQL ou SQL Server.
<code>databaseUserName</code>	Nom du compte d'utilisateur pour se connecter à la base de données.
<code>databaseAdvanceParameter</code>	Facultatif. Entrez les paramètres de connexion JDBC avancés utilisés pour vous connecter au référentiel Analyse des actifs de données. Remarque: Vous devez placer les paramètres entre guillemets simples (').

- Sur une ligne de commande shell, entrez la commande suivante pour exécuter l'utilitaire à partir du répertoire d'extraction des fichiers : `./daoutil.sh`.
- Appuyez sur **1** pour sélectionner le mode de mise à niveau.
- Entrez le mot de passe utilisé pour vous connecter à la base de données.

Remarque: Pour connaître le statut d'exécution, reportez-vous au fichier `daoutil.log` du répertoire d'exécution de l'utilitaire.

Étape 2. Sauvegarder les référentiels et les détails de configuration

Sauvegarder le domaine

Avant de mettre à niveau le domaine, vous devez sauvegarder ses métadonnées de configuration.

Effectuez les étapes suivantes pour sauvegarder le domaine :

- Exécutez la commande `infasetup BackupDomain` pour sauvegarder les tables de la base de données de configuration du domaine dans un fichier.
- Sauvegardez les fichiers de configuration des métadonnées dans tout répertoire accessible par les machines sur lesquelles vous installez Informatica.

Informatica `infasetup` inclut des programmes de ligne de commande pour sauvegarder et restaurer le domaine. `infasetup` est situé dans le répertoire suivant :

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

Pour sauvegarder le domaine avec infasetup, utilisez la syntaxe suivante :

```
BackupDomain
<<-DatabaseAddress|-da> database_hostname:database_port|

<-DatabaseConnectionString|-cs> database_connection_string>

<-DatabaseUserName|-du> database_user_name

<-DatabasePassword|-dp> database_password

<-DatabaseType|-dt> database_type

[<-DatabaseServiceName|-ds> database_service_name]

<-BackupFile|-bf> backup_file_name

[<-Force|-f>]

<-DomainName|-dn> domain_name

[<-Tablespace|-ts> tablespace_name (used for IBM DB2 only)]

[<-SchemaName|-sc> schema_name (used for Microsoft SQL Server only)]

[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]

[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]

[<-TrustedConnection|-tc> trusted_connection (used for Microsoft SQL Server only)]

[<-EncryptionKeyLocation|-kl> encryption_key_location]
```

Sauvegardez les fichiers de configuration des métadonnées dans tout répertoire accessible par les machines sur lesquelles vous installez Informatica. Le tableau suivant décrit les fichiers de métadonnées et les emplacements où vous pouvez les trouver :

Fichier de métadonnées	Description	Emplacement
nodemeta.xml	Contient les métadonnées d'un nœud.	Stocké dans le répertoire isp/config sur chaque nœud du domaine. Si vous utilisez le même nom de répertoire de sauvegarde sur tous les nœuds, renommez nodemeta.xml avant de le copier vers l'emplacement de la sauvegarde. Par exemple, vous sauvegardez nodemeta.xml dans le répertoire /nodebak sur nodeA et nodeB. Renommez les fichiers de configuration de sorte que, sur nodeA, le fichier soit sauvegardé sous /nodebak/nodemeta_A.xml et, sur nodeB, il soit sauvegardé sous /nodebak/nodemeta_B.xml.
domains.infa	Contient les informations de connectivité pour les nœuds passerelle.	Stocké dans un des emplacements suivants : <ul style="list-style-type: none">- Le répertoire d'installation Informatica sur les machines client et serveur.- L'emplacement configuré via la variable d'environnement INFA_DOMAINS_FILE.

Sauvegarder le référentiel modèle

Sauvegardez le contenu du référentiel modèle à l'aide de l'outil Administrator tool.

Pour sauvegarder un référentiel modèle, sélectionnez le service de référentiel modèle dans l'outil Administrator tool. Dans le menu Actions du domaine, cliquez sur **Contenu de référentiel > Sauvegarder**.

Sauvegarder les données du catalogue à l'aide de l'utilitaire export

Sauvegardez les données du catalogue à l'aide de l'utilitaire `export.jar` afin de pouvoir restaurer les données du catalogue après la mise à niveau.

Utilisez l'utilitaire `export` si vous avez effectué une mise à niveau d'une version de cluster Hadoop vers un cluster non-Hadoop et que vous souhaitez migrer les données de catalogue existantes vers la version 10.5.3. Contactez le support client international pour télécharger l'utilitaire.

Avant d'exécuter l'utilitaire, vérifiez les prérequis suivants :

- Le service de cluster Informatica est en cours d'exécution.
- Aucun travail n'est en cours d'exécution dans Enterprise Data Catalog. Pour vérifier, consultez l'onglet **Surveillance** dans Catalog Administrator.
- Le service de catalogue est en cours d'exécution.
- Si la sauvegarde contient des données de profil de similarité volumineuses, assurez-vous que le processus `infacmd` inclut une taille de segment de mémoire de 4 Go. Vous pouvez définir la valeur de la taille du segment de mémoire JAVA avec la propriété suivante dans le fichier `Infacmd.sh` : `export ICMD_JAVA_OPTS=-Xmx4096m`
- Activez le mode lecture seule pour le catalogue de service. Pour activer le service en mode lecture seule, consultez les exemples de commandes `curl` suivantes :
 - Si le service de catalogue est activé pour SSL, utilisez la commande `curl -k -u <DomainUserName>:<DomainPassword> -X POST "https://<host name>:<Catalog Service port>/access/1/catalog/catalogMode/READONLYMODE" -H "accept: /*/*"`.
 - Si le service de catalogue n'est pas activé pour SSL, utilisez la commande `curl -k -u <DomainUserName>:<DomainPassword> -X POST "http://<host name>:<Catalog Service port>/access/1/catalog/catalogMode/READONLYMODE" -H "accept: /*/*"`.
- À partir de votre installation existante, copiez le fichier `application.properties` de `<$INFA_HOME>/logs/<NODE_NAME>/services/CatalogService/<SERVICE_NAME>/<SCN_NAME>/spark/` vers le répertoire de copie du fichier `export.jar`.
- Si le service de catalogue est activé pour SSL, définissez les variables d'environnement suivantes :
 - `INFA_TRUSTSTORE`. Définissez la variable sur l'emplacement du fichier `truststore` Informatica. L'emplacement par défaut est `$INFA_HOME/services/shared/security`.
 - `INFA_TRUSTSTORE_PASSWORD`. Chiffrez le mot de passe que vous avez défini. Consultez l'exemple de commande pour définir le mot de passe chiffré : `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA=="`

Remarque: Reportez-vous à l'exemple de commande suivant pour chiffrer le mot de passe : `$INFA_HOME/server/bin/pmpasswd <password>`
- Si les données du catalogue sont volumineuses, exécutez l'utilitaire `export.jar` avec une taille de segment de mémoire de 20 Go. Par exemple, `java -Xmx20960m -jar export.jar export`. Pour plus d'informations sur le dimensionnement des performances, reportez-vous au *Guide de réglage des performances d'Enterprise Data Catalog*.
- Définissez l'option d'intervalle de validation sur 48 heures lorsque vous exécutez l'utilitaire `export`. Par exemple, `java -Dexport.commit.interval.ms=172800000 -jar export.jar export`

Exécutez l'utilitaire à l'aide de la commande suivante : `- java -jar export.jar export`

Vous pouvez vérifier le fichier `export.log` généré à l'emplacement d'exécution de l'utilitaire.

Sauvegarder le catalogue Données utilisant la commande `ldm backupContents`

Sauvegardez les données du catalogue avant de mettre à niveau Enterprise Data Catalog. La sauvegarde du catalogue garantit la disponibilité des métadonnées, attributs, associations, valeurs, planifications et tâches existants en cas d'échec de la mise à niveau. Sauvegardez les données du catalogue pour les conserver à partir de l'environnement Hadoop en cas d'échec de la restauration ou de la mise à niveau. Vous devez disposer du rôle Informatica Administrator pour effectuer la sauvegarde.

Avant d'exécuter la commande `infacmd ldm backupContents`, vérifiez les prérequis suivants :

- Définissez les variables d'environnement suivantes si le service de catalogue est activé pour SSL :
 - `INFA_TRUSTSTORE`. Consultez l'exemple de commande suivant pour définir la variable : `export INFA_TRUSTSTORE= <Location of the Informatica truststore file>`. L'emplacement par défaut est `$INFA_HOME/services/shared/security`.
 - `INFA_KEYSTORE`. Reportez-vous à l'exemple de commande suivant pour définir la variable : `export INFA_KEYSTORE=<Location of the keystore file>`. L'emplacement par défaut est `$INFA_HOME/services/shared/security`. Cette variable est requise uniquement si vous avez utilisé une configuration SSL personnalisée. Pour les configurations SSL et non-SSL par défaut, vous devez désactiver la variable.
 - `INFA_TRUSTSTORE_PASSWORD`. Chiffrez le mot de passe que vous avez défini. Reportez-vous à l'exemple de commande suivant pour définir le mot de passe chiffré : `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA=="`.
 - `INFA_KEYSTORE_PASSWORD`. Chiffrez le mot de passe que vous avez défini. Reportez-vous à l'exemple de commande suivant pour définir le mot de passe chiffré : `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI=="`. Cette variable est requise uniquement si vous avez utilisé une configuration SSL personnalisée. Pour les configurations SSL et non-SSL par défaut, vous devez désactiver la variable.

Vous pouvez contacter le support client international Informatica pour obtenir les mots de passe par défaut du truststore et du keystore.

Remarque: Reportez-vous à l'exemple de commande suivant pour chiffrer le mot de passe : `$INFA_HOME/server/bin/pmpasswd <password>`

- Estimez la consommation d'espace disque HDFS des données du catalogue. Exécutez la commande suivante pour afficher la taille du répertoire : `hdfs -du /Informatica/LDM/<SCN>`.
- Assurez-vous qu'un espace disque suffisant est disponible dans un hôte de domaine afin que l'espace disque de la sauvegarde soit suffisant.

La commande `infacmd ldm BackupContents`, telle qu'elle s'affiche dans l'exemple suivant, crée un fichier .zip du répertoire sur la machine locale : `./infacmd.sh LDM backupContents -dn <name of the Informatica domain> -un <username to connect to the Informatica domain> -pd <password for the username> -sn <name of the Catalog Service> -of <name of the backup ZIP file>`

Pour plus d'informations sur la syntaxe, les paramètres et la description de la commande, consultez la [Informatica Command Reference](#).

Remarque: Si la sauvegarde échoue avec un problème de mémoire insuffisante, vous devez augmenter la taille du segment de mémoire JAVA pour la propriété `ICMD_JAVA_OPTS` dans le fichier `infacmd.sh` suivant. Par exemple, `ICMD_JAVA_OPTS=-Xmx20g`.

Sauvegarder la configuration SSL

Sauvegardez les fichiers de configuration SSL suivants à partir de l'emplacement par défaut : `<Informatica installation directory>/services/shared/security`.

- Sauvegardez les fichiers keystore et truststore de domaine.
- Sauvegardez les fichiers keystore par défaut.
- Sauvegardez tous les fichiers keystore et truststore que les services d'application utilisent.

Sauvegarder les informations du domaine

Sauvegardez les fichiers de configuration :

- `<Informatica installation directory>/isp/config/keys/siteKey`
- `<Informatica installation directory>/domains.infa`
- `<Informatica installation directory>/tomcat/conf/server.xml`
- `<Informatica installation directory>/isp/config/nodemeta.xml`

Remarque: Vous devez sauvegarder les fichiers binaires à partir du répertoire d'installation d'Informatica.

Sauvegarder le schéma de base de données de l'analyse des actifs de données

Si vous avez configuré le référentiel de l'analyse des actifs de données, effectuez une sauvegarde du schéma de base de données de l'analyse des actifs de données.

Remarque: Utilisez un outil de base de données pour effectuer une sauvegarde.

Sauvegarder MetaDex

Si vous avez configuré le référentiel de MetaDex, sauvegardez le référentiel MetaDex.

Remarque: Dans la version 10.4, le planificateur de travaux de MetaDex était désactivé par défaut. À partir de la version 10.5, par défaut, le planificateur de travaux supprime les travaux toutes les six heures, ne laissant que les trois derniers travaux. Vous pouvez modifier ce comportement en modifiant les paramètres dans le fichier `repository.properties`. Pour plus d'informations, reportez-vous à la section « Suppression des travaux » du *Guide de l'administrateur de MetaDex*.

1. Utilisez un outil de base de données pour effectuer une sauvegarde du schéma de base de données MetaDex.

Remarque: Veillez à créer une sauvegarde de l'intégralité de la base de données, pas seulement du contenu des données.

2. Créez une sauvegarde des fichiers de configuration suivants :

- `<workspace>/etc`
- `<workspace>/setup.env`

3. Créez une sauvegarde du registre de connexion.

4. Dans l'outil MetaDex, exportez vos configurations et projets.

Reportez-vous aux sections « Page de projets » et « Page de configuration » du *Guide de l'administrateur de MetaDex*.

Sauvegarder les enrichissements de la ressource Tableau à l'aide de l'utilitaire de migration

Si le catalogue contient des ressources Tableau, vous devez sauvegarder les enrichissements des ressources Tableau à l'aide de l'utilitaire de migration avant d'effectuer une mise à niveau vers Enterprise Data Catalog version 10.5.3.

1. Depuis Akamai Download Manager, téléchargez et extrayez le fichier `Informatica_1053_TableauEnrichmentMigrationUtility.zip` sur la machine du domaine.
2. Exécutez la commande suivante pour sauvegarder les enrichissements des ressources Tableau :

```
java -jar EnrichmentUtility.jar export <Catalog Service hostname> <Catalog Service admin port number> <username> <password> <location to download enrichments json> <resourceName> <SSL Enabled true/false>
```

Étape 3. Préparer la mise à niveau

Désactivation du service de catalogue

Pour désactiver un service d'application, sélectionnez le service de catalogue dans Informatica Administrator et cliquez sur **Actions > Désactiver le service**.

Désactiver les services d'application

Vous devez désactiver les services d'application Informatica suivants avant de sauvegarder le catalogue :

1. Service de cluster Informatica
2. Service de gestion de contenu
3. Service d'intégration de données
4. Service de référentiel modèle

Pour désactiver un service d'application, sélectionnez-le dans Informatica Administrator et cliquez sur **Actions > Désactiver le service**.

Arrêter le domaine Informatica.

Depuis Informatica Administrator, arrêtez le domaine Informatica.

Étape 4. Mettre à niveau le domaine Informatica

L'assistant de mise à niveau lit les informations sur le domaine à partir des fichiers de la version précédente et utilise les mêmes paramètres pour configurer les fichiers de domaine et de serveur pour la mise à niveau. Il met à niveau les tables du référentiel de configuration de domaine dans la même base de données que la version précédente. Vous pouvez effectuer la mise à niveau en mode console ou silencieux.

Effectuez les tâches de préparation à la mise à niveau avant de commencer. Exécutez le programme d'installation sur toutes les machines qui hébergent des versions précédentes d'Informatica que vous souhaitez mettre à niveau.

Remarque: Dans un domaine à plusieurs nœuds, mettez à niveau le nœud de passerelle avant les autres nœuds et mettez à niveau tous les nœuds de travail en parallèle.

Vous pouvez effectuer la mise à niveau depuis le répertoire dans lequel vous avez téléchargé les fichiers d'installation.

Une fois le domaine mis à niveau, mettez à niveau l'outil client Informatica vers la même version Informatica.

Avant d'effectuer la mise à niveau, vérifiez que le fichier truststore du domaine Informatica contient uniquement TrustedCertEntry. Vous devez supprimer toutes les entrées PrivateKeyEntry du fichier.

Exécuter l'utilitaire de validation de cluster

Exécutez l'utilitaire de validation du scanner pour valider les prérequis de la mise à niveau d'Enterprise Data Catalog.

Effectuez les étapes suivantes pour exécuter l'utilitaire :

1. Vérifiez que chaque nœud de cluster dispose d'au moins quatre cœurs de processeur, 16 Go de mémoire et 60 Go d'espace disque libre.

Remarque: La configuration matérielle requise répertoriée ici correspond aux valeurs minimales recommandées pour installer le produit et démarrer les services. Elle varie en fonction de la taille du déploiement. Pour plus d'informations sur la configuration matérielle requise en fonction des tailles de déploiement, reportez-vous au Guide de réglage des performances d'Enterprise Data Catalog.

2. Vérifiez que le répertoire racine () dispose d'un minimum de 10 Go d'espace disque libre.
3. Téléchargez l'utilitaire de validation de cluster Informatica pour la version 10.5.3 d'Akamai Download Manager.

Remarque: Si vous avez appliqué un Service Pack, vous devez télécharger l'utilitaire correspondant à la version du Service Pack.

4. Extrayez le fichier ZIP sur le domaine Informatica que vous prévoyez de mettre à niveau.
5. Accédez au répertoire d'extraction des fichiers et ouvrez les fichiers input.properties.

Remarque: Vous devez disposer des autorisations de lecture et d'écriture sur le répertoire et des autorisations d'exécution sur les fichiers exécutables.

6. Dans le fichier input.properties, configurez les propriétés requises.
7. Désactivez le pare-feu sur chaque hôte du cluster.
8. Activez SSH sans mot de passe entre les nœuds suivants :

- Nœud qui héberge le domaine Informatica et le nœud qui héberge la passerelle.
- Hôte de passerelle et nœuds de données.
- Hôte de passerelle et nœuds de traitement.
- Nœuds de sauvegarde et nœud de passerelle.
- Tous les nœuds du cluster et les nœuds de données.

Remarque: Si vous avez activé la configuration avancée pour le service de cluster Informatica et que les services MongoDB, PostgreSQL, Solr et Nomad s'exécutent sur des hôtes différents, activez l'accès sans mot de passe de l'hôte de passerelle aux hôtes qui exécutent ces services.

9. Sur une ligne de commande shell, accédez au répertoire d'extraction des fichiers utilitaires et exécutez la commande suivante : `java -jar InformaticaClusterValidationUtility.jar -in <Location of the input.properties file>`.

L'utilitaire propose les options suivantes :

Option	Description
-hp	Affichez le contenu de l'aide.
-in	Spécifiez l'emplacement du fichier input.properties.
-lf	Facultatif. Spécifiez le répertoire de stockage des fichiers journaux générés par l'utilitaire.
-v	Facultatif. Activez le journal de débogage.
-vf	Facultatif. Si vous avez déplacé les scripts de validation vers un répertoire différent, spécifiez l'emplacement de stockage des scripts de validation.

Remarque: Si un message d'erreur de validation d'autorisation pour le répertoire personnalisé du cluster s'affiche, vous pouvez ignorer l'erreur.

10. Vérifiez l'état de validation à partir des fichiers journaux suivants situés dans le répertoire d'exécution de l'utilitaire :
- clusterPrevalidation.log
 - clusterPrevalidation.err

Mettre à niveau en mode console

Vous pouvez effectuer une mise à niveau en mode console pour mettre à niveau le domaine sur la même machine et la même base de données de référentiel de configuration du domaine. Vous pouvez mettre à niveau le domaine en mode console.

Lorsque vous exécutez le programme d'installation en mode console, les mots Quitter, Retour et Aide sont des mots réservés. Ne les utilisez pas comme texte d'entrée.

1. Connectez-vous à la machine avec le même compte d'utilisateur que vous avez utilisé pour installer la version précédente.
2. Arrêtez tous les processus qui accèdent au répertoire et aux sous-répertoires du produit Informatica à mettre à niveau, y compris les invites de commande et suivis d'audit.
3. Sur une ligne de commande shell, exécutez le fichier d'installation.

Le programme d'installation affiche un message vous invitant à vérifier que les variables d'environnement régionales sont définies.

4. Si les variables d'environnement ne sont pas définies, appuyez sur la touche **n** pour quitter le programme d'installation et définissez-les de façon appropriée.

Si les variables d'environnement sont définies, appuyez sur **y** pour continuer.

5. Appuyez sur **2** pour mettre à niveau Informatica.
6. Appuyez sur **2** pour ignorer l'exécution d'Informatica Upgrade Advisor.

Informatica fournit des utilitaires pour faciliter le processus d'installation des services Informatica. Vous pouvez exécuter l'utilitaire avant de mettre à niveau les services Informatica. Informatica Upgrade

Advisor valide les services et vérifie la présence de services obsolètes dans le domaine avant d'effectuer une mise à niveau.

Le programme d'installation affiche un avertissement vous demandant d'arrêter le domaine Informatica que vous souhaitez mettre à niveau avant de poursuivre la mise à niveau.

7. Lisez les conditions du kit d'utilisation du produit Informatica et sélectionnez **2** pour poursuivre la mise à niveau.

Soumis à vos droits de retrait décrits ci-dessous, le logiciel transmettra automatiquement certaines informations à Informatica (aux États-Unis) concernant l'environnement informatique et réseau dans lequel le Logiciel est déployé et les statistiques du système et d'utilisation des données du déploiement. Cette transmission est considérée comme faisant partie des Services selon la politique de confidentialité d'Informatica et Informatica utilisera et traitera par ailleurs ces informations conformément à la politique de confidentialité d'Informatica disponible sur <https://www.informatica.com/in/privacy-policy.html>. Il est possible de désactiver la collecte d'utilisation dans l'outil Administrator tool.

8. La page **Prérequis de mise à niveau** affiche les spécifications système pour la mise à niveau.

Vérifiez les spécifications avant de poursuivre la mise à niveau.

9. Vérifiez les informations de mise à niveau et appuyez sur **Entrée** pour continuer.

Le panneau **Répertoire de mise à niveau** s'affiche.

10. Lorsque vous y êtes invité, entrez le répertoire de la version d'Informatica à mettre à niveau et le répertoire dans lequel vous souhaitez effectuer la mise à niveau vers Informatica 10.5.3.

Le tableau suivant décrit les répertoires que vous devez indiquer :

Répertoire	Description
Répertoire du produit Informatica à mettre à niveau	Répertoire qui contient la version des services Informatica que vous souhaitez mettre à niveau.
Répertoire pour Informatica 10.5.3	<p>Répertoire d'installation d'Informatica 10.5.3.</p> <p>Entrez le chemin absolu du répertoire d'installation. Ce répertoire ne peut pas être le même que celui qui contient la version précédente des services Informatica. Les noms de répertoires dans le chemin ne doivent pas contenir d'espaces ni les caractères spéciaux suivants : @ * \$ # ! % () { } [] , ; ' .</p> <p>Remarque: Si vous utilisez un caractère spécial comme á ou €, des résultats inattendus peuvent se produire lors de l'exécution.</p>

11. Parmi les options d'installation suivantes, sélectionnez l'environnement de mise à niveau en fonction de vos besoins :

- Sandbox. Utilisé pour la preuve de concepts ou comme sandbox avec un minimum d'utilisateurs.
- Développement. Utilisé pour un environnement de conception.
- Test. Utilisé pour un environnement de traitement de gros volumes qui ressemble à un environnement de production.
- Production. Utilisé pour les environnements de production pour un traitement de gros volumes avec des niveaux élevés d'accès concurrentiel destinés aux utilisateurs finaux.

12. Choisissez si vous souhaitez modifier le nom d'hôte de nœud, les numéros de port ou le référentiel de configuration du domaine. Appuyez sur **1** pour utiliser la même configuration de nœud que dans la version précédente. Appuyez sur **2** pour modifier la configuration du nœud.

Le panneau **Sélection des composants** s'affiche.

13. Appuyez sur **1** pour mettre à niveau les services Informatica.
Le panneau **Sécurité du domaine - Clé de chiffrement** s'affiche.
14. Si vous avez configuré un service de catalogue sur le nœud, vous devez valider la sauvegarde du catalogue avant d'effectuer une mise à niveau. Appuyez sur **1** si le nœud ne comporte aucun service de catalogue ou sur **2** s'il en comporte un, puis appuyez sur **Entrée** pour continuer.
15. Appuyez sur **2** pour confirmer que vous avez sauvegardé le catalogue à l'aide de l'utilitaire export et de la commande `infacmd LDM backupContents`.
16. Spécifiez l'emplacement du répertoire contenant la sauvegarde du catalogue.
La sauvegarde du catalogue est validée.
17. Appuyez sur **1** si vous voulez configurer le référentiel MetaDex et fournissez les détails suivants :

Propriété	Description
Type de base de données	Spécifiez la base de données à configurer comme référentiel pour MetaDex. Vous pouvez sélectionner l'une des options suivantes : - Oracle - SQLServer
Nom d'utilisateur de la base de données	Nom d'utilisateur configuré pour accéder à la base de données avant la mise à niveau.
Mot de passe de la base de données	Mot de passe configuré pour le nom d'utilisateur.
Nom du schéma	Non applicable si vous avez sélectionné Oracle comme base de données. Spécifiez le schéma à utiliser.
La base de données est-elle sécurisée ?	Spécifiez si la base de données est activée pour SSL.
Chemin d'accès au fichier truststore de la base de données	S'applique si vous avez spécifié que la base de données est activée pour SSL. Fournissez le chemin d'accès complet au fichier truststore de la base de données.
Mot de passe du truststore	S'applique si vous avez spécifié que la base de données est activée pour le mot de passe SSL pour accéder au fichier truststore.
Paramètres JDBC sécurisés	S'applique si vous avez spécifié que la base de données est activée pour SSL. Spécifiez les paramètres de base de données sécurisés, comme indiqué dans l'exemple suivant : <code>EncryptionMethod=SSL;HostNameInCertificate=ORATLS.informatica.com;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;</code> Enterprise Data Catalog 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 aucun paramètre dans le champ Paramètres JDBC sécurisés.

Propriété	Description
Chaîne de connexion JDBC	Chaîne de connexion JDBC pour la connexion à la base de données. Utilisez les formats suivants pour spécifier les chaînes de connexion : <ul style="list-style-type: none"> - Oracle. jdbc:Informatica:oracle://<host name>: :<port number>;ServiceName= - SQLServer. jdbc:Informatica: sqlserver://<host name>: <portnumber>;SelectMethod=cursor;DatabaseName=
MetaDex	Port unique du serveur de référentiel MetaDex. La valeur par défaut est de 48 090.
Activer la communication sécurisée pour le référentiel MetaDex ?	Spécifiez si TLS est activé pour la communication avec le référentiel MetaDex.
Certificats SSL pour sécuriser le référentiel MetaDex ?	Indiquez si vous souhaitez utiliser les certificats SSL par défaut ou les certificats SSL personnalisés pour sécuriser le référentiel MetaDex. Spécifiez les propriétés suivantes si vous souhaitez utiliser les certificats SSL personnalisés : <ul style="list-style-type: none"> - Type de keystore. Spécifiez le type de keystore. - Alias du keystore. Alias unique permettant d'accéder à l'entrée du keystore. - Fichier keystore. Spécifiez le fichier keystore qui contient les clés et les certificats requis. - Mot de passe du keystore. Mot de passe pour accéder au fichier keystore.

Si vous n'aviez pas choisi de configurer le référentiel MetaDex lors de l'installation, vous pouvez le configurer une fois celle-ci terminée. Effectuez les étapes répertoriées dans la section [“Configurer le référentiel MetaDex \(facultatif\)” à la page 62.](#)

18. Choisissez si vous souhaitez installer des packages d'intégration tiers avec le programme d'installation d'Informatica.

Remarque: Vous devez installer un package d'intégration si vous configurez les services Informatica pour effectuer les tâches suivantes :

- Transférez le traitement vers l'environnement Hadoop ou Databricks.
- Traitez des fichiers complexes dans le domaine Informatica.
- Connectez-vous à l'environnement Hadoop, mais effectuez un traitement dans le domaine Informatica.

Vous pouvez choisir d'installer les packages maintenant ou ultérieurement via Integration Package Manager.

- Appuyez sur **1** pour installer le domaine Informatica sans packages d'intégration.
- Appuyez sur **2** pour installer le domaine Informatica avec des packages d'intégration.

La valeur par défaut est 1.

19. Si vous choisissez d'installer des packages d'intégration, sélectionnez-en un ou plusieurs que vous souhaitez installer dans la liste. Séparez plusieurs packages par une virgule.

La valeur par défaut est 1.

Remarque: Les fichiers du programme d'installation des packages sélectionnés doivent être disponibles dans le répertoire : <Informatica installer files>/source

20. Appuyez sur **Entrée**.

- Le panneau **Sécurité du domaine - Clé de chiffrement** s'affiche.
21. Entrez le nom d'utilisateur et le mot de passe du domaine Informatica.
La page **Récapitulatif de pré-installation** s'affiche.
 22. Vérifiez les informations de mise à niveau et appuyez sur **Entrée** pour continuer.
Une fois la mise à niveau du domaine terminée, le panneau **Référentiel de configuration de domaine** s'affiche.
 23. Appuyez sur **Entrée** pour continuer la mise à niveau.
Le programme d'installation copie les fichiers de serveur dans le répertoire d'installation d'Informatica 10.5.3.
Le programme d'installation affiche les informations de la base de données et du compte d'utilisateur pour le référentiel de configuration du domaine à mettre à niveau. Il affiche la chaîne de connexion à la base de données pour le référentiel de configuration du domaine en se basant sur la manière dont la chaîne de connexion de la version précédente a été créée lors de l'installation :
 - Si la version précédente utilisait une URL JDBC lors de l'installation, le programme d'installation affiche les propriétés de connexion JDBC, y compris l'adresse et le nom de service de la base de données.
 - Si la version précédente utilisait une chaîne de connexion JDBC personnalisée lors de l'installation, le programme d'installation affiche la chaîne de connexion personnalisée.
 24. Si vous utilisez une URL JDBC, vous pouvez spécifier des paramètres supplémentaires à inclure dans la chaîne de connexion.
Si vous utilisez une chaîne de connexion personnalisée, vous ne pouvez pas spécifier de paramètres supplémentaires.
 25. Vérifiez les informations et appuyez sur **Entrée**.
La mise à niveau se termine et le panneau **Résumé de post-installation** s'affiche.
 26. Appuyez sur **Entrée** pour terminer la procédure d'installation et quitter le programme d'installation.
Vérifiez le fichier upgrade.log pour obtenir plus d'informations sur les tâches effectuées par l'assistant de mise à niveau et pour afficher la configuration des composants installés.

Appliquer le dernier Service Pack ou correctif cumulatif

Appliquez le dernier Service Pack ou correctif cumulatif disponible après la mise à niveau du domaine.

Configurer le référentiel MetaDex (facultatif)

Si vous n'aviez pas configuré le référentiel MetaDex lors de la mise à niveau, vous pouvez le faire après avoir mis à niveau Enterprise Data Catalog.

Effectuez les étapes suivantes pour configurer le référentiel :

1. Accédez au répertoire d'extraction des fichiers du programme d'installation et accédez au sous-répertoire suivant : `\properties\MetaDex\`.

2. Ouvrez le fichier `MetaDex.properties` et configurez les propriétés suivantes :

Propriété	Description
USER_INSTALL_DIR	Répertoire d'installation d'Informatica.
MDX_DB_UNAME	Nom d'utilisateur configuré pour accéder à la base de données avant la mise à niveau.
MDX_DB_PASSWD	Mot de passe pour accéder à la base de données.
MDX_DB_TYPE	Type de base de données à configurer. Spécifiez <code>Oracle</code> ou <code>MSSQLServer</code> .
MDX_SQLSERVER_SCHEMA_NAME	S'applique si <code>MDX_DB_TYPE=MSSQLServer</code> . Spécifiez le nom du schéma à utiliser. Si vous ne spécifiez aucun schéma, Enterprise Data Catalog utilise celui par défaut.
MDX_DB_CUSTOM_STRING	Chaîne de connexion JDBC pour la connexion à la base de données. Utilisez les formats suivants pour spécifier les chaînes de connexion : <ul style="list-style-type: none"> - Oracle. jdbc:informatica:oracle: //<host name>:<port number>;ServiceName= - SQLServer. jdbc:informatica:sqlserver: //<host name>:<portnumber>;SelectMethod=cursor;DatabaseName=
MDX_SERVER_PORT	Port unique du serveur de référentiel MetaDex. La valeur par défaut est de 48 090.
MDX_SSL_ENABLED	Spécifiez <code>true</code> si la base de données est activée pour SSL, sinon <code>false</code> . La valeur par défaut est <code>false</code> .
MDX_DB_TRUSTSTORE_FILE	S'applique si vous avez spécifié que la base de données est activée pour SSL. Fournissez le chemin d'accès complet au fichier truststore de la base de données.
MDX_DB_TRUSTSTORE_PASSWD	S'applique si vous avez spécifié que la base de données est activée pour le mot de passe SSL pour accéder au fichier truststore.
MDX_SSL_DEFAULT_STRING	S'applique si vous avez spécifié que la base de données est activée pour SSL. Spécifiez les paramètres de base de données sécurisés, comme indiqué dans l'exemple suivant : <pre>EncryptionMethod=SSL;HostNameInCertificate= ORATLS.informatica.com; ValidateServerCertificate=true; CryptoProtocolVersion=TLSv1.2;</pre> Enterprise Data Catalog 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 aucun paramètre dans le champ Paramètres JDBC sécurisés.

Propriété	Description
MDX_CUSTOM_SELECTION	S'applique si vous avez spécifié que la base de données est activée pour SSL. Indiquez si vous souhaitez utiliser les certificats SSL par défaut ou les certificats SSL personnalisés pour sécuriser le référentiel. Définissez la propriété sur <code>true</code> pour utiliser des certificats SSL personnalisés. Définissez la propriété sur <code>false</code> pour utiliser le certificat SSL par défaut.
MDX_KEYSTORE_FILE	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Spécifiez le fichier keystore qui contient les clés et les certificats requis.
MDX_KEYSTORE_PASSWD	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Mot de passe pour accéder au fichier keystore.
MDX_KEYSTORE_TYPE	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Spécifiez le type de keystore.
MDX_KEYSTORE_ALIAS	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Alias unique permettant d'accéder à l'entrée du keystore.

- Entrez la commande suivante : `./configureMetaDex.sh`

Remarque: Installez MetaDex uniquement sur le nœud de domaine.

- Si le service de catalogue est en cours d'exécution, recyclez le service.

Copier les pilotes de ressources tiers

Effectuez les postrequis suivants après avoir mis à niveau le domaine Informatica :

- Copiez les fichiers JAR ou ZIP tiers que vous aviez configurés pour des ressources telles que Teradata, JDBC et IBM Netezza de l'emplacement suivant `<Informatica installation directory>services/CatalogService/ScannerBinaries` vers le même emplacement de la machine qui héberge le domaine Informatica mis à niveau.

Activer et mettre à niveau les services d'application

Pour activer un service d'application, sélectionnez-le dans Informatica Administrator et cliquez sur **Actions > Activer le service**.

Activez les services d'application Informatica suivants :

- Service de référentiel modèle
- Service d'intégration de données
- Service de gestion de contenu

Après avoir activé les services d'application Informatica, exécutez l'assistant de mise à niveau des services pour mettre à niveau ceux-ci.

Remarque: Vous devez désactiver l'analyse des actifs de données avant de mettre à niveau le service de cluster Informatica. Pour désactiver l'analyse des actifs de données, sélectionnez le service de catalogue dans Informatica Administrator. Modifiez les propriétés de configuration de l'analyse des actifs de données et décochez la case **Activer l'analyse des actifs de données**.

Mettre à niveau les services d'application à l'aide de l'assistant de mise à niveau des services

Utilisez l'assistant de mise à niveau des services pour mettre à niveau les services d'application et le contenu des bases de données qui leur sont associées. L'assistant de mise à niveau des services affiche les services mis à niveau dans une liste contenant également les services et les bases de données associées qui nécessitent une mise à niveau. Vous pouvez également enregistrer le rapport de mise à niveau actuel ou le précédent.

1. Dans la zone d'en-tête Informatica Administrator, cliquez sur **Gérer > Mettre à niveau**.
2. Sélectionnez les services d'application et les bases de données associées à mettre à niveau.
3. Vous pouvez éventuellement sélectionner l'option **Recycler automatiquement les services après une mise à niveau**.

Si vous choisissez de redémarrer automatiquement les services d'application après la mise à niveau, l'assistant de mise à niveau redémarre les services après leur mise à niveau.

4. Cliquez sur **Suivant**.
5. En cas d'erreurs de dépendance, la boîte de dialogue **Erreurs de dépendance** s'affiche. Examinez les erreurs de dépendance et cliquez sur **OK**. Ensuite, résolvez les erreurs de dépendance et cliquez sur **Suivant**.
6. Entrez les informations de connexion au référentiel.
7. Cliquez sur **Suivant**.

L'assistant de mise à niveau des services met à niveau chaque service d'application et chaque base de données associée, puis affiche le statut et les détails du traitement.

8. Une fois la mise à niveau terminée, la section **Résumé** affiche la liste des services d'application et leur statut de mise à niveau. Cliquez sur chaque service pour afficher les détails dans la section **Détails du service**.
9. Vous pouvez éventuellement cliquer sur **Enregistrer le rapport** pour enregistrer les détails de la mise à niveau dans un fichier.

Si vous choisissez de ne pas enregistrer le rapport, vous pouvez cliquer sur **Enregistrer le rapport précédent** au prochain lancement de l'assistant de mise à niveau des services.

10. Cliquez sur **Fermer**.
11. Si vous n'avez pas choisi de redémarrer automatiquement les services d'application après la mise à niveau, redémarrez les services mis à niveau.

Vous pouvez afficher le rapport de mise à niveau et l'enregistrer. Lors de la deuxième exécution de l'assistant de mise à niveau des services, l'option Enregistrer le rapport précédent s'affiche. Si vous n'avez pas enregistré le rapport de mise à niveau après la mise à niveau des services, vous pouvez sélectionner cette option pour afficher ou enregistrer le rapport de mise à niveau précédent.

Ajouter la licence du domaine Informatica

Effectuez les étapes suivantes pour ajouter la nouvelle licence pour le domaine Informatica :

1. Connectez-vous à Informatica Administrator.
2. Sélectionnez le domaine Informatica.
3. Cliquez sur **Nouveau > Licence**.
4. Donnez un nom à la nouvelle licence.
5. Sélectionnez la nouvelle clé de licence dans la liste déroulante **Licence**.

Étape 5. Effectuer la mise à niveau du domaine Informatica

Vérifier les prérequis de l'utilisateur de la passerelle

L'utilisateur de la passerelle doit être un utilisateur non-racine avec un accès sudo. Vous devez activer une connexion SSH sans mot de passe entre le domaine Informatica et l'hôte de passerelle pour l'utilisateur de la passerelle. L'utilisateur de la passerelle doit disposer des privilèges requis pour exécuter la commande ping.

Configurer les privilèges Sudo pour l'utilisateur de la passerelle (facultatif)

Si vous prévoyez de modifier les propriétés du service de cluster Informatica ou de remplacer les certificats SSL configurés pour le service de cluster Informatica, attribuez des privilèges sudo à l'utilisateur de la passerelle.

Les commandes suivantes nécessitent des privilèges sudo pour l'utilisateur de la passerelle lorsque vous activez le service de cluster Informatica pour la première fois :

- mkdir
- chown
- chmod
- echo
- systemctl
- cp
- mv
- sysctl
- rm
- tee
- sed
- sshd

Pour configurer les privilèges sudo pour les commandes, vous devez ajouter les commandes au fichier `/etc/sudoers`, comme illustré dans l'exemple suivant : `/bin/mkdir, /bin/chown, /bin/chmod, /bin/echo, /bin/systemctl, /bin/cp, /bin/mv, /usr/sbin/sysctl, /bin/rm, /usr/bin/tee, /usr/bin/sed, /usr/sbin/sshd`.

Remarque: Les commandes `tee` et `sed` ne nécessitent aucun privilège sudo dans les versions 10.5.1.1 et ultérieures.

Vous pouvez déterminer le répertoire où se trouve chaque commande à l'aide de la commande `which <command name>`.

Après avoir activé le service de cluster Informatica pour la première fois, vous pouvez choisir de désactiver la validation des autorisations sudo pour le service de cluster Informatica. Pour désactiver la validation, configurez la propriété personnalisée suivante pour le service de cluster Informatica :

`IcsCustomOptions.IcsGatewayUserSudoEnabled` et définissez la valeur sur `false`. Après la désactivation de la validation, les privilèges sudo ne sont pas requis lorsque vous redémarrez le service de cluster

Informatica. Pour arrêter cependant le service de cluster Informatica, l'autorisation sudo est toujours requise pour la commande `systemctl`.

Pour exécuter la commande `infacmd ics cleanCluster` afin de nettoyer le service de cluster Informatica, l'autorisation sudo doit être configurée pour les commandes `systemctl` et `rm`.

Remarque: Les services associés au service de cluster Informatica, tels qu'Apache Solr, PostgreSQL et Nomad nécessitent un utilisateur non racine disposant de privilèges sudo pour exécuter les services. Sudo permet à un utilisateur d'exécuter des programmes ou des commandes avec des privilèges élevés pendant une période spécifique. Enterprise Data Catalog nécessite un utilisateur non-racine avec des autorisations sudo pour exécuter certaines commandes lors de l'exécution de tâches administratives telles que l'installation, la mise à niveau et la surveillance du statut des services. Pour plus d'informations sur les commandes utilisées et le rôle de chaque commande lors de la mise à niveau, reportez-vous à l'article de la base de connaissances "[Configurer les privilèges Sudo pour l'utilisateur de la passerelle \(facultatif\)](#)" à la [page 101](#).

Effectuer la configuration SSL par défaut(Facultatif)

Si le domaine Informatica est activé pour SSL à l'aide des certificats SSL par défaut, vous pouvez configurer le service de cluster Informatica et le service de catalogue pour utiliser le nouveau keystore.

Pour configurer les services afin d'utiliser le keystore 10.5.3, procédez comme suit :

1. Désactivez le service de cluster Informatica et le service de catalogue.
2. Modifiez les options de processus pour le service de cluster Informatica et le service de catalogue, et indiquez l'emplacement du fichier `Default.keystore` de la version 10.5.3. Le chemin d'accès par défaut au fichier est `<Informatica installation directory>/tomcat/conf/Default.keystore`.
3. À partir du fichier 10.5.3 `<Informatica installation directory>/services/shared/security/infactruststore.jks`, supprimez la valeur existante configurée pour l'alias `infactruststore` et importez le fichier `<Informatica installation directory>/tomcat/conf/Default.keystore`.
4. Activez le service de cluster Informatica et le service de catalogue.

Étape 6. Activer et mettre à niveau les services Enterprise Data Catalog

Créer et activer le service de cluster Informatica

Lorsque vous créez le service de cluster Informatica, vous devez utiliser la licence pour la version 10.5.3 du service de cluster Informatica.

Effectuez les étapes suivantes pour créer le service de cluster Informatica :

1. Dans l'outil Administrator tool, sélectionnez un domaine, et cliquez sur l'onglet **Services et nœuds**.
2. Dans le menu **Actions**, cliquez sur **Nouveau > Service de cluster Informatica**
La boîte de dialogue **Nouveau service de cluster Informatica - Étape 1 sur 4** s'affiche.

3. Configurez les propriétés générales dans la boîte de dialogue :

Propriété	Description
Nom	Nom du service. 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. Les caractères inclus dans le nom doivent être compatibles avec la page de codes du référentiel modèle. Le nom ne peut pas contenir les caractères spéciaux suivants : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Description	Description du service. La description ne peut pas dépasser 765 caractères.
Emplacement	Sélectionnez le nœud de domaine Informatica.
Licence	Licence à attribuer au service de cluster Informatica. Remarque: Sélectionnez la licence pour la version 10.5.3 du service de cluster Informatica.
Nœud	Nœud principal sur lequel le service de cluster Informatica s'exécute. Si vous modifiez le nœud, vous devez redémarrer le service de cluster Informatica.
Nœuds de sauvegarde	Nœuds sur lesquels le service peut s'exécuter si le nœud principal n'est pas disponible.

4. Cliquez sur **Suivant**.
La boîte de dialogue **Nouveau service de cluster Informatica - Étape 2 sur 4** s'affiche.
5. Configurez les propriétés de sécurité dans la boîte de dialogue :

Propriété	Description
Port HTTP	Numéro de port HTTP unique pour le service. La valeur par défaut est de 9075.
Activer TLS (Transport Layer Security)	Sélectionnez cette option pour activer TLS du service de cluster Informatica.
Port HTTPS	Numéro de port de la connexion HTTPS. Nécessaire si vous sélectionnez Activer TLS (Transport Layer Security) . La valeur par défaut est de 9 533.
Fichier keystore	Chemin et nom du fichier keystore. Le fichier keystore contient les clés et les certificats requis si vous utilisez le protocole de sécurité SSL avec l'administrateur de catalogue. Requis si vous sélectionnez Activer TLS (Transport Layer Security) . Remarque: Vérifiez que vous avez spécifié le fichier keystore correct pour le service de cluster Informatica. Les certificats du keystore doivent être approuvés par le truststore du domaine. Le fichier truststore doit contenir des certificats signés par une autorité de certification (CA) pour une configuration SSL personnalisée.
Mot de passe keystore	Mot de passe du fichier keystore. Nécessaire si vous sélectionnez Activer TLS (Transport Layer Security) .
Protocole SSL	Protocole Secure Sockets Layer à utiliser.

6. Cliquez sur **Suivant**.
La boîte de dialogue **Nouveau service de cluster Informatica - Étape 3 sur 4** s'affiche.

7. Configurez les propriétés du cluster dans la boîte de dialogue :

Propriété	Description
Hôte de passerelle	Nom de domaine complet (FQDN) du nœud à configurer comme hôte de passerelle. Vous pouvez utiliser la commande <code>hostname -f</code> pour afficher le nom de domaine complet (FQDN) du nœud. Le nœud que vous configurez comme hôte de passerelle doit être un nœud de données ou un nœud de traitement. Remarque: Vous devez configurer un nouvel hôte de passerelle pour le service de cluster Informatica.
Nœuds de données	Liste de noms de domaine complets de nœuds séparée par des virgules à configurer comme nœuds de données. Vous pouvez utiliser la commande <code>hostname -f</code> pour afficher le nom de domaine complet (FQDN) du nœud.
Nœuds de traitement	Liste de noms de domaine complets de nœuds séparée par des virgules à configurer comme nœuds de traitement. Vous pouvez utiliser la commande <code>hostname -f</code> pour afficher le nom de domaine complet (FQDN) du nœud.
Utilisateur de passerelle	Nom d'utilisateur de l'hôte de la passerelle. L'utilisateur de la passerelle doit être un utilisateur non-racine avec un accès sudo. Vous devez activer une connexion SSH sans mot de passe entre les nœuds suivants pour l'utilisateur de la passerelle : <ul style="list-style-type: none"> - Domaine Informatica et hôte de passerelle. - Domaine Informatica vers l'hôte de passerelle et celui-ci vers les nœuds de données et les nœuds de traitement. - Si vous avez activé la configuration avancée, activez la connexion entre l'hôte de passerelle et tous les nœuds de service configurés.
Répertoire personnalisé de cluster	Répertoire du service. La valeur par défaut est <code>/opt/informatica/ics</code> . Remarque: Si vous souhaitez modifier le répertoire personnalisé du cluster, vous devez cliquer sur Activer la configuration avancée . Après avoir modifié le répertoire, vous devez modifier ceux configurés pour les services associés au service de cluster Informatica.
Chemin du système de fichiers partagés du cluster	S'applique si vous déployez le service sur plusieurs nœuds. Répertoire partagé sur tous les nœuds du cluster. Le service utilise ce répertoire sur tous les nœuds du cluster pour sauvegarder les données d'Apache Solr. Configurez les prérequis de répertoire suivants : <ul style="list-style-type: none"> - Le répertoire doit être vide. - Le système de fichiers NFS doit être monté dans le répertoire. - L'ID d'utilisateur pour accéder au répertoire doit être le même dans tous les nœuds de cluster. - L'utilisateur configuré pour accéder au répertoire doit être un utilisateur non-racine.

8. Facultatif. Cliquez sur l'option **Activer la configuration avancée** si vous souhaitez configurer les propriétés des applications et des services associés. Par défaut, les services utilisent les valeurs que vous avez fournies pour les nœuds de données comme noms d'hôte. La base de données PostgreSQL utilise la valeur spécifiée pour l'hôte de passerelle comme nom d'hôte.
Pour plus d'informations sur les paramètres que vous devez configurer pour les services associés, reportez-vous à la section [Informatica Cluster Service Advanced Configuration à la page 105](#).

9. Sélectionnez **Activer le service** pour activer le service après avoir cliqué sur **Terminer**.

Remarque: Par défaut, les services associés utilisent les valeurs que vous avez fournies pour les nœuds de données comme noms d'hôte. La base de données PostgreSQL utilise la valeur spécifiée pour l'hôte de passerelle comme nom d'hôte.

10. Cliquez sur **Suivant**.
La boîte de dialogue **Nouveau service de cluster Informatica - Étape 4 sur 4** s'affiche.
11. Cliquez sur **Terminer**.

Configuration avancée du service de cluster Informatica

Si vous avez sélectionné **Activer la configuration avancée** lors de la configuration du service de cluster Informatica, vous devez configurer toutes les propriétés des services associés.

Configurez les propriétés suivantes pour les services associés au service de cluster Informatica :

Propriétés du service Nomad

Propriété	Description
Hôtes du serveur Nomad	Liste de noms de domaine complets de nœuds séparée par des virgules qui hébergent les serveurs Nomad.
Port HTTP Nomad	Numéro de port HTTP configuré pour le serveur Nomad. La valeur par défaut est de 4646.
Port Serf Nomad	Port Serf configuré comme protocole gossip pour les serveurs Nomad. La valeur par défaut est de 4648.
Port RPC Nomad	Port d'appel de procédure distante (RPC, Remote Procedure Call) configuré pour la communication. La valeur par défaut est de 4647.
Répertoire de travail du serveur Nomad	Répertoire qui comprend les sous-répertoires avec les tâches exécutées sur le serveur Nomad. La valeur par défaut est <code><Cluster custom directory>/nomad/nomadserver</code> .
Répertoire de travail du client Nomad	Répertoire configuré pour les tâches dans le client Nomad. La valeur par défaut est <code><Cluster custom directory>/nomad/nomadclient</code> .
Options personnalisées de Nomad	Spécifiez les options personnalisées pour le service au format suivant : <code>[OptionGroupName.OptionName = OptionValue]</code> . Vous pouvez séparer plusieurs options à l'aide d'un espace blanc. Si OptionValue comprend un espace blanc, vous devez placer OptionValue entre doubles guillemets, comme illustré dans l'exemple suivant : « sample value ».

Propriétés du service ZooKeeper

Propriété	Description
Hôtes ZooKeeper	Liste de noms de domaine complets de nœuds séparée par des virgules qui hébergent le serveur Apache ZooKeeper.
Port ZooKeeper	Numéro de port configuré pour le serveur Apache ZooKeeper. La valeur par défaut est de 2181.
Port d'homologue ZooKeeper	Numéro de port configuré pour la communication entre entités homologues d'Apache ZooKeeper. La valeur par défaut est de 2888.
Port leader de ZooKeeper	Numéro de port configuré pour le serveur ZooKeeper identifié comme leader. La valeur par défaut est de 3888.

Propriété	Description
Répertoire d'installation de ZooKeeper	Spécifiez le chemin d'accès au répertoire dans lequel vous souhaitez installer Apache ZooKeeper. La valeur par défaut est <code><Cluster custom directory>/zk/install</code> .
Répertoire de données de ZooKeeper	Spécifiez le chemin d'accès au répertoire dans lequel vous souhaitez stocker les données d'Apache ZooKeeper. La valeur par défaut est <code><Cluster custom directory>/zk/data</code> .
Options personnalisées de ZooKeeper	Spécifiez les options personnalisées pour le service au format suivant : <code>[OptionGroupName.OptionName = OptionValue]</code> . Vous pouvez séparer plusieurs options à l'aide d'un espace blanc. Si OptionValue comprend un espace blanc, vous devez placer OptionValue entre doubles guillemets, comme illustré dans l'exemple suivant : « sample value ».

Propriétés du service Apache Solr

Propriété	Description
Hôtes Solr	Liste de noms de domaine complets de nœuds séparée par des virgules qui hébergent le serveur Apache Solr.
Port Solr	Numéro de port configuré pour le serveur Apache Solr. La valeur par défaut est de 8983.
Répertoire d'installation de Solr	Spécifiez le chemin d'accès au répertoire d'installation d'Apache Solr Server. La valeur par défaut est <code><Cluster custom directory>/solr/install</code> .
Répertoire de données de Solr	Spécifiez le chemin d'accès au répertoire de stockage des données d'Apache Solr. La valeur par défaut est <code><Cluster custom directory>/solr/data</code> .
Options personnalisées de Solr	Spécifiez les options personnalisées pour le service au format suivant : <code>[OptionGroupName.OptionName = OptionValue]</code> . Vous pouvez séparer plusieurs options à l'aide d'un espace blanc. Si OptionValue comprend un espace blanc, vous devez placer OptionValue entre doubles guillemets, comme illustré dans l'exemple suivant : « sample value ».

Propriétés du service MongoDB

Propriété	Description
Hôtes MongoDB	Liste de noms de domaine complets de nœuds séparée par des virgules qui hébergent la base de données MongoDB.
Port MongoDB	Numéro de port configuré pour MongoDB. La valeur par défaut est de 27017. Remarque: Vous ne pouvez pas modifier le port MongoDB après avoir activé le service de cluster Informatica.
Répertoire de journaux de MongoDB	Spécifiez le chemin d'accès au répertoire de stockage des fichiers journaux. La valeur par défaut est <code><Cluster custom directory>/mongo/log</code> .

Propriété	Description
Répertoire de données de MongoDB	Spécifiez le chemin d'accès au répertoire de stockage des données de la base de données MongoDB. La valeur par défaut est <code><Cluster custom directory>/mongo/data</code> .
Options personnalisées de MongoDB	Spécifiez les options personnalisées pour le service au format suivant : <code>[OptionGroupName.OptionName = OptionValue]</code> . Vous pouvez séparer plusieurs options à l'aide d'un espace blanc. Si OptionValue comprend un espace blanc, vous devez placer OptionValue entre doubles guillemets, comme illustré dans l'exemple suivant : « sample value ».

Propriétés du service PostgreSQL

Propriété	Description
Hôte de base de données PostgreSQL	Nom de domaine complet de la machine qui héberge la base de données PostgreSQL. La valeur par défaut est l'hôte de passerelle. Remarque: Si vous n'avez pas sélectionné l'option Activer la configuration avancée, le service utilise la valeur d'hôte de passerelle spécifiée comme valeur d'hôte
Port de base de données PostgreSQL	Numéro de port configuré pour PostgreSQL. La valeur par défaut est de 5432.
Répertoire d'installation de la base de données PostgreSQL	Spécifiez le chemin d'accès au répertoire d'installation de la base de données PostgreSQL. La valeur par défaut est <code><Cluster custom directory>/postgres/install</code> .
Répertoire de journaux de la base de données PostgreSQL	Spécifiez le chemin d'accès au répertoire de stockage des fichiers journaux de la base de données PostgreSQL. La valeur par défaut est <code><Cluster custom directory>/postgres/log</code> .
Répertoire de données de la base de données PostgreSQL	Spécifiez le chemin d'accès au répertoire dans lequel vous souhaitez stocker les données PostgreSQL. La valeur par défaut est <code><Cluster custom directory>/postgres/data</code> .
Options personnalisées de la base de données PostgreSQL	Spécifiez les options personnalisées pour le service au format suivant : <code>[OptionGroupName.OptionName = OptionValue]</code> . Vous pouvez séparer plusieurs options à l'aide d'un espace blanc. Si OptionValue comprend un espace blanc, vous devez placer OptionValue entre doubles guillemets, comme illustré dans l'exemple suivant : « sample value ».

Associer le service de cluster Informatica au service de catalogue

Modifiez le service de catalogue dans Informatica Administrator pour associer le service de cluster Informatica au service de catalogue.

Activer et mettre à niveau le service de catalogue

Pour activer et mettre à niveau le service de catalogue, sélectionnez celui-ci, puis cliquez sur **Activer le service** depuis le menu **Actions** dans Informatica Administrator.

Après avoir démarré le service de catalogue, Informatica Administrator vous invite à mettre à niveau le service de catalogue.

Effectuez les étapes suivantes :

1. Mettez à niveau le service de catalogue.
2. Activez le service de messagerie si vous aviez configuré le service pour le service de catalogue.

Remarque:

- Si vous avez activé l'analyse des actifs de données, le démarrage du service de catalogue prend plus de temps. Le service ne sera pas disponible avant la fin de la mise à niveau du référentiel d'analyse des actifs de données.
- Pour connaître l'état de la mise à niveau du référentiel de l'analyse des actifs de données, reportez-vous au fichier `daa_upgrade.log` à partir du répertoire d'installation.
- Si vous avez activé l'analyse des actifs de données, exécutez ["Remplir les prérequis de l'analyse des actifs de données" à la page 47.](#)

Étape 7. Migrer et vérifier les données du catalogue

Migrer les données du catalogue

Utilisez la commande `infacmd.sh ldm migrateContents` pour migrer les données que vous avez sauvegardées à l'aide de l'utilitaire export.

Effectuez les étapes suivantes pour migrer les données de catalogue :

1. Définissez les variables d'environnement suivantes si le service de catalogue est activé pour SSL :
 - **INFA_TRUSTSTORE.** Consultez l'exemple de commande suivant pour définir la variable : `export INFA_TRUSTSTORE= <Location of the Informatica truststore file>`. L'emplacement par défaut est `<Informatica installation directory>/services/shared/security`.
 - **INFA_KEYSTORE.** Reportez-vous à l'exemple de commande suivant pour définir la variable : `export INFA_KEYSTORE=<Location of the keystore file>`. L'emplacement par défaut est `<Informatica installation directory>/services/shared/security`. Cette variable est requise uniquement si vous avez utilisé une configuration SSL personnalisée. Pour les configurations SSL et non-SSL par défaut, vous devez désactiver la variable.
 - **INFA_TRUSTSTORE_PASSWORD.** Chiffrez le mot de passe que vous avez défini. Reportez-vous à l'exemple de commande suivant pour définir le mot de passe chiffré : `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA=="`.
 - **INFA_KEYSTORE_PASSWORD.** Chiffrez le mot de passe que vous avez défini. Reportez-vous à l'exemple de commande suivant pour définir le mot de passe chiffré : `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI=="`. Cette variable est requise uniquement si vous avez utilisé une configuration SSL personnalisée. Pour les configurations SSL et non-SSL par défaut, vous devez désactiver la variable.

Vous pouvez contacter le support client international Informatica pour obtenir les mots de passe par défaut du truststore et du keystore.

Remarque: Reportez-vous à l'exemple de commande suivant pour chiffrer le mot de passe :

`<Informatica installation directory>/server/bin/pmpasswd <password>`.

2. Si les données de catalogue exportées sont volumineuses, mettez à jour la propriété `xdocs.content.systemProperties=-Xmx20G` dans le fichier `<Informatica installation directory>/`

services/CatalogService/Binaries/MigrationModuleConfigurations.properties, puis réinitialisez la propriété ICMD_JAVA_OPTS=-Xmx20g dans le fichier <Informatica installation directory>/isp/bin/infacmd.sh . Pour plus d'informations sur le dimensionnement des performances, reportez-vous au *Guide de réglage des performances d'Enterprise Data Catalog*.

3. Exécutez la commande infacmd.sh LDM migrateContents comme indiqué : ./infacmd.sh LDM migrateContents -un <Informatica domain user name> -pd <Informatica Domain Password> -dn <Informatica Domain Name> -sn <Name of the Catalog Service> -id <Export directory>

Remarque: L'élément <Export Directory> signifie le répertoire dans lequel le contenu sauvegardé est disponible.

Pour régler les paramètres de performances pour migrer les données ou ignorer des ressources ayant échoué, modifiez les paramètres spécifiés dans le fichier MigrationModuleConfigurations.properties disponible à l'emplacement suivant : <Informatica installation directory>/services/CatalogService/Binaries

Pour plus d'informations sur les paramètres de performances, reportez-vous au tableau suivant :

Propriété	Description
enableModule=	Définissez la valeur sur true si vous souhaitez activer un module spécifique, sinon définissez la propriété sur false. Par exemple, similarity.content.enableModule=true permet la migration des données de profilage de similarité.
Dblacklist =	Répertoriez les ressources à ignorer au format suivant : -Dblacklist=<resource name1>,<resource name2>
DmaxParallelRestores=	Spécifiez le nombre de threads à exécuter en parallèle lorsque vous migrez des données.
systemProperties=	Utilisez la propriété pour spécifier les ressources système à utiliser. Par exemple, xdocs.content.systemProperties=-Xmx6G -XX:+HeapDumpOnOutOfMemoryError

Vérifier les données de catalogue migrées

Vous pouvez utiliser la commande infacmd migrateContents -verify comme indiqué dans l'exemple suivant pour vérifier le contenu migré : ./infacmd.sh LDM migrateContents -un Administrator -pd Administrator -dn Domain -sn CS -id /data/Installer1050/properties/utils/upgrade/EDC/export -verify.

Après avoir exécuté la commande infacmd migrateContents -verify, celle-ci génère un fichier nommé results.txt.

Le tableau suivant décrit les messages qui s'affichent dans le fichier results.txt :

Message d'erreur	Description
missing from backup	Indique que certaines ressources ont été analysées avant de vérifier les données de catalogue migrées.
missing from warehouse	Indique que les actifs n'étaient pas compris dans la version 10.5.3.

Remarque: Assurez-vous que la ressource n'est pas purgée ou rechargée avant de vérifier les données de catalogue migrées.

CHAPITRE 5

Après la mise à niveau Catalogue de données d'entreprise

Ce chapitre comprend les rubriques suivantes :

- [Tâches générales postérieures à la mise à niveau, 110](#)
- [Importer les transports SAP, 111](#)
- [Mettre à jour les fichiers binaires pour les ressources Informatica Platform, 112](#)
- [Restaurer les enrichissements de ressources pour Tableau, 112](#)
- [Restaurer les enrichissements de ressources pour Erwin, 112](#)
- [Sauvegarder et restaurer des enrichissements de ressources pour SAP Business Objects, 113](#)
- [Tâches postérieures à la mise à niveau pour la ressource Qlik Sense, 114](#)
- [Tâches postérieures à la mise à niveau pour la ressource Salesforce, 114](#)
- [Afficher les résultats de similarité des colonnes, 114](#)
- [Synchroniser les événements d'actifs de données pour l'analyse des actifs de données, 115](#)
- [Restaurer les enrichissements de clé, 115](#)
- [Exécuter ou créer des ressources, 116](#)
- [Purger et réexécuter les ressources de référence, 117](#)
- [Tâches postérieures à la mise à niveau pour MetaDex, 118](#)
- [Mettre à jour les fichiers du pilote pour les ressources, 119](#)
- [Supprimer les ressources effacées migrées par l'utilitaire d'exportation, 120](#)
- [Tâche postérieure à la mise à niveau pour atténuer la vulnérabilité Log4j, 120](#)
- [Observations postérieures à la mise à niveau, 120](#)

Tâches générales postérieures à la mise à niveau

Après avoir mis à niveau le service de catalogue, effectuez les étapes suivantes :

- Après la mise à niveau vers la version 10.5.3, un message d'avertissement s'affiche dans Informatica Administrator pour le service de catalogue indiquant que vous n'avez pas configuré l'analyse des actifs de données. Vous pouvez configurer l'analyse des actifs de données pour Enterprise Data Catalog afin d'afficher des recommandations analytiques sur le catalogue sous la forme de rapports et de graphiques.

- Copiez les fichiers `odbc.ini` des répertoires externes vers les nouveaux répertoires correspondants créés après la mise à niveau. Vérifiez que les fichiers `odbc.ini` comprennent les entrées appropriées.
- Après la mise à niveau, la sensibilité à la casse est activée par défaut pour toutes les ressources du type **Gestion de fichiers et Nuage**.
- Après la mise à niveau, la sensibilité à la casse est désactivée pour toutes les ressources de type **Gestion de base de données**.

Remarque: Vous pouvez configurer les ressources pour la sensibilité à la casse selon les besoins et réexécuter la ressource.

- Installez l'agent Enterprise Data Catalog. Reportez-vous au [Informatica Catalog Administrator Guide](#) pour plus d'informations.
- Définissez à nouveau les mots vides si vous les avez définis dans la version précédente d'Enterprise Data Catalog.
- Si vous avez configuré des ressources de référence, vous devez les réexécuter.
- Si vous avez mis à niveau le référentiel d'analyse des actifs de données, supprimez la propriété `ProcessTerminationTimeout` que vous avez définie pour le domaine.

Effectuez les étapes suivantes pour modifier ou exécuter les ressources d'UCF après avoir mis à niveau le service de catalogue :

1. Contactez le support client international Informatica pour obtenir une licence UCF.
2. Appliquez la nouvelle licence UCF au service de catalogue.
3. Recyclez le service de catalogue.
4. Exécutez la ressource d'UCF.
5. Si l'analyse de la ressource d'UCF échoue, contactez le support client international Informatica.

Importer les transports SAP

Effectuez les étapes suivantes si vous utilisez les ressources SAP BW, SAP BW/4HANA et SAP S/4HANA :

1. Téléchargez les versions compatibles des transports SAP.
Remarque: Les transports se trouvent dans le fichier `SAP_Scanner_Binaries.zip` téléchargé à partir de l'emplacement du programme d'installation Informatica.
2. Importez les transports SAP dans le serveur SAP.

Mettre à jour les fichiers binaires pour les ressources Informatica Platform

Dans la version d'Enterprise Data Catalog 10.5.3, Informatica a mis à jour certains fichiers binaires que vous devez télécharger et installer pour exécuter les ressources Informatica Platform.

Le fichier ScannerBinaries.zip comprend les fichiers binaires de ressources Informatica Platform pour la version 10.5.3 et le fichier ExtendedScannerBinaries.zip comprend les fichiers binaires de ressources Informatica Platform de la version 10.2 à 10.5.2.

Après la mise à niveau d'Enterprise Data Catalog, effectuez les étapes suivantes si vous voulez exécuter les ressources Informatica Platform :

1. Téléchargez le fichier ZIP à partir d'Akamai Download Manager.
2. En fonction de la version de la ressource, extrayez la version requise du fichier zip vers l'emplacement suivant où vous avez installé Enterprise Data Catalog :

`<Informatica installation directory>/services/CatalogService/ScannerBinaries`

Important: Vérifiez que le répertoire contient uniquement la dernière version des fichiers binaires. Le répertoire doit comporter au moins 50 Go d'espace disque libre.

Restaurer les enrichissements de ressources pour Tableau

Après la mise à niveau d'Enterprise Data Catalog, les enrichissements des ressources Tableau sont perdus. Si le catalogue contient des ressources Tableau, vous devez restaurer les enrichissements de ressources à l'aide de l'utilitaire de migration.

1. Réexécutez la ressource Tableau.
2. Exportez les enrichissements à l'aide de la commande suivante :
`java -jar EnrichmentUtility.jar
export <Catalog Service hostname> <Catalog Service admin port number> <Username>
<Password> <Location to download enrichments json> <Resource name> <SSL enabled true/
false>.`

Remarque: Vous devez spécifier un nouveau répertoire pour stocker les fichiers JSON.

3. Exécutez la commande suivante pour restaurer les enrichissements :
`java -Xms512M -Xmx19524M -jar
EnrichmentUtility.jar import <Catalog Service host name> <Catalog Service admin port
number> <Username> <Password> <Location to the enrichment scanned in an earlier release>
<Location to the enrichment scanned in the current release> <SSL Enabled true/false>`

Restaurer les enrichissements de ressources pour Erwin

Si le catalogue contient des ressources Erwin, vous devez restaurer les enrichissements de ressources Erwin à l'aide de l'utilitaire de migration.

1. Réexécutez la ressource Erwin.

2. Exportez les enrichissements à l'aide de la commande suivante : `java -jar ErwinEnrichmentsCLIMigrator.jar export <Catalog Service hostname> <Catalog Service port number> <Catalog administrator user name> <Catalog administrator password> <location to download enrichments json> <resourceName> <SSL Enabled true/false>`

Remarque: Vous devez spécifier un nouveau répertoire pour stocker les fichiers JSON.
3. Exécutez la commande suivante pour restaurer les enrichissements : `java -Xms512M -Xmx19524M -jar ErwinEnrichmentsCLIMigrator.jar import <Catalog Service hostname> <Catalog Service port number> <Catalog administrator user name> <Catalog administrator password> <location to enrichment scanned in an earlier release> <location to enrichment scanned in the current release> <SSL Enabled true/false>`

Sauvegarder et restaurer des enrichissements de ressources pour SAP Business Objects

Après la mise à niveau, si le catalogue contient des ressources SAP Business Objects, effectuez les étapes suivantes pour exécuter l'utilitaire de migration avant d'exécuter la ressource :

1. Copiez et extrayez le fichier `BOEnrichmentsMigrator.jar` à partir de l'emplacement suivant sur la machine du domaine Informatica :
`<Informatica installation directory>/services/CatalogService/ScannerBinaries/bo-utility/lib`
2. Exécutez la commande suivante pour sauvegarder les enrichissements de la ressource SAP Business Objects :
`java -jar BOEnrichmentsMigrator.jar export <Catalog Service hostname> <Catalog Service port number> <Catalog administrator user name> <Catalog administrator password> <location to download enrichments json> <resourceName> <SSL Enabled true/false>`
3. Exécutez à nouveau la ressource.
4. Exportez les enrichissements à l'aide de la commande suivante :
`java -jar BOEnrichmentsMigrator.jar export <Catalog Service hostname> <Catalog Service port number> <Catalog administrator user name> <Catalog administrator password> <location to download enrichments json> <resourceName> <SSL Enabled true/false>`

Remarque: Vous devez spécifier un nouveau répertoire pour stocker les fichiers JSON.
5. Exécutez la commande suivante pour restaurer les enrichissements :
`java -Xms512M -Xmx19524M -jar BOEnrichmentsMigrator.jar import <Catalog Service hostname> <Catalog Service port number> <Catalog administrator user name> <Catalog administrator password> <location to enrichment scanned in an earlier release> <location to enrichment scanned in the current release> <SSL Enabled true/false>`

Tâches postérieures à la mise à niveau pour la ressource Qlik Sense

Après la mise à niveau d'Enterprise Data Catalog, les enrichissements des ressources Qlik Sense sont perdus. Si le catalogue contient des ressources Qlik Sense, vous devez restaurer les enrichissements des ressources à l'aide de l'utilitaire de migration.

1. Réexécutez la ressource Qlik Sense.
2. Exportez les enrichissements à l'aide de la commande suivante :

```
java -jar QlikSenseEnrichmentsCLIMigrator.jar export <Catalog Service hostname> <Catalog Service admin port number> <Username> <Password> <Location to download enrichments json> <Resource name> <SSL enabled true/false>.
```

Remarque: Vous devez spécifier un nouveau répertoire pour stocker les fichiers JSON.

3. Exécutez la commande suivante pour restaurer les enrichissements :

```
java -Xms512M -Xmx19524M -jar QlikSenseEnrichmentsCLIMigrator.jar import <Catalog Service host name> <Catalog Service admin port number> <Username> <Password> <Location to the enrichment scanned in an earlier release> <Location to the enrichment scanned in the current release> <SSL Enabled true/false>
```

Tâches postérieures à la mise à niveau pour la ressource Salesforce

Après la mise à niveau d'Enterprise Data Catalog, les enrichissements de la ressource Salesforce sont perdus. Si le catalogue contient des ressources Salesforce, vous devez restaurer les enrichissements des ressources à l'aide de l'utilitaire de migration.

1. Réexécutez la ressource Salesforce.
2. Exportez les enrichissements à l'aide de la commande suivante :

```
java -jar EnrichmentUtility.jar export <Catalog Service hostname> <Catalog Service admin port number> <Username> <Password> <Location to download enrichments json> <Resource name> <SSL enabled true/false>.
```

Remarque: Vous devez spécifier un nouveau répertoire pour stocker les fichiers JSON.

3. Exécutez la commande suivante pour restaurer les enrichissements :

```
java -Xms512M -Xmx19524M -jar EnrichmentUtility.jar import <Catalog Service host name> <Catalog Service admin port number> <Username> <Password> <Location to the enrichment scanned in an earlier release> <Location to the enrichment scanned in the current release> <SSL Enabled true/false>
```

Afficher les résultats de similarité des colonnes

Après avoir mis à niveau Enterprise Data Catalog, procédez comme suit pour afficher les résultats de similarité des colonnes de la version précédente d'Informatica dans la version actuelle :

1. Dans Catalog Administrator, réexécutez toutes les ressources existantes contenant des résultats de similarité.

2. Créez une ressource Informatica Similarity Discovery. Pour plus d'informations sur la création de ressources de découverte de similarité, reportez-vous à la rubrique Ressource Informatica Similarity Discovery du *Guide de configuration des scanners Informatica*.
3. Dans le champ **Ressources à regrouper**, sélectionnez les ressources à partir desquelles vous souhaitez afficher les résultats de similarité des colonnes dans Enterprise Data Catalog.
4. Exécutez la ressource Informatica Similarity Discovery.

Synchroniser les événements d'actifs de données pour l'analyse des actifs de données

Effectuez également les étapes suivantes pour synchroniser les événements d'actifs de données si vous avez configuré l'analyse des actifs de données pour la première fois dans la version actuelle :

1. Dans Informatica Administrator, ajoutez la propriété personnalisée `LdmCustomOptions.ingest.store.events.on.reindex.bool` pour le service de catalogue et définissez la valeur sur `true`.
2. Recyclez le service de catalogue.
3. Réindexez le service de catalogue.

Restaurer les enrichissements de clé

Après avoir effectué la mise à niveau vers Enterprise Data Catalog version 10.5.3, vous devez effectuer les étapes suivantes pour restaurer les enrichissements de clé primaire-clé étrangère à l'aide de l'utilitaire de migration :

1. Réexécutez toutes les ressources relationnelles et exportez les enrichissements à l'aide de la commande suivante :

```
java -jar PKFKErichmentsRestoreUtility.jar export <Catalog Service hostname>
<Catalog Service admin port number> <username> <password> <location to download
enrichments json> <comma separated resource type IDs> <SSL Enabled true false>
```

Veillez à fournir un emplacement différent pour stocker les fichiers JSON.

2. Exécutez la commande suivante pour restaurer les enrichissements :

```
java -Xms512M -Xmx19524M -jar PKFKErichmentsRestoreUtility.jar import <Catalog
Service hostname> <Catalog Service admin port number> <username> <password>
<location to enrichment scanned in an earlier release> <comma separated resource
type IDs> <SSL Enabled true false> <location to enrichment scanned in the current
release>
```

Exécuter ou créer des ressources

Après la mise à niveau d'Enterprise Data Catalog, vous devez réexécuter ou recréer les ressources pour utiliser certaines fonctionnalités.

Reportez-vous au tableau suivant pour décider si vous devez réexécuter ou recréer une ressource après la mise à niveau :

Nom de la ressource	Critères d'exécution de la ressource
PowerCenter	Exécutez la ressource pour obtenir le lignage au niveau des colonnes pour une ressource PowerCenter avec des sources et des cibles impliquant des fichiers locaux et un lignage pour la transformation WebService Java.
SQL Server Integration Service	Exécutez la ressource pour obtenir les fonctionnalités suivantes : <ul style="list-style-type: none">- Lignage détaillé de SQL Server Integration Service- Lignage au niveau des colonnes pour les sources et les cibles impliquant des fichiers- Lignage de contrôle et pont de référentiel de base de données SQL Server Integration Service.
Informatica Intelligent Cloud Service	Exécutez la ressource pour obtenir les fonctionnalités suivantes : <ul style="list-style-type: none">- Connectez Informatica Intelligent Cloud Service avec des connecteurs Common Client Interface basés sur le nuage, tels que :<ul style="list-style-type: none">- Amazon S3- Microsoft Azure Blob- Microsoft Azure Data Lake Store- Vérifiez le lignage au niveau des colonnes pour les sources et les cibles impliquant des fichiers locaux et des sources basées sur le nuage.
IBM InfoSphere DataStage	Exécutez la ressource pour obtenir le lignage au niveau des colonnes pour les sources et les cibles DataStage impliquant les fichiers locaux.
Informatica Platform	Exécutez la ressource pour obtenir le lignage au niveau des colonnes pour Data Engineering Integration avec les sources et les cibles suivantes : <ul style="list-style-type: none">- Fichiers locaux- Microsoft Azure Data Lake Store- Microsoft Azure Blob- Amazon S3
Hive	Exécutez la ressource pour inclure les objets de référence et l'attribution de connexions manuelles et automatiques pour les cas de schémas croisés lorsque vous analysez Hive en tant que ressources distinctes.
Microstrategy	Exécutez la ressource pour obtenir les modifications requises pour la correction du lignage, la suppression de l'encombrement et l'analyse incrémentielle. Les enrichissements sont perdus après la première réanalyse, mais ils sont conservés après les prochaines réanalyses.
Tableau	Exécutez la ressource pour obtenir des correctifs et des modifications d'ID d'objets. Les enrichissements sont perdus. Pour conserver les enrichissements, utilisez l'utilitaire de migration des enrichissements Tableau. Reportez-vous à la section "Sauvegarder les enrichissements de la ressource Tableau à l'aide de l'utilitaire de migration " à la page 53.
Qlik Sense	Exécutez la ressource pour obtenir les modifications de l'ID d'objet. Les enrichissements sont perdus. Pour conserver les enrichissements, utilisez l'utilitaire de migration des enrichissements Qlik Sense. Pour plus d'informations, reportez-vous à la section "Sauvegarder les enrichissements de la ressource Qlik Sense à l'aide de l'utilitaire de migration " à la page 53.

Nom de la ressource	Critères d'exécution de la ressource
IBM Cognos	Exécutez la ressource pour obtenir les modifications de l'ID d'objet. Les enrichissements sont perdus.
Oracle Business Intelligence	Exécutez la ressource pour obtenir les modifications de l'ID d'objet. Les enrichissements sont perdus.
Salesforce	Exécutez la ressource pour obtenir les modifications de l'ID d'objet. Les enrichissements sont perdus. Pour conserver les enrichissements, utilisez l'utilitaire de migration des enrichissements Salesforce. Pour plus d'informations, reportez-vous à la section "Sauvegarder les enrichissements de la ressource Salesforce à l'aide de l'utilitaire de migration" à la page 54.
Microsoft SQL Server	Exécutez la ressource pour inclure les objets de référence et l'attribution de connexions manuelles et automatiques pour les cas de schémas croisés lorsque vous analysez Microsoft SQL Server en tant que ressources distinctes.
Amazon S3	Exécutez la ressource pour inclure le profilage des fichiers Parquet sur le système de fichiers S3. Remarque: Passez le mode d'exécution en Spark et réexécutez la ressource avec le profilage.
Microsoft Azure Data Lake Store	Exécutez la ressource pour inclure l'extraction de métadonnées et le profilage des fichiers Parquet. Remarque: Passez le mode d'exécution à Spark et exécutez la ressource avec le profilage.
SAP BW	Exécutez la ressource pour inclure les fonctionnalités suivantes : <ul style="list-style-type: none"> - Lignage pour le module de fonction - Prise en charge du profilage des données - Filtrer en fonction des différents types d'actifs - Prise en charge d'une connexion réseau sécurisée
SAP BW/4HANA	Exécutez la ressource pour inclure les fonctionnalités suivantes : <ul style="list-style-type: none"> - Lignage pour le module de fonction - Prise en charge du profilage des données - Filtrer en fonction des différents types d'actifs - Prise en charge d'une connexion réseau sécurisée
SAP S/4HANA	Exécutez la ressource pour inclure les fonctionnalités suivantes : <ul style="list-style-type: none"> - Lignage pour le module de fonction - Prise en charge du profilage des données - Filtrer en fonction des différents types d'actifs - Prise en charge d'une connexion réseau sécurisée
Apache Atlas	Créez la ressource pour extraire le paramètre de filtre d'entités qui autorise la nouvelle syntaxe de recherche Atlas.
Workday	Exécutez la ressource pour inclure les HotFixes liés à un actif d'entité distribuée.

Purger et réexécuter les ressources de référence

Pour utiliser les fonctionnalités ajoutées aux ressources de référence après la mise à niveau vers Enterprise Data Catalog version 10.5.3, vous devez purger et réexécuter les ressources si vous les aviez utilisées avant la mise à niveau.

Tâches postérieures à la mise à niveau pour MetaDex

Pour utiliser les fonctionnalités ajoutées à MetaDex après avoir mis à niveau Enterprise Data Catalog, effectuez les tâches postérieures à la mise à niveau.

1. Sur la machine du serveur MetaDex, vérifiez que les variables d'environnement suivantes sont définies :
 - SCANNERS_HOME
 - SCANNERS_WORKSPACE

2. Associez Enterprise Data Catalog à MetaDex en effectuant les actions suivantes :

- a. Démarrez le service de catalogue dans Informatica Administrator.
- b. Connectez-vous à l'outil MetaDex en tant qu'administrateur.

Remarque: Vous pouvez accéder à l'interface Web en fournissant l'URL au format <host>:<port>. Où :

<host> représente le nom d'hôte configuré pour le domaine Informatica

<port> représente le numéro de port configuré pour le référentiel MetaDex.

Reportez-vous à la section « Connexion à l'outil MetaDex » du *Guide de l'administrateur de MetaDex*.

Pour une sécurité renforcée, vous devez modifier le mot de passe après vous être connecté pour la première fois.

- c. Dans l'en-tête, cliquez sur **Administration** et accédez à **Instance d'EDC**.
- d. Configurez les variables suivantes :

Variable	Valeur
EDC_USER	Nom d'utilisateur de l'administrateur du catalogue.
EDC_PASSWORD	Mot de passe configuré pour l'administrateur. Remarque: Lorsque vous ajoutez le mot de passe, dans la fenêtre Nouvelle variable globale , cliquez sur l'icône Chiffrer le mot de passe pour chiffrer le mot de passe.
EDC_URL	Nom d'hôte et numéro de port configurés pour Enterprise Data Catalog au format suivant : <host>:<port>

- e. Arrêtez le serveur MetaDex à l'aide de la commande `server.sh stop` disponible dans le répertoire suivant : <INFA_HOME>/services/CatalogService/AdvancedScannersApplication/app/.
 - f. Démarrez le serveur MetaDex à l'aide de la commande suivante : <Informatica installation directory>/services/CatalogService/AdvancedScannersApplication/app/server.sh
3. Pour charger la définition de modèle dans le catalogue, exécutez le script suivant : <Informatica installation directory>/services/CatalogService/AdvancedScannerApplication/app/utils/scanners/installScanners.sh
 4. Recyclez le service de catalogue.

5. En fonction des enrichissements pour MetaDex, effectuez l'une des actions suivantes :

Option	Description
Si aucun enrichissement n'a été configuré pour MetaDex	Actualisez les ressources MetaDex d'Enterprise Data Catalog avec le même nom en effectuant les actions suivantes : 1. Supprimez la ressource MetaDex existante dans Enterprise Data Catalog à l'aide de Catalog Administrator. 2. Exécutez la configuration de la ressource à partir de l'outil MetaDex avec le même nom de ressource.
Si des enrichissements ont été configurés pour MetaDex	Effectuez les actions suivantes : 1. Modifiez la configuration existante à partir de l'outil MetaDex et renommez la ressource Enterprise Data Catalog. 2. Exécutez la configuration mise à jour à partir de l'outil MetaDex. Remarque: Une ressource Enterprise Data Catalog est créée dans l'outil Catalog Administrator avec le nom que vous avez fourni dans la configuration. Cette ressource ne comprend aucun enrichissement. Vous devez attribuer les enrichissements manuellement. La ressource MetaDex existante comportant des métadonnées personnalisées est conservée avec des enrichissements.

Mettre à jour les fichiers du pilote pour les ressources

Après avoir mis à niveau Enterprise Data Catalog, mettez à jour les fichiers JAR du pilote à partir de l'installation précédente.

Effectuez les étapes suivantes pour copier les fichiers JAR du pilote :

1. Désactivez le service de catalogue.
2. Copiez les fichiers JAR du répertoire suivant : `<Backup directory>/services/CatalogService/ScannerJars/externalDependencies`.
3. Pour chaque type de ressource disponible dans le catalogue, copiez les fichiers JAR aux emplacements correspondants comme indiqué :

Oracle

Copiez `ojdbc7.jar` dans le répertoire suivant : `<Informatica installation directory>/services/CatalogService/ScannerJars/externalDependencies/OracleScanner`

Microsoft SQL Server

Copiez `mssql-jdbc-7.4.1.jre8.jar` dans le répertoire suivant : `<Informatica installation directory>/services/CatalogService/ScannerJars/externalDependencies/MSSQLServerScanner`

Microsoft Azure SQL Server

Copiez `mssql-jdbc-7.4.1.jre8.jar` dans le répertoire suivant : `<Informatica installation directory>/services/CatalogService/ScannerJars/externalDependencies/AzureMssqlScanner`

Microsoft Azure SQL Data Warehouse

Copiez mssql-jdbc-7.4.1.jre8.jar dans le répertoire suivant : <Informatica installation directory>/services/CatalogService/ScannerJars/externalDependencies/AzureSqlDWScanner

IBM DB2

Copiez db2jcc4.jar dans le répertoire suivant : <Informatica installation directory>/services/CatalogService/ScannerJars/externalDependencies/IBMDB2Scanner

4. Recyclez le service de catalogue.

Supprimer les ressources effacées migrées par l'utilitaire d'exportation

Lorsque vous exécutez l'utilitaire export.jar pour migrer des données dans le cadre de la mise à niveau depuis la version 10.4 ou 10.4.1, l'utilitaire exporte les xdocs des ressources effacées. Celles-ci peuvent alors s'afficher dans le catalogue. Pour récupérer la liste des ressources effacées et supprimer celles-ci du catalogue, exécutez la commande `infacmd ldm removeDeletedMigratedResources`.

Pour plus d'informations sur l'exécution de la commande, reportez-vous à la *Référence des commandes Informatica*.

Tâche postérieure à la mise à niveau pour atténuer la vulnérabilité Log4j

Pour atténuer la vulnérabilité Log4j, supprimez les versions précédentes des fichiers binaires des ressources Informatica Platform des nœuds de domaine Informatica et des nœuds qui exécutent le service de cluster Informatica. Pour plus d'informations, reportez-vous à l'article de la base de connaissances [Log4j remediation for Enterprise Data Catalog](#).

Observations postérieures à la mise à niveau

Dans Catalog Administrator, vous remarquerez peut-être une différence dans le nombre d'objets découverts pour les ressources avant et après la mise à niveau.

La non-correspondance d'objets se produit pour les raisons suivantes :

- Tous les objets auxquels aucun type de classe n'est associé ne sont pas stockés dans MongoDB.
- Pour les objets marqués comme insensibles à la casse dans le catalogue et marqués comme sensibles à la casse dans la source de données, un seul objet est inclus dans le nombre total d'objets.
- Pour les actifs de type table qui portent le même nom, mais avec des différences de casse, un seul objet est utilisé pour compter le nombre total d'objets.
- Pour les objets de référence, les objets proxy ne sont pas créés pour chaque répertoire, mais au maximum deux objets proxy sont ajoutés au nombre d'objets.

- Dans l'outil Catalog Administrator, onglet **Sécurité**, les noms des ressources de référence s'affichent au format suivant : <Resource name>\$\$<Provider ID>\$\$<Connection>.
- Dans l'outil Catalog Administrator, onglet **Attribution de connexion**, seules les attributions de connexion contenues dans le fichier XDOC de la ressource s'affichent.
- S'il existe des objets portant le même ID, un seul objet est ajouté au nombre d'objets.
- Si plusieurs valeurs d'un objet sont associées à une valeur d'attribut, toutes les valeurs sont incluses dans le nombre d'objets.
- Pour les ressources Teradata et Azure Microsoft SQL Server, le nombre affiché après la mise à niveau indique le nombre total de tous les actifs, qui n'était pas visible dans la version 10.4.1.
- Après avoir migré les données de catalogue dans le cadre de la mise à niveau, l'ID et le nom des objets de référence sont convertis en majuscules si la ressource à laquelle vous avez attribué la connexion est insensible à la casse.
- Pour une ressource de référence, le filtre d'accès ResourceName_ProviderId_Connexion sera supprimé et le filtre d'accès ResourceName\$\$ProviderId\$\$Connexion sera conservé

CHAPITRE 6

Dépannage de la mise à niveau

Ce chapitre comprend les rubriques suivantes :

- [Présentation du dépannage de la mise à niveau, 122](#)
- [Dépannage des problèmes de mise à niveau , 122](#)

Présentation du dépannage de la mise à niveau

Voici les problèmes que vous pourriez rencontrer lors de la mise à niveau du catalogue de données d'entreprise. Vous pouvez vous référer aux solutions fournies pour résoudre les problèmes.

Dépannage des problèmes de mise à niveau

Mise à niveau du catalogue

ICMD_10033] La commande [BackupData] a échoué avec l'erreur [[BackupRestoreClient_10002] L'erreur suivante s'est produite lors de la sauvegarde des données : [BackupRestoreClient_00027] Il existe déjà un instantané nommé [IdmCluster] dans le répertoire d'instantanés HDFS [/Informatica/LDM/IdmCluster].

L'erreur peut se produire en raison du déploiement d'un instantané externe du catalogue pour l'instance d'Enterprise Data Catalog dans un cluster interne.

Exécutez la commande `removesnapshot` pour supprimer l'instantané externe, puis exécutez la commande `BackupContents` pour en créer un autre.

org.apache.hadoop.ipc.RemoteException(java.io.IOException): File /tmp/cat_ihs_backup/scanner/MRS_INFACMD_10.zip could only be replicated to 0 nodes instead of minReplication (=1). There are 1 datanode(s) running and no node(s) are excluded in this operation.

Cette erreur peut se produire lors de la restauration des données HDFS si l'espace disque disponible est insuffisant sur la machine sur laquelle les données doivent être restaurées.

Vérifiez que la machine sur laquelle les données HDFS sont restaurées dispose d'un espace disque suffisant.

java.util.concurrent.ExecutionException: java.lang.OutOfMemoryError : limite de surcharge GC dépassée

Vous pouvez rencontrer cette erreur lorsque vous restaurez la sauvegarde du magasin de similarités et que la taille du segment de mémoire Java par défaut de 512 Mo est configurée.

Définissez la variable d'environnement ICMD_JAVA_OPTS sur -Xmx4096m pour augmenter la taille du segment de mémoire à 4 096 Mo.

Si la sauvegarde et la restauration échouent pour le service de catalogue, définissez les propriétés suivantes pour le cluster et restaurez le catalogue :

- `set -mode=HDFS`
- Pour un cluster externe, vérifiez que la propriété `yarn.nodemanager.aux-services` de YARN inclut `mapreduce_shuffle`.

Le mot de passe du keystore Informatica est incorrect ou corrompu.

Vérifiez que vous avez défini la variable d'environnement `INFA_KEYSTORE_PASSWORD` correctement.

Échec de la commande `[restorecontents]` avec l'erreur `[/data/Informatica/LDM/services/shared/security/infa_truststore.jks (No such file or directory)]`

Vérifiez que vous avez défini les variables d'environnement `INFA_TRUSTSTORE` et `INFA_TRUSTSTORE_PASSWORD` correctement.

Si la mise à niveau échoue pour un travail Nomad avec le message d'erreur suivant : la surveillance de la mise à niveau a trouvé `{0}` travaux en échec pour les ressources `{1}`. Où puis-je afficher les détails du fichier journal ?

Vous pouvez rechercher le fichier journal à l'emplacement suivant : `$ServiceLogDirectory/UpgradeJobs/`. Par exemple, `$ServiceLogDirectory/UpgradeJobs/Dummy_Upgrade_Module/DummyResource/0dafa11-adc0-4abe-8ca9-d48681b097d7/Publish/log.zip`

Où puis-je surveiller la progression de la mise à niveau ?

Vous pouvez surveiller la progression de la mise à niveau dans le fichier `LDM_Upgrade.log` à l'emplacement suivant : `$ServiceLogDirectory`.

Lorsque vous migrez les données sauvegardées du catalogue, le message d'erreur suivant s'affiche dans le fichier `Migration.log` : erreur du serveur sur `https://host.informatica.com:8983/solr/collection1` : erreur du serveur à la valeur `Null` : impossible d'analyser la réponse avec le codage `ISO-8859-1` `org.apache.solr.client.solrj.impl.HttpSolrClient$RemoteSolrException` : erreur du serveur sur `https://host.informatica.com:8983/solr/collection1` : erreur du serveur à la valeur `Null` : impossible d'analyser la réponse avec le codage `ISO-8859-1`

Vérifier que `ntpd` est synchronisé entre le nœud de domaine Informatica et les nœuds de cluster

Mise à niveau du domaine

Si la connexion SAML échoue avec le message d'erreur suivant : « `AADSTS900235` : la valeur `RequestedAuthenticationContext` Comparison de la demande d'authentification SAML doit être « exact ». Valeur reçue : « Minimum ». »

Modifiez la valeur de propriété de l'option Activer la comparaison de contexte d'autorisation=`EXACT` dans Informatica Administrator sous la section **Configuration SAML** de l'onglet **Service de catalogue > Processus**.

Après avoir activé le service de catalogue, l'outil Catalog Administrator n'est pas accessible

Supprimez les répertoires suivants :

```
<Informatica installation directory>/tomcat/temp/<Catalog Service name>
<Informatica installation directory>/services/CatalogService/ldmadmin
<Informatica installation directory>/services/CatalogService/ldmcatalog
```

Le service de cluster Informatica ne démarre pas

Ouvrez le fichier `sshd_config` à partir du répertoire suivant : `/etc/ssh`. Passez la valeur du paramètre `MaxSessions` à 60 et le paramètre `MaxStartups` à 1024, puis redémarrez le service démon SSH.

Le service de catalogue échoue avec le message d'erreur suivant : « unable to create INITIAL extent for segment in tablespace ».

Augmentez la taille de l'espace de table pour la base de données du service de référentiel modèle.

ANNEXE A

Mettre à niveau en mode silencieux

Pour mettre à niveau les services du domaine Informatica et d'application sans intervention de l'utilisateur, vous pouvez le faire en mode silencieux. Vous pouvez utiliser le fichier de propriétés fourni avec le programme d'installation pour spécifier les options de mise à niveau. Le programme d'installation lit le fichier pour déterminer les options de mise à niveau. Vous pouvez utiliser la mise à niveau en mode silencieux pour mettre à niveau les services du domaine Informatica sur plusieurs machines du réseau ou pour normaliser la mise à niveau entre les machines.

Pour mettre à jour en mode silencieux, effectuez les tâches suivantes :

1. Copiez les fichiers d'installation Informatica sur la machine qui héberge l'instance d'Informatica que vous prévoyez de mettre à niveau.
2. Configurez le fichier de propriétés de la mise à niveau et spécifiez les options de mise à niveau dans ce fichier.
3. Exécutez le programme de mise à niveau avec le fichier de propriétés.

Configuration du fichier de propriétés

Informatica fournit deux versions du fichier de propriétés. Vous pouvez utiliser l'un des fichiers suivants pour spécifier les options de cette mise à niveau.

Fichier SilentInput_upgrade_NewConfig.properties

Utilisez le fichier de propriétés de nouvelle configuration de mise à niveau d'entrée en mode silencieux pour mettre à niveau le domaine les services d'application et de domaine Informatica avec les modifications apportées à la configuration du nœud.

Le fichier de propriétés de nouvelle configuration de mise à niveau d'entrée en mode silencieux contient les propriétés nécessaires à la mise à niveau des services d'application et de domaine Informatica en mode silencieux. Utilisez ce fichier si vous souhaitez afficher les exemples de valeurs spécifiés pour chaque propriété.

Fichier SilentInput_upgrade.properties par défaut

Utilisez le fichier de propriétés de mise à niveau d'entrée en mode silencieux pour mettre à niveau les services d'application et de domaine Informatica sans interaction de l'utilisateur.

Le fichier de propriétés d'entrée silencieuse par défaut contient des valeurs par défaut pour de nombreuses propriétés de configuration. Vous pouvez utiliser ce fichier si vous prévoyez de mettre à niveau les services de domaine Informatica à l'aide des valeurs de propriétés par défaut.

Informatica fournit un exemple de fichier de propriétés qui inclut les paramètres requis par le programme de mise à niveau. Vous pouvez personnaliser l'exemple de fichier de propriétés pour spécifier les options de mise à niveau.

L'exemple de fichier de propriétés de mise à niveau est nommé `SilentInput_upgrade.properties` et se trouve à l'emplacement où vous avez téléchargé les fichiers du programme d'installation. Une fois que vous avez personnalisé le fichier, enregistrez-le avec le nom `SilentInput.properties`.

1. Accédez au répertoire de téléchargement des fichiers du programme d'installation.
2. Recherchez le fichier nommé `SilentInput_upgrade.properties`.
3. Sauvegardez le fichier `SilentInput_upgrade.properties` avant de le modifier.
4. Utilisez un éditeur de texte pour ouvrir le fichier et modifier les valeurs des paramètres de mise à niveau le cas échéant.

Le tableau suivant décrit les paramètres de mise à niveau que vous pouvez modifier :

Nom de la propriété	Description
ENABLE_USAGE_COLLECTION	Active Informatica DiscoveryIQ, un outil d'utilisation de produit qui envoie des rapports de routine quant à l'utilisation des données et aux statistiques du système Informatica. Informatica DiscoveryIQ charge les données vers Informatica 15 minutes après l'installation et la configuration du domaine Informatica. Ensuite, le domaine envoie des données tous les 30 jours. Vous pouvez choisir de ne pas envoyer de statistiques d'utilisation à Informatica. Pour en savoir plus sur la désactivation de l'envoi de statistiques d'utilisation, reportez-vous au <i>Guide d'Informatica Administrator</i> . Vous devez définir la valeur sur 1 pour effectuer la mise à niveau.
INSTALL_TYPE	Indique s'il faut installer Informatica ou le mettre à niveau. La valeur par défaut est 1. Pour effectuer une nouvelle installation d'Informatica, utilisez le fichier <code>SilentInput.properties</code> . Pour mettre à niveau Informatica vers une autre configuration de nœud, utilisez le fichier <code>SilentInput_upgrade_NewConfig.properties</code> .
INSTALL_LDM	Indique s'il faut également mettre à niveau Enterprise Data Catalog avec les services de domaine. La valeur par défaut est 0. Si la valeur est 1, le programme d'installation met à niveau une version précédente d'Informatica. Si la valeur est 0, le programme d'installation met à niveau Informatica sans Enterprise Data Catalog.
USER_INSTALL_DIR	Répertoire d'installation de la nouvelle version des services Informatica. Le répertoire ne peut pas être celui qui contient la version précédente des services Informatica.
UPG_BACKUP_DIR	Répertoire contenant la version précédente des services Informatica que vous souhaitez mettre à niveau.

Nom de la propriété	Description
INSTALLATION_ENVIRONMENT	<p>Représente l'environnement d'installation. Vous pouvez définir l'une des propriétés suivantes comme type d'environnement d'installation :</p> <ul style="list-style-type: none"> - Sandbox. Environnement de base utilisé comme preuve de concept avec un minimum d'utilisateurs. - Développement. Environnement de conception. - Test. Traitement de volume élevé proche de celui d'un environnement de production. - Production. Traitement de volume élevé avec des niveaux élevés d'accès concurrentiel pour les utilisateurs finaux. Les environnements de production avancés sont généralement des configurations à plusieurs nœuds. <p>Cette valeur est sensible à la casse.</p>
EDC_CATALOG_INST	Définissez la propriété sur true si le service de catalogue s'exécute sur le nœud que vous souhaitez mettre à niveau.
EDC_UPGR_BACKUP	Définissez la propriété sur true si vous avez exécuté l'utilitaire de sauvegarde du catalogue et la commande infacmd Idm BackupContents avant la mise à niveau.
EDC_BACKUP_DIR	Entrez l'emplacement du répertoire de sauvegarde du catalogue.
INSTALL_HADOOP_LIBRARIES	<p>Détermine s'il faut installer des packages pour intégrer le domaine à l'environnement Hadoop ou Databricks.</p> <p>Le domaine et le client Informatica nécessitent les packages d'intégration pour transférer le traitement vers Hadoop ou Databricks, pour traiter des fichiers complexes dans le domaine Informatica ou pour se connecter à Hadoop ou à Databricks lorsque vous les traitez dans le domaine Informatica.</p> <p>Si vous n'installez pas les packages d'intégration maintenant, vous pouvez le faire ultérieurement via Integration Package Manager.</p> <p>Définissez la valeur sur true si vous souhaitez installer les packages d'intégration.</p>
SELECTED_HADOOP_LIBRARIES	<p>Détermine les packages d'intégration que vous souhaitez installer à partir de la liste des packages pris en charge.</p> <p>Entrez les packages à installer. Séparez plusieurs packages par une virgule.</p> <p>Remarque: Les fichiers du programme d'installation des packages sélectionnés doivent être disponibles dans le répertoire : <code><Informatica installer files>/source</code></p>
DOMAIN_USER	Nom d'utilisateur du domaine Informatica.
DOMAIN_PSSWD	Mot de passe du domaine Informatica.
DOMAIN_CNFRM_PSSWD	Confirmez le mot de passe du domaine Informatica.
SECURITY_DOMAIN_NAME	Si vous ne souhaitez pas utiliser le domaine de sécurité par défaut, spécifiez le nom de domaine de sécurité que vous souhaitez utiliser.
KEY_DEST_LOCATION	Répertoire de stockage de la clé de chiffrement du nœud créé lors de l'installation.

Nom de la propriété	Description
CREATE_MDX_SERVICE	Définissez la valeur de la propriété sur true si vous souhaitez créer le référentiel MetaDex. Définissez la valeur de la propriété sur false si vous souhaitez créer le référentiel MetaDex.
MDX_DB_TYPE	La propriété représente le type de base de données pour le référentiel MetaDex. Définissez la propriété sur l'un des types de bases de données suivants : - Oracle - MSSQLServer Cette valeur est sensible à la casse.
MDX_DB_UNAME	Cette propriété représente le nom de compte d'utilisateur de la base de données pour le référentiel MetaDex.
MDX_DB_PASSWD	Cette propriété représente le mot de passe de base de données pour le compte d'utilisateur de la base de données.
MDX_SQLSERVER_SCHEMA_NAME	Cette propriété représente le nom du schéma. Vous devez configurer cette propriété si MDX_DB_TYPE=MSSQLServer
MDX_DB_SSL_ENABLED	Indique si la base de données du référentiel MetaDex est sécurisée ou non. Pour créer le référentiel de configuration du domaine dans une base de données sécurisée, définissez la valeur de propriété sur true. Pour utiliser l'option de chaîne personnalisée, si la propriété est définie sur true, vous devez définir la valeur de la propriété MDX_DB_CUSTOM_STRING sur 1. La propriété MDX_DB_CUSTOM_STRING doit inclure les paramètres de la base de données sécurisée suivants : - EncryptionMethod=SSL - HostNameInCertificate= - ValidateServerCertificate=
MDX_DB_TRUSTSTORE_FILE	Indique le chemin et le nom du fichier truststore de la base de données du référentiel MetaDex. La propriété est requise si vous définissez la valeur de propriété MDX_DB_SSL_ENABLED sur true.
MDX_DB_TRUSTSTORE_PASSWD	Mot de passe du fichier truststore pour la base de données du référentiel MetaDex. La propriété est requise si vous définissez la valeur de propriété MDX_DB_SSL_ENABLED sur true.
MDX_SSL_DEFAULT_STRING	Cette propriété est requise uniquement si la valeur de la propriété MDX_DB_SSL_ENABLED est définie sur true. Cette propriété doit inclure les paramètres de la base de données sécurisée suivants : - EncryptionMethod=SSL - HostNameInCertificate= - ValidateServerCertificate=
MDX_DB_CUSTOM_STRING	Cette propriété représente une chaîne de connexion JDBC personnalisée valide.

Nom de la propriété	Description
MDX_SERVER_PORT	La propriété représente le port du serveur de base de données du référentiel MetaDex.
MDX_SSL_ENABLED	Facultatif. Définissez cette propriété sur true si vous souhaitez activer la communication sécurisée à la base de données MetaDex.
MDX_CUSTOM_SELECTION	Vous devez configurer la propriété si la propriété MDX_SSL_ENABLED est définie sur true. Pour utiliser les fichiers de certificat SSL par défaut, définissez la propriété MDX_CUSTOM_SELECTION sur false. Pour utiliser les fichiers de certificat SSL personnalisés, définissez la propriété MDX_CUSTOM_SELECTION sur true. La valeur par défaut est false.
MDX_KEYSTORE_FILE	Vous devez configurer les propriétés suivantes si la propriété MDX_CUSTOM_SELECTION est définie sur true. - MDX_KEYSTORE_PASSWD - MDX_KEYSTORE_TYPE - MDX_KEYSTORE_ALIAS Il n'est pas nécessaire de configurer la propriété MDX_KEYSTORE_FILE si la propriété MDX_CUSTOM_SELECTION est définie sur false.
MDX_KEYSTORE_PASSWD	Mot de passe du keystore.
MDX_KEYSTORE_TYPE	Indique le type du certificat du keystore.
MDX_KEYSTORE_ALIAS	La propriété représente l'alias du keystore.

- Enregistrez le fichier de propriétés sous le nom SilentInput.properties.

Exécution du programme d'installation silencieuse

Effectuez les étapes suivantes pour exécuter le programme d'installation silencieuse :

- Accédez au répertoire contenant les fichiers d'installation.
- Vérifiez que le répertoire contient l'élément SilentInput.properties que vous avez mis à jour avec les options de mise à niveau.
- Sur une ligne de commande shell, entrez la commande suivante pour exécuter le programme d'installation silencieuse : `./silentInstall.sh`.

Le programme de mise à jour silencieuse s'exécute en tâche de fond. Le processus peut prendre du temps. Le processus de mise à niveau silencieuse est terminé lorsqu'Informatica_<Version>_Services_InstallLog<timestamp>.log est créé dans le répertoire d'installation.

La mise à niveau silencieuse échoue si vous n'avez pas configuré le fichier de propriétés correctement ou si le répertoire d'installation n'est pas disponible. Si la mise à niveau échoue, corrigez les erreurs dans le fichier journal silentErrorLog.log et réexécutez la commande.

ANNEXE B

Installation et suppression des distributions tierces

Cette annexe comprend les rubriques suivantes :

- [Présentation de l'installation et de la suppression des distributions tierces, 130](#)
- [Présentation d'Integration Package Manager, 131](#)
- [Avant de commencer, 131](#)
- [Installer ou supprimer des distributions en mode console, 132](#)
- [Installer ou supprimer des distributions en mode silencieux, 132](#)
- [Configurer les variables d'environnement pour utiliser les distributions installées, 133](#)

Présentation de l'installation et de la suppression des distributions tierces

Le programme d'installation d'Informatica n'inclut pas les distributions tierces. Vous pouvez télécharger et installer les distributions avec le programme d'installation d'Informatica lorsque vous installez, mettez à niveau ou appliquez le HotFix aux services Informatica et aux machines clientes. Dans un domaine existant, vous pouvez utiliser l'utilitaire nommé Integration Package Manager pour installer ou supprimer les distributions des services Informatica et des machines clientes.

Les machines de service et clientes nécessitent des distributions dans les scénarios suivants :

- Pour transférer le traitement vers l'environnement Hadoop ou Databricks.
- Pour traiter des fichiers complexes dans le domaine Informatica.
- Pour vous connecter à l'environnement Hadoop ou Databricks en cas de traitement dans le domaine Informatica.

Présentation d'Integration Package Manager

Dans un domaine existant, vous pouvez utiliser Integration Package Manager pour installer ou supprimer des distributions tierces. Les distributions doivent être installées ou supprimées sur toutes les machines de service ou clientes. Vous pouvez exécuter Integration Package Manager en mode console ou silencieux.

Vous pouvez utiliser Integration Package Manager dans les scénarios suivants dans un domaine existant :

- Pour installer une ou plusieurs distributions supplémentaires.
- Pour supprimer les distributions inutilisées existantes.

Avant de commencer

Avant d'exécuter Integration Package Manager, téléchargez les fichiers de celui-ci et du programme du programme d'installation de distribution tiers.

1. Arrêtez les services Informatica.
2. Définissez les variables d'environnement suivantes :

Variable	Description
INFA_JDK_HOME	Emplacement du dossier qui contient le kit de développement Java (JDK) pris en charge. Définissez la variable d'environnement INFA_JDK_HOME dans les scénarios suivants : <ul style="list-style-type: none">- Le domaine Informatica se trouve sur la plate-forme Windows ou Linux- Client Informatica
INFA_JRE_HOME	Emplacement du dossier contenant le Java Runtime Environment (JRE) pris en charge. Si le domaine Informatica est sur la plate-forme AIX, définissez la variable d'environnement INFA_JRE_HOME.

3. Vérifiez que vous disposez des autorisations suivantes :
 - Autorisations de lecture et d'écriture sur le répertoire d'installation.
 - Autorisation d'exécution sur les fichiers exécutables.
4. Téléchargez les fichiers suivants depuis l'emplacement de téléchargement d'Akamai vers un répertoire local ou un lecteur réseau partagé mappé à votre machine :
 - Fichier ZIP d'Integration Package Manager
 - Fichiers ZIP de distribution que vous souhaitez installer
5. Extrayez le fichier ZIP d'Integration Package Manager sur un lecteur local.
6. Copiez les fichiers ZIP de distribution à l'emplacement suivant : `<Integration Package Manager directory>/source`

Installer ou supprimer des distributions en mode console

Vous pouvez exécuter Integration Package Manager en mode console pour installer une ou plusieurs distributions ou pour supprimer des distributions existantes. Vous devez installer ou supprimer les distributions sur toutes les machines de service ou clientes.

1. Dans le répertoire d'Integration Package Manager, exécutez l'une des commandes suivantes :

- Linux ou UNIX :

```
./Server.sh console
```

- Windows :

```
Server.bat console
```

- Client :

```
Client.bat console
```

Remarque: Pour les services Informatica sur la plate-forme Windows et sur les machines clientes, exécutez la commande dans l'invite de commandes de l'administrateur.

2. Entrez le répertoire d'installation des services ou du client et appuyez sur **Entrer**.

3. Choisissez le type d'opération et appuyez sur **Entrer**.

- Sélectionnez 1 pour supprimer les distributions existantes.
- Sélectionnez 2 pour installer une ou plusieurs distributions.

La console répertorie les distributions que vous pouvez installer ou supprimer.

4. Entrez les distributions que vous souhaitez installer ou supprimer, en séparant plusieurs distributions par une virgule et appuyez sur **Entrer**.

5. Vérifiez le statut de l'installation ou de la suppression dans le fichier journal d'Integration Package Manager.

Vous trouverez le fichier journal à l'emplacement suivant : <Integration Package Manager directory>/ IntegrationPackageManager_<date and timestamp>.log

Installer ou supprimer des distributions en mode silencieux

Vous pouvez exécuter Integration Package Manager en mode silencieux pour installer une ou plusieurs distributions ou pour supprimer des distributions existantes. Vous devez installer ou supprimer les distributions sur toutes les machines de service ou clientes. Le fichier de propriétés d'entrée en mode silencieux pour Integration Package Manager contient les propriétés permettant d'installer ou de supprimer les distributions en mode silencieux pour les services et les clients. Définissez la valeur appropriée pour chaque propriété du fichier.

1. Recherchez le fichier de propriétés d'entrée en mode silencieux à l'emplacement suivant :

```
<Integration Package Manager directory>/IntegrationPackageManager.properties
```

2. Modifiez le fichier de propriétés dans un éditeur de texte.

Le tableau suivant décrit les propriétés que vous pouvez modifier :

Nom de la propriété	Description
USER_INSTALL_DIR	Répertoire d'installation du service ou du client.
OPERATION_TYPE	Opération à effectuer : <ul style="list-style-type: none"> - Définissez la propriété sur DELETE pour supprimer les distributions existantes. - Définissez la propriété sur EXTRACT pour installer une ou plusieurs distributions.
SELECTED_HADOOP_LIBRARIES	Répertorie les distributions et les versions. Entrez les distributions à installer ou à supprimer. Séparez plusieurs distributions par une virgule. Remarque: Si vous souhaitez installer des distributions, assurez-vous que les fichiers de distribution sont disponibles à l'emplacement suivant : <Integration Package Manager directory>/source

- Enregistrez le fichier de propriétés.
- Dans le répertoire d'Integration Package Manager, exécutez l'une des commandes suivantes :
 - Linux ou UNIX :

```
./Server.sh silent
```
 - Windows :

```
Server.bat silent
```
 - Client :

```
Client.bat silent
```

Remarque: Pour les services Informatica sur la plate-forme Windows et sur les machines clientes, exécutez la commande dans l'invite de commandes de l'administrateur.
- Vérifiez le statut de l'installation ou de la suppression dans le fichier journal d'Integration Package Manager.

Le fichier journal se trouve à l'emplacement suivant :

```
<Integration Package Manager directory>/ IntegrationPackageManager_<date and timestamp>.log
```

Configurer les variables d'environnement pour utiliser les distributions installées

Pour utiliser les distributions installées à l'aide d'Integration Package Manager, configurez les variables d'environnement dans les machines de service et clientes.

Configurer Informatica Developer

Après avoir installé les distributions dans l'outil Developer tool, mettez à jour le fichier developerCore.ini avec la distribution installée.

1. Recherchez le fichier developerCore.ini à l'emplacement suivant :
`<Informatica installation directory>\clients\DeveloperClient`
2. Modifiez le fichier pour mettre à jour la propriété suivante :
`-DINFA_HADOOP_DIST_DIR=hadoop\<Hadoop distribution name>_<version>`
3. Redémarrez l'outil Developer tool.

Configurer le service d'intégration de données

Pour traiter les fichiers complexes dans certains adaptateurs PowerExchange, configurez la variable d'environnement INFA_PARSER_HOME dans le service d'intégration de données.

Les adaptateurs suivants nécessitent une configuration de variable d'environnement :

- PowerExchange for Amazon S3
- PowerExchange for Google Cloud Storage
- PowerExchange for HDFS
- PowerExchange for Microsoft Azure Blob Storage
- PowerExchange for Microsoft Azure Data Lake Storage Gen1
- PowerExchange for Microsoft Azure Data Lake Storage Gen2

Pour configurer la propriété INFA_PARSER_HOME, procédez comme suit :

1. Connectez-vous à Informatica Administrator.
2. Cliquez sur le service d'intégration de données, puis sur l'onglet **Processus** dans le volet de droite.
3. Cliquez sur **Modifier** dans la section **Variables d'environnement**.
4. Cliquez sur **Nouveau** pour ajouter une variable d'environnement.
5. Entrez le nom de la variable d'environnement comme suit : INFA_PARSER_HOME.
6. Associez à la variable d'environnement le chemin d'accès absolu du répertoire de distribution Hadoop sur l'ordinateur qui exécute le service d'intégration de données.
7. Recyclez le service d'intégration de données.

Configurer le service d'accès aux métadonnées

Pour importer les métadonnées des fichiers complexes dans certains des adaptateurs PowerExchange, configurez la variable d'environnement INFA_PARSER_HOME pour le service d'accès aux métadonnées dans Informatica Administrator.

Les adaptateurs suivants nécessitent une configuration de variable d'environnement :

- PowerExchange for Google Cloud Storage
- PowerExchange for Microsoft Azure Data Lake Storage Gen2

Pour configurer la propriété INFA_PARSER_HOME, procédez comme suit :

1. Connectez-vous à Informatica Administrator.
2. Cliquez sur le service d'accès aux métadonnées, puis sur l'onglet **Processus** dans le volet de droite.
3. Cliquez sur **Modifier** dans la section **Variables d'environnement**.

4. Cliquez sur **Nouveau** pour ajouter une variable d'environnement.
5. Entrez le nom de la variable d'environnement comme suit : INFA_PARSER_HOME.
6. Définissez la valeur de la variable d'environnement INFA_PARSER_HOME sur le chemin d'accès absolu du répertoire de distribution Hadoop sur la machine qui exécute le service d'accès aux métadonnées.

```
<Informatica installation directory>/Informatica/services/shared/hadoop/<Hadoop  
distribution name>_<version>
```
7. Vérifiez que la même version de la distribution Hadoop est configurée dans les propriétés suivantes :
 - Propriété INFA_PARSER_HOME pour le service d'accès aux métadonnées dans l'outil Administrator tool.
 - -Variable d'environnement DINFA_HADOOP_DIST_DIR dans le fichier developerCore.ini sur la machine sur laquelle vous avez installé Informatica Developer.

INDEX

M

mode console
mise à niveau des services Informatica [58, 93](#)
mode silencieux
mise à niveau des services Informatica [125](#)

S

services Informatica
mise à niveau en mode console [58, 93](#)

services Informatica (*a continué*)
mise à niveau en mode silencieux [125](#)

U

UNIX
mise à niveau des services Informatica en mode console [58, 93](#)