



Informatica®

10.2 .2

Guide d'installation et de configuration d'Enterprise Data Catalog

© Copyright Informatica LLC 2015, 2019

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. Une liste actuelle des marques déposées d'Informatica est disponible sur le site <http://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.

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

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 LÉTAT », SANS GARANTIE NI CONDITION D'AUCUNE SORTE, expresse ou implicite. Se reporter aux Licences pour la langue spécifique régissant les droits et limitations dans le cadre des Licences.

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

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

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

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

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

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

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

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

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

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

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

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

Ce produit comprend des logiciels sous licence dont les conditions se trouvent aux adresses : <http://www.tcl.tk/software/tcltk/license.html>, <http://www.bosrup.com/web/overlib/?License>, <http://www.stlport.org/doc/license.html>, <http://asm.ow2.org/license.html>, <http://www.cryptix.org/LICENSE.TXT>, <http://>

hsqldb.org/web/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- 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/javaservice/>, <http://www.postgresql.org/about/licence.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.

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

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

Date de publication: 2019-05-17

Sommaire

Préface.....	10
Ressources Informatica.....	10
Informatica Network.....	10
Base de connaissances Informatica.....	10
Documentation Informatica.....	11
Matrices de disponibilité des produits Informatica.....	11
Informatica Velocity.....	11
Informatica Marketplace.....	11
Support client international Informatica.....	11
Partie I: Présentation de l'installation.....	12
Chapitre 1: Enterprise Data Catalog.....	13
Présentation de l'installation d'Enterprise Data Catalog.....	13
Installation Processus.....	14
Services d'Enterprise Data Catalog.....	15
Référentiels d'Enterprise Data Catalog.....	16
Liste de contrôle de l'installation et de la configuration.....	16
Partie II: Avant l'installation Enterprise Data Catalog.....	18
Chapitre 2: Planification du domaine.....	19
Introduction au domaine Informatica.....	19
Domaine à un ou plusieurs nœuds.....	19
Nœuds.....	20
Gestionnaire de service.....	21
Services d'application.....	21
Clé de licence.....	22
Authentification utilisateur.....	22
Clé de chiffrement pour le stockage des données sécurisé.....	22
Sécurité de domaine.....	23
Clients Informatica.....	23
Processus de planification de domaine.....	24
Planification des services d'application.....	25
Service d'intégration de données.....	25
Service de référentiel modèle.....	26
Service de catalogue.....	26
Service de cluster Informatica.....	27
Service de gestion de contenu.....	27
Vérification de la configuration système requise.....	28

Vérification des spécifications d'installation des services.	28
Vérification de l'espace disque temporaire requis.	28
Vérifications des spécifications de port.	29
Vérification des spécifications de la base de données.	30
Vérification de la configuration matérielle des services d'application.	31
Enregistrer les informations relatives au domaine et au nœud Informatica.	32
Conventions de dénomination d'objet de domaine.	32
Domaine.	33
Nœuds.	34
Services d'application.	34
Stockage des données sécurisé.	35
Sécurité de domaine.	35
Chapitre 3: Préparer les bases de données pour le domaine Informatica	37
Préparer les bases de données du domaine Informatica - Présentation.	37
Configurer des comptes utilisateur de base de données	38
Spécifications de la base de données du référentiel de configuration du domaine.	38
Prérequis de la base de données IBM DB2.	38
Configuration requise pour la base de données Microsoft SQL Server.	40
Spécifications de la base de données Oracle.	40
Spécifications de la base de données Sybase ASE.	41
Spécifications de la base de données du cache d'objet de données.	41
Spécifications de la base de données IBM DB2.	42
Spécifications de la base de données Microsoft SQL Server.	42
Configuration requise pour la base de données Oracle.	42
Configuration requise pour la base de données du référentiel modèle.	43
Prérequis de la base de données IBM DB2.	43
Configuration requise pour la base de données Microsoft SQL Server.	45
Configuration requise pour la base de données Oracle.	45
Configuration requise pour l'entrepôt de profilage profilage.	45
Configuration requise pour la base de données IBM DB2.	46
Spécifications de la base de données Microsoft SQL Server.	46
Configuration requise de la base de données Oracle.	46
Spécifications de l'entrepôt de données de référence.	47
Spécifications de la base de données IBM DB2.	47
Spécifications de la base de données Microsoft SQL Server.	48
Configuration requise pour la base de données Oracle.	48
Chapitre 4: Méthodes de déploiement.	49
Présentation des méthodes de déploiement.	49
Déploiement du cluster Hadoop intégré Prérequis.	49
Prérequis du cluster intégré	50
Prérequis du système d'exploitation.	50

Prérequis du nœud hôte.	53
Prérequis pour déployer Enterprise Data Catalog sur plusieurs nœuds.	53
Prérequis du nœud de cluster.	54
Prérequis d'Apache Ambari.	54
Prérequis d'Apache Ranger.	54
Limite de descripteurs de fichiers.	54
Prérequis de SSL.	54
Prérequis de Kerberos.	55
Service de cluster Informatica.	55
Préparation de l'environnement de cluster Hadoop intégré.	60
Gestion des nœuds de cluster intégré.	60
Prérequis du cluster existant.	61
Prérequis du nœud hôte.	61
Prérequis du nœud de cluster.	61
Prérequis d'Apache Ranger.	61
Limite de descripteurs de fichiers.	61
Prérequis de SSL.	62
Prérequis de Kerberos.	62
Prérequis du domaine Informatica.	63
Autorisations de l'utilisateur.	63
Déploiement du cluster Hadoop existant.	63
Préparation de l'environnement de cluster Hadoop existant.	64
Configuration de Kerberos et de SSL pour un cluster existant.	64
Partie III: Installation d'Enterprise Data Catalog.	67
Chapitre 5: Installation des services d'Enterprise Data Catalog.	68
Présentation de l'installation des services d'Enterprise Data Catalog.	68
Reprise de l'installation.	69
Créer ou joindre un domaine.	69
Installation des services d'Enterprise Data Catalog en mode console.	70
Répertoire sécurisé pour la clé de chiffrement et les fichiers de configuration.	70
Installation en joignant un domaine.	85
Installation de Enterprise Data Catalog sur un nœud de domaine.	95
Création des services d'application Enterprise Data Catalog.	96
Installation d'Enterprise Data Catalog en mode silencieux.	107
Configuration du fichier de propriétés.	107
Exécution du programme d'installation silencieux.	125
Installation des services d'application Enterprise Data Catalog en mode silencieux.	125
Configuration du fichier de propriétés.	126
Exécution du programme d'installation silencieuse pour installer les services.	126
Sécurisation des mots de passe dans le fichier de propriétés.	127

Partie IV: Après l'installation d'Enterprise Data Catalog.....	128
Chapitre 6: Configuration du domaine.....	129
Présentation de la configuration du domaine.	129
Vérification de la compatibilité de la page de code.	129
Configurer les variables d'environnement régionales sur Linux.	130
Configuration des variables d'environnement.	130
Configurer les variables d'environnement d'Enterprise Data Catalog.	130
Configurer les variables d'environnement de chemin de bibliothèque sous Linux.	132
Privilèges du service de catalogue.	132
Chapitre 7: Préparation de la création des services d'application.....	134
Préparation de la création des services d'application - Présentation.	134
Connexion à Informatica Administrator.	134
Création de connexions.	135
Propriétés de la connexion IBM DB2.	136
Propriétés de connexion Microsoft SQL Server.	137
Propriétés de connexion Oracle.	138
Création d'une connexion.	139
Chapitre 8: Créer les services d'application.....	140
Créer des services d'applications - Présentation.	140
Vérification des prérequis du service d'application.	140
Dépendances des services d'application.	142
Créer et configurer le service de référentiel modèle.	142
Créer le service de référentiel modèle.	142
Après la création du service de référentiel modèle.	145
Créer et configurer le service d'intégration de données.	147
Créer le service d'intégration de données.	147
Après la création du service d'intégration de données.	150
Création d'un service de catalogue.	150
Configuration du service de catalogue pour Azure HDInsight.	155
Créer et configurer le service de gestion de contenu.	156
Créer le service de gestion de contenu.	157
Chapitre 9: Configuration de l'authentification unique avec l'authentification SAML.....	159
Présentation de l'authentification unique utilisant l'authentification SAML.	159
Configuration du paramètre d'URL Relaystate par défaut dans OKTA.. . . .	159
Configuration des points de terminaison d'URL des applications d'Enterprise Data Catalog dans les services de fédération Active Directory (AD FS).	160

Partie V: Désinstallation.....	161
Chapitre 10: Désinstallation.....	162
Présentation de la désinstallation.	162
Règles et instructions pour la désinstallation.	162
Désinstallation d'Enterprise Data Catalog.	163
Désinstallation d'Enterprise Data Catalog en mode silencieux.	163
Partie VI: Dépannage.....	164
Chapitre 11: Dépannage	165
Présentation du dépannage.	165
Dépannage à l'aide des fichiers journaux d'installation.	165
Fichiers journaux de débogage.	166
Fichier journal d'installation.	166
Fichiers journaux de Service Manager.	166
Dépannage des domaines et des nœuds.	167
Création du référentiel de configuration de domaine.	167
Création ou jointure d'un domaine.	168
Exécution d'une ressource.	168
Démarrage d'Enterprise Data Catalog.	168
Ping sur le domaine.	169
Ajout d'une licence.	169
Dépannage des problèmes courants de déploiement des clusters.	169
Dépannage du déploiement de clusters existants.	175
Dépannage du déploiement de clusters incorporés.	176
Dépannage des problèmes liés au services d'application.	180
Annexe A: Démarrage et arrêt des services d'Enterprise Data Catalog.....	181
Démarrage et arrêt des services d'Enterprise Data Catalog sous Linux.	181
Arrêt des services d'Enterprise Data Catalog dans l'outil Administrator tool.	181
Règles et instructions de démarrage et d'arrêt d'Enterprise Data Catalog.	182
Annexe B: Supprimer l'accès sudo après la création d'un cluster incorporé..	183
Suppression de l'accès sudo après la création d'un cluster incorporé.	183
Annexe C: Configurer un répertoire journal personnalisé pour Ambari.....	185
Configuration d'un répertoire journal personnalisé pour Ambari.	185
Annexe D: Configurer Enterprise Data Catalog pour un cluster avec WANdisco Fusion activé.....	186
Configuration d'Enterprise Data Catalog pour un cluster avec WANdisco Fusion activé.	186

Annexe E: Configurer Informatica Custom Service Descriptor.....	188
Présentation.	188
Prérequis.	189
Création du service Informatica Custom Service Descriptor.	189
Foire aux questions.	191
Annexe F: Créer des utilisateurs et des groupes d'utilisateurs personnalisés pour les services déployés dans un cluster incorporé.....	192
Présentation.	192
Prérequis.	193
Création d'utilisateurs et de groupes d'utilisateurs personnalisés pour les services déployés dans un cluster incorporé.	193
Annexe G: Configurer des ports personnalisés pour les applications Hadoop.....	195
Présentation.	195
Configuration de ports personnalisés pour les applications Hadoop.	197
Index.	198

Préface

Le *Guide d'installation et de configuration Informatica* est écrit pour l'administrateur système responsable de l'installation du produit Informatica. Ce guide part du principe que vous connaissez les systèmes d'exploitation, les concepts des bases de données relationnelles, ainsi que les moteurs de base de données, les fichiers plats ou les systèmes mainframe de votre environnement. Il suppose également que vous êtes familier des spécifications requises en matière d'interface pour vos applications.

Ressources Informatica

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

Informatica Network

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

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

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

Base de connaissances Informatica

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

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

Documentation Informatica

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

Informatica conserve la documentation de nombreux produits dans la base de connaissances Informatica, ainsi que sur le portail de documentation. Si vous ne trouvez pas la documentation de votre produit ou version de produit sur le portail de documentation, recherchez dans la base de connaissances à l'adresse <https://search.informatica.com>.

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

Matrices de disponibilité des produits Informatica

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

Informatica Velocity

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

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

Informatica Marketplace

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

Support client international Informatica

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

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

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

Partie I : Présentation de l'installation

- [Enterprise Data Catalog, 13](#)

CHAPITRE 1

Enterprise Data Catalog

Ce chapitre comprend les rubriques suivantes :

- [Présentation de l'installation d'Enterprise Data Catalog, 13](#)
- [Installation Processus, 14](#)
- [Services d'Enterprise Data Catalog, 15](#)
- [Référentiels d'Enterprise Data Catalog, 16](#)
- [Liste de contrôle de l'installation et de la configuration, 16](#)

Présentation de l'installation d'Enterprise Data Catalog

Informatica fournit un programme d'installation unique qui installe Enterprise Data Catalog et ses services. Enterprise Data Catalog est installé dans le domaine Informatica. Enterprise Data Catalog utilise le service de catalogue et d'autres services d'application pour regrouper des ressources de données configurées dans une entreprise et présenter une vue complète des ressources de données et des relations correspondantes.

Vous pouvez déployer Enterprise Data Catalog et ses services soit sur un cluster Hadoop incorporé, soit sur un cluster Hadoop existant.

Cluster incorporé

Fait référence à une distribution Hadoop fournie avec le programme d'installation de Enterprise Data Catalog. Vous pouvez configurer le cluster lorsque vous installez Enterprise Data Catalog.

Cluster existant

Fait référence à un cluster Hadoop dans votre environnement d'entreprise où vous désirez déployer Enterprise Data Catalog. Vérifiez que le cluster Hadoop que vous utilisez est répertorié dans [Product Availability Matrices \(PAM\) for Enterprise Data Catalog](#). Assurez-vous de configurer le cluster avant de déployer Enterprise Data Catalog.

Pour utiliser Enterprise Data Catalog, vous devez installer les services correspondants et créer un domaine. Utilisez le programme d'installation d'Enterprise Data Catalog pour installer les services. Lorsque vous installez Enterprise Data Catalog, vous devez configurer le domaine et les services d'application qu'Enterprise Data Catalog utilisent. Enterprise Data Catalog requiert un domaine dédié avant de pouvoir commencer à l'utiliser.

Les services d'Enterprise Data Catalog sont constitués de services pour prendre en charge ceux de domaine et d'application pour effectuer les tâches et gérer les bases de données. Le domaine Informatica est l'unité administrative de l'environnement Enterprise Data Catalog. Le domaine recluster des nœuds qui représentent

les machines sur lesquelles les services d'applications sont exécutés. Lorsque vous installez les services d'Enterprise Data Catalog sur une machine, vous installez tous les fichiers pour tous les services.

Si vous installez Enterprise Data Catalog sur une machine unique, vous devez créer le domaine Informatica et un nœud sur la machine. Si vous effectuez l'installation sur plusieurs machines, vous devez créer un nœud de passerelle et le domaine Informatica pour la première installation. Lors de l'installation sur les machines supplémentaires, vous devez créer des nœuds de travail que vous joignez au domaine.

Enterprise Data Catalog contient les applications clientes suivantes :

- Informatica Administrator
- Informatica Catalog Administrator
- Outil de recherche d'Enterprise Data Catalog

Vous devez utiliser ces clients pour accéder aux services dans le domaine.

Installation Processus

L'installation d'Enterprise Data Catalog se compose de plusieurs phases.

Les voici en détail :

1. Avant d'installer les services d'Enterprise Data Catalog, effectuez les tâches suivantes pour planifier et préparer l'installation des services :
 - a. Planifiez le domaine Informatica. Prenez en compte le nombre de nœuds dans le domaine, les services d'application qui s'exécutent sur chaque nœud, les prérequis du système et le type d'authentification utilisateur utilisé par le domaine.
 - b. Préparez les bases de données pour le domaine. Vérifiez les prérequis de bases de données, puis configurez celles requises pour Enterprise Data Catalog.
 - c. Configurez les machines pour répondre aux prérequis de Linux pour vous assurer que vous pouvez installer et exécuter correctement les services d'Enterprise Data Catalog.
 - d. Déterminez si vous devez modifier la taille du jeu de données par défaut pour l'installation d'Enterprise Data Catalog. Enterprise Data Catalog possède des tailles de jeu de données Petite, Moyenne, Grande, Par défaut et Démo que vous pouvez configurer dans Informatica Administrator à l'aide de propriétés personnalisées. Les jeux de données sont classés en fonction de la quantité de métadonnées à traiter et du nombre de nœuds utilisés pour traiter les métadonnées.

Remarque:

- Après l'installation, vous pouvez passer la taille du jeu de données de plus petite à plus grande. Par exemple, si vous aviez sélectionné une petite taille de jeu de données lors de l'installation, vous pouvez la passer à Moyenne ou Grande après l'installation. Si vous aviez sélectionné, cependant, une valeur de jeu de données supérieure lors de l'installation, par exemple Grande, vous ne pouvez pas passer la taille du jeu de données à une taille de jeu de données inférieure, telle que Moyenne, Petite ou Par défaut après l'installation.
- Vous ne pouvez pas modifier la taille du jeu de données si vous aviez sélectionné une taille de jeu de données Démo durant l'installation.
- Veillez à redémarrer et indexer le service de catalogue si vous changez de taille de jeu de données après avoir installé Enterprise Data Catalog.

Pour plus d'informations sur les tailles de jeu de données et le réglage des performances, consultez l'article de la Bibliothèque de procédures Informatica : *Réglage des performances d'Enterprise Data Catalog*

2. Installer Enterprise Data Catalog.

Utilisez le programme d'installation pour installer les services d'Enterprise Data Catalog sur une ou plusieurs machines Linux. La première fois que vous exécutez le programme d'installation, vous devez créer le domaine. Lors de l'installation sur les machines supplémentaires, vous devez créer des nœuds de travail que vous joignez au domaine.

3. Après avoir installé les services d'Enterprise Data Catalog, effectuez les tâches suivantes pour finaliser le processus :

- a. Effectuez la configuration du domaine. Vérifiez la compatibilité des pages de code, effectuez les tâches requises par le type d'authentification utilisateur utilisé par le domaine et configurez les variables d'environnement. Le cas échéant, configurez une communication sécurisée pour le domaine.
- b. Préparez éventuellement la création des services d'application. Vérifiez les prérequis du système d'exploitation pour les services d'application, puis créez les utilisateurs et les connexions requis par ces services.

Vous pouvez créer les services d'application de l'une des manières suivantes :

- Automatiquement lorsque vous installez Enterprise Data Catalog.
- Manuellement dans Informatica Administrator après avoir installé Enterprise Data Catalog.
- Manuellement à l'aide du programme d'installation, à un moment ultérieur après avoir installé Enterprise Data Catalog et avoir quitté le programme d'installation.

Si l'installation est incomplète à cause d'un échec, d'une interruption ou d'une sortie involontaire du programme d'installation, vous pouvez utiliser le programme d'installation pour reprendre l'installation à l'endroit où elle s'est arrêtée.

Services d'Enterprise Data Catalog

Les services d'application d'Enterprise Data Catalog représentent les fonctionnalités basées sur le serveur. Après avoir terminé l'installation, vous pouvez éventuellement créer les services d'application selon la clé de licence générée pour votre organisation.

Lorsque vous configurez un service d'application, vous désignez un nœud pour exécuter le processus de service. Le processus de service est la représentation d'exécution d'un service actif sur un nœud. Le type de service détermine le nombre de processus de service qui peuvent s'exécuter en même temps.

Si vous disposez de l'option Haute disponibilité, vous pouvez exécuter un service d'application sur plusieurs nœuds. Dans le cas contraire, configurez chaque service pour qu'il s'exécute sur un seul nœud.

Certains services d'applications requièrent des bases de données pour stocker les informations traitées par le service d'application. Lorsque vous planifiez le domaine Informatica, vous devez également prévoir les bases de données requises par chaque service d'application.

Enterprise Data Catalog utilise les services d'application suivants :

- Service d'intégration de données
- Service de référentiel modèle
- Service de catalogue

- Service de cluster Informatica
- Service de gestion de contenu

Référentiels d'Enterprise Data Catalog

Enterprise Data Catalog utilise différents types de référentiels en fonction du type de données et des métadonnées qu'il stocke.

Enterprise Data Catalog requiert les référentiels suivants :

Référentiel de configuration du domaine

Une base de données relationnelle qui stocke les informations sur les utilisateurs et la configuration des domaines.

Référentiel modèle

Une base de données relationnelle qui stocke les métadonnées créées par Enterprise Data Catalog et les services d'application pour permettre la collaboration entre les clients et les services. Le référentiel modèle stocke également les informations sur la configuration des ressources et les domaines de données.

Entrepôt de profilage

Une base de données relationnelle qui stocke les résultats des profils. Les statistiques de profil font partie de la vue complète des métadonnées fournie par Enterprise Data Catalog.

Entrepôt de données de référence

Une base de données relationnelle qui stocke des valeurs de données pour les objets de table de référence que vous définissez dans le référentiel modèle. Lorsque vous ajoutez des données à une table de référence, le service de gestion de contenu écrit les valeurs des données dans une table de l'entrepôt de données de référence.

Liste de contrôle de l'installation et de la configuration

La liste de contrôle de l'installation et de la configuration récapitule les tâches que vous devez effectuer pour terminer l'installation d'Enterprise Data Catalog.

Effectuez les tâches suivantes pour terminer le processus :

1. Planifiez le domaine.
2. Préparez les bases de données pour le domaine.
3. Assurez-vous que les machines répondent aux prérequis de Linux. Vérifiez que les utilitaires TAR et ZIP sont disponibles dans l'environnement Linux pour extraire les fichiers d'installation et déployer les services.
4. Choisissez la taille du jeu de données ou le type de charge de travail pour l'installation. Pour modifier la taille du jeu de données par défaut, vous devez choisir une des tailles de jeu de données suivantes dans Informatica Administrator : Petite, Moyenne, Grande ou Démo. Vous pouvez déterminer la taille de

données appropriée en fonction de la quantité de métadonnées qu'Enterprise Data Catalog doit traiter et le nombre de nœuds utilisés pour traiter les métadonnées. Pour plus d'informations

Remarque:

- Après l'installation, vous pouvez passer la taille du jeu de données de plus petite à plus grande. Par exemple, si vous aviez sélectionné une petite taille de jeu de données lors de l'installation, vous pouvez la passer à Moyenne ou Grande après l'installation. Si vous aviez sélectionné, cependant, une valeur de jeu de données supérieure lors de l'installation, par exemple Grande, vous ne pouvez pas passer la taille du jeu de données à une taille de jeu de données inférieure, telle que Moyenne, Petite ou Par défaut après l'installation.
- Vous ne pouvez pas modifier la taille du jeu de données si vous aviez sélectionné une taille de jeu de données Démo durant l'installation.

Pour plus d'informations sur les tailles de jeu de données et le réglage des performances, consultez l'article de la Bibliothèque de procédures Informatica : *Réglage des performances d'Enterprise Data Catalog*.

5. Installer Enterprise Data Catalog.
6. Connectez-vous à Informatica Administrator.
7. Si vous n'aviez pas choisi de créer des services d'application lors de l'installation, créez et activez les services d'application. Ceux-ci incluent le service de référentiel modèle, le service d'intégration de données, le service de catalogue, le service de cluster Informatica et le service de gestion de contenu.
8. Créez les utilisateurs du domaine.
9. Attribuez les autorisations et privilèges requis aux utilisateurs et aux groupes.
10. Installez Informatica Developer si vous souhaitez exécuter la découverte de domaines de données dans les sources de métadonnées avec des domaines de données qui utilisent des tables de référence.
11. Si vous devez utiliser des domaines de données prédéfinis dans les statistiques de profilage, importez les domaines de données requis à l'aide d'Informatica Developer.
12. Lancez Catalog Administrator et l'outil de recherche Enterprise Data Catalog depuis Informatica Administrator.

Partie II : Avant l'installation Enterprise Data Catalog

Cette partie contient les chapitres suivants :

- [Planification du domaine, 19](#)
- [Préparer les bases de données pour le domaine Informatica , 37](#)
- [Méthodes de déploiement, 49](#)

CHAPITRE 2

Planification du domaine

Ce chapitre comprend les rubriques suivantes :

- [Introduction au domaine Informatica, 19](#)
- [Processus de planification de domaine, 24](#)
- [Planification des services d'application, 25](#)
- [Vérification de la configuration système requise, 28](#)
- [Enregistrer les informations relatives au domaine et au nœud Informatica, 32](#)

Introduction au domaine Informatica

Un domaine Informatica est un ensemble de nœuds et de services. Un nœud est la représentation logique d'une machine dans un domaine. Les services du domaine incluent le gestionnaire de service qui gère toutes les opérations du domaine et un ensemble de services d'application qui représentent des fonctionnalités basées sur le serveur.

Le domaine requiert une base de données relationnelle pour stocker les informations de configuration ainsi que les privilèges et les autorisations des comptes utilisateur. La première fois que vous installez les services d'Enterprise Data Catalog, vous devez créer le référentiel de configuration du domaine dans une base de données relationnelle.

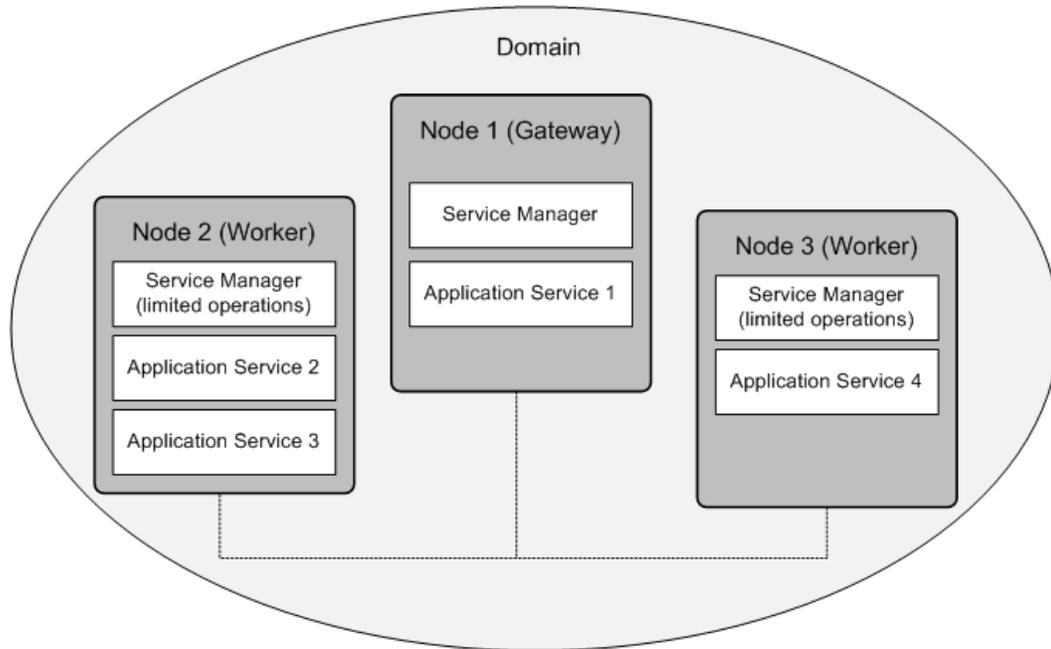
Domaine à un ou plusieurs nœuds

Lorsque vous installez les services d'Enterprise Data Catalog sur une machine, vous créez un nœud et un domaine. Vous pouvez installer les services d'Enterprise Data Catalog sur plusieurs machines pour créer des nœuds supplémentaires que vous joignez au domaine.

Une installation à un seul nœud se compose d'un domaine à un nœud. Le nœud héberge le domaine. Le gestionnaire de service et tous les services d'application Informatica s'exécutent sur le nœud.

Une installation sur plusieurs nœuds se compose d'un nœud de passerelle, qui héberge le domaine, et d'autres nœuds qui exécutent les services d'application Informatica. Le gestionnaire de service s'exécute sur tous les nœuds du domaine.

L'image suivante montre une installation sur plusieurs nœuds :



Nœuds

Chaque nœud du domaine exécute le gestionnaire de service chargé des fonctions du domaine sur ce nœud. Le gestionnaire de service prend également en charge les services d'application qui s'exécutent sur le nœud.

Les configurations de nœud suivantes déterminent quelles fonctions du domaine un nœud prend en charge et quels services il exécute :

Type de nœud

Le type de nœud détermine si le nœud peut servir de nœud de passerelle ou de nœud de travail et quelles fonctions du domaine il prend en charge. À la première installation des services d'Enterprise Data Catalog, vous créez un nœud de passerelle et le domaine Informatica. Lorsque vous installez les services d'Enterprise Data Catalog sur d'autres machines, vous créez d'autres nœuds de passerelle ou de travail que vous joignez au domaine.

Un nœud de passerelle sert de nœud principal de passerelle pour le domaine. Le nœud principal de passerelle reçoit des demandes de service provenant de clients et les dirige vers le service et le nœud appropriés. Le gestionnaire de service du nœud principal de passerelle effectue toutes les opérations de domaine sur ce nœud. Les gestionnaires de service s'exécutant sur d'autres nœuds de passerelle exécutent des opérations de domaine limitées sur ces nœuds.

Un nœud de travail est un nœud qui n'est pas configuré en tant que passerelle. Un nœud de travail peut exécuter des services d'application, mais il ne peut pas servir de passerelle. Le gestionnaire de service effectue des opérations de domaine limitées sur un nœud de travail.

Rôle du nœud

Le rôle d'un nœud définit sa fonction. Un nœud doté du rôle de service peut exécuter des services d'application. Un nœud doté du rôle de calcul peut effectuer les calculs requis par des services d'application distante. Un nœud doté des deux rôles peut exécuter des services d'application et effectuer localement des calculs pour ces services. Par défaut, chaque nœud de passerelle et de travail est doté des rôles de service et de calcul.

Si un nœud est attribué à une grille du service d'intégration de données, vous pouvez éventuellement mettre son rôle à jour. Activez uniquement le rôle de service pour dédier le nœud à l'exécution du processus de service d'intégration de données. Activez uniquement le rôle de calcul pour dédier le nœud à l'exécution de mappages du service d'intégration de données.

Pour en savoir plus sur les nœuds, consultez le document *Informatica Administrator Guide*.

Pour plus d'informations sur les grilles du service d'intégration de données, consultez le *Guide des services d'application Informatica*.

Prérequis pour déployer Enterprise Data Catalog sur plusieurs nœuds

Si vous prévoyez de déployer Enterprise Data Catalog sur plusieurs nœuds, vérifiez que vous vous conformez aux prérequis suivants :

- Veillez à utiliser les mêmes informations d'identification utilisateur pour démarrer tous les nœuds.
- Avant de déployer Enterprise Data Catalog sur un cluster incorporé, activez la connexion SSH sans mot de passe pour tous les nœuds hôtes au nœud de cluster.
- Assurez-vous que les mêmes versions des fichiers binaires Apache Ambari sont présents sur tous les nœuds avant de déployer Enterprise Data Catalog sur un cluster incorporé.
- Vérifiez qu'une copie identique de tous les fichiers binaires de ressources est présente sur tous les nœuds.
- Si vous prévoyez de déployer Enterprise Data Catalog sur plusieurs nœuds, veillez à configurer le service de cluster Informatica et le service de catalogue sur des nœuds distincts.

Gestionnaire de service

Le gestionnaire de service dans le domaine Informatica prend en charge le domaine et les services d'applications. Le gestionnaire de service s'exécute sur chaque nœud du domaine.

Le gestionnaire de service s'exécute sur tous les nœuds du domaine pour prendre en charge les aspects suivants :

Domaine

Le gestionnaire de service exécute des fonctions sur chaque nœud pour prendre en charge le domaine. Les fonctions du domaine comprennent l'authentification, l'autorisation et la connexion. Les fonctions exécutées sur un nœud par le gestionnaire de service dépendent du type et du rôle de ce nœud. Par exemple, le gestionnaire de service, lorsqu'il est exécuté sur le nœud principal de passerelle, effectue toutes les fonctions du domaine sur ce nœud. Le gestionnaire de service exécuté sur tout autre type de nœud effectue un nombre limité de fonctions du domaine sur ce nœud.

services d'applications

Lorsqu'un nœud est doté du rôle de service, le gestionnaire de service démarre les services d'applications configurés pour s'exécuter sur ce nœud. Il démarre et arrête les services et les processus de services selon les demandes des clients Informatica.

Pour plus d'informations sur le gestionnaire de service, consultez le document *Informatica Administrator Guide*.

Services d'application

Les services d'application représentent des fonctionnalités basées sur le serveur. Les services d'application incluent des services qui peuvent avoir plusieurs instances dans le domaine et des services système qui peuvent n'en avoir qu'une seule. Les services système sont créés pour vous lorsque vous créez le domaine.

Une fois l'installation terminée, vous créez d'autres services d'application en fonction de la clé de licence générée pour votre organisation.

Lorsque vous créez un service d'application, vous désignez un nœud qui joue le rôle de service pour exécuter le processus du service. Le processus de service est la représentation d'exécution d'un service actif sur un nœud. Le type de service détermine le nombre de processus de service qui peuvent s'exécuter en même temps.

Si vous choisissez l'option Haute disponibilité, vous pouvez exécuter un service d'application sur plusieurs nœuds. Dans le cas contraire, configurez chaque service d'application pour qu'il s'exécute sur un seul nœud.

Certains services d'application requièrent des bases de données pour stocker les informations traitées par le service d'application. Lorsque vous planifiez le domaine Informatica, vous devez également prévoir les bases de données requises par chaque service d'application.

Pour plus d'informations sur les services d'application, consultez le document *Informatica Application Service Guide*.

Clé de licence

Informatica génère une clé de licence en fonction du produit et des options achetées votre organisation. La clé de licence contrôle les services d'application et les fonctionnalités que vous pouvez utiliser.

Lorsque vous installez les services d'Enterprise Data Catalog, vous devez entrer le chemin et le nom de fichier de la clé de licence Informatica. Le programme d'installation crée un objet de licence dans le domaine en fonction de la clé de licence indiquée. Lorsque vous créez des services d'application, vous devez affecter l'objet de licence à chaque service avant d'exécuter le service.

Authentification utilisateur

Lors de l'installation, vous pouvez sélectionner l'authentification à utiliser pour le domaine Informatica.

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

- Authentification utilisateur native
- Authentification utilisateur LDAP

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

Le programme d'installation configure le domaine Informatica de façon à utiliser l'authentification native. Après l'installation, vous pouvez configurer une connexion à un serveur LDAP et configurer le domaine Informatica pour utiliser l'authentification LDAP en plus de l'authentification native.

Pour plus d'informations sur l'authentification utilisateur, consultez le *Guide de sécurité d'Informatica*.

Clé de chiffrement pour le stockage des données sécurisé

Informatica chiffre les données sensibles, telles que les mots de passe et les paramètres de connexion sécurisée avant de stocker les données dans les référentiels d'Enterprise Data Catalog. Informatica utilise un mot-clé pour créer une clé de chiffrement avec laquelle chiffrer les données sensibles.

Lorsque vous installez les services d'Enterprise Data Catalog et que vous créez un domaine, vous devez spécifier un mot-clé pour le programme d'installation qui servira à générer la clé de chiffrement pour le domaine. Selon le mot-clé, le programme d'installation génère un fichier de clé de cryptage nommé *siteKey* et le stocke dans le répertoire que vous spécifiez. Si vous n'indiquez pas de répertoire, le programme

d'installation stocke le fichier *siteKey* dans le répertoire par défaut : <Répertoire d'installation d'Enterprise Data Catalog>/isp/config/keys

Tous les nœuds du domaine doivent utiliser la même clé de chiffrement. En cas d'installation sur plusieurs nœuds, le programme d'installation utilise la même clé de chiffrement pour tous les nœuds du domaine. Lorsque vous exécutez le programme d'installation après avoir créé le domaine, vous devez spécifier la même clé de chiffrement pour tous les nœuds que vous joignez au domaine.

Vous devez spécifier un mot-clé, même si vous n'activez pas une communication sécurisée pour le domaine.

Important: Vous devez conserver le nom du domaine, le mot clé de la clé de cryptage et le fichier de clé de cryptage dans un emplacement sécurisé. La clé de chiffrement est requise lorsque vous modifiez la clé de chiffrement du domaine ou déplacez un référentiel vers un autre domaine. Si vous ne disposez pas de la clé de chiffrement, vous devez avoir le nom de domaine et le mot clé utilisés pour générer la clé de chiffrement.

Sécurité de domaine

Lorsque vous installez les services d'Enterprise Data Catalog et créez un domaine, vous pouvez activer les options pour configurer la sécurité dans le domaine.

Vous pouvez configurer les options de sécurité suivantes pour le domaine :

Communication sécurisée pour les services et le gestionnaire de service

Lorsque vous configurez une communication sécurisée pour le domaine, vous sécurisez les connexions entre le gestionnaire de service et les services du domaine. Informatica fournit un certificat SSL que vous pouvez utiliser pour sécuriser le domaine. Cependant, pour une meilleure sécurité, vous pouvez fournir le certificat SSL lors de l'installation. Indiquez les fichiers entrepôts de clés et truststore contenant les certificats SSL à utiliser.

Base de données sécurisée du référentiel de configuration de domaine

Lorsque vous installez les services d'Enterprise Data Catalog et que vous créez un domaine, vous pouvez créer le référentiel de configuration du domaine dans une base de données sécurisée avec le protocole SSL. L'accès à la base de données sécurisée requiert un fichier truststore contenant les certificats de la base de données. Lors de l'installation, vous indiquez le fichier truststore contenant le certificat SSL à utiliser.

Connexion sécurisée pour l'outil Administrator

Informatica Administrator ou l'outil Administrator tool est l'outil utilisé pour gérer le domaine Informatica. Lors de l'installation, vous pouvez configurer une connexion sécurisée HTTPS pour l'outil Administrator. Vous pouvez fournir le fichier entrepôt de clés à utiliser pour la connexion HTTPS.

Remarque: Enterprise Data Catalog ne prend pas en charge un domaine Informatica activé pour l'authentification Kerberos.

Clients Informatica

Les clients Informatica sont un groupe de clients que vous utilisez pour accéder aux fonctionnalités sous-jacentes d'Enterprise Data Catalog. Les clients font des demandes au gestionnaire de service ou aux services d'applications.

Les clients Informatica se composent de plusieurs applications de client léger ou Web. Vous devez utiliser ces clients pour accéder aux services dans le domaine. Lorsque vous exécutez l'installation des clients Informatica, vous pouvez choisir d'installer Informatica Developer, une application de client léger, que vous utilisez pour importer des domaines de données. Pour afficher les informations sur le domaine de données dans Enterprise Data Catalog, vous devez installer Informatica Developer. L'outil Developer tool est une application cliente que vous utilisez pour créer, exporter et importer des domaines de données. Les objets

que vous créez dans l'outil Developer tool sont stockés dans un référentiel modèle, et le service d'intégration de données exécute les objets. Si vous utilisez des domaines de données prédéfinis dans la configuration des profils, le service de gestion de contenu exécute les objets de domaine de données.

Les clients que vous utilisez dépendent de la clé de licence générée pour votre organisation.

Vous pouvez installer les applications suivantes de client léger :

Informatica Administrator

Informatica Administrator est l'outil d'administration que vous utilisez pour administrer le domaine et la sécurité Informatica. L'outil Administrator tool est une application de client léger ou Web. Vous pouvez effectuer des tâches d'administration de domaine, telles que la gestion des journaux et des objets de domaine, ainsi que des tâches d'administration de sécurité, telles que la gestion des utilisateurs, des groupes et des rôles, dans l'outil Administrator tool. Vous pouvez également créer les services d'application requis, tels que le service d'intégration de données, le service de référentiel modèle et le service de catalogue, à l'aide d'Informatica Administrator.

Enterprise Data Catalog

Enterprise Data Catalog est un client Web qui affiche une vue complète des métadonnées à partir des ressources de données configurées. Les analyseurs extraient les métadonnées des sources de données externes. Vous pouvez effectuer une recherche de métadonnées et afficher des informations relatives aux relations et au lignage des ressources de données, par exemple.

Informatica Catalog Administrator

Informatica Catalog Administrator est l'outil d'administration que vous utilisez pour administrer les ressources, les analyseurs, les planifications, les attributs et les connexions.

Processus de planification de domaine

Avant d'installer les services d'Enterprise Data Catalog, vous devez planifier tous les composants du domaine Informatica.

Lorsque vous planifiez le domaine, vous devez prendre en compte le nombre de nœuds dont il a besoin, les types de services d'application qui lui sont nécessaires et le nombre de services d'application exécutés sur chaque nœud. Vous devez déterminer le type de base de données et le nom d'hôte pour le référentiel de configuration du domaine et pour les bases de données requises par chaque service d'application.

Vous devez fournir un mot clé que le programme d'installation utilisera pour générer la clé de cryptage du domaine. Informatica utilise la clé de cryptage pour crypter les données sensibles.

Si vous décidez de configurer la sécurité du domaine, vous devez connaître l'emplacement et le mot de passe de l'entrepôt de clés et des fichiers truststore. Dans le cadre de la planification, vous devez également vérifier que chaque machine et serveur de base de données du domaine répond aux prérequis minimaux du système.

Remarque: Assurez-vous d'installer l'utilitaire de ligne de commande de l'interface *ktutil* dans la machine du domaine Informatica.

Planification des services d'application

Lorsque vous planifiez le domaine Informatica, vous devez également prévoir les services d'application qui s'exécuteront dans le domaine. Vous devez créer les services d'application en fonction de la clé de licence générée pour votre organisation.

Lorsque vous planifiez les services d'application, vous devez tenir compte des services associés qui se connectent au service d'application. Vous devez également prévoir les bases de données relationnelles qui sont requises pour créer le service d'application.

Le programme d'installation vous invite à la création éventuelle de services pendant le processus d'installation.

Pour plus d'informations sur les services d'application, consultez le document *Informatica Application Service Guide*.

Service d'intégration de données

Le service d'intégration de données est un service d'application qui exécute des profils dans le domaine Informatica. Le service d'intégration de données génère des résultats de profils pour les ressources que vous avez configurées pour extraire des métadonnées de profils, puis écrit les résultats de profils dans l'entrepôt de profilage.

Services associés

Le service d'intégration de données se connecte aux autres services d'application dans le domaine.

Lorsque vous créez le service d'intégration de données, vous pouvez l'associer au service d'application suivant :

Service de référentiel modèle

Le service d'intégration de données se connecte au service de référentiel modèle pour effectuer des tâches telles que l'exécution de profils. Lorsque vous créez le service d'intégration de données, vous indiquez le nom du service de référentiel modèle.

Bases de données requises

Le service d'intégration de données peut se connecter à plusieurs bases de données relationnelles. Les bases de données auxquelles le service peut se connecter dépendent de la clé de licence générée pour l'entreprise. Lorsque vous créez le service d'intégration de données, vous fournissez des informations de connexion aux bases de données.

Créez les bases de données suivantes avant de créer le service d'intégration de données :

Base de données du cache d'objet de données

Met en cache des objets de données logiques et des tables virtuelles. La mise en cache des objets de données permet au service d'intégration de données d'accéder à des objets de données logiques et des tables virtuelles prédéfinis. Vous avez besoin d'une base de données du cache d'objet de données afin d'améliorer les performances des requêtes de service de données SQL et des demandes de service Web.

Entrepôt de profilage

Stocke les informations de profilage, telles que les résultats des profils. Il vous faut un entrepôt de profilage pour stocker les statistiques de profilage qu'une analyse de ressources génère.

Service de référentiel modèle

Le service de référentiel modèle est un service d'application qui gère le référentiel modèle. Le référentiel modèle stocke les métadonnées créées par les clients Informatica et les services d'application dans une base de données relationnelle pour permettre la collaboration entre les clients et les services.

Lorsque vous accédez à un objet de référentiel modèle à partir de Catalog Administrator ou du service d'intégration de données, le client ou le service envoie une demande au service de référentiel modèle. Le processus du service de référentiel modèle extrait, insère et met à jour les métadonnées stockées dans les tables de base de données du référentiel modèle.

Remarque: Lorsque vous créez le service de référentiel modèle, vous ne l'associez pas à d'autres services d'application.

Bases de données requises

Le service de référentiel modèle requiert un référentiel modèle dans une base de données relationnelles. Lorsque vous créez le service de référentiel modèle, vous devez fournir des informations de connexion à la base de données.

Créez la base de données suivante avant de créer le service de référentiel modèle :

Référentiel modèle

Stocke les métadonnées créées par les clients Informatica et les services d'application dans une base de données relationnelles pour permettre la collaboration entre les clients et les services. Vous devez disposer d'un référentiel modèle pour stocker les objets de conception et d'exécution créés par les clients Informatica et les services d'application.

Service de catalogue

Le service de catalogue est un service d'application qui exécute Enterprise Data Catalog dans le domaine Informatica. Le service de catalogue gère les connexions entre les composants de service et les utilisateurs qui ont accès à l'interface de recherche d'Enterprise Data Catalog et à Catalog Administrator.

Le catalogue représente un inventaire indexé de toutes les ressources de données configurées dans une entreprise. Vous pouvez trouver des informations sur les métadonnées et les statistiques, telles que les statistiques de profils, les évaluations de ressources de données, les domaines de données et les relations de données dans le catalogue.

Remarque: Veillez à importer les certificats du cluster Hadoop dans le truststore du domaine avant de créer un service de catalogue pour un cluster Hadoop qui utilise le protocole SSL.

Services associés

Le service de catalogue se connecte à d'autres services d'application du domaine.

Lorsque vous créez le service de catalogue, vous pouvez l'associer aux services d'application suivants :

Service de référentiel modèle

Le service de catalogue se connecte au service de référentiel modèle pour accéder aux informations sur la configuration des ressources et les domaines de données à partir du référentiel modèle. Lorsque vous créez le service de catalogue, vous indiquez le nom du service de référentiel modèle.

Service d'intégration de données

Le service de catalogue se connecte au service d'intégration de données pour effectuer des tâches, telles que la génération de statistiques de profils pour les ressources. Lorsque vous créez le service de catalogue, vous indiquez le nom du service d'intégration de données.

Service de cluster Informatica

Si vous avez installé Enterprise Data Catalog sur le cluster incorporé, le service de catalogue se connecte au service de cluster Informatica pour administrer et gérer tous les services du cluster Hadoop incorporés, le serveur Apache Ambari et les agents Apache Ambari. Lorsque vous créez le service de catalogue pour un déploiement de cluster incorporé, vous devez fournir le nom du service de cluster Informatica.

Service de gestion de contenu

Le service de catalogue utilise le service de gestion de contenu pour extraire des données de référence pour les domaines de données qui utilisent des tables de référence. Lorsque vous créez le service de catalogue, vous pouvez éventuellement fournir le nom du service de gestion de contenu.

Service de cluster Informatica

Le service de cluster Informatica est un service d'application qui exécute et gère tous les services Hadoop, le serveur Apache Ambari et les agents Apache Ambari sur un cluster Hadoop intégré. Si vous choisissez le mode de déploiement du cluster intégré lors de l'installation d'Enterprise Data Catalog, vous devez créer le service de cluster Informatica avant de créer le service de catalogue. Vous pouvez ensuite spécifier la valeur du service de cluster Informatica lorsque vous créez le service de catalogue.

Service de gestion de contenu

Le service de gestion de contenu est un service d'applications qui gère les données de référence. Un objet de données de référence contient un ensemble de valeurs de données qu'Enterprise Data Catalog recherche lors de la découverte de domaine de données sur les données sources. La découverte de domaine de données détecte la sémantique d'entreprise en fonction des données de colonnes. Par exemple, un numéro de sécurité sociale, un numéro de téléphone et un numéro de carte de crédit.

Le service de gestion de contenu utilise le service d'intégration de données pour exécuter des mappages en vue de transférer des données entre les tables de référence et les sources de données externes.

Services associés

Le service de gestion de contenu se connecte à d'autres services d'application dans le domaine.

Lorsque vous créez le service de gestion de contenu, vous pouvez l'associer aux services d'application suivants :

Service d'intégration de données

Le service de gestion de contenu utilise le service d'intégration de données pour transférer des données entre les tables de référence et les sources de données externes. Lorsque vous créez le service de gestion de contenu, vous indiquez le nom du service d'intégration de données. Vous devez créer le service d'intégration de données et service de gestion de contenu sur le même nœud.

Service de référentiel modèle

Le service de gestion de contenu se connecte au service de référentiel modèle pour stocker les métadonnées des objets de données de référence dans le référentiel modèle. Lorsque vous créez le service de gestion de contenu, vous indiquez le nom du service de référentiel modèle.

Bases de données requises

Le service de gestion de contenu requiert un entrepôt de données de référence dans une base de données relationnelles. Lorsque vous créez le service de gestion de contenu, vous devez fournir des informations de connexion à l'entrepôt de données de référence.

Créez la base de données suivante avant de créer le service de gestion de contenu :

Entrepôt de données de référence

Stocke les valeurs de données pour les objets de la table de référence que vous définissez dans le référentiel modèle. Lorsque vous ajoutez des données à une table de référence, le service de gestion de contenu écrit les valeurs des données dans une table de l'entrepôt de données de référence. Vous avez besoin d'un entrepôt de données de référence pour gérer les données de table de référence dans Enterprise Data Catalog.

Vérification de la configuration système requise

Vérifiez que votre environnement répond à la configuration système minimale requise pour le processus d'installation, l'espace disque temporaire, la disponibilité des ports, les bases de données et le matériel des services d'applications.

Pour obtenir plus d'informations sur les spécifications de produit et les plates-formes prises en charge, consultez la matrice de disponibilité de produits sur Informatica Network :

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

Vérification des spécifications d'installation des services

Veillez à ce que votre machine réponde à la configuration système minimale requise pour installer les services d'Enterprise Data Catalog.

La configuration système requise diffère en fonction des conditions suivantes :

Si le domaine Informatica et le cluster Hadoop se trouvent sur la même machine

La configuration mémoire minimale requise pour le système d'exploitation Linux est de 32 Go de RAM. L'espace disque minimal requis est de 135 Go. Le nombre de cœurs de processeur requis est de 24.

Si le domaine Informatica et le cluster Hadoop se trouvent sur des machines différentes

La configuration mémoire minimale requise pour le système d'exploitation Linux est de 24 Go pour un nœud de cluster et de 32 Go pour la machine sur laquelle le Domaine Informatica s'exécute. L'espace disque minimal requis est de 75 Go. Le nombre de cœurs de processeur requis est de 8 cœurs pour un nœud de cluster et de 16 cœurs pour la machine sur laquelle le Domaine Informatica s'exécute.

Vérification de l'espace disque temporaire requis

Le programme d'installation écrit des fichiers temporaires sur le disque dur. Assurez-vous de disposer de suffisamment d'espace disponible sur le disque de la machine pour permettre l'installation. Lorsque l'installation est terminée, le programme d'installation efface les fichiers temporaires et libère l'espace disque.

Le programme d'installation requiert 8 Go d'espace disque temporaire.

Vérifications des spécifications de port

Le programme d'installation configure les ports pour les composants du domaine Informatica et désigne une plage de ports dynamiques à utiliser pour certains services d'applications.

Vous pouvez indiquer les numéros de ports à utiliser pour les composants et une plage de numéros de ports dynamiques à utiliser pour les services d'applications. Vous pouvez également utiliser les numéros de ports par défaut fournis par le programme d'installation. Vérifiez que les numéros de port sont disponibles sur les machines sur lesquelles vous installez les services d'Enterprise Data Catalog.

Le tableau suivant décrit les ports utilisés par Enterprise Data Catalog :

Type de port	Description
Port du nœud	Numéro de port du nœud créé lors de l'installation. La valeur par défaut est 6005.
Port de gestionnaire de service	Numéro de port utilisé par le gestionnaire de service sur le nœud. Le gestionnaire de service écoute les demandes de connexions entrantes sur ce port. Les applications clientes utilisent ce port pour communiquer avec les services du domaine. Les programmes de ligne de commande Informatica utilisent ce port pour communiquer avec le domaine. Le pilote JDBC/ODBC du service de données SQL utilise également ce port. La valeur par défaut est 6006.
Port d'arrêt du gestionnaire de service	Numéro de port qui contrôle l'arrêt du serveur pour le gestionnaire de service du domaine. Le gestionnaire de service écoute les commandes d'arrêt sur ce port. La valeur par défaut est 6007.
Port d'Informatica Administrator	Numéro de port utilisé par Informatica Administrator. La valeur par défaut est 6008. Le port HTTPS par défaut est 8443.
Port d'arrêt d'Informatica Administrator	Numéro de port qui contrôle l'arrêt du serveur pour Informatica Administrator. Informatica Administrator écoute les demandes d'arrêt sur ce port. La valeur par défaut est 6009.
Plage de ports dynamiques pour les services d'applications	<p>Plage de numéros de port qui peuvent être affectés dynamiquement aux processus de service d'application au fur et à mesure qu'ils démarrent. Lorsque vous démarrez un service d'application qui utilise un port dynamique, le Gestionnaire de service attribue dynamiquement le premier port disponible de cette plage au processus de service. Le nombre de ports figurant dans la plage doit être au moins le double du nombre de processus des services d'applications qui s'exécuteront sur ce nœud. Par défaut, le port est compris entre 6014 et 6114.</p> <p>Le gestionnaire de service attribue dynamiquement les numéros de port de cette plage au service de référentiel modèle.</p>
Port HTTPS pour les distributions Hadoop	<p>Si vous déployez Enterprise Data Catalog dans une distribution Hadoop compatible HTTPS, les numéros de port par défaut sont les suivants :</p> <ul style="list-style-type: none">- Cloudera. 7183- Hortonworks. 8443- Azure HDInsight. 8443
Ports statiques pour les services d'applications	<p>Les ports statiques ont des numéros dédiés qui ne changent pas. Lorsque vous créez le service d'application, vous pouvez accepter le numéro de port par défaut ou l'affecter manuellement.</p> <p>Les services suivants utilisent des numéros de port statiques :</p> <ul style="list-style-type: none">- Service de gestion de contenu. La valeur par défaut est 8105 pour HTTP.- Service d'intégration de données. La valeur par défaut est 8095 pour HTTP.

Instructions pour la configuration des ports

Le programme d'installation valide les numéros de port que vous spécifiez pour garantir qu'il n'y aura pas de conflit de numéro de port dans le domaine.

Utilisez les directives suivantes pour définir les numéros de port :

- Le numéro de port que vous spécifiez pour le domaine et pour chaque composant du domaine doit être unique.
- Le numéro de port du domaine et des composants du domaine ne peut pas figurer dans la plage des numéros de port que vous avez définie pour les processus de service d'application.
- Le plus grand numéro de port de la plage des numéros de port que vous définissez pour les processus de service d'application doit être au minimum trois numéros au-dessus du plus petit numéro de port. Par exemple, si le numéro de port minimum de la plage est 6400, le numéro de port maximum doit être au moins 6403.
- Les numéros de port que vous spécifiez ne peuvent pas être inférieurs à 1025 ou supérieurs à 65535.

Vérification des spécifications de la base de données

Vérifiez que le serveur de bases de données dispose d'un espace disque suffisant pour le référentiel de configuration de domaine et pour les autres bases de données nécessaires aux services d'applications.

Le tableau suivant décrit les spécifications de la base de données pour le référentiel de configuration du domaine et pour les autres bases de données nécessaires aux services d'applications :

Base de données	Configuration requise
Référentiel de configuration du domaine Informatica	Le référentiel de configuration du domaine prend en charge les types de base de données suivants : <ul style="list-style-type: none">- IBM DB2 UDB- Microsoft SQL Server- Base de données SQL Microsoft Azure- Oracle- Sybase ASE Autorisez 200 Mo d'espace disque pour la base de données.
Base de données du cache d'objet de données	La base de données du cache d'objet de données prend en charge les types de base de données suivants : <ul style="list-style-type: none">- IBM DB2 UDB- Microsoft SQL Server- Base de données SQL Microsoft Azure- Oracle Autorisez 200 Mo d'espace disque pour la base de données. Allouez de l'espace supplémentaire selon la quantité de données à mettre en cache.
Référentiel modèle	Le référentiel modèle prend en charge les types de base de données suivants : <ul style="list-style-type: none">- IBM DB2 UDB- Microsoft SQL Server- Base de données SQL Microsoft Azure- Oracle Autorisez 3 Go d'espace disque pour DB2. Autorisez 200 Mo d'espace disque pour tous les autres types de base de données. Allouez de l'espace supplémentaire selon la quantité de métadonnées à stocker.

Base de données	Configuration requise
Entrepôt de profilage	<p>L'entrepôt de profilage prend en charge les types de base de données suivants :</p> <ul style="list-style-type: none"> - IBM DB2 UDB - Microsoft SQL Server - Base de données SQL Microsoft Azure - Oracle <p>Autorisez 10 Go d'espace disque pour la base de données.</p>
Entrepôt de données de référence	<p>L'entrepôt de données de référence prend en charge les types de base de données suivants :</p> <ul style="list-style-type: none"> - IBM DB2 UDB - Microsoft SQL Server - Base de données SQL Microsoft Azure - Oracle <p>Autorisez 200 Mo d'espace disque pour la base de données.</p>

Vérification de la configuration matérielle des services d'application

Vérifiez que les nœuds du domaine disposent du matériel adéquat pour le gestionnaire de service et les services d'applications qui s'exécutent sur les nœuds.

Vous pouvez créer un domaine Informatica avec un nœud et exécuter tous les services d'applications sur le même nœud. Si vous créez un domaine Informatica avec plusieurs nœuds, vous pouvez exécuter les services d'applications sur des nœuds séparés. Lorsque vous planifiez les services d'applications pour le domaine, examinez la configuration système requise en fonction des services que vous exécutez sur un nœud.

Remarque: Selon la charge de travail et les besoins en termes de simultanéité, vous devrez peut-être ajouter des cœurs de processeur et de la mémoire dans un nœud afin d'optimiser les performances.

Le tableau suivant répertorie les spécifications système minimales pour un nœud en fonction de certains scénarios de configuration courants. Utilisez ces informations à titre indicatif pour d'autres configurations dans votre domaine.

Services	Processeur	Mémoire	Espace disque
Un nœud exécute les services suivants : <ul style="list-style-type: none"> - Service d'intégration de données - Service de référentiel modèle - Service de catalogue - Service de gestion de contenu - Service de cluster Informatica Remarque: S'applique au déploiement Hadoop incorporé sur HortonWorks.	2 processeurs avec un minimum de 4 cœurs	16 Go	60 Go
Un nœud exécute les services suivants : <ul style="list-style-type: none"> - Service d'intégration de données - Service de référentiel modèle - Service de catalogue - Service de gestion de contenu Remarque: Si vous installez Enterprise Data Catalog sur un cluster existant compatible Kerberos sur Cloudera, HortonWorks ou Azure HDInsight, la configuration minimale requise est de 4 processeurs, avec un minimum de 4 cœurs, 32 Go de mémoire et 60 Go d'espace disque.	2 processeurs avec un minimum de 4 cœurs	16 Go	60 Go

Enregistrer les informations relatives au domaine et au nœud Informatica

Lorsque vous installez les services d'Enterprise Data Catalog, vous devez disposer d'informations sur le domaine, les nœuds, les services d'application et les bases de données vous prévoyez de créer.

Utilisez les tableaux de cette section pour enregistrer les informations requises.

Conventions de dénomination d'objet de domaine

Choisissez une convention de dénomination à utiliser pour le domaine, les nœuds et les services d'applications lorsque vous prévoyez le domaine.

Vous ne pouvez pas modifier les noms de domaines, de nœuds et de services d'applications. Utilisez des noms qui pourront toujours être valides si vous migrez un nœud vers une autre machine ou si vous ajoutez d'autres nœuds et services au domaine. En outre, utilisez les noms qui désignent l'utilisation de l'objet de domaine dans Enterprise Data Catalog.

Pour obtenir plus d'informations sur les conventions de dénomination d'objet de domaine, consultez l'article Meilleures pratiques d'Informatica Velocity disponible sur le portail Informatica MySupport : [Informatica Platform Naming Conventions](#).

Le tableau suivant répertorie les conventions de dénomination recommandées pour les objets de domaine :

Objet	Convention de dénomination	Exemples
Domaine	DMN, DOM, DOMAIN, _<ORG>_<ENV>	DOM_FIN_DEV (développement financier) DOMAIN_ICC_PD (production du centre de compétences en intégration)
Nœud	Node<node##>_<ORG>_<optional distinguisher>_<ENV>	Node01_ICC_DEV Node07_FIN_REVENUE_DV
Service de gestion de contenu	CMS_<ORG>_<ENV>	CMS_FIN_DEV
Service d'intégration de données	DIS_<ORG>_<ENV>	DIS_ICC_DEV
Service de Référentiel Modèle	MRS_<ORG>_<ENV>	MRS_FIN_DEV
Service de catalogue	CS_<ORG>_<ENV>	CS_HR_DEV
Service de cluster Informatica	ICS_<ORG>_<ENV>	ICS_FIN_DEV

Domaine

La première fois que vous installez les services d'Enterprise Data Catalog, vous créez le nœud maître de passerelle et le domaine Informatica.

Utilisez le tableau suivant pour enregistrer les informations de domaine dont vous avez besoin :

Informations de domaine	Description	Valeur
Nom de domaine	Nom du domaine que vous prévoyez de créer. Le nom ne doit pas dépasser 128 caractères et doit être en ASCII 7 bits uniquement. Il ne peut pas contenir d'espaces ni les caractères spéciaux suivants : ` % * + ; " ? , < > \ /	
Nom d'hôte du nœud principal de passerelle	Nom d'hôte complet de la machine sur laquelle créer le nœud principal de passerelle. Si la machine a un nom de réseau unique, utilisez le nom d'hôte par défaut. Le nom d'hôte du nœud ne peut pas contenir le caractère de soulignement (_). Si la machine dispose de plusieurs noms de réseau, vous pouvez modifier le nom d'hôte par défaut pour utiliser un autre nom de réseau. Si la machine a un nom de réseau unique, utilisez le nom d'hôte par défaut. Remarque: N'utilisez pas localhost. Le nom d'hôte doit explicitement identifier la machine.	
Nom du nœud principal de passerelle	Nom du nœud principal de passerelle que vous prévoyez de créer sur cette machine. Le nom du nœud n'est pas le nom d'hôte de la machine.	

Nœuds

Lorsque vous installez les services d'Enterprise Data Catalog, vous ajoutez la machine d'installation au domaine en tant que nœud. Vous pouvez ajouter plusieurs nœuds à un domaine.

Utilisez le tableau suivant pour enregistrer les informations requises sur les nœuds :

Informations sur les nœuds	Description	Valeur pour Nœud1	Valeur pour Nœud2	Valeur pour Nœud3
Nom d'hôte du nœud	Nom d'hôte complet de la machine sur laquelle créer le nœud. Si la machine a un nom de réseau unique, utilisez le nom d'hôte par défaut. Le nom d'hôte du nœud ne peut pas contenir le caractère de soulignement (_). Si la machine dispose de plusieurs noms de réseau, vous pouvez modifier le nom d'hôte par défaut pour utiliser un autre nom de réseau. Si la machine a un nom de réseau unique, utilisez le nom d'hôte par défaut. Remarque: N'utilisez pas localhost. Le nom d'hôte doit explicitement identifier la machine.			
Nom du nœud	Nom du nœud que vous prévoyez de créer sur cette machine. Le nom du nœud n'est pas le nom d'hôte de la machine.			

Services d'application

Les services d'application que vous créez dépendent de la clé de licence générée pour votre organisation.

Utilisez le tableau suivant pour enregistrer les services d'application dont vous avez besoin dans le domaine ainsi que les nœuds qui exécutent les services d'application :

Service d'application	Nom du service	Nom du nœud
Service de catalogue		
Service de gestion de contenu		
Service d'intégration de données		
Service de référentiel modèle		
Service de cluster Informatica		

Stockage des données sécurisé

Lorsque vous installez les services d'Enterprise Data Catalog, vous devez fournir un mot clé que le programme d'installation utilise pour générer la clé de chiffrement du domaine.

Utilisez le tableau suivant pour enregistrer les informations requises pour configurer le stockage des données sécurisé :

Informations sur la clé de chiffrement	Description	Valeur
Mot clé	Mot clé à utiliser pour créer une clé de cryptage personnalisée afin de sécuriser les données sensibles du domaine. Le mot clé doit respecter les critères suivants : <ul style="list-style-type: none">- Il comporte entre 8 et 20 caractères.- Il doit inclure au moins une lettre en majuscule.- Il doit inclure au moins une lettre en minuscule.- Il doit inclure au moins un chiffre.- Il ne doit pas contenir d'espaces. La clé de cryptage est créée en fonction du mot clé que vous indiquez lorsque vous créez le domaine Informatica.	
Répertoire de la clé de chiffrement	Répertoire dans lequel stocker la clé de chiffrement pour le domaine. L'emplacement par défaut est le répertoire suivant : <Enterprise Data Catalog installation directory>/isp/config/keys.	

Sécurité de domaine

Lorsque vous installez les services d'application Informatica, vous pouvez activer des options dans le domaine Informatica pour configurer la sécurité du domaine.

Communication sécurisée pour les services et le gestionnaire de service

Vous pouvez éventuellement configurer une communication sécurisée entre les services et le gestionnaire de service.

Important: Si vous choisissez d'utiliser les certificats SSL au lieu des certificats par défaut, vous devez fournir des informations sur les certificats SSL lors de l'installation. Vous pouvez fournir un certificat auto-signé ou un certificat émis par une autorité de certification (CA). Vous devez fournir les certificats SSL dans le format PEM et dans des fichiers keystore Java (JKS, Java Keystore). Informatica requiert des noms de fichiers de certificat SSL spécifiques pour le domaine Informatica.

Utilisez le tableau suivant pour enregistrer des informations sur le fichier entrepôt de clés et truststore contenant les certificats SSL à utiliser :

Informations de sécurité	Description	Valeur
Répertoire de fichiers keystore	Répertoire contenant les fichiers keystore. Il doit contenir les fichiers infa_keystore.jks et infa_keystore.pem.	
Mot de passe keystore	Mot de passe du fichier keystore infa_keystore.jks.	

Informations de sécurité	Description	Valeur
Répertoire de fichiers truststore	Répertoire contenant les fichiers truststore. Il doit contenir les fichiers infa_truststore.jks et infa_truststore.pem.	
Mot de passe truststore	Mot de passe du fichier infa_truststore.jks.	

Base de données sécurisée du référentiel de configuration de domaine

Vous pouvez éventuellement créer le référentiel de configuration de domaine dans une base de données sécurisée avec le protocole SSL.

Important: L'accès à la base de données sécurisée requiert un fichier truststore contenant les certificats de la base de données.

Utilisez le tableau suivant pour enregistrer les informations sur le fichier truststore pour la base de données sécurisée :

Informations de sécurité	Description	Valeur
Fichier truststore de base de données	Chemin et nom du fichier truststore de la base de données sécurisée.	
Mot de passe du fichier truststore de la base de données	Mot de passe du fichier truststore.	

Connexion sécurisée pour Informatica Administrator

Vous pouvez éventuellement configurer une connexion HTTPS sécurisée pour Informatica Administrator.

Important: Si vous choisissez de créer un fichier entrepôt de clés au lieu du fichier par défaut, vous devez fournir des informations sur le fichier lors de l'installation.

Utilisez le tableau suivant pour enregistrer les informations sur le fichier entrepôt de clés à utiliser :

Informations de sécurité	Description	Valeur
Mot de passe keystore	Mot de passe en texte clair pour le fichier entrepôt de clés.	
Répertoire de fichiers keystore	Emplacement du fichier entrepôt de clés.	

CHAPITRE 3

Préparer les bases de données pour le domaine Informatica

Ce chapitre comprend les rubriques suivantes :

- [Préparer les bases de données du domaine Informatica - Présentation, 37](#)
- [Configurer des comptes utilisateur de base de données , 38](#)
- [Spécifications de la base de données du référentiel de configuration du domaine, 38](#)
- [Spécifications de la base de données du cache d'objet de données, 41](#)
- [Configuration requise pour la base de données du référentiel modèle, 43](#)
- [Configuration requise pour l'entrepôt de profilage profilage, 45](#)
- [Spécifications de l'entrepôt de données de référence, 47](#)

Préparer les bases de données du domaine Informatica - Présentation

Avant de créer le domaine et les services d'application, configurez les bases de données et les comptes d'utilisateur de base de données pour les référentiels.

Configurez une base de données et un compte d'utilisateur pour les référentiels suivants :

- Référentiel de configuration du domaine
- Référentiel du cache d'objet de données
- Référentiel modèle
- Entrepôt de profilage
- Entrepôt de données de référence

Pour préparer les bases de données, vérifiez les prérequis correspondants, puis configurez la base de données. Les prérequis de la base de données dépendent des services d'application que vous créez dans le domaine et du nombre d'objets d'intégration de données que vous générez et enregistrez dans les référentiels.

Configurer des comptes utilisateur de base de données

Configurez une base de données et un compte d'utilisateur pour le référentiel de configuration du domaine et pour les bases de données du référentiel associées aux services d'application.

Lorsque vous configurez les comptes d'utilisateur, utilisez les règles et directives suivantes :

- Le compte d'utilisateur de la base de données doit avoir les permissions pour créer et supprimer des tables, des indexes et des vues, et pour sélectionner, insérer, mettre à jour et supprimer des données dans les tables.
- Créez le mot de passe du compte en ASCII-7 bits.
- Pour éviter que des erreurs de base de données dans un référentiel n'affectent d'autres référentiels, créez chaque référentiel dans un schéma de base de données distinct avec un compte d'utilisateur de base de données différent. Ne créez pas de référentiel dans le même schéma de base de données que le référentiel de configuration du domaine ou d'autres référentiels du domaine.
- Si vous créez plusieurs domaines, chaque référentiel de configuration du domaine doit disposer d'un compte d'utilisateur propre.

Spécifications de la base de données du référentiel de configuration du domaine

Les composants Informatica stockent les métadonnées dans des référentiels de base de données relationnelle. Le domaine stocke la configuration et les informations utilisateur dans un référentiel de configuration de domaine.

Vous devez configurer une base de données et un compte utilisateur pour le référentiel de configuration du domaine avant d'exécuter l'installation. La base de données doit être accessible à tous les nœuds de passerelle du domaine Informatica.

Lorsque vous installez Enterprise Data Catalog, vous indiquez les informations sur la base de données et le compte utilisateur pour le référentiel de configuration du domaine. Le programme d'installation d'Enterprise Data Catalog utilise JDBC pour communiquer avec le référentiel de configuration du domaine.

Le référentiel de configuration du domaine prend en charge les types de base de données suivants :

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle
- Sybase ASE

Autorisez 200 Mo d'espace disque.

Prérequis de la base de données IBM DB2

Utilisez les directives suivantes lors de la configuration du référentiel dans IBM DB2 :

- Si le référentiel se trouve dans une base de données IBM DB2, vérifiez qu'IBM DB2 Version 10.5 est installé.

- Dans l'instance d'IBM DB2 sur laquelle vous créez la base de données, définissez les paramètres suivants sur ON :
 - DB2_SKIPINSERTED
 - DB2_EVALUNCOMMITTED
 - DB2_SKIPDELETED
 - AUTO_RUNSTATS
- Dans la base de données, définissez les paramètres de configuration.

Le tableau suivant répertorie les paramètres de configuration que vous devez définir :

Paramètre	Valeur
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

Paramètre	Valeur
applheapsz	8192
appl_ctl_heap_sz	8192
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Définissez le paramètre pageSize de l'espace de table sur 32 768 octets.
 Dans une base de données à partition unique, indiquez un espace de table qui répond à la configuration requise de pageSize. Si vous n'indiquez pas un espace de table, l'espace de table par défaut doit répondre à la configuration requise de pageSize.
 Dans une base de données à plusieurs partitions, indiquez un espace de table qui répond à la configuration requise de pageSize. Définissez l'espace de table dans la partition de catalogue de la base de données.
- Définissez le paramètre NPAGES sur au moins 5000. Le paramètre NPAGES détermine le nombre de pages dans l'espace de table.
- Assurez-vous que l'utilisateur de la base de données dispose des privilèges CREATETAB, CONNECT et BINDADD.
- Informatica ne prend pas en charge les alias de table IBM DB2 pour les tables de référentiel. Vérifiez que des alias de table n'ont été créés pour aucune table de la base de données.

- Dans l'utilitaire DataDirect Connect for JDBC, mettez à jour le paramètre DynamicSections sur 3000.
La valeur par défaut de DynamicSections est trop faible pour les référentiels d'Enterprise Data Catalog. Enterprise Data Catalog requiert un package DB2 plus grand que celui par défaut. Lorsque vous configurez la base de données DB2 pour le référentiel de configuration du domaine ou un référentiel modèle, vous devez définir le paramètre DynamicSections sur 3000 au minimum. Si le paramètre DynamicSections est défini sur un nombre inférieur, vous pouvez rencontrer des problèmes lors de l'installation ou de l'exécution des services d'Enterprise Data Catalog.

Configuration requise pour la base de données Microsoft SQL Server

Utilisez les directives suivantes lorsque vous configurez le référentiel :

- Spécifiez le nom de schéma de base de données lorsque vous utilisez Microsoft SQL Server comme base de données de référentiel modèle.
- Définissez les niveaux d'isolation des captures instantanées sur ALLOW_SNAPSHOT_ISOLATION et READ_COMMITTED_SNAPSHOT afin de minimiser les problèmes de verrouillage.

Pour définir le niveau d'isolation de base de données, exécutez les commandes suivantes :

```
ALTER DATABASE NomBaseDeDonnées SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE NomBaseDonnées SET READ_COMMITTED_SNAPSHOT ON
```

Pour vérifier que le niveau d'isolation de la base de données est correct, exécutez les commandes suivantes :

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[NomBaseDeDonnées]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = NomBaseDonnées
```

- Le compte d'utilisateur de base de données doit posséder les privilèges CONNECT, CREATE TABLE et CREATE VIEW.

Spécifications de la base de données Oracle

Utilisez les directives suivantes lorsque vous définissez le référentiel dans Oracle :

- Définissez le paramètre open_cursors sur 4000 ou plus.
- Définissez les autorisations de l'utilisateur de la base de données concernant la vue \$parameter.
- Définissez les privilèges de l'utilisateur de la base de données pour exécuter *show parameter open_cursors* dans la base de données Oracle.
Lorsque vous exécutez l'outil Pre-Installation System Check (i10Pi), celui-ci exécute la commande sur la base de données pour identifier le paramètre OPEN_CURSORS avec les justificatifs d'identité de l'utilisateur de la base de données du domaine.

Vous pouvez exécuter la requête suivante pour déterminer le paramètre open_cursors pour le compte d'utilisateur de la base de données du domaine :

```
SELECT VALUE OPEN_CURSORS FROM V$PARAMETER WHERE UPPER(NAME)=UPPER('OPEN_CURSORS')
```

- Vérifiez que l'utilisateur de la base de données dispose des privilèges suivants :

```
CREATE SEQUENCE
```

```
CREATE SESSION
```

```
CREATE SYNONYM
```

```
CREATE TABLE
```

CREATE VIEW

- Informatica ne prend pas en charge les synonymes publics d'Oracle pour les tables de référentiel. Vérifiez que des synonymes publics n'ont été créés pour aucune table de la base de données.

Spécifications de la base de données Sybase ASE

Utilisez les instructions suivantes lors de la configuration du référentiel dans Sybase ASE :

- Définissez la taille de page du serveur de base de données sur 8 K au minimum. Ceci est une configuration unique qui n'est pas modifiable par la suite.

La base de données du référentiel de l'analyseur de données requiert une taille de page d'au moins 8 Ko. Si vous configurez une base de données de l'analyseur de données sur une instance de Sybase ASE avec une taille de page inférieure à 8 Ko, l'analyseur de données peut générer des erreurs lors de l'exécution des rapports. Sybase ASE assouplit la restriction de taille de ligne lorsque vous augmentez la taille de page.

L'analyseur de données comprend une clause GROUP BY dans la requête SQL pour le rapport. Lors de l'exécution du rapport, Sybase ASE stocke toutes les clauses GROUP BY et regroupe les colonnes dans une table de travail temporaire. La taille maximale de ligne d'index de la table de travail est limitée par la taille de page de la base de données. Par exemple, si Sybase ASE est installé avec la taille de page par défaut de 2 Ko, la taille de ligne d'index ne peut pas dépasser 600 octets. Toutefois, la clause GROUP BY dans la requête SQL pour la plupart des rapports de l'analyseur de données génère une taille de ligne d'index supérieure à 600 octets.

- Vérifiez que l'utilisateur de la base de données dispose des privilèges CREATE TABLE et CREATE VIEW.
- Définissez « autoriser les nulls par défaut » sur TRUE.
- Activez l'option Gestion des transactions distribuées (DTM) dans le serveur de base de données.
- Créez un compte d'utilisateur DTM et accordez le dtm_tm_role à l'utilisateur.

Le tableau suivant indique le paramètre de configuration DTM pour la valeur dtm_tm_role :

Configuration de DTM	Procédure de système Sybase	Valeur
Privilège Gestion des transactions distribuées	sp_role "grant"	dtm_tm_role, username

Spécifications de la base de données du cache d'objet de données

La base de données de cache d'objet de données stocke les objets de données logiques mis en cache et les tables virtuelles pour le service d'intégration de données. Vous devez spécifier la connexion de base de données du cache d'objet de données lorsque vous créez le service d'intégration de données.

La base de données du cache d'objet de données prend en charge les types de base de données suivants :

- IBM DB2 UDB
- Microsoft SQL Server
- Base de données SQL Microsoft Azure
- Oracle

Autorisez 200 Mo d'espace disque pour la base de données.

Remarque: Veillez à installer le client de base de données sur la machine sur laquelle vous voulez exécuter le service d'intégration de données.

Spécifications de la base de données IBM DB2

Utilisez les directives suivantes lors de la configuration du référentiel dans IBM DB2 :

- Vérifiez que le compte utilisateur de la base de données dispose des privilèges CREATETAB et CONNECT.
- Informatica ne prend pas en charge les alias de table IBM DB2 pour les tables de référentiel. Vérifiez que des alias de table n'ont été créés pour aucune table de la base de données.
- Définissez le paramètre pageSize de l'espace de table sur 32 768 octets.
- Définissez le paramètre NPAGES sur au moins 5000. Le paramètre NPAGES détermine le nombre de pages dans l'espace de table.

Spécifications de la base de données Microsoft SQL Server

Utilisez les directives suivantes lorsque vous configurez le référentiel :

- Vérifiez que le compte d'utilisateur de base de données dispose des privilèges CONNECT et CREATE TABLE.

Configuration requise pour la base de données Oracle

Utilisez les directives suivantes lorsque vous définissez le référentiel dans Oracle :

- Vérifiez que l'utilisateur de la base de données dispose des privilèges suivants :
 - CREATE INDEX
 - CREATE SESSION
 - CREATE SYNONYM
 - CREATE TABLE
 - CREATE VIEW
 - DROP TABLE
 - INSERT INTO TABLE
 - UPDATE TABLE
- Informatica ne prend pas en charge les synonymes publics d'Oracle pour les tables de référentiel. Vérifiez que des synonymes publics n'ont été créés pour aucune table de la base de données.

Configuration requise pour la base de données du référentiel modèle

Les services d'Enterprise Data Catalog et les clients Informatica stockent des données et des métadonnées dans le référentiel modèle. Avant de créer le service de référentiel modèle, configurez une base de données et un compte utilisateur correspondant pour le référentiel modèle.

Le référentiel modèle prend en charge les types de base de données suivants :

- IBM DB2 UDB
- Microsoft SQL Server
- Base de données SQL Microsoft Azure
- Oracle

Autorisez 3 Go d'espace disque pour DB2. Autorisez 200 Mo d'espace disque pour tous les autres types de base de données.

Pour plus d'informations sur la configuration de la base de données, consultez la documentation de votre système de base de données.

Prérequis de la base de données IBM DB2

Utilisez les directives suivantes lors de la configuration du référentiel dans IBM DB2 :

- Si le référentiel se trouve dans une base de données IBM DB2, vérifiez qu'IBM DB2 Version 10.5 est installé.
- Dans l'instance d'IBM DB2 sur laquelle vous créez la base de données, définissez les paramètres suivants sur ON :
 - DB2_SKIPINSERTED
 - DB2_EVALUNCOMMITTED
 - DB2_SKIPDELETED
 - AUTO_RUNSTATS
- Dans la base de données, définissez les paramètres de configuration.

Le tableau suivant répertorie les paramètres de configuration que vous devez définir :

Paramètre	Valeur
logfilsiz	8000
maxlocks	98

Paramètre	Valeur
locklist	50000
auto_stmt_stats	ON

Paramètre	Valeur
applheapsz	8192
appl_ctl_heap_sz	8192
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Définissez le paramètre `pageSize` de l'espace de table sur 32 768 octets.
 Dans une base de données à partition unique, indiquez un espace de table qui répond à la configuration requise de `pageSize`. Si vous n'indiquez pas un espace de table, l'espace de table par défaut doit répondre à la configuration requise de `pageSize`.
 Dans une base de données à plusieurs partitions, indiquez un espace de table qui répond à la configuration requise de `pageSize`. Définissez l'espace de table dans la partition de catalogue de la base de données.
- Définissez le paramètre `NPAGES` sur au moins 5000. Le paramètre `NPAGES` détermine le nombre de pages dans l'espace de table.
- Assurez-vous que l'utilisateur de la base de données dispose des privilèges `CREATETAB`, `CONNECT` et `BINDADD`.
- Informatica ne prend pas en charge les alias de table IBM DB2 pour les tables de référentiel. Vérifiez que des alias de table n'ont été créés pour aucune table de la base de données.
- Dans l'utilitaire `DataDirect Connect for JDBC`, mettez à jour le paramètre `DynamicSections` sur 3000.
 La valeur par défaut de `DynamicSections` est trop faible pour les référentiels d'Enterprise Data Catalog. Enterprise Data Catalog requiert un package DB2 plus grand que celui par défaut. Lorsque vous configurez la base de données DB2 pour le référentiel de configuration du domaine ou un référentiel modèle, vous devez définir le paramètre `DynamicSections` sur 3000 au minimum. Si le paramètre `DynamicSections` est défini sur un nombre inférieur, vous pouvez rencontrer des problèmes lors de l'installation ou de l'exécution des services d'Enterprise Data Catalog.

Configuration requise pour la base de données Microsoft SQL Server

Utilisez les directives suivantes lorsque vous configurez le référentiel :

- Définissez les niveaux d'isolation des captures instantanées sur ALLOW_SNAPSHOT_ISOLATION et READ_COMMITTED_SNAPSHOT afin de minimiser les problèmes de verrouillage.
Pour définir le niveau d'isolation de base de données, exécutez les commandes suivantes :

```
ALTER DATABASE NomBaseDeDonnées SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE NomBaseDonnées SET READ_COMMITTED_SNAPSHOT ON
```

Pour vérifier que le niveau d'isolation de la base de données est correct, exécutez les commandes suivantes :

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[NomBaseDeDonnées]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = NomBaseDonnées
```

- Le compte d'utilisateur de base de données doit posséder les privilèges CONNECT, CREATE TABLE et CREATE VIEW.

Configuration requise pour la base de données Oracle

Utilisez les directives suivantes lorsque vous définissez le référentiel dans Oracle :

- Définissez le paramètre OPEN_CURSORS sur 4 000 ou plus.
Vérifiez que l'utilisateur de la base de données dispose des privilèges suivants :

```
CREATE SEQUENCE
```

```
CREATE SESSION
```

```
CREATE SYNONYM
```

```
CREATE TABLE
```

```
CREATE VIEW
```

- Informatica ne prend pas en charge les synonymes publics d'Oracle pour les tables de référentiel. Vérifiez que des synonymes publics n'ont été créés pour aucune table de la base de données.

Configuration requise pour l'entrepôt de profilage profilage

La base de données de l'entrepôt de profilage stocke les résultats du profilage et de la fiche d'évaluation. Vous devez spécifier la connexion de l'entrepôt de profilage lorsque vous créez le service d'intégration de données.

L'entrepôt de profilage prend en charge les types de base de données suivants :

- IBM DB2 UDB
- Microsoft SQL Server
- Base de données SQL Microsoft Azure
- Oracle

Autorisez 10 Go d'espace disque pour la base de données.

Remarque: Veillez à installer le client de base de données sur la machine sur laquelle vous voulez exécuter le service d'intégration de données. Vous pouvez spécifier une connexion JDBC ou Hive en tant que connexion d'entrepôt de profilage pour les types de base de données IBM DB2 UDB, Microsoft SQL Server et Oracle.

Pour plus d'informations sur la configuration de la base de données, consultez la documentation de votre système de base de données.

Configuration requise pour la base de données IBM DB2

Utilisez les directives suivantes lors de la configuration du référentiel dans IBM DB2 :

- Le compte d'utilisateur de la base de données doit avoir les privilèges CREATETAB, CONNECT, CREATE VIEW et CREATE FUNCTION.
- Informatica ne prend pas en charge les alias de table IBM DB2 pour les tables de référentiel. Vérifiez que des alias de table n'ont été créés pour aucune table de la base de données.
- Définissez le paramètre pageSize de l'espace de table sur 32 768 octets.
- Définissez le paramètre NPAGES sur au moins 5000. Le paramètre NPAGES détermine le nombre de pages dans l'espace de table.

Remarque: Si vous utilisez une connexion JDBC comme connexion d'entrepôt de profilage, Informatica ne prend pas en charge l'environnement de base de données partitionnée pour les bases de données IBM DB2.

Spécifications de la base de données Microsoft SQL Server

Utilisez les directives suivantes lorsque vous configurez le référentiel :

- Le compte utilisateur de la base de données doit avoir les privilèges CONNECT, CREATE TABLE, CREATE VIEW et CREATE FUNCTION.

Configuration requise de la base de données Oracle

Utilisez les directives suivantes lorsque vous définissez le référentiel dans Oracle :

- Vérifiez que l'utilisateur de la base de données dispose des privilèges suivants :
 - ALTER TABLE
 - CREATE ANY INDEX
 - CREATE PROCEDURE
 - CREATE SESSION
 - CREATE TABLE
 - CREATE VIEW
 - DROP TABLE
 - UPDATE TABLE
- Informatica ne prend pas en charge les synonymes publics d'Oracle pour les tables de référentiel. Vérifiez que des synonymes publics n'ont été créés pour aucune table de la base de données.
- Définissez le paramètre Espace de table.

- Définissez les paramètres suivants sur les valeurs recommandées par Informatica :

Paramètre	Valeur recommandée
open_cursors	3 000
Sessions	1 000
Processus	1 000

Spécifications de l'entrepôt de données de référence

L'entrepôt de données de référence stocke les valeurs de données des objets de table de référence que vous définissez dans un référentiel modèle. Vous configurez un service de gestion de contenu pour identifier l'entrepôt de données de référence et le référentiel modèle.

Vous associez un entrepôt de données de référence à un seul référentiel modèle. Vous pouvez sélectionner un entrepôt de données de référence commun sur plusieurs services de gestion de contenu si ces derniers identifient un référentiel modèle commun. L'entrepôt de données de référence doit prendre en charge les noms de colonne à casse mixte.

L'entrepôt de données de référence prend en charge les types de base de données suivants :

- IBM DB2 UDB
- Microsoft SQL Server
- Base de données SQL Microsoft Azure
- Oracle

Autorisez 200 Mo d'espace disque pour la base de données.

Remarque: Veillez à installer le client de base de données sur la machine sur laquelle vous voulez exécuter le service de gestion de contenu.

Spécifications de la base de données IBM DB2

Utilisez les directives suivantes lors de la configuration du référentiel dans IBM DB2 :

- Vérifiez que le compte utilisateur de la base de données dispose des privilèges CREATETAB et CONNECT.
- Vérifiez que l'utilisateur de la base de données dispose des privilèges SELECT sur les tables SYSCAT.DBAUTH et SYSCAT.DBTAUTH.
- Informatica ne prend pas en charge les alias de table IBM DB2 pour les tables de référentiel. Vérifiez que des alias de table n'ont été créés pour aucune table de la base de données.
- Définissez le paramètre pageSize de l'espace de table sur 32 768 octets.
- Définissez le paramètre NPAGES sur au moins 5000. Le paramètre NPAGES détermine le nombre de pages dans l'espace de table.

Spécifications de la base de données Microsoft SQL Server

Utilisez les directives suivantes lorsque vous configurez le référentiel :

- Vérifiez que le compte d'utilisateur de base de données dispose des privilèges CONNECT et CREATE TABLE.

Configuration requise pour la base de données Oracle

Utilisez les directives suivantes lorsque vous définissez le référentiel dans Oracle :

- Vérifiez que l'utilisateur de la base de données dispose des privilèges suivants :

ALTER SEQUENCE

ALTER TABLE

CREATE SEQUENCE

CREATE SESSION

CREATE TABLE

CREATE VIEW

DROP SEQUENCE

DROP TABLE

- Informatica ne prend pas en charge les synonymes publics d'Oracle pour les tables de référentiel. Vérifiez que des synonymes publics n'ont été créés pour aucune table de la base de données.

CHAPITRE 4

Méthodes de déploiement

Ce chapitre comprend les rubriques suivantes :

- [Présentation des méthodes de déploiement, 49](#)
- [Déploiement du cluster Hadoop intégré Prérequis, 49](#)
- [Prérequis du cluster intégré , 50](#)
- [Prérequis du cluster existant, 61](#)
- [Déploiement du cluster Hadoop existant, 63](#)
- [Préparation de l'environnement de cluster Hadoop existant, 64](#)
- [Configuration de Kerberos et de SSL pour un cluster existant, 64](#)

Présentation des méthodes de déploiement

Vous pouvez déployer Enterprise Data Catalog soit dans une distribution Hadoop incorporée sur Hortonworks, soit sur une distribution Hadoop existante sur Cloudera, Hortonworks ou Azure HDInsight. Si vous choisissez l'option de cluster Hadoop existante pour déployer Enterprise Data Catalog, configurez l'environnement de cluster Cloudera, Hortonworks ou Azure HDInsight dans votre entreprise avant l'installation d'Enterprise Data Catalog. Si vous choisissez l'option de cluster Hadoop intégrée, vous effectuez la configuration de cluster Hortonworks lorsque vous installez Enterprise Data Catalog.

Déploiement du cluster Hadoop intégré Prérequis

Lorsque vous installez Enterprise Data Catalog sur un cluster Hadoop intégré, vous pouvez choisir de créer des services d'application, tels que le service de référentiel modèle, le service d'intégration de données et le service de catalogue.

Le programme d'installation d'Enterprise Data Catalog crée un **service de cluster Informatica** si vous choisissez la distribution Hadoop intégrée. Enterprise Data Catalog utilise Apache Ambari pour gérer et surveiller le cluster Hadoop intégré. Le cluster Hadoop intégré pour Enterprise Data Catalog prend en charge l'option haute disponibilité.

Les composants suivants des environnements de cluster Hadoop intégré d'Enterprise Data Catalog prennent en charge l'option haute disponibilité :

- HDFS

- HBase
- Yarn
- Solr

Prérequis du cluster intégré

Avant d'installer Enterprise Data Catalog dans un cluster Hadoop intégré, vous devez vérifier que l'environnement système répond aux prérequis nécessaires au déploiement d'Enterprise Data Catalog.

Prérequis du système d'exploitation

Avant d'installer Enterprise Data Catalog sur un cluster intégré, consultez les sections suivantes relatives aux prérequis du système d'exploitation sur les nœuds de cluster :

- ["Prérequis courants du système d'exploitation de Red Hat Enterprise Linux et de SUSE Linux Enterprise Server" à la page 50](#)
- ["Prérequis du système d'exploitation pour Red Hat Enterprise Linux" à la page 52](#)
- ["Prérequis du système d'exploitation pour SUSE Linux Enterprise Server" à la page 53](#)

Prérequis courants du système d'exploitation de Red Hat Enterprise Linux et de SUSE Linux Enterprise Server

Vous pouvez installer Enterprise Data Catalog sur une machine qui s'exécute sur Red Hat Enterprise Linux Server ou sur SUSE Linux Enterprise Server.

Vérifiez les prérequis courants suivants des SUSE et Red Hat Enterprise Linux Servers :

- Vérifiez que le système d'exploitation est de version 64 bits.
- Veillez à installer `file`.
- Assurez-vous que `Bash` est le shell par défaut.
- Si vous utilisez un compte d'utilisateur sans privilèges racine et que vous voulez supprimer l'accès à la commande `sudo`, assurez-vous que `defaults requiretty` est commenté dans `/etc/sudoers`.
- Si vous utilisez un compte d'utilisateur sans privilèges racine, vérifiez que l'utilisateur Hadoop dispose des privilèges `sudo`.
- Assurez-vous d'avoir désactivé l'invite de mot de passe de l'utilisateur Hadoop.
- Assurez-vous d'avoir installé `python-devel`.
- Assurez-vous d'avoir défini `UMASK` sur `022` (`0022`) ou sur `027` (`0027`).
- Veillez à avoir défini le nom de domaine complet (FQDN) du nom d'hôte `-f`.
- Assurez-vous que l'emplacement de `/var` ne dispose pas du privilège d'écriture pour tout le monde.
- Veillez à avoir configuré les référentiels de base de Linux.
- Assurez-vous d'avoir installé l'outil utilitaire réseau de ligne de commande `netstat`.
- Vérifiez que le répertoire racine (`/`) dispose d'un minimum de 10 Go d'espace disque libre.

- Si vous prévoyez d'installer Enterprise Data Catalog dans un cluster intégré et que vous voulez monter le service de cluster Informatica dans un emplacement de montage distinct, vérifiez que celui-ci dispose d'un minimum de 50 Go d'espace disque libre.
- Assurez-vous que l'indicateur NOEXEC n'est pas défini pour le système de fichiers monté dans le répertoire `/tmp`.
- Pour optimiser les performances, vous souhaitez peut-être vous assurer que le répertoire `/tmp` dispose d'un minimum de 20 Go d'espace disque libre.
- Veillez à avoir installé les utilitaires `scp`, `curl`, `unzip`, `wget` et `tar`.
- Assurez-vous d'avoir configuré le répertoire `home` avec l'autorisation d'écriture.
- Vérifiez que le fichier `/etc/hosts` configuré de toutes les machines incluent le nom de domaine complet des machines.
- Veillez à ce que le démon NTP (Network Time Protocol) soit synchronisé et en cours d'exécution.
- Vérifiez que le répertoire `/tmp` dispose de l'accès `chmod 777` configuré pour le répertoire.
- Vérifiez que les répertoires `/et` et `/var` ne disposent pas de l'autorisation `chmod 777` configurée.
- Vérifiez que le répertoire `/var` dispose d'un minimum de 2 Go d'espace disque libre.
- Vérifiez que le répertoire `/usr` dispose d'un minimum de 2 Go d'espace disque libre.
- Veillez à désactiver Selinux ou définir Selinux sur le mode permissif.
- Vérifiez que le répertoire `/etc/hosts` dispose d'une entrée pour l'adresse de bouclage `127.0.0.1 localhost localhost.domain.com`
- Assurez-vous d'avoir défini la limite de cœurs sur `unlimited` pour un utilisateur sans privilèges racine.
- Pour configurer le répertoire `workingDir` sur `/`, confirmez que l'indicateur EXEC est défini dans le système de fichiers monté dans les répertoires `/tmp` et `/var`.
- Si `workingDir` n'est pas configuré sur `/`, confirmez que les autorisations de lecture, d'écriture et d'exécution sont configurées pour le répertoire `workingDir`. Confirmez que l'indicateur EXEC est également défini pour le répertoire.
- Assurez-vous de disposer de l'autorisation d'écriture dans le répertoire `/home`. Vous pouvez configurer l'autorisation dans le fichier `/etc/default/useradd`.
- Assurez-vous que chaque machine du cluster inclut l'entrée `127.0.0.1 localhost localhost.localdomain` dans le fichier `/etc/hosts`.
- Vérifiez que le fichier `/etc/hosts` inclut les noms d'hôtes complets pour tous les nœuds de cluster. Vous pouvez également vérifier que la recherche DNS inversée renvoie les noms d'hôtes complets pour tous les nœuds de cluster.
- Vérifiez que le répertoire Linux inclut postgresql version 8.14.18, publication 1.el6_4 ou versions ultérieures.
- Assurez-vous d'avoir défini la limite non stricte du nombre max. de processus utilisateur à 32 000 au minimum.
- Assurez-vous d'avoir défini la limite stricte du nombre max. de processus utilisateur à 32 000 au minimum.
- Assurez-vous d'avoir défini la limite non stricte du nombre max. de processus utilisateur à 10 000 au minimum pour les nœuds de cluster.
- Assurez-vous d'avoir défini la limite stricte du nombre max. de processus utilisateur à 10 000 au minimum pour les nœuds de cluster.

- Sur chaque machine hôte, vérifiez que les outils et applications suivants sont disponibles :
 - YUM et RPM (RHEL/CentOS/Oracle Linux)
 - Zypper
 - scp, curl, unzip, tar et wget
 - awk
 - OpenSSL version 1.0.1e-30.el6_6.5.x86_64 ou versions ultérieures.

Remarque: Assurez-vous que la variable \$PATH pointe vers le répertoire /usr/bin pour utiliser la version correcte de Linux OpenSSL.
- Pour Enterprise Data Catalog installé dans un cluster intégré, installez les packages suivants si vous n'avez pas configuré le référentiel de base Linux ou si vous n'avez aucune connexion Internet :
 - Les RPM suivants sur l'hôte du serveur Ambari :
 - postgresql-libs
 - postgresql-server
 - postgresql
 - Les RPM suivants sur tous les nœuds de cluster :
 - nc
 - redhat-lsb
 - psmisc
 - python-devel

Prérequis du système d'exploitation pour Red Hat Enterprise Linux

Vérifiez les prérequis suivants de Red Hat Linux Enterprise Server si vous prévoyez d'installer Enterprise Data Catalog sur Red Hat Enterprise Linux Server :

Systeme d'exploitation	Prerequis
Red Hat Enterprise Linux versions 6 et 7	<ul style="list-style-type: none"> - Pour Red Hat Enterprise Linux version 7.0, veillez à utiliser Sudo version 1.8.16 ou versions ultérieures. - Installez kernel-headers et kernel-devel. - Installez libtirpc-devel. - Installez openssl version v1.01 build 16 ou versions ultérieures ou v1.0.2k. - Installez YUM. - Assurez-vous que le répertoire /etc/sysconfig/network existe et configurez l'autorisation de lecture pour celui-ci. - /etc/sysconfig/network inclut la même entrée que celle configurée pour le nom d'hôte -f. - Installez Python version 2.6.x ou 2.7.x. Applicable à Red Hat Enterprise Linux version 6. - Installez Python version 2.7.x. Applicable à Red Hat Enterprise Linux version 7. - Désactivez la validation du certificat SSL.

Prérequis du système d'exploitation pour SUSE Linux Enterprise Server

Vérifiez les prérequis suivants de SUSE Linux Enterprise Server si vous prévoyez d'installer Enterprise Data Catalog sur SUSE Linux Enterprise Server :

Système d'exploitation	Prérequis
SUSE Linux Enterprise Server versions 11 et 12	<ul style="list-style-type: none">- Installez netcat-openbsd.- Installez kernel-default-devel.- Assurez-vous que le répertoire <code>/etc/HOSTNAME</code> existe et configurez l'autorisation de lecture pour celui-ci.- Vérifiez que le répertoire <code>/etc/HOSTNAME</code> inclut la même entrée que celle configurée pour le nom d'hôte <code>-f</code>- Installez Zypper.- Installez les versions suivantes de Python :<ul style="list-style-type: none">- 2.6.8/2.6.9/2.7.x pour SUSE Linux version 11.- 2.7.x pour SUSE Linux version 12.- Pour SUSE Enterprise Linux Server 11, mettez à jour tous les hôtes à la version de Python 2.6.8-0.15.1.- Si vous installez Enterprise Data Catalog sur SUSE Linux Enterprise Server 12, veillez à installer le RPM Package Manager (les RPM) suivant sur tous les nœuds de cluster :<ul style="list-style-type: none">- openssl-1.0.1c-2.1.3.x86_64.rpm- libopenssl1_0_0-1.0.1c-2.1.3.x86_64.rpm- libopenssl1_0_0-32bit-1.0.1c-2.1.3.x86_64.rpm- python-devel-2.6.8-0.15.1.x86_64- N'installez pas libsnappy si vous installez Enterprise Data Catalog sur SUSE Linux Enterprise Server.

Prérequis du nœud hôte

Vérifiez les prérequis suivants pour les nœuds hôte :

- Confirmez que SSH sans mot de passe est activé de la machine du domaine vers le serveur Apache Ambari.
- Confirmez que SSH sans mot de passe est activé du serveur Apache Ambari vers tous les agents Apache Ambari.
- Confirmez que le nombre d'agents Apache Ambari configurés est de 1 ou plus de 2.

Prérequis pour déployer Enterprise Data Catalog sur plusieurs nœuds

Vérifiez les prérequis suivants pour déployer Enterprise Data Catalog sur plusieurs nœuds :

- Veillez à utiliser les mêmes informations d'identification utilisateur pour démarrer tous les nœuds.
- Activez la connexion SSH sans mot de passe pour tous les nœuds hôte sur le nœud de cluster.
- Veillez à utiliser la même version des fichiers binaires d'Apache Ambari sur tous les nœuds.
- Vérifiez que vous utilisez les mêmes fichiers binaires de ressources sur tous les nœuds.
- Veillez à configurer le service de cluster Informatica et le service de catalogue sur des nœuds distincts.

Prérequis du nœud de cluster

Vérifiez que les nœuds de cluster répondent aux prérequis suivants :

Type de nœud	Prérequis minimaux
Nœud maître	<ul style="list-style-type: none">- Le nombre de processeurs est de 4.- La mémoire inutilisée disponible pour l'utilisation est de 12 Go.- La mémoire totale disponible pour l'utilisation est de 16 Go.- L'espace disque est de 60 Go.
Nœud esclave	<ul style="list-style-type: none">- Le nombre de processeurs est de 4.- La mémoire inutilisée disponible pour l'utilisation est de 12 Go.- La mémoire totale disponible pour l'utilisation est de 16 Go.- L'espace disque est de 60 Go.

Prérequis d'Apache Ambari

Vérifiez les prérequis suivants pour Apache Ambari :

- Apache Ambari requiert certains ports ouverts et disponibles pendant l'installation pour communiquer avec les hôtes qu'Apache Ambari déploie et gère. Vous devez désactiver temporairement les iptables pour répondre à ce prérequis.
- Vérifiez que vous répondez aux prérequis de mémoire et de package pour Apache Ambari. Pour plus d'informations, consultez la documentation Hortonworks.

Prérequis d'Apache Ranger

Avant de déployer Enterprise Data Catalog sur les clusters où Apache Ranger est activé, veillez à configurer les autorisations suivantes pour l'utilisateur du domaine Informatica :

- Autorisation d'écriture sur le dossier HDFS.
- Autorisation de soumettre des applications à la file d'attente YARN.

Limite de descripteurs de fichiers

Vérifiez que le nombre maximal de descripteurs de fichiers ouverts est de 10 000 ou plus. Utilisez la commande `ulimit` pour vérifier la valeur actuelle et la modifier si nécessaire.

Prérequis de SSL

Pour activer le protocole SSL du cluster, vérifiez les prérequis suivants :

- Si le cluster est activé pour SSL, assurez-vous d'importer le certificat de serveur Ambari dans le truststore du domaine Informatica.
- Si le cluster est activé pour SSL, il est recommandé d'activer SSL pour le domaine Informatica et les services d'application.
- Veillez à importer les certificats du cluster Hadoop dans le truststore du domaine avant de créer un service de catalogue pour un cluster Hadoop qui utilise le protocole SSL.

- Si vous souhaitez activer l'authentification SSL pour Enterprise Data Catalog déployé sur un domaine Informatica à plusieurs nœuds, assurez-vous de remplir les prérequis suivants :
 - Exportez le fichier Default.keystore de chaque nœud vers infa_truststore.jks sur tous les nœuds.
 - Assurez-vous que le fichier Default.keystore est unique pour chaque nœud hôte.
 - Copiez le fichier Default.keystore à un emplacement unique sur chaque nœud.
 - Si le service de cluster Informatica et le service de catalogue se trouvent sur des nœuds différents, exportez le certificat de serveur Apache Ambari vers infa_truststore.jks sur tous les nœuds.

Prérequis de Kerberos

Pour activer l'authentification Kerberos du cluster, vérifiez les prérequis suivants :

- Veillez à fusionner les fichiers keytab de l'utilisateur et de l'hôte avant d'activer l'authentification Kerberos pour le service de catalogue.
- Définissez la valeur `udp_preference_limit` sur 1 dans `$INFA_HOME/services/shared/security/krb5.conf`
- Assurez-vous que le certificat KDC est présent dans le nœud de domaine.
- Pour activer l'authentification Kerberos d'Enterprise Data Catalog déployé sur un domaine Informatica à plusieurs nœuds, assurez-vous de remplir les prérequis suivants :
 - Assurez-vous que tous les nœuds de domaine incluent le fichier `krb5.conf` dans les répertoires suivants :
 - `$INFA_HOME/services/shared/security/`
 - `/etc/` dans tous les nœuds du cluster.
 - Veillez à utiliser le même fichier `krb5.conf` dans le domaine Informatica et les nœuds du cluster.
 - Assurez-vous que le fichier `/etc/hosts` de tous les nœuds du cluster et de domaine inclut l'entrée d'hôte `krb` et une entrée d'hôte pour d'autres nœuds.
 - Installez `krb5-Workstation` dans tous les nœuds de domaine.
 - Assurez-vous que le fichier `keytab` est présent dans un emplacement commun dans tous les nœuds de domaine.
- Vérifiez que vous avez installé les packages de prérequis suivants avant d'activer Kerberos pour Enterprise Data Catalog sur Red Hat Enterprise Linux :
 - `krb5-workstation`
 - `krb5-libs`
- Pour Enterprise Data Catalog sur SUSE Linux Enterprise Server, assurez-vous d'avoir installé les packages de prérequis suivants :
 - `krb5-server`
 - `krb5-client`

Service de cluster Informatica

Le service de cluster Informatica est un service d'application qui exécute et gère tous les services Hadoop, le serveur Apache Ambari et les agents Apache Ambari sur un cluster Hadoop intégré. Si vous choisissez le mode de déploiement du cluster intégré, vous devez créer le service de cluster Informatica avant de créer le

service de catalogue. Ensuite, vous pouvez passer la valeur du service de cluster Informatica au service de catalogue.

Le service de cluster Informatica distribue les fichiers binaires Hortonworks et lance les services Hadoop requis sur les hôtes où le cluster intégré s'exécute.

Vous pouvez déployer le service de cluster Informatica sur les hôtes où Centrify est activé. Centrify s'intègre à une infrastructure Active Directory existante pour gérer l'authentification des utilisateurs sur les hôtes Linux distants.

Remarque: Informatica ne s'intègre pas à Centrify pour gérer ou générer des fichiers keytab.

Vous pouvez déployer le service de cluster Informatica sur les hôtes qui fournissent l'accès à l'aide des algorithmes de chiffrement SSH JSch.

Le tableau suivant répertorie les méthodes et algorithmes pris en charge :

Méthode	Algorithme
Échange de clés	<ul style="list-style-type: none">- diffie-hellman-group-exchange-sha1- diffie-hellman-group1-sha1- diffie-hellman-group14-sha1- diffie-hellman-group-exchange-sha256- ecdh-sha2-nistp256- ecdh-sha2-nistp384- ecdh-sha2-nistp521
Chiffrement	<ul style="list-style-type: none">- blowfish-cbc- 3des-cbc- aes128-cbc- aes192-cbc- aes256-cbc- aes128-ctr- aes192-ctr- aes256-ctr- 3des-ctr- arcfour- arcfour128- arcfour256
MAC	<ul style="list-style-type: none">- hmac-md5- hmac-sha1- hmac-md5-96- hmac-sha1-96
Type de clé d'hôte	<ul style="list-style-type: none">- ssh-dss- ssh-rsa- ecdsa-sha2-nistp256- ecdsa-sha2-nistp384- ecdsa-sha2-nistp521

Flux de travail du service de cluster Informatica

Le service de cluster Informatica est un service ISP qui gère le cluster Hadoop intégré dans Enterprise Data Catalog.

Après la création du service de cluster Informatica, il effectue les actions suivantes :

1. Lance le serveur Apache Ambari et ses agents associés.

2. Crée les services Hadoop et systèmes de surveillance sur Apache Ambari, y compris HDFS, Apache Zookeeper, Yarn et les services de surveillance connexes.
3. Démarre les services Hadoop.
4. Lorsque vous arrêtez Enterprise Data Catalog, le service de cluster Informatica arrête tous les services Hadoop ainsi que le serveur Apache Ambari et ses agents.

Création d'un service de cluster Informatica

Vous pouvez choisir de générer le service de cluster Informatica lors de l'installation d'Enterprise Data Catalog ou de créer manuellement le service d'application à l'aide d'Informatica Administrator.

Si vous prévoyez de déployer Enterprise Data Catalog sur plusieurs nœuds, veillez à configurer le service de cluster Informatica et le service de catalogue sur des nœuds distincts.

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.

Le tableau suivant décrit les propriétés :

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'espace. Les caractères qui composent le nom doivent être compatibles avec la page de code du référentiel modèle que vous associez au service de catalogue. Le nom ne peut pas contenir les caractères spéciaux suivants : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Description	Description du service. La description ne peut pas dépasser 765 caractères.
Emplacement	Domaine dans lequel le service d'application s'exécute.
Licence	Licence à attribuer au service de cluster Informatica. Sélectionnez la licence que vous avez installée avec Enterprise Data Catalog.
Nœud	Nœud dans le domaine Informatica sur lequel s'exécute le service de cluster Informatica. Si vous modifiez le nœud, vous devrez recycler le service de cluster Informatica.
Nœuds de sauvegarde	Si votre licence comprend la haute disponibilité, il s'agit des nœuds sur lesquels le service peut s'exécuter si le nœud principal est indisponible.

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.

Le tableau suivant décrit les propriétés :

Propriété	Description
Port HTTP	Numéro de port HTTP unique utilisé pour chaque processus de service d'intégration de données. La valeur par défaut est 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) .
Fichier keystore	Chemin d'accès 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. Nécessaire si vous sélectionnez Activer TLS (Transport Layer Security) .
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 Hadoop dans la boîte de dialogue.

Le tableau suivant décrit les propriétés :

Propriété	Description
Hôte de passerelle Hadoop	Hôte où s'exécute le serveur Apache Ambari.
Port de passerelle Hadoop	Port Web du serveur Apache Ambari.
Utilisateur de passerelle	Nom d'utilisateur du serveur Apache Ambari.
Nœuds Hadoop	Hôtes où les agents Apache Ambari s'exécutent.
Remplacer le mot de passe par défaut	Sélectionnez cette option pour modifier le mot de passe par défaut du cluster. Fournissez le nouveau mot de passe dans la zone de texte Mot de passe de l'administrateur du serveur Ambari .

Propriété	Description
Activer l'authentification Kerberos	Sélectionnez cette option pour activer l'authentification Kerberos du cluster.
Type de KDC	<p>Sélectionnez un des types de centre de distribution de clés Kerberos (KDC) suivants si vous aviez sélectionné l'option Activer l'authentification Kerberos :</p> <ul style="list-style-type: none"> - Active Directory. Sélectionnez cette option pour utiliser le KDC Active Directory. - KDC MIT. Sélectionnez cette option pour utiliser le KDC MIT. <p>Spécifiez les options suivantes après avoir sélectionné le type de KDC</p> <ul style="list-style-type: none"> - Hôte du KDC. Nom de la machine hôte du KDC. - Hôte du serveur administrateur. Le nom de la machine du serveur administrateur qui héberge le serveur KDC. - Domaine. Nom du domaine Kerberos sur la machine qui héberge le serveur KDC. - Administrateur principal. L'administrateur principal de Kerberos. - Mot de passe de l'administrateur. Le mot de passe de l'administrateur de Kerberos. - URL LDAP. Cette propriété s'applique à Microsoft Active Directory et représente l'URL de l'annuaire du serveur LDAP. - DN du conteneur. Cette propriété s'applique à Microsoft Active Directory et représente le nom unique du conteneur auquel l'utilisateur appartient. - Chemin d'accès au certificat du KDC. Si vous utilisez KDC avec Active Directory, indiquez le chemin d'accès au certificat KDC sur la machine exécutant le domaine Informatica.

8. Cliquez sur **Suivant**.

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

9. Configurez les options de sécurité du domaine du service de cluster Informatica.

Le tableau suivant décrit les propriétés :

Propriété	Description
Le domaine est activé pour SSL	Spécifiez si le domaine Informatica est activé pour SSL.
Emplacement du fichier truststore du domaine	Emplacement du fichier truststore du domaine.
Mot de passe du fichier truststore du domaine	Mot de passe du fichier truststore du domaine.
Activer le service	Sélectionnez cette option pour activer le service de cluster Informatica immédiatement après avoir créé le service.

10. Cliquez sur **Terminer**.

Remarque: Après avoir mis à jour les options de sécurité du service de cluster Informatica dans Informatica Administrator, redémarrez le service de cluster Informatica.

Avant d'activer celui-ci, vérifiez les prérequis suivants selon les options de sécurité que vous avez configurées pour le cluster :

- Cluster activé pour Kerberos :

- Vous devez configurer le nom d'hôte et l'adresse IP du centre de distribution de clés (KDC) sur toutes les machines exécutant les nœuds du cluster et le domaine dans le répertoire `/etc/hosts`

- Assurez-vous que le fichier `krb5.conf` se trouve sur toutes les machines exécutant les nœuds du cluster et le domaine dans le répertoire `/etc`.
- Cluster activé pour SSL :
 - Pour un cluster activé pour SSL, assurez-vous que le fichier `truststore` du domaine est configuré et copié vers un emplacement commun accessible à tous les nœuds du cluster.
 - Si le `keystore` et le mot de passe Solr sont différents de ceux du service de cluster Informatica, vous devez exporter le certificat public de Solr dans tous les nœuds du cluster et importer le certificat dans le `truststore YARN` et le `truststore` du domaine.

Préparation de l'environnement de cluster Hadoop intégré

Vous devez effectuer plusieurs contrôles de validation avant d'installer Enterprise Data Catalog sur un cluster Hadoop intégré.

Procédez comme suit avant d'installer Enterprise Data Catalog sur un environnement de cluster Hadoop intégré :

- Configurez le fichier `/etc/hosts` sur chaque machine afin d'obtenir les noms de domaines complets. Informatica recommande le format de nom d'hôte suivant en minuscules : `<machine ipaddress> <fully qualified name> <alias>`.
- Remarque:** Pour vérifier le nom d'hôte configuré, exécutez la commande `#hostname -f`.
- Configurez les connexions SSH (Secure Shell) sans mot de passe entre les composants suivants :
 - Du service de cluster Informatica à la passerelle Hadoop.
 - De la passerelle Hadoop aux nœuds Apache Hadoop.
- Assurez-vous que le fichier `/etc/hosts` sur la machine qui héberge le domaine Informatica inclut des entrées pour tous les hôtes Hadoop.

Gestion des nœuds de cluster intégré

Un cluster Hadoop possède un ensemble de machines configuré pour exécuter des applications et services Hadoop. Un cluster Hadoop typique comprend un nœud maître et plusieurs nœuds esclaves ou de travail. Le nœud maître exécute les démons maîtres `JobTracker` et `NameNode`. Un nœud esclave exécute les démons `DataNode` et `TaskTracker`. Dans les petits clusters, le nœud maître peut également exécuter les démons esclaves.

Cluster à haute disponibilité

Vous pouvez utiliser l'option haute disponibilité pour les composants `HDFS`, `HBase`, `Yarn` et `Solr` de l'environnement de cluster Hadoop intégré. Si vous configurez le service de cluster Informatica sur un cluster à plusieurs nœuds et à haute disponibilité, il vous faut un minimum de trois nœuds pour qu'Enterprise Data Catalog fonctionne correctement. Si vous avez déjà configuré le service de cluster Informatica sur un nœud unique, vous ne pouvez pas rendre le cluster à haute disponibilité en y ajoutant d'autres nœuds.

Si le cluster intégré ne contient que trois nœuds, Enterprise Data Catalog distribue tous les services maîtres et esclaves sur tous les trois nœuds. Si le cluster intégré contient plus de trois nœuds, Enterprise Data Catalog choisit automatiquement les trois nœuds supérieurs avec la configuration système la plus élevée en tant que nœuds maîtres. Les nœuds restants servent de nœuds esclaves. Lorsque vous ajoutez des nœuds au cluster intégré, les nœuds nouvellement ajoutés servent de nœuds esclaves. Les nœuds que vous ajoutez au cluster doivent répondre aux prérequis de la configuration minimale pour les nœuds esclaves.

Cluster sans haute disponibilité

Vous pouvez configurer le service de cluster Informatica sur un nœud unique qui n'est pas à haute disponibilité. Dans de tels cas, les nœuds maîtres et de travail sont conservés dans le même nœud. Vous ne pouvez pas afficher le service de cluster Informatica si vous ajoutez un nœud unique à un cluster à nœud unique existant ou si vous essayez de configurer le service de cluster Informatica avec deux nœuds.

Supprimer des nœuds

Vous pouvez supprimer des nœuds du cluster intégré à condition qu'ils répondent aux conditions suivantes :

- Vous ne pouvez pas supprimer un nœud maître.
- Vous ne pouvez pas supprimer un nœud si le nombre de nœuds de données en direct dans le cluster devient inférieur à trois lors de la suppression du nœud.

Prérequis du cluster existant

Avant d'installer Enterprise Data Catalog dans un cluster Hadoop existant, vous devez vérifier que l'environnement système répond aux prérequis nécessaires au déploiement d'Enterprise Data Catalog.

Prérequis du nœud hôte

Sur chaque machine hôte, vérifiez que les utilitaires de compression et de décompression sont disponibles.

Prérequis du nœud de cluster

Vérifiez les prérequis suivants sur tous les nœuds de cluster :

- La version d'OpenSSL sur les nœuds de cluster est openssl-1.0.1e-30.el6_6.5.x86_64 ou versions ultérieures ou v1.0.2k.
- Veillez à installer Java Development Kit (JDK) 1.8 sur tous les nœuds du cluster.
- Vérifiez que la limite maximale de processus est définie au minimum sur 32 000.

Prérequis d'Apache Ranger

Avant de déployer Enterprise Data Catalog sur les clusters où Apache Ranger est activé, assurez-vous que l'utilisateur du domaine Informatica dispose de l'autorisation requise pour soumettre des applications à la file d'attente YARN.

Limite de descripteurs de fichiers

Vérifiez que le nombre maximal de descripteurs de fichiers ouverts est de 10 000 ou plus. Utilisez la commande `ulimit` pour vérifier la valeur actuelle et la modifier si nécessaire.

Prérequis de SSL

Pour activer le protocole SSL du cluster, vérifiez les prérequis suivants :

- Lorsque vous créez le service de catalogue qui se connecte à un cluster existant activé pour SSL, veillez à configurer les propriétés suivantes :
 - Chemin d'accès au fichier keystore de Solr et au mot de passe correspondant.
 - Importez les certificats de cluster Hadoop dans le truststore du domaine Informatica.
- Si le cluster est activé pour SSL, veillez à activer SSL pour le domaine Informatica et le service de catalogue.
- Si vous créez un keystore Solr, veillez à exporter le certificat public Solr vers tous les nœuds de cluster.
- Veillez à importer les certificats publics du domaine Informatica vers tous les truststores YARN.
- Si vous souhaitez activer l'authentification SSL pour Enterprise Data Catalog déployé sur un domaine Informatica à plusieurs nœuds, assurez-vous de remplir les prérequis suivants :
 - Exportez le fichier Default.keystore de chaque nœud vers infa_truststore.jks sur tous les nœuds.
 - Assurez-vous que le fichier Default.keystore est unique pour chaque nœud hôte.
 - Copiez le fichier Default.keystore à un emplacement unique sur chaque nœud.

Prérequis de Kerberos

Pour activer Kerberos du cluster, vérifiez les prérequis suivants :

- Vérifiez d'avoir installé les packages prérequis suivants avant d'activer Kerberos :
 - krb5-workstation
 - krb5-libs
- Veillez à configurer les prérequis suivants :
 - Un fichier keytab qui contient tous les utilisateurs dans LDAP.
 - Nom du domaine Kerberos.
 - Namenode HDFS et principaux du service gestionnaire de ressource YARN.
- Veillez à fusionner le keytab http avec les fichiers keytab de l'utilisateur et de l'hôte.
- Pour collecter les fichiers journaux à un emplacement commun, créez le répertoire `service-logs` sous `/Informatica/LDM/<service cluster name>/` et attribuez la propriété du répertoire à l'utilisateur du cluster de service si le cluster est activé pour Kerberos.

Remarque: Si ce n'est pas le cas, créez le répertoire `service-logs` sous `/Informatica/LDM/<service cluster name>/` et attribuez la propriété du répertoire à l'utilisateur du domaine.
- Si le cluster n'est pas activé pour Kerberos. Créez le répertoire `<domain user name>` sous `/user` et attribuez la propriété du répertoire à l'utilisateur de domaine.

Remarque: Si le cluster est activé pour Kerberos, créez le répertoire `<service cluster name>` sous `/user` et attribuez la propriété du répertoire à l'utilisateur du cluster de service. Si le cluster n'est pas activé pour Kerberos, attribuez la propriété du répertoire à l'utilisateur du domaine.
- Pour activer l'authentification Kerberos d'Enterprise Data Catalog déployé sur un domaine Informatica à plusieurs nœuds, assurez-vous de remplir les prérequis suivants :
 - Assurez-vous que tous les nœuds de domaine incluent le fichier `krb5.conf` dans les répertoires suivants :
 - `$INFA_HOME/services/shared/security/`

- /etc
- Assurez-vous que le fichier /etc/hosts de chaque nœud de cluster et de domaine inclut l'entrée d'hôte krb et une entrée d'hôte pour d'autres nœuds.
- Installez `krb5-Workstation` dans tous les nœuds de domaine.
- Assurez-vous que le fichier `keytab` est présent dans un emplacement commun dans tous les nœuds de domaine.
- Assurez-vous que l'utilisateur du cluster de service est configuré sur tous les nœuds de cluster.

Prérequis du domaine Informatica

Veillez à ne pas créer le domaine Informatica sur un nœud du cluster Hadoop existant.

Autorisations de l'utilisateur

Configurez les autorisations suivantes pour les comptes d'utilisateurs si vous prévoyez de déployer Enterprise Data Catalog sur un cluster existant :

- Veillez à configurer les autorisations de lecture, d'écriture et d'exécution pour les propriétaires, les groupes et autres dans les répertoires HDFS.
- Si vous prévoyez de déployer Enterprise Data Catalog sur une distribution Cloudera Hadoop, veillez à attribuer l'un des rôles suivants dans Cloudera Manager pour le compte d'utilisateur Cloudera que vous utilisez pour démarrer le service de catalogue :
 - Opérateur
 - Configurateur
 - Administrateur de cluster
 - Administrateur de navigateur
 - Administrateur complet

Déploiement du cluster Hadoop existant

Vous pouvez déployer Enterprise Data Catalog sur un cluster Hadoop que vous avez configuré sur Cloudera, Hortonworks ou Azure HDInsight. Si vous avez activé l'authentification Kerberos dans votre entreprise pour authentifier les utilisateurs et services sur un réseau, vous pouvez configurer le domaine Informatica pour qu'il utilise l'authentification réseau Kerberos.

Vous devez configurer les spécifications Yarn, ZooKeeper et HDFS lorsque vous installez Enterprise Data Catalog sur un cluster Hadoop existant de votre entreprise. Le service de catalogue utilise les spécifications suivantes et lance les services et composants suivants sur le cluster Hadoop en tant qu'application Yarn :

- Solr version 5.2.1
- HBase version 0.98
- Composants de l'analyseur

Préparation de l'environnement de cluster Hadoop existant

Vous devez effectuer plusieurs contrôles de validation avant d'installer Enterprise Data Catalog sur un cluster Hadoop existant.

Procédez comme suit avant d'installer Enterprise Data Catalog pour utiliser un cluster existant.:

- Créez les répertoires suivants dans HDFS avant de créer le service de catalogue :

```
- /Informatica/LDM/<service cluster name>
- /user/<user name>
```

Où `<service cluster name>` est le nom du cluster de service à entrer lorsque vous créez le service de catalogue et `<user name>` est le nom d'utilisateur du domaine Informatica.

- Faites de `<user name>` qui est l'utilisateur du domaine Informatica, le propriétaire des répertoires `/Informatica/LDM/<service cluster name>` et `/user/<user name>`.

Configuration de Kerberos et de SSL pour un cluster existant

Vous pouvez installer Enterprise Data Catalog sur un cluster existant qui utilise l'authentification réseau Kerberos pour authentifier les utilisateurs et services sur un réseau. Enterprise Data Catalog prend également en charge l'authentification SSL pour une communication sécurisée dans le cluster.

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

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

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

Prérequis pour l'authentification SSL

Vérifiez que le cluster existant répond aux prérequis suivants avant d'activer l'authentification SSL dans le cluster :

- Le domaine Informatica est configuré en mode SSL.
- Les points de terminaison de cluster et de YARN REST sont activés pour Kerberos.
- Créez un fichier keystore pour l'application Apache Solr sur tous les nœuds du cluster. Importez les certificats publics des fichiers keystore Apache Solr sur tous les hôtes dans tous les fichiers truststore

configurés pour HDFS et YARN. Cette étape est nécessaire pour que les tâches d'Apache Spark et de l'analyseur se connectent à l'application Apache Solr.

- Importez les certificats publics des applications Apache Solr et YARN dans le fichier truststore du domaine Informatica. Cette étape est nécessaire pour que le service de catalogue se connecte aux applications YARN et Solr.
- Importez les certificats publics du domaine Informatica et le service de catalogue dans le truststore YARN.
- Importez le certificat public du service de catalogue dans le truststore du domaine Informatica.
- Si vous prévoyez de déployer Enterprise Data Catalog sur un cluster Hortonworks version 2.5 existant qui ne prend pas en charge l'authentification SSL, procédez comme suit :
 1. Configurez les propriétés suivantes dans le fichier `/etc/hadoop/conf/ssl-client.xml` :
`ssl.client.truststore.location` et `ssl.client.truststore.password`.
 2. Veillez à ce que la valeur `ssl.client.truststore.location` soit définie sur le répertoire `/opt` et pas sur le répertoire `/etc`. Veillez à configurer le chemin d'accès complet au fichier truststore pour la propriété `ssl.client.truststore.location`. Par exemple, vous pouvez définir la valeur semblable à `/opt/truststore/infa_truststore.jks`.
 3. Exportez le certificat keystore utilisé dans le domaine Informatica.
 4. Importez le certificat keystore dans le fichier truststore du domaine Informatica.
 5. Placez le fichier truststore de domaine dans tous les nœuds Hadoop du répertoire `/opt`. Par exemple, `/opt/truststore/infa_truststore.jks`.
 6. Ouvrez le fichier `/etc/hadoop/conf/ssl-client.xml`.
 7. Modifiez les propriétés `ssl.client.truststore.location` et `ssl.client.truststore.password`.

Prérequis de l'authentification Kerberos

Procédez comme suit avant d'activer l'authentification Kerberos pour le cluster existant :

- Créez les utilisateurs suivants dans le domaine de sécurité LDAP où `<user name>` est le nom du cluster de services.
 - `<user name>@KERBEROSDOMAIN.COM`
 - `<user name>/<hostname>@KERBEROSDOMAIN.COM`
Remarque: Créez l'ID d'utilisateur de tous les hôtes du cluster.
 - `HTTP/<host name>@KERBEROSDOMAIN.COM`
Remarque: Créez l'ID d'utilisateur de tous les hôtes du cluster.
 - Créez un fichier keytab avec des informations d'identification pour tous ces utilisateurs créés dans LDAP. Vous pouvez créer des fichiers keytab pour chacun des utilisateurs du serveur KDC et les fusionner à l'aide de la commande `ktutil` pour créer un fichier keytab unique.
 - Créez les dossiers suivants dans HDFS qu'Enterprise Data Catalog utilise comme répertoires de données pour le service de catalogue : `/Informatica/LDM/<user name>` et `/user/<user name>`.
 - Remplacez le propriétaire de ces deux dossiers par `<user name>`.
 - Créez un utilisateur local avec nom d'utilisateur `<user name>` sur tous les hôtes du cluster. Cette étape est nécessaire pour lancer l'application dans YARN en tant qu'utilisateur configuré pour le service de catalogue.

- Configurez le paramètre `udp_preference_limit` dans le fichier de configuration Kerberos `krb5.conf` sur 1. Ce paramètre détermine le protocole qu'utilise Kerberos lors de l'envoi d'un message au KDC. Définissez `udp_preference_limit = 1` pour toujours utiliser TCP. Le domaine Informatica prend uniquement en charge le protocole TCP. Si le paramètre `udp_preference_limit` est défini sur une autre valeur, il est possible que le domaine Informatica s'arrête inopinément.

Partie III : Installation d'Enterprise Data Catalog

- [Installation des services d'Enterprise Data Catalog, 68](#)

CHAPITRE 5

Installation des services d'Enterprise Data Catalog

Ce chapitre comprend les rubriques suivantes :

- [Présentation de l'installation des services d'Enterprise Data Catalog, 68](#)
- [Installation des services d'Enterprise Data Catalog en mode console, 70](#)
- [Installation d'Enterprise Data Catalog en mode silencieux, 107](#)
- [Installation des services d'application Enterprise Data Catalog en mode silencieux, 125](#)
- [Sécurisation des mots de passe dans le fichier de propriétés, 127](#)

Présentation de l'installation des services d'Enterprise Data Catalog

Vous pouvez installer les services d'Enterprise Data Catalog sur une machine Linux. Vous pouvez exécuter le programme d'installation en mode console ou silencieux.

Effectuez les tâches de pré-installation pour préparer l'installation. Vous pouvez installer les services d'Enterprise Data Catalog sur plusieurs machines. Le processus d'installation crée un service nommé Informatica qui s'exécute en tant que démon sur Linux. Le démarrage du service Informatica entraîne celui du gestionnaire de service, qui gère toutes les opérations du domaine.

Après l'installation, utilisez Informatica Administrator pour vous connecter au domaine et configurer les services d'applications.

Reprendre une installation incomplète

Si l'installation est incomplète à cause d'un échec, d'une interruption ou d'une sortie involontaire du programme d'installation, vous pouvez reprendre l'installation à l'endroit où elle s'est arrêtée. Vous devez vous assurer que le Domaine Informatica est en cours d'exécution avant de reprendre l'installation. Pour reprendre l'installation, exécutez la commande `./install.sh`.

Si l'installation s'arrête lorsque vous créez l'un des services d'application, le programme d'installation conserve les valeurs que vous avez fournies. Lorsque vous reprenez l'installation, le programme d'installation vous invite à confirmer les valeurs conservées puis poursuit sur la saisie de licence. Si vous avez créé et activé un service d'application, le programme d'installation passe à l'étape suivante.

Reprise de l'installation

Lorsque le processus d'installation s'arrête à mi-chemin, vous pouvez reprendre l'installation depuis l'instant où elle a échoué ou s'est terminée.

Avant de reprendre l'installation, effectuez les étapes requises suivantes :

- Dans le fichier journal d'installation présent dans le répertoire `<INFA_HOME>`, vérifiez que le domaine Informatica et un service d'application ont été créés. Le nom du fichier journal du programme d'installation possède le format suivant : `Informatica_<Version>_Services_<timestamp>.log`
- Assurez-vous de ne pas supprimer le fichier `installInst.obj` présent dans le répertoire `outils` situé dans le répertoire d'installation.
- Si vous utilisez le programme d'installation silencieux, assurez-vous que la propriété `RESUME_INSTALLATION` est définie sur `True` dans le fichier `SilentInput.properties`.

Effectuez les étapes suivantes pour reprendre l'installation :

1. Ouvrez une invite de commande et naviguez jusqu'à l'emplacement des fichiers d'installation.
2. Pour reprendre l'installation, exécutez la commande `./install.sh`. Si vous avez utilisé le mode silencieux pour l'installation, exécutez `silentInstall.sh` pour reprendre l'installation.
3. Lorsque le programme d'installation s'exécute, une invite peut apparaître pour vous demander de confirmer la reprise de l'installation précédente.
 - Si vous désirez reprendre l'installation, saisissez **2**.
 - Si vous ne désirez pas reprendre l'installation, saisissez **1**. La valeur par défaut est **1**.

Avant de reprendre l'installation, le programme d'installation valide les services d'application que vous avez configurés avant l'arrêt du programme d'installation.

Créer ou joindre un domaine

Créez un domaine s'il s'agit d'une première installation. Joignez un domaine si vous effectuez l'installation sur plusieurs machines et que vous avez créé un domaine sur une autre machine.

Le domaine Informatica est l'unité administrative fondamentale utilisée pour les services, les utilisateurs et les ressources. Un nœud est la représentation logique d'une seule machine. Un domaine contient un ou plusieurs nœuds.

Si vous effectuez l'installation sur plusieurs machines, vous pouvez créer plusieurs domaines. Si vous créez un domaine, le nœud sur la machine sur laquelle vous effectuez l'installation devient un nœud de passerelle dans le domaine. Vous pouvez sélectionner l'option Activer la communication sécurisée pour configurer une communication sécurisée entre les services au sein du domaine.

Lorsque vous installez les services d'Enterprise Data Catalog, vous créez un nœud sur la machine. Vous pouvez créer un domaine et ajouter le nœud au domaine. Si vous ne créez pas un domaine, vous pouvez associer le nœud à un autre domaine.

Si vous joignez un domaine, vous pouvez configurer le nœud que vous créez pour qu'il soit un nœud de passerelle. Lorsque vous créez un nœud de passerelle, vous pouvez sélectionner Activer une connexion HTTPS sécurisée dans Informatica Administrator.

Installation des services d'Enterprise Data Catalog en mode console

Vous pouvez installer les services d'Enterprise Data Catalog en mode console sous Linux.

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

Répertoire sécurisé pour la clé de chiffrement et les fichiers de configuration

Lorsque vous installez ou mettez à niveau Informatica, le programme d'installation crée des répertoires pour stocker les fichiers Informatica qui nécessitent un accès restreint, tels que le fichier de clé de chiffrement du domaine et le fichier `nodemeta.xml`. Sous Linux, le programme d'installation attribue des autorisations différentes d'accès aux répertoires et aux fichiers à l'intérieur.

Par défaut, le programme d'installation crée les répertoires suivants dans le répertoire d'installation d'Informatica :

<Informatica installation directory>/isp/config

Contient le fichier `nodemeta.xml`. Contient également le répertoire `/keys` dans lequel est stocké le fichier de clé de chiffrement. Vous pouvez spécifier un répertoire différent dans lequel stocker les fichiers. Le programme d'installation attribue les mêmes autorisations au répertoire spécifié qu'au répertoire par défaut.

<Informatica installation directory>/services/shared/security

Ce répertoire n'est pas utilisé par Enterprise Data Catalog.

Le programme d'installation attribue les autorisations suivantes aux répertoires et aux fichiers dans les répertoires :

Autorisations des répertoires

Le propriétaire du répertoire dispose des autorisations `-wx` pour le répertoire mais d'aucune autorisation `r`. Le propriétaire du répertoire est le compte d'utilisateur utilisé pour exécuter le programme d'installation. Le groupe auquel le propriétaire appartient dispose également des autorisations `-wx` pour le répertoire mais d'aucune autorisation `r`.

Par exemple, le compte d'utilisateur `ediqa` possède le répertoire et appartient au groupe `infaadmin`. Le compte d'utilisateur `ediqa` et le groupe `infaadmin` disposent des autorisations suivantes : `-wx-wx---`

Le compte d'utilisateur `ediqa` et le groupe `infaadmin` peuvent écrire dans le répertoire et exécuter des fichiers dans celui-ci. Ils ne peuvent pas afficher la liste de fichiers du répertoire mais peuvent lister un fichier spécifique par nom.

Si vous connaissez le nom d'un fichier dans le répertoire, vous pouvez copier le fichier depuis le répertoire vers un autre emplacement. Si vous ne connaissez pas le nom du fichier, vous devez modifier l'autorisation pour le répertoire afin d'inclure l'autorisation d'accès en lecture avant de pouvoir copier le fichier. Vous pouvez utiliser la commande `chmod 730` pour accorder l'autorisation d'accès en lecture au propriétaire du répertoire et des sous-répertoires.

Par exemple, vous devez copier le fichier de clé de chiffrement nommé `siteKey` vers un répertoire temporaire afin de le rendre accessible à un autre nœud dans le domaine. Exécutez la commande `chmod 730` sur le répertoire `<Informatica installation directory>/isp/config` pour attribuer les autorisations suivantes : `rw-x-wx---`. Vous pouvez ensuite copier le fichier de clé de chiffrement du sous-répertoire `/keys` vers un autre répertoire.

Après avoir terminé la copie des fichiers, rétablissez les autorisations de lecture et d'exécution pour le répertoire. Vous pouvez utiliser la commande `chmod 330` pour supprimer l'autorisation d'accès en lecture.

Remarque: N'utilisez pas l'option `-R` pour modifier de façon récursive les autorisations pour le répertoire et fichiers. Le répertoire et les fichiers dans le répertoire ont des autorisations différentes.

Autorisations d'accès aux fichiers

Le propriétaire des fichiers du répertoire dispose des autorisations `rwx` pour les fichiers. Le propriétaire des fichiers du répertoire est le compte d'utilisateur utilisé pour exécuter le programme d'installation. Le groupe auquel appartient le propriétaire dispose également d'une autorisation `rwx` pour les fichiers du répertoire.

Le propriétaire et le groupe ont un accès complet au fichier et peuvent afficher ou modifier le fichier dans le répertoire.

Remarque: Vous devez connaître le nom du fichier pour pouvoir afficher ou modifier le fichier.

Installation en créant un domaine

Créez un domaine si vous installez pour la première fois ou si vous voulez administrer des nœuds dans des domaines séparés.

1. Connectez-vous à la machine à l'aide d'un compte utilisateur système.
2. Fermez toutes les autres applications.
3. Exécutez la commande `./install.sh` pour démarrer le programme d'installation.

Le programme d'installation affiche un message vous invitant à lire la documentation d'Informatica avant de procéder à l'installation.

4. Appuyez sur **0** pour continuer l'installation.
5. Appuyez sur **1** pour installer les produits de la suite Informatica Big Data.
6. Appuyez sur **1** pour exécuter l'outil Pre-installation System Check. L'outil vérifie si votre machine répond à la configuration système minimale requise pour installer ou mettre à niveau Informatica.

Remarque: Vous pouvez ignorer cette étape si vous êtes sûr que votre machine répond à la configuration système minimale requise pour installer ou mettre à niveau Informatica.

7. Appuyez sur **3** pour installer Informatica.
8. Appuyez sur **2** pour accepter les conditions générales de l'installation ou de la mise à niveau.
9. Appuyez sur **2** pour confirmer que vous comprenez que la version 10.2.2 est spécifique à la suite de produits Big Data et poursuivre l'installation.
10. Appuyez sur **2** pour installer les services d'application Informatica avec Enterprise Data Catalog.
Le programme d'installation vous invite à confirmer que la version actuelle des services d'application Informatica n'est pas installée sur le nœud.
11. Appuyez sur **1** si la version actuelle des services d'application Informatica n'est pas installée sur votre ordinateur. Sinon, appuyez sur **2**.
12. Choisissez le type de cluster Hadoop pour Enterprise Data Catalog. Appuyez sur **2** pour déployer Enterprise Data Catalog sur une distribution Hadoop intégrée. Appuyez sur **1** pour déployer Enterprise Data Catalog sur une distribution Hadoop existante.

- Si vous avez choisi la distribution Hadoop intégrée, indiquez les informations suivantes après la configuration du domaine Informatica, du service de référentiel modèle et du service d'intégration de données :

Option	Description
Nom d'utilisateur SSH	Nom d'utilisateur de la connexion Secure Shell (SSH) sans mot de passe
Nom du service de cluster Informatica	Nom du service de cluster Informatica pour le cluster intégré.
Port du service de cluster Informatica	Numéro de port du service de cluster Informatica.
Hôte du serveur Ambari	Informations d'hôte du serveur Ambari. Ambari est un outil Web destiné à l'approvisionnement, à la gestion et à la surveillance des grappes Hadoop Apache. Il prend en charge Hadoop HDFS, Hadoop MapReduce, Hive, HBase et ZooKeeper.
Hôtes de l'agent Ambari séparés par des virgules	S'applique à la haute disponibilité. Si vous utilisez plusieurs hôtes d'agents Ambari, spécifiez leurs noms séparés par des virgules.
Port Web Ambari	Numéro de port sur lequel le serveur Ambari doit s'exécuter.
Nom du service de catalogue	Nom du service de catalogue.
Port du service de catalogue	Numéro de port du service de catalogue.
Emplacement du fichier keytab	S'applique à un cluster activé pour Kerberos. Emplacement du fichier keytab fusionné de l'utilisateur et de l'hôte.
Fichier de configuration Kerberos	S'applique à un cluster activé pour Kerberos. Emplacement du fichier de configuration Kerberos.

- Spécifiez les détails suivants si vous sélectionnez un cluster existant :

Propriété	Description
Distribution Hadoop	Sélectionnez l'une des options suivantes : <ul style="list-style-type: none"> - ClouderaManager - HDInsight - Hortonworks
URL du cluster	Nom d'hôte complet pour accéder au cluster.
Nom d'utilisateur de l'URL du cluster	Nom d'utilisateur pour accéder au cluster.
Mot de passe de l'URL du cluster	Mot de passe du nom d'utilisateur de l'URL du cluster.

- Si vous avez choisi la distribution Hadoop existante ClouderaManager ou Hortonworks, indiquez les informations suivantes :

Option	Description
Nom du service de catalogue	Nom du service de catalogue.
Port du service de catalogue	Numéro de port du service de catalogue.
URI du gestionnaire de ressources Yarn	Service au sein d'Hadoop qui envoie les tâches MapReduce aux nœuds spécifiques dans la grappe. Utiliser le format suivant : <hostname>:<port> Où <ul style="list-style-type: none"> • <code>hostname</code> est le nom ou l'adresse IP du gestionnaire de ressources Yarn. • <code>port</code> est le port sur lequel le gestionnaire de ressources Yarn écoute les appels de procédure distante (RPC).
URI http du gestionnaire de ressources Yarn	Valeur de l'URI http du gestionnaire de ressources Yarn.
URI du planificateur du gestionnaire de ressources Yarn	Valeur de l'URI du planificateur du gestionnaire de ressources Yarn.
URI du cluster Zookeeper	URI du service Zookeeper, un service de coordination hautes performances pour les applications distribuées.
URI du namenode HDFS	L'URI pour accéder à HDFS. Utilisez le format suivant pour spécifier l'URI du NameNode dans la distribution Cloudera : hdfs://<namenode>:<port> Où <ul style="list-style-type: none"> • <code><namenode></code> est le nom d'hôte ou l'adresse IP du NameNode. • <code><port></code> est le port sur lequel le NameNode écoute les appels de procédure distante (RPC).
Nom du cluster de service	Nom du cluster de service. Assurez-vous d'avoir un répertoire <code>/Informatica/LDM/<ServiceClusterName></code> dans HDFS avant que l'installation soit complète. Remarque: Si vous ne spécifiez pas un nom de cluster de service, Enterprise Data Catalog considère <code>DomainName_CatalogServiceName</code> comme la valeur par défaut. Le répertoire <code>/Informatica/LDM/<DomainName>_<CatalogServiceName></code> doit alors se trouver dans HDFS. Sinon, le service de catalogue pourrait échouer.
URI HTTP du serveur d'historique	URI HTTP pour accéder au serveur d'historique.

Option	Description
Le cluster est-il sécurisé ?	Définissez cette propriété sur l'une des valeurs suivantes si vous disposez d'un cluster existant sécurisé : <ul style="list-style-type: none"> • 1 : spécifie que le cluster existant n'est pas sécurisé. • 2 : spécifie que le cluster existant est sécurisé. La valeur par défaut est 1.
L'authentification SSL est-elle activée sur le cluster ?	Uniquement applicable si vous aviez sélectionné la distribution Hadoop Hortonworks et ClouderaManager. Définissez cette propriété sur l'une des valeurs suivantes si vous disposez d'un cluster existant activé pour SSL : <ul style="list-style-type: none"> • 1 : spécifie que le cluster existant n'est pas activé pour SSL. • 2 : spécifie que le cluster existant est activé pour SSL. La valeur par défaut est 1.
Activer l'authentification Kerberos	Uniquement applicable si vous aviez sélectionné la distribution Hadoop Hortonworks et ClouderaManager. Définissez cette propriété sur l'une des valeurs suivantes si vous disposez d'un cluster existant activé pour Kerberos : <ul style="list-style-type: none"> • 1 : spécifie que le cluster existant n'est pas activé pour Kerberos. • 2 : spécifie que le cluster existant est activé pour Kerberos.

Selon les paramètres que vous spécifiez, Enterprise Data Catalog crée un service de cluster Informatica pour la distribution Hadoop intégrée.

- Appuyez sur **Entrée** pour continuer.
- Appuyez sur **2** pour que le programme d'installation règle les services d'application Informatica en fonction de la taille des données à déployer.

Le programme d'installation affiche les options suivantes pour différentes tailles de données :

- Sandbox
- De base
- Standard
- Concurrence élevée et volume élevé

- Tapez le chemin d'accès et le nom de fichier de la clé de licence Informatica, puis appuyez sur **Entrée**.
- Tapez le chemin d'accès absolu du répertoire d'installation.

Les noms de répertoires du chemin d'accès ne doivent pas contenir d'espaces ni les caractères spéciaux suivants : @|* \$ # ! % () { } [] , ; ' Par défaut /home/toolinst.

Remarque: Informatica recommande d'utiliser des caractères alphanumériques dans le chemin d'accès au répertoire d'installation. Si vous utilisez un caractère spécial comme á ou €, des résultats inattendus peuvent se produire lors de l'exécution.

- Appuyez sur **2** pour exécuter l'utilitaire de pré-validation. L'utilitaire vous aide à valider les prérequis pour installer Enterprise Data Catalog dans un cluster intégré. L'utilitaire valide également la configuration du domaine Informatica, des hôtes de cluster et des services de cluster Hadoop.

Le programme d'installation vous invite à confirmer si vous souhaitez activer l'authentification Kerberos pour le cluster.

18. Appuyez sur **2** pour activer l'authentification Kerberos du cluster, et indiquez les détails suivants :
 - a. **Emplacement du fichier keytab.** Emplacement du fichier keytab fusionné de l'utilisateur et de l'hôte.
 - b. **Fichier de configuration Kerberos.** Emplacement du fichier de configuration Kerberos.
19. Tapez le nom d'utilisateur de la passerelle, et appuyez sur **Entrée**. La valeur par défaut est **racine**.
20. Tapez le nom d'hôte de passerelle du cluster Hadoop d'Informatica au format suivant : `<hostname>.<FQDN>` et appuyez sur la touche **Entrée**.
21. Tapez la liste des nœuds du cluster Hadoop d'Informatica séparés par des virgules, comme indiqué au format suivant : `<hostname>.<FQDN>, <hostname1>.<FQDN>, <hostname2>.<FQDN>` et appuyez sur la touche **Entrée**.
22. Tapez le port de passerelle du cluster Hadoop d'Informatica, et appuyez sur **Entrée**. La valeur par défaut est **8080**.
 Pour éviter un conflit de ports, veillez à ne pas configurer Oracle avec le port 8080 sur la même machine où le service de cluster Informatica s'exécute.
23. Tapez le chemin d'accès au répertoire de travail, et appuyez sur **Entrée**. Le chemin d'accès indique l'emplacement où vous souhaitez monter le service de cluster Informatica.
 Le programme d'installation démarre l'utilitaire de pré-validation.
24. Appuyez sur **Entrée** pour continuer après avoir exécuté l'utilitaire de pré-validation.
25. Examinez les informations d'installation, et appuyez sur **Entrée** pour continuer.
 Le programme d'installation copie les fichiers d'Enterprise Data Catalog dans le répertoire d'installation. Vous voyez une invite pour créer ou joindre un domaine.
26. Appuyez sur **1** pour créer un domaine.
 Lorsque vous créez un domaine, le nœud que vous créez devient un nœud de passerelle dans le domaine. Le nœud de passerelle contient un gestionnaire de service qui gère toutes les opérations du domaine.
27. Pour activer la communication sécurisée pour les services du domaine, appuyez sur **2**. Pour désactiver la communication sécurisée pour le domaine, appuyez sur **1**.
 Par défaut, si vous activez la communication sécurisée pour le domaine, le programme d'installation configure une connexion HTTPS pour Informatica Administrator. Vous pouvez également créer un référentiel de configuration du domaine sur une base de données sécurisée.
28. Tapez les détails de connexion pour Informatica Administrator.
 - a. Si vous n'activez pas la communication sécurisée pour le domaine, vous pouvez indiquer si vous souhaitez configurer une connexion HTTPS sécurisée pour Informatica Administrator.
 Le tableau suivant décrit les options disponibles permettant d'activer ou de désactiver une connexion sécurisée à Informatica Administrator :

Option	Description
1 - Activer HTTPS pour Informatica Administrator	Configurer une connexion sécurisée à Informatica Administrator.
2 - Désactiver HTTPS	Ne pas configurer une connexion sécurisée à Informatica Administrator.

- b. Si vous activez la communication sécurisée pour le domaine ou si vous activez une connexion HTTPS pour Informatica Administrator, entrez le fichier entrepôt de clés et le numéro de port pour la connexion HTTPS à Informatica Administrator.

Le tableau suivant décrit les informations de connexion que vous devez entrer si vous activez HTTPS :

Option	Description
Port	Numéro de port de la connexion HTTPS.
Fichier keystore	Indiquez si vous souhaitez utiliser un fichier keystore généré par le programme d'installation ou un fichier keystore que vous créez. Vous pouvez utiliser un fichier keystore avec un certificat auto-signé ou un certificat signé par une autorité de certification. 1 - Utiliser un keystore généré par le programme d'installation 2 - Spécifier un fichier et un mot de passe keystore Si vous choisissez d'utiliser un fichier keystore généré par le programme d'installation, ce dernier crée un fichier keystore auto-signé nommé Default.keystore à l'emplacement suivant : <Répertoire d'installation Informatica>/tomcat/conf/

- c. Si vous spécifiez le keystore, entrez le mot de passe et l'emplacement du fichier keystore.
29. Appuyez sur **2** pour activer l'authentification unique utilisant l'authentification SAML pour les applications d'Enterprise Data Catalog.
 30. Tapez l'URL du fournisseur d'identité (IdP) SAML, et appuyez sur **Entrée**.
 Consultez la section *Configurer l'authentification unique avec l'authentification SAML* pour en savoir plus sur la configuration à effectuer après avoir installé Enterprise Data Catalog.
 Si vous avez activé la communication sécurisée pour le domaine, la section **Sécurité du domaine - Communication sécurisée** s'affiche. Si vous n'avez pas activé la communication sécurisée pour le domaine, la page **Référentiel de configuration du domaine** s'affiche.
 31. Sur la page Sécurité du domaine - Communication sécurisée, indiquez si vous souhaitez utiliser les certificats SSL Informatica par défaut ou des certificats SSL que vous fournissez pour sécuriser la communication du domaine.
 - a. Sélectionnez le type de certificat SSL à utiliser.

Le tableau suivant décrit les options des certificats SSL que vous pouvez utiliser pour sécuriser le domaine Informatica :

Option	Description
1 - Utiliser les fichiers de certificat SSL Informatica par défaut	Permet d'utiliser les certificats SSL par défaut fournis par Informatica. Remarque: Si vous ne fournissez pas de certificat SSL, Informatica utilise la même clé privée par défaut pour toutes les installations d'Informatica. Si vous utilisez les fichiers entrepôt de clés et truststore Informatica par défaut, la sécurité de votre domaine peut être compromise. Pour assurer un niveau élevé de sécurité pour le domaine, sélectionnez l'option permettant de spécifier l'emplacement des fichiers de certificat SSL.
2 - Spécifier l'emplacement des fichiers de certificat SSL	Permet d'utiliser les certificats SSL que vous fournissez. Vous devez spécifier l'emplacement des fichiers keystore et truststore. Vous pouvez fournir un certificat auto-signé ou un certificat émis par une autorité de certification (CA). Vous devez fournir les certificats SSL dans le format PEM et dans des fichiers keystore Java (JKS, Java Keystore). Informatica requiert des noms de fichier de certificat SSL spécifiques pour le domaine Informatica. Vous devez utiliser les mêmes certificats SSL pour tous les nœuds du domaine. Stockez les fichiers truststore et keystore dans un répertoire accessible à tous les nœuds du domaine et spécifiez le même répertoire de fichiers keystore et truststore pour tous les nœuds d'un même domaine.

- b. Si vous indiquez le certificat SSL, spécifiez l'emplacement et les mots de passe des fichiers keystore et truststore.

Le tableau suivant décrit les paramètres que vous devez entrer pour les fichiers de certificat SSL :

Propriété	Description
Répertoire de fichiers keystore	Répertoire contenant les fichiers keystore. Il doit contenir les fichiers infa_keystore.jks et infa_keystore.pem.
Mot de passe keystore	Mot de passe du fichier keystore infa_keystore.jks.
Répertoire de fichiers truststore	Répertoire contenant les fichiers truststore. Il doit contenir les fichiers infa_truststore.jks et infa_truststore.pem.
Mot de passe truststore	Mot de passe du fichier infa_truststore.jks.

La page Référentiel de configuration du domaine s'affiche.

32. Sélectionnez la base de données à utiliser pour le référentiel de configuration du domaine.

Le tableau suivant répertorie les bases de données que vous pouvez utiliser pour le référentiel de configuration de domaine :

Invite	Description
Type de base de données	Type de base de données pour le référentiel de configuration du domaine. Sélectionnez parmi les options suivantes : 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - Sybase ASE

Le référentiel de configuration du domaine Informatica stocke les métadonnées des opérations du domaine et l'authentification de l'utilisateur. Le référentiel de configuration du domaine doit être accessible à tous les nœuds de passerelle du domaine.

33. Entrez les propriétés de la base de données et du compte d'utilisateur.

Le tableau suivant répertorie les propriétés pour le compte utilisateur de la base de données :

Propriété	Description
ID d'utilisateur de la base de données	Nom du compte de l'utilisateur de la base de données de configuration du domaine.
Mot de passe utilisateur	Mot de passe du compte de l'utilisateur de la base de données de configuration du domaine.

34. Choisissez si vous souhaitez créer un référentiel de configuration du domaine sécurisé.

Vous pouvez créer un référentiel de configuration du domaine dans une base de données sécurisée avec le protocole SSL. Pour créer un référentiel de configuration de domaine dans une base de données sécurisée, appuyez sur 1.

Pour créer un référentiel de configuration du domaine dans une base de données non sécurisée, appuyez sur 2.

35. Si vous ne voulez pas créer un référentiel de configuration du domaine, entrez les paramètres de la base de données.
- a. Si vous sélectionnez IBM DB2, indiquez si vous souhaitez configurer un espace de table et entrez le nom de ce dernier.

Le tableau suivant décrit les propriétés que vous devez configurer pour la base de données IBM DB2 :

Propriété	Description
Configurer l'espace de table	Indiquez si vous souhaitez spécifier un espace de table : 1 - Non 2 - Oui Dans une base de données à partition unique, le programme d'installation crée les tables dans l'espace de table par défaut si vous sélectionnez Non. Dans une base de données à plusieurs partitions, vous devez sélectionner Oui.
Espace de table	Nom de l'espace de table dans lequel les tables sont créées. Spécifiez un espace de table qui correspond aux spécifications de pageSize de 32 768 octets. Dans une base de données à partition unique, si vous sélectionnez Oui pour configurer l'espace de table, entrez le nom de l'espace de table dans lequel créer les tables. Dans une base de données à plusieurs partitions, indiquez le nom de l'espace de table qui se trouve dans la partition de catalogue de la base de données.

- b. Si vous sélectionnez Microsoft SQL Server, entrez le nom de schéma de la base de données.

Le tableau suivant décrit les propriétés que vous devez configurer pour la base de données Microsoft SQL Server :

Propriété	Description
Nom du schéma	Nom du schéma qui contiendra les tables de configuration du domaine. Si ce paramètre est vide, le programme d'installation crée les tables dans le schéma par défaut.

- c. Pour entrer les informations de connexion JDBC à l'aide des informations d'URL JDBC, appuyez sur **1**. Pour entrer les informations de connexion JDBC à l'aide d'une chaîne de connexion JDBC personnalisée, appuyez sur **2**.

- d. Entrez les informations de connexion JDBC.

- Pour entrer les informations de connexion à l'aide des informations d'URL JDBC, spécifiez les propriétés de l'URL JDBC.

Le tableau suivant décrit les informations de connexion à la base de données :

Invite	Description
Nom d'hôte de la base de données	Nom d'hôte de la base de données.
Numéro de port de la base de données	Numéro de port de la base de données.

Invite	Description
Nom du service de la base de données	Mot de passe du compte de l'utilisateur de la base de données de configuration du domaine. Nom du service pour les bases de données Oracle et IBM DB2 ou nom de la base de données pour Microsoft Microsoft SQL Server et Sybase ASE.
Configurer les paramètres JDBC	Indiquez si vous souhaitez ajouter des paramètres JDBC supplémentaires à la chaîne de connexion : 1 - Oui 2 - Non Si vous sélectionnez Oui, entrez les paramètres ou appuyez sur Entrée pour accepter la valeur par défaut. Si vous sélectionnez Non, le programme d'installation crée la chaîne de connexion JDBC sans paramètre.

- Pour entrer les informations de connexion à l'aide d'une chaîne de connexion JDBC personnalisée, tapez la chaîne de connexion.

Utilisez la syntaxe suivante pour la chaîne de connexion JDBC des bases de données :

IBM DB2

```
jdbc:Informatica:db2://host_name:port_no;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://host_name:port_no;ServiceName=
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
host_name:port_no;SelectMethod=cursor;DatabaseName=
```

Sybase

```
jdbc:Informatica:sybase://host_name:port_no;DatabaseName=
```

Vérifiez que la chaîne de connexion contient tous les paramètres de connexion requis par votre système de base de données.

36. Si vous créez un référentiel de configuration du domaine, entrez les paramètres de la base de données sécurisée.

Si vous créez le référentiel de configuration du domaine sur une base de données sécurisée, vous devez fournir les informations de truststore pour la base de données. Vous devez aussi fournir une chaîne de connexion JDBC qui comprend les paramètres de sécurité de la base de données.

Le tableau suivant décrit les options disponibles pour créer une base de données de référentiel de configuration du domaine sécurisée :

Propriété	Description
Fichier truststore de base de données	Chemin d'accès et nom du fichier truststore de la base de données sécurisée.
Mot de passe truststore de la base de données	Mot de passe du fichier truststore.
Chaîne de connexion JDBC personnalisée	Fournissez les informations pour la connexion JDBC à la base de données sécurisée, en indiquant notamment le nom d'hôte, le numéro de port et les paramètres de la base de données sécurisée.

Outre le nom d'hôte et le numéro de port du serveur de base de données, vous devez inclure les paramètres de base de données sécurisée suivants :

EncryptionMethod

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

ValidateServerCertificate

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

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

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

La valeur par défaut est *True*.

HostNameInCertificate

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

cryptoProtocolVersion

Requis. Indique le protocole cryptographique à utiliser pour la connexion à une base de données sécurisée. Vous pouvez définir le paramètre sur *cryptoProtocolVersion=TLsv1.1* ou *cryptoProtocolVersion=TLsv1.2* en fonction du protocole cryptographique utilisé par le serveur de base de données.

Vous pouvez utiliser la syntaxe suivante pour les chaînes de connexion :

- **Oracle** : `jdbc:Informatica:oracle://
host_name:port_no;ServiceName=service_name;EncryptionMethod=SSL;HostNameInCertificate=
DB_host_name;ValidateServerCertificate=true_or_false`
- **IBM DB2** : `jdbc:Informatica:db2://
host_name:port_no;DatabaseName=database_name;EncryptionMethod=SSL;HostNameInCertificat
e=DB_host_name;ValidateServerCertificate=true_or_false`
- **Microsoft SQL Server** : `jdbc:Informatica:sqlserver://
host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;EncryptionMethod=SSL;
HostNameInCertificate=DB_host_name;ValidateServerCertificate=true_or_false`

Remarque: Le programme d'installation ne valide pas la chaîne de connexion. Vérifiez que la chaîne de connexion contient tous les paramètres de connexion et de sécurité requis par votre base de données.

37. Si la base de données contient un référentiel de configuration d'un précédent domaine, choisissez de remplacer les données ou de configurer une autre base de données.

Le tableau suivant décrit les options de remplacement des données ou de configuration d'une autre base de données lorsque vous créez un référentiel de configuration pour un domaine précédent :

Option	Description
1 - OK	Entrez les informations de connexion pour une nouvelle base de données.
2 - Continuer	Le programme d'installation remplace les données dans la base de données par une nouvelle configuration du domaine.

38. Dans la section **Sécurité du domaine - Clé de chiffrement**, entrez le mot clé et le répertoire de la clé de chiffrement du domaine Informatica.

Le tableau suivant décrit les paramètres de clé de cryptage que vous devez spécifier :

Propriété	Description
Mot clé	Mot clé à utiliser pour créer une clé de cryptage personnalisée afin de sécuriser les données sensibles du domaine. Le mot clé doit respecter les critères suivants : <ul style="list-style-type: none">- Il comporte entre 8 et 20 caractères.- Il doit inclure au moins une lettre en majuscule.- Il doit inclure au moins une lettre en minuscule.- Il doit inclure au moins un chiffre.- Il ne doit pas contenir d'espaces. La clé de cryptage est créée en fonction du mot clé que vous indiquez lorsque vous créez le domaine Informatica.
Répertoire de la clé de cryptage	Répertoire dans lequel stocker la clé de cryptage pour le domaine. L'emplacement par défaut est le répertoire suivant : <Répertoire d'installation Informatica >/isp/config/keys.

Le programme d'installation définit des autorisations différentes pour le répertoire et les fichiers dans le répertoire.

39. Appuyez sur **Entrée**.
La page **Configuration de domaine et de nœud** s'affiche.
40. Entrez les informations relatives au domaine et au nœud à créer.

Le tableau suivant décrit les propriétés que vous définissez pour le domaine et le nœud de passerelle :

Propriété	Description
Nom de domaine	Nommer le domaine à créer. Le nom de domaine par défaut est Domain_<MachineName>. Le nom ne doit pas dépasser 128 caractères et doit être en ASCII 7 bits uniquement. Il ne peut pas contenir d'espaces ni les caractères spéciaux suivants : ` % * + ; " ? , < > \ /
Nom d'hôte du nœud	Nom d'hôte de la machine sur laquelle le nœud est créé. Le nom d'hôte du nœud ne peut pas contenir le caractère de soulignement (_). Si la machine a un nom de réseau unique, utilisez le nom d'hôte par défaut. Si la machine dispose de plusieurs noms de réseau, vous pouvez modifier le nom d'hôte par défaut pour utiliser un autre nom de réseau. Vous pouvez éventuellement utiliser l'adresse IP. Remarque: N'utilisez pas localhost. Le nom d'hôte doit explicitement identifier la machine.
Nom du nœud	Nom du nœud à créer sur cette machine. Le nom du nœud n'est pas le nom d'hôte de la machine.
Numéro de port du nœud	Numéro de port du nœud. Le numéro de port par défaut pour le nœud est 6005. Si le numéro de port n'est pas disponible sur la machine, le programme d'installation affiche le numéro de port suivant disponible.
Nom d'utilisateur de domaine	Nom d'utilisateur de l'administrateur du domaine. Vous pouvez utiliser ce nom d'utilisateur pour vous connecter la première fois à Informatica Administrator. Utilisez les directives suivantes : <ul style="list-style-type: none"> - Le nom n'est pas sensible à la casse et ne doit pas dépasser 128 caractères. - Le nom ne doit pas contenir de tabulation, de caractère fin de ligne ou les caractères spéciaux suivants : % * + / ? ; < > - Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Tous les autres caractères d'espacement sont interdits.
Mot de passe du domaine	Mot de passe de l'administrateur du domaine. Le mot de passe doit contenir plus de 2 caractères et ne doit pas dépasser 16 caractères.
Confirmer le mot de passe	Entrez une nouvelle fois le mot de passe pour le confirmer.

41. Indiquez si vous souhaitez afficher les ports par défaut pour les composants de domaine et de nœud attribués par le programme d'installation.

Le tableau suivant décrit la page de configuration avancée des ports :

Invite	Description
Afficher la page de configuration avancée des ports	Indiquez si vous souhaitez afficher les numéros de port pour les composants de domaine et de nœud attribués par le programme d'installation : 1 - Non 2 - Oui Si vous sélectionnez Oui, le programme d'installation affiche les numéros de port par défaut attribués aux composants du domaine. Vous pouvez indiquer les numéros de port à utiliser pour les composants de domaine et de nœud. Vous pouvez également indiquer une plage de numéros de port à utiliser pour le processus de service qui s'exécute sur le nœud. Vous pouvez utiliser les numéros de port par défaut ou spécifier de nouveaux numéros de port. Vérifiez que les numéros de ports que vous entrez ne sont pas utilisés par d'autres applications.

42. Si vous affichez la page de configuration des ports, entrez les nouveaux numéros de port à l'invite ou appuyez sur **Entrée** pour utiliser les numéros de port par défaut.

Port	Description
Port de gestionnaire de service	Numéro de port utilisé par le Gestionnaire de service sur le nœud. Le gestionnaire de service écoute les demandes de connexions entrantes sur ce port. Les applications clientes utilisent ce port pour communiquer avec les services du domaine. Les programmes de ligne de commande Informatica utilisent ce port pour communiquer avec le domaine. Ce port est également utilisé par le pilote JDBC/ODBC du service de données SQL. La valeur par défaut est 6006.
Port d'arrêt du gestionnaire de service	Numéro de port qui contrôle l'arrêt du serveur pour le Gestionnaire de service du domaine. Le gestionnaire de service écoute les commandes d'arrêt sur ce port. La valeur par défaut est 6007.
Port d'Informatica Administrator	Numéro de port utilisé par Informatica Administrator. La valeur par défaut est 6008.
Port HTTPS d'Informatica Administrator	Aucun port par défaut. Entrez le numéro de port requis lorsque vous créez le service. Configurer le port sur 0 désactive la connexion HTTPS à l'outil Administrator tool.
Port d'arrêt d'Informatica Administrator	Numéro de port qui contrôle l'arrêt du serveur pour Informatica Administrator. Informatica Administrator écoute les demandes d'arrêt sur ce port. La valeur par défaut est 6009.
Numéro de port minimal	Plus petit numéro de port de la plage des numéros de port pouvant être attribués aux processus de service d'application exécutés sur ce nœud. Le numéro par défaut est 6014.
Numéro de port maximal	Plus grand numéro de port de la plage des numéros de port pouvant être attribués aux processus de service d'application exécutés sur ce nœud. Le numéro par défaut est 6114.

43. Indiquez si vous souhaitez créer un service de référentiel modèle, un service d'intégration de données et un service de catalogue dans le cadre de l'installation. Vous pouvez créer ces services après l'installation dans Informatica Administrator. Appuyez sur **1** pour créer les services, ou appuyez sur **2** pour effectuer l'installation sans créer les services.
- Si vous avez appuyé sur 1, la section **Base de données du service de référentiel modèle** s'affiche.
44. Si vous avez appuyé sur 1, choisissez le type de base de données, et saisissez les paramètres de base de données du référentiel modèle.
45. Indiquez si vous souhaitez configurer une base de données sécurisée. Appuyez sur **1** pour configurer une base de données sécurisée, ou sur **2** pour ignorer l'étape.
46. Pour configurer les informations de connexion JDBC, appuyez sur **1** et entrez les paramètres de JDBC. Appuyez sur **2** pour ignorer la configuration de la connexion JDBC.
47. Choisissez le type de base de données pour le référentiel modèle, et saisissez les informations d'identification, y compris l'ID et le mot de passe de l'utilisateur.
48. Configurez éventuellement la connexion JDBC et ses paramètres.

49. Saisissez les informations suivantes : nom du service de référentiel modèle, nom du service d'intégration de données et numéro de port du service d'intégration de données si vous ne souhaitez pas utiliser la valeur par défaut.

Option	Description
Nom MRS	Nom du service de référentiel modèle.
Nom DIS	Nom du service d'intégration de données.
Type de protocole HTTP	Protocole de sécurité que le service d'intégration de données utilise.
Port	Numéro de port.

Vous voyez des messages sur la création du service de référentiel modèle et du service d'intégration de données.

50. Entrez les informations requises suivantes en plus du service de référentiel modèle et du service d'intégration de données pour créer les bases de données de l'entrepôt de profilage et de l'entrepôt de données de référence :

Type de base de données pour l'entrepôt de données de référence

Type de base de données pour l'entrepôt de données de référence. L'entrepôt de données de référence prend en charge IBM DB2 UDB, Microsoft SQL Server ou Oracle.

Nom d'hôte de la base de données pour l'entrepôt de données de référence

Le nom de la machine hébergeant l'entrepôt de données de référence.

Type de base de données d'entrepôt de profilage

Type de base de données pour l'entrepôt de profilage. L'entrepôt de profilage prend en charge IBM DB2 UDB, Microsoft SQL Server ou Oracle.

Nom d'hôte de la base de données de l'entrepôt de profilage

Le nom de la machine hébergeant l'entrepôt de profilage.

Le résumé post-installation indique si l'installation est réussie. Vous pouvez visualiser les fichiers journaux de l'installation pour obtenir plus d'informations sur les tâches effectuées par le programme d'installation et pour voir les propriétés de configuration des composants installés.

Installation en joignant un domaine

Vous pouvez joindre un domaine si vous effectuez l'installation sur plusieurs machines et que vous avez créé un domaine sur une autre machine.

1. Connectez-vous à la machine à l'aide d'un compte utilisateur système.
2. Fermez toutes les autres applications.
3. Exécutez la commande `./install.sh` pour démarrer le programme d'installation.

Le programme d'installation affiche un message vous invitant à lire la documentation d'Informatica avant de procéder à l'installation.

4. Appuyez sur **O** pour continuer l'installation.
5. Appuyez sur **1** pour installer les produits de la suite Informatica Big Data.
6. Appuyez sur **1** pour exécuter l'outil Pre-installation System Check. L'outil vérifie si votre machine répond à la configuration système minimale requise pour installer ou mettre à niveau Informatica.

Remarque: Vous pouvez ignorer cette étape si vous êtes sûr que votre machine répond à la configuration système minimale requise pour installer ou mettre à niveau Informatica.

7. Appuyez sur **3** pour installer Informatica.
8. Appuyez sur **2** pour accepter les conditions générales de l'installation ou de la mise à niveau.
9. Appuyez sur **2** pour confirmer que vous comprenez que la version 10.2.2 est spécifique à la suite de produits Big Data et poursuivre l'installation.
10. Appuyez sur **2** pour installer les services Informatica avec Enterprise Data Catalog.
Le programme d'installation vous invite à confirmer que la version actuelle des services Informatica n'est pas installée sur le nœud.
11. Appuyez sur **1** si vous n'avez pas la version actuelle des services Informatica installée. Sinon, appuyez sur **2**.
12. Choisissez le type de cluster Hadoop pour Enterprise Data Catalog. Appuyez sur 2 pour déployer Enterprise Data Catalog sur une distribution Hadoop interne sur HortonWorks à l'aide de l'outil Ambari. Appuyez sur 1 pour déployer Enterprise Data Catalog sur une distribution Hadoop existante sur Cloudera, HortonWorks ou Azure HDInsight.

Selon les paramètres que vous spécifiez, Enterprise Data Catalog crée un service de cluster Informatica pour la distribution Hadoop interne.

13. Si vous avez choisi la distribution Hadoop intégrée, indiquez les informations suivantes après la configuration du domaine Informatica, du service de référentiel modèle et du service d'intégration de données :

-

Option	Description
Nom d'utilisateur SSH	Nom d'utilisateur de la connexion Secure Shell (SSH) sans mot de passe
Nom du service de cluster Informatica	Nom du service de cluster Informatica pour le cluster interne.
Port du service de cluster Informatica	Numéro de port du service de cluster Informatica.
Hôte du serveur Ambari	Informations d'hôte du serveur Ambari. Ambari est un outil Web destiné à l'approvisionnement, à la gestion et à la surveillance des grappes Hadoop Apache. Il prend en charge Hadoop HDFS, Hadoop MapReduce, Hive, HBase et ZooKeeper.
Hôtes de l'agent Ambari séparés par des virgules	S'applique à la haute disponibilité. Si vous utilisez plusieurs hôtes d'agents Ambari, spécifiez leurs noms séparés par des virgules.
Port Web Ambari	Numéro de port sur lequel le serveur Ambari doit s'exécuter.
Nom du service de catalogue	Nom du service de catalogue.
Port du service de catalogue	Numéro de port du service de catalogue.
Emplacement du fichier keytab	S'applique à un cluster activé pour Kerberos. Emplacement du fichier keytab fusionné de l'utilisateur et de l'hôte.

Option	Description
Fichier de configuration Kerberos	S'applique à un cluster activé pour Kerberos. Emplacement du fichier de configuration Kerberos.

- Spécifiez les détails suivants si vous sélectionnez un cluster existant :

Propriété	Description
Distribution Hadoop	Sélectionnez l'une des options suivantes : - ClouderaManager - HDInsight - Hortonworks
URL du cluster	Nom d'hôte complet pour accéder au cluster.
Nom d'utilisateur de l'URL du cluster	Nom d'utilisateur pour accéder au cluster.
Mot de passe de l'URL du cluster	Mot de passe du nom d'utilisateur de l'URL du cluster.

- Si vous avez choisi la distribution Hadoop existante `ClouderaManager` ou `Hortonworks`, indiquez les informations suivantes :

Option	Description
Nom du service de catalogue	Nom du service de catalogue.
Port du service de catalogue	Numéro de port du service de catalogue.
URI du gestionnaire de ressources Yarn	Service au sein d'Hadoop qui envoie les tâches MapReduce aux nœuds spécifiques dans la grappe. Utiliser le format suivant : <hostname>:<port> Où <ul style="list-style-type: none"> • <code>hostname</code> est le nom ou l'adresse IP du gestionnaire de ressources Yarn. • <code>port</code> est le port sur lequel le gestionnaire de ressources Yarn écoute les appels de procédure distante (RPC).
URI http du gestionnaire de ressources Yarn	Valeur de l'URI http du gestionnaire de ressources Yarn.
URI du planificateur du gestionnaire de ressources Yarn	Valeur de l'URI du planificateur du gestionnaire de ressources Yarn.
URI du cluster Zookeeper	URI du service Zookeeper, un service de coordination hautes performances pour les applications distribuées.

Option	Description
URI du namenode HDFS	L'URI pour accéder à HDFS. Utilisez le format suivant pour spécifier l'URI du NameNode dans la distribution Cloudera : hdfs://<namenode>:<port> Où <ul style="list-style-type: none"> • <namenode> est le nom d'hôte ou l'adresse IP du NameNode. • <port> est le port sur lequel le NameNode écoute les appels de procédure distante (RPC).
Nom du cluster de service	Nom du cluster de service. Assurez-vous d'avoir un répertoire /Informatica/LDM/<ServiceClusterName> dans HDFS avant que l'installation soit complète. Remarque: Si vous ne spécifiez pas un nom de cluster de service, Enterprise Data Catalog considère DomainName_CatalogServiceName comme la valeur par défaut. Le répertoire /Informatica/LDM/<DomainName> <CatalogServiceName> doit alors se trouver dans HDFS. Sinon, le service de catalogue pourrait échouer.
URI HTTP du serveur d'historique	URI HTTP pour accéder au serveur d'historique.
Le cluster est-il sécurisé ?	Définissez cette propriété sur l'une des valeurs suivantes si vous disposez d'un cluster existant sécurisé : <ul style="list-style-type: none"> • 1 : spécifie que le cluster existant n'est pas sécurisé. • 2 : spécifie que le cluster existant est sécurisé. La valeur par défaut est 1.
L'authentification SSL est-elle activée sur le cluster ?	Uniquement applicable si vous aviez sélectionné la distribution Hadoop Hortonworks et ClouderaManager. Définissez cette propriété sur l'une des valeurs suivantes si vous disposez d'un cluster existant activé pour SSL : <ul style="list-style-type: none"> • 1 : spécifie que le cluster existant n'est pas activé pour SSL. • 2 : spécifie que le cluster existant est activé pour SSL. La valeur par défaut est 1.
Activer l'authentification Kerberos	Définissez cette propriété sur l'une des valeurs suivantes si vous disposez d'un cluster existant activé pour Kerberos : <ul style="list-style-type: none"> • 1 : spécifie que le cluster existant n'est pas activé pour Kerberos. • 2 : spécifie que le cluster existant est activé pour Kerberos.

14. Appuyez sur **Entrée** pour continuer.

Vous voyez un message d'invite sur le fichier de clé de licence.

15. Appuyez sur **2** pour que le programme d'installation règle les services d'applications Informatica en fonction de la taille des données déployées.

Le programme d'installation affiche les options suivantes pour différentes tailles de données :

- Sandbox
- De base
- Standard

- Concurrence élevée et volume élevé
16. Tapez le chemin d'accès et le nom de fichier de la clé de licence Informatica, puis appuyez sur **Entrée**.
 17. Tapez le chemin d'accès absolu du répertoire d'installation.
Les noms de répertoires du chemin d'accès ne doivent pas contenir d'espaces ni les caractères spéciaux suivants : @|* \$ # ! % () { } [] , ; ' Par défaut /home/toolinst.
Remarque: Informatica recommande d'utiliser des caractères alphanumériques dans le chemin d'accès au répertoire d'installation. Si vous utilisez un caractère spécial comme á ou €, des résultats inattendus peuvent se produire lors de l'exécution.
 18. Appuyez sur **2** pour exécuter l'utilitaire de pré-validation. L'utilitaire vous aide à valider les prérequis pour installer Enterprise Data Catalog dans un cluster intégré. L'utilitaire valide également la configuration du domaine Informatica, des hôtes de cluster et des services de cluster Hadoop.
Le programme d'installation vous invite à confirmer si vous souhaitez activer l'authentification Kerberos pour le cluster.
 19. Appuyez sur **2** pour activer l'authentification Kerberos du cluster, et indiquez les détails suivants :
 - a. **Emplacement du fichier keytab.** Emplacement du fichier keytab fusionné de l'utilisateur et de l'hôte.
 - b. **Fichier de configuration Kerberos.** Emplacement du fichier de configuration Kerberos.
 20. Indiquez le nom d'utilisateur de la passerelle, et appuyez sur **Entrée**. La valeur par défaut est **racine**.
 21. Indiquez le nom d'hôte de passerelle du cluster Hadoop d'Informatica au format suivant : `<hostname>.<FQDN>` et appuyez sur la touche **Entrée**.
 22. Indiquez la liste des nœuds du cluster Hadoop d'Informatica séparés par des virgules, comme indiqué au format suivant : `<hostname>.<FQDN>, <hostname1>.<FQDN>, <hostname2>.<FQDN>` et appuyez sur la touche **Entrée**.
 23. Indiquez le port de passerelle du cluster Hadoop d'Informatica, et appuyez sur **Entrée**. La valeur par défaut est **8080**.
Assurez-vous que vous ne configurez pas Oracle avec le port 8080 sur la même machine où le service de cluster Informatica s'exécute.
 24. Indiquez le chemin d'accès au répertoire de travail, et appuyez sur **Entrée**. Le chemin d'accès indique l'emplacement où vous souhaitez monter le service de cluster Informatica.
Le programme d'installation démarre l'utilitaire de pré-validation.
 25. Appuyez sur **Entrée** pour continuer après avoir exécuté l'utilitaire de pré-validation.
 26. Examinez les informations d'installation, et appuyez sur **Entrée** pour continuer.
Le programme d'installation copie les fichiers d'Enterprise Data Catalog dans le répertoire d'installation. Vous voyez une invite pour créer ou joindre un domaine.
 27. Appuyez sur **2** pour joindre un domaine.
Le programme d'installation crée un nœud sur la machine sur laquelle vous effectuez l'installation. Vous pouvez indiquer le type de nœud à créer et le domaine à joindre.
 28. Indiquez si la communication sécurisée est activée sur le domaine que vous voulez joindre.
Appuyez sur 1 pour joindre un domaine non sécurisé ou sur 2 pour joindre un domaine sécurisé.
 29. Sélectionnez le type de nœud à créer.

Le tableau suivant décrit les types de nœuds que vous pouvez créer :

Propriété	Description
Configurer ce nœud comme une passerelle	Indiquez si vous souhaitez configurer le nœud comme une passerelle ou un nœud de travail. 1 - Oui 2 - Non Sélectionnez 1 pour configurer un nœud de passerelle ou 2 pour configurer un nœud de travail.

Si vous configurez le nœud en tant que passerelle, vous pouvez activer une connexion HTTPS sécurisée à Informatica Administrator.

30. Spécifiez les détails de connexion à Informatica Administrator.

a. Indiquez si vous souhaitez définir une connexion HTTPS sécurisée à Informatica Administrator.

Le tableau suivant décrit les options disponibles permettant d'activer ou de désactiver une connexion sécurisée à Informatica Administrator :

Option	Description
1 - Activer HTTPS pour Informatica Administrator	Configurer une connexion sécurisée à Informatica Administrator.
2 - Désactiver HTTPS	Ne pas configurer une connexion sécurisée à Informatica Administrator.

b. Si vous activez une connexion HTTPS pour Informatica Administrator, entrez le fichier keystore et le numéro de port à utiliser pour sécuriser la connexion.

Le tableau suivant décrit les informations de connexion que vous devez entrer si vous activez HTTPS :

Option	Description
Port	Numéro de port de la connexion HTTPS.
Fichier keystore	Indiquez si vous souhaitez utiliser un fichier keystore généré par le programme d'installation ou un fichier keystore que vous créez. Vous pouvez utiliser un fichier keystore avec un certificat auto-signé ou un certificat signé par une autorité de certification. 1 - Utiliser un keystore généré par le programme d'installation 2 - Spécifier un fichier et un mot de passe keystore Si vous choisissez d'utiliser un fichier keystore généré par le programme d'installation, ce dernier crée un fichier keystore auto-signé nommé Default.keystore à l'emplacement suivant : <Répertoire d'installation Informatica>/tomcat/conf/

c. Si vous spécifiez le keystore, entrez le mot de passe et l'emplacement du fichier keystore.

31. Appuyez sur **2** pour activer l'authentification unique utilisant l'authentification SAML pour les applications d'Enterprise Data Catalog.

32. Indiquez l'URL du fournisseur d'identité (IdP) SAML, et appuyez sur **Entrée**.
Consultez la section *Configurer l'authentification unique avec l'authentification SAML* pour en savoir plus sur la configuration à effectuer après avoir installé Enterprise Data Catalog.

Si vous avez activé la communication sécurisée pour le domaine, la section **Sécurité du domaine - Communication sécurisée** s'affiche. Si vous n'avez pas activé la communication sécurisée pour le domaine, la page **Référentiel de configuration du domaine** s'affiche.

33. Sur la page Sécurité du domaine - Communication sécurisée, indiquez si vous souhaitez utiliser les certificats SSL Informatica par défaut ou des certificats SSL que vous fournissez pour sécuriser la communication du domaine.
- a. Sélectionnez le type de certificat SSL à utiliser.

Le tableau suivant décrit les options des certificats SSL que vous pouvez utiliser pour sécuriser le domaine Informatica :

Option	Description
1 - Utiliser les fichiers de certificat SSL Informatica par défaut	Permet d'utiliser les certificats SSL par défaut fournis par Informatica. Remarque: Si vous ne fournissez pas de certificat SSL, Informatica utilise la même clé privée par défaut pour toutes les installations d'Informatica. Si vous utilisez les fichiers entrepôt de clés et truststore Informatica par défaut, la sécurité de votre domaine peut être compromise. Pour assurer un niveau élevé de sécurité pour le domaine, sélectionnez l'option permettant de spécifier l'emplacement des fichiers de certificat SSL.
2 - Spécifier l'emplacement des fichiers de certificat SSL	Permet d'utiliser les certificats SSL que vous fournissez. Vous devez spécifier l'emplacement des fichiers keystore et truststore. Vous pouvez fournir un certificat auto-signé ou un certificat émis par une autorité de certification (CA). Vous devez fournir les certificats SSL dans le format PEM et dans des fichiers keystore Java (JKS, Java Keystore). Informatica requiert des noms de fichier de certificat SSL spécifiques pour le domaine Informatica. Vous devez utiliser les mêmes certificats SSL pour tous les nœuds du domaine. Stockez les fichiers truststore et keystore dans un répertoire accessible à tous les nœuds du domaine et spécifiez le même répertoire de fichiers keystore et truststore pour tous les nœuds d'un même domaine.

- b. Si vous indiquez le certificat SSL, spécifiez l'emplacement et les mots de passe des fichiers keystore et truststore.

Le tableau suivant décrit les paramètres que vous devez entrer pour les fichiers de certificat SSL :

Propriété	Description
Répertoire de fichiers keystore	Répertoire contenant les fichiers keystore. Il doit contenir les fichiers infa_keystore.jks et infa_keystore.pem.
Mot de passe keystore	Mot de passe du fichier keystore infa_keystore.jks.

Propriété	Description
Répertoire de fichiers truststore	Répertoire contenant les fichiers truststore. Il doit contenir les fichiers infa_truststore.jks et infa_truststore.pem.
Mot de passe truststore	Mot de passe du fichier infa_truststore.jks.

La page Référentiel de configuration du domaine s'affiche.

34. À l'invite, entrez les informations relatives au domaine à joindre.

Le tableau suivant décrit les propriétés que vous indiquez pour le domaine :

Propriété	Description
Nom de domaine	Nom du domaine à joindre.
Hôte du nœud de passerelle	Nom d'hôte de la machine qui héberge le nœud de passerelle pour le domaine.
Port du nœud de passerelle	Numéro de port du nœud de passerelle.
Nom d'utilisateur de domaine	Nom d'utilisateur de l'administrateur du domaine à joindre.
Mot de passe du domaine	Mot de passe de l'administrateur du domaine.

La page **Sécurité du domaine - Clé de chiffrement** s'affiche.

35. Entrez les informations sur la clé de chiffrement pour le domaine Informatica à joindre.

Si l'emplacement de la clé de chiffrement dans le nœud de passerelle n'est pas accessible au nœud actuel, copiez le fichier de clé de chiffrement dans un répertoire accessible. Vous devrez peut-être attribuer une autorisation de lecture au répertoire qui contient le fichier de clé de chiffrement sur le nœud de passerelle pour pouvoir copier le fichier.

Le tableau suivant décrit les paramètres de clé de chiffrement que vous devez spécifier lorsque vous joignez un domaine :

Propriété	Description
Sélectionnez la clé de chiffrement	Chemin et nom de fichier de la clé de chiffrement pour le domaine Informatica à joindre. Tous les nœuds du domaine Informatica utilisent la même clé de chiffrement. Vous devez spécifier le fichier de clé de chiffrement créé sur le nœud de passerelle pour le domaine à joindre. Si vous avez copié le fichier de clé de chiffrement vers un répertoire temporaire pour le rendre disponible aux nœuds dans le domaine, spécifiez le chemin et le nom du fichier de la clé de chiffrement dans le répertoire temporaire.
Répertoire de la clé de chiffrement	Répertoire dans lequel stocker la clé de chiffrement sur le nœud créé lors de cette installation. Le programme d'installation copie le fichier de clé de chiffrement du domaine dans le répertoire de la clé de chiffrement du nouveau nœud.

36. Sur la page Joindre une configuration de nœud de domaine, entrez les informations du nœud à créer.

Le tableau suivant décrit les propriétés que vous définissez pour le nœud :

Propriété	Description
Nom d'hôte du nœud	Nom d'hôte de nœud. Le nom d'hôte du nœud ne peut pas contenir le caractère de soulignement (_). Remarque: N'utilisez pas localhost. Le nom d'hôte doit explicitement identifier la machine.
Nom du nœud	Nom du nœud Informatica à créer sur cette machine. Le nom du nœud n'est pas le nom d'hôte de la machine.
Numéro de port du nœud	Numéro de port du nœud.
Fichier truststore de base de données	Chemin d'accès et nom du fichier truststore de la base de données sécurisée. Sélectionnez le même fichier truststore de base de données que celui utilisé par le nœud principal de passerelle dans le domaine. Disponible lorsque vous joignez un nœud de passerelle à un domaine qui utilise une base de données de référentiel de configuration du domaine qui est sécurisée avec le protocole SSL.
Mot de passe truststore	Mot de passe du fichier truststore de la base de données sécurisée. Disponible lorsque vous joignez un nœud de passerelle à un domaine qui utilise une base de données de référentiel de configuration du domaine qui est sécurisée avec le protocole SSL.

37. Indiquez si vous souhaitez afficher les ports par défaut pour les composants de domaine et de nœud attribués par le programme d'installation.

Le tableau suivant décrit la page de configuration avancée des ports :

Invite	Description
Afficher la page de configuration avancée des ports	Indiquez si vous souhaitez afficher les numéros de port pour les composants de domaine et de nœud attribués par le programme d'installation : 1 - Non 2 - Oui Si vous sélectionnez Oui, le programme d'installation affiche les numéros de port par défaut attribués aux composants du domaine. Vous pouvez indiquer les numéros de port à utiliser pour les composants de domaine et de nœud. Vous pouvez également indiquer une plage de numéros de port à utiliser pour le processus de service qui s'exécute sur le nœud. Vous pouvez utiliser les numéros de port par défaut ou spécifier de nouveaux numéros de port. Vérifiez que les numéros de ports que vous entrez ne sont pas utilisés par d'autres applications.

38. Si vous affichez la page de configuration des ports, entrez les nouveaux numéros de port à l'invite ou appuyez sur **Entrée** pour utiliser les numéros de port par défaut.

Port	Description
Port de gestionnaire de service	Numéro de port utilisé par le Gestionnaire de service sur le nœud. Le gestionnaire de service écoute les demandes de connexions entrantes sur ce port. Les applications clientes utilisent ce port pour communiquer avec les services du domaine. Les programmes de ligne de commande Informatica utilisent ce port pour communiquer avec le domaine. Ce port est également utilisé par le pilote JDBC/ODBC du service de données SQL. La valeur par défaut est 6006.
Port d'arrêt du gestionnaire de service	Numéro de port qui contrôle l'arrêt du serveur pour le Gestionnaire de service du domaine. Le gestionnaire de service écoute les commandes d'arrêt sur ce port. La valeur par défaut est 6007.
Port d'Informatica Administrator	Numéro de port utilisé par Informatica Administrator. La valeur par défaut est 6008.
Port HTTPS d'Informatica Administrator	Aucun port par défaut. Entrez le numéro de port requis lorsque vous créez le service. Configurer le port sur 0 désactive la connexion HTTPS à l'outil Administrator tool.
Port d'arrêt d'Informatica Administrator	Numéro de port qui contrôle l'arrêt du serveur pour Informatica Administrator. Informatica Administrator écoute les demandes d'arrêt sur ce port. La valeur par défaut est 6009.
Numéro de port minimal	Plus petit numéro de port de la plage des numéros de port pouvant être attribués aux processus de service d'application exécutés sur ce nœud. Le numéro par défaut est 6014.
Numéro de port maximal	Plus grand numéro de port de la plage des numéros de port pouvant être attribués aux processus de service d'application exécutés sur ce nœud. Le numéro par défaut est 6114.

39. Indiquez si vous souhaitez configurer une base de données sécurisée. Appuyez sur **1** pour configurer une base de données sécurisée, ou sur **2** pour ignorer l'étape.
40. Pour configurer les informations de connexion JDBC, appuyez sur **1** et entrez les paramètres de JDBC. Appuyez sur **2** pour ignorer la configuration de la connexion JDBC.
41. Choisissez le type de base de données pour le référentiel modèle, et saisissez les informations d'identification, y compris l'ID et le mot de passe de l'utilisateur.
42. Configurez éventuellement la connexion JDBC et ses paramètres.
43. Saisissez les informations suivantes : nom du service de référentiel modèle, nom du service d'intégration de données et numéro de port du service d'intégration de données si vous ne souhaitez pas utiliser la valeur par défaut.

Option	Description
Nom MRS	Nom du service de référentiel modèle.
Nom DIS	Nom du service d'intégration de données.
Type de protocole HTTP	Protocole de sécurité que le service d'intégration de données utilise.

Option	Description
Port	Numéro de port.

Vous voyez des messages sur la création du service de référentiel modèle et du service d'intégration de données.

Le résumé post-installation indique si l'installation est réussie. Vous pouvez visualiser les fichiers journaux de l'installation pour obtenir plus d'informations sur les tâches effectuées par le programme d'installation et pour voir les propriétés de configuration des composants installés.

Installation de Enterprise Data Catalog sur un nœud de domaine

Vous pouvez utiliser le programme d'installation d'Informatica pour installer Enterprise Data Catalog après avoir installé Informatica. Pour installer Enterprise Data Catalog après avoir installé Informatica, procédez comme suit :

1. Connectez-vous à la machine à l'aide d'un compte d'utilisateur système.
2. Arrêtez le domaine Informatica.
3. Fermez toutes les applications.
4. Dans une ligne de commande shell, exécutez `install.sh` à partir du répertoire racine.

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

5. Appuyez sur 1 pour sélectionner l'option d'installation ou de mise à niveau d'Informatica.

Le programme d'installation vérifie si la version actuelle d'Informatica est installée.

6. Appuyez sur 2 pour installer les services Informatica avec Enterprise Data Catalog.

Le programme d'installation vous invite à confirmer l'installation de la version actuelle des services Informatica.

7. Appuyez sur 2 pour installer Enterprise Data Catalog. La sélection de cette option suppose que la version actuelle d'Informatica est installée.
8. Indiquez l'emplacement de `<INFA_HOME>` lorsque le programme d'installation vous invite à effectuer l'installation. `INFA_HOME` fait référence au répertoire d'installation d'Enterprise Data Catalog.

Le résumé post-installation indique si l'installation est réussie. Vous pouvez visualiser les fichiers journaux de l'installation pour obtenir plus d'informations sur les tâches effectuées par le programme d'installation et pour voir les propriétés de configuration des composants installés.

Remarque: Les instructions fournies dans cette section supposent que vous ayez créé les services d'application Informatica lorsque vous avez installé Informatica. Si vous n'avez pas créé les services, consultez la section *Installation en joignant un domaine* pour plus d'informations sur la création de services d'application.

Après avoir terminé l'installation, procédez comme suit :

1. Supprimez les répertoires suivants :
 - `INFA_HOME/service/work_dir`
 - `INFA_HOME/tomcat/bin/workspace/.metadata`
2. Démarrez le domaine Informatica.

3. Activez le service de référentiel modèle et mettez à niveau le contenu correspondant à l'aide de l'une des méthodes suivantes :
 - Informatica Administrator : sélectionnez le service de référentiel modèle et cliquez sur **Actions > Contenu du référentiel > Mettre à niveau**.
 - Interface de ligne de commande Informatica : exécutez la commande `INFA_HOME/isp/bin/infacmd.sh mrs upgradeContents -dn DOMAINNAME -un domainUsername -pw domainPassword -sn MRSServiceName`
4. Créez et activez le service de catalogue. Veillez à utiliser le service de référentiel modèle mis à niveau.

Création des services d'application Enterprise Data Catalog

Enterprise Data Catalog requiert la création et l'exécution de services d'application avant de pouvoir être utilisé.

Vous pouvez créer les services d'application en utilisant l'une des méthodes suivantes :

En utilisant le programme d'installation lorsque vous installez Enterprise Data Catalog

Pour plus d'informations sur l'utilisation du programme d'installation pour créer les services d'application lorsque vous installez Enterprise Data Catalog, consultez https://network.informatica.com/onlinehelp/edc/Install_Help/index.htm

En utilisant Informatica Administrator après avoir installé Enterprise Data Catalog

Pour plus d'informations sur la création des services d'application en utilisant Informatica Administrator, consultez le chapitre *Créer les services d'application* de ce guide.

En utilisant le programme d'installation après avoir installé Enterprise Data Catalog

Pour plus d'informations sur la création des services d'application après avoir installé Enterprise Data Catalog, consultez les étapes listées dans la rubrique *Création des services d'application Enterprise Data Catalog à l'aide du programme d'installation*.

Si les services d'application ne sont pas créés ou si le processus échoue, vous ne pouvez pas reprendre le processus à partir du point d'échec à l'aide du programme d'installation. Vous pouvez redémarrer le processus à l'aide du programme d'installation.

Création des services d'application Enterprise Data Catalog à l'aide du programme d'installation

Effectuez les étapes suivantes pour créer les services d'application à l'aide du programme d'installation après avoir installé Enterprise Data Catalog :

1. Connectez-vous à la machine à l'aide d'un compte utilisateur système.
2. Fermez toutes les applications en cours d'exécution sur la machine.
3. Sur une ligne de commande shell, exécutez la commande `./install.sh` pour démarrer le programme d'installation.
4. Appuyez sur **y** pour poursuivre l'installation.
5. Appuyez sur **3** pour sélectionner l'option d'installation des services d'application pour Enterprise Data Catalog ou Enterprise Data Preparation.
6. Appuyez sur **2** pour accepter les conditions générales.
7. Appuyez sur **2** pour accepter de poursuivre l'installation de produits Big Data.
8. Appuyez sur **1** pour configurer les services pour Enterprise Data Catalog.

9. Appuyez sur **1** pour confirmer que la dernière version des services Enterprise Data Catalog n'est pas installée.
10. Saisissez le répertoire où vous avez installé Enterprise Data Catalog et appuyez sur **Entrée**.
11. Saisissez les informations de domaine suivantes que vous avez configurées quand vous avez installé Enterprise Data Catalog :
 - a. Nom du domaine. Indiquez le nom du Domaine Informatica que vous avez créé et appuyez sur **Entrée**.
 - b. Nom du nœud. Indiquez le nom du nœud que vous avez créé sur la machine où vous avez installé Enterprise Data Catalog et appuyez sur **Entrée**.
 - c. Mot de passe d'utilisateur du domaine. Indiquez le mot de passe que vous avez configuré pour l'administrateur de Domaine Informatica et appuyez sur **Entrée**.
12. Appuyez sur **1** pour confirmer que vous désirez créer le Service de référentiel modèle et le Service d'intégration de données.
13. Appuyez sur **1** si vous désirez créer la Surveillance de Service de référentiel modèle pour surveiller les statistiques du Domaine Informatica.
14. Appuyez sur **2** pour spécifier que vous ne désirez pas créer de configuration de cluster. Vous devez créer une configuration de cluster dans le domaine Informatica si vous prévoyez de configurer les services Enterprise Data Preparation.
15. Appuyez sur **1** si vous désirez créer une connexion à l'entrepôt de profilage.
16. Appuyez sur **1** pour configurer le service de gestion de contenu.
17. Vous devez créer le service de cluster Informatica si vous déployez Enterprise Data Catalog sur un cluster incorporé. Appuyez sur **1** si vous désirez configurer le service de cluster Informatica. Passez en revue les points suivants pour décider si vous désirez créer le service de cluster Informatica.
 - Créer le service de cluster Informatica. Le programme d'installation crée le service de cluster Informatica.
 - Sélectionnez l'option pour spécifier si vous désirez créer le service de cluster Informatica. Le programme d'installation vous invite à spécifier si vous désirez associer un service de cluster Informatica au service de catalogue. Si vous sélectionnez cette option, le programme d'installation ne crée pas de nouveau service de cluster Informatica. Le programme d'installation vous invite à associer un service de cluster Informatica au service de catalogue.
 - Sélectionnez les options pour spécifier que vous ne voulez pas créer de service de cluster Informatica et associer un service de cluster Informatica existant au service de catalogue. Le programme d'installation ne crée pas le service de cluster Informatica et passe à la création du service de catalogue.
18. Appuyez sur **1** si vous désirez configurer le service de catalogue.
19. Effectuez les étapes des sections suivantes pour créer les services d'application.

Création du service de référentiel modèle

Fournissez les informations suivantes pour le service de référentiel modèle :

1. Nom du service de référentiel modèle.
2. Nom du nœud sur lequel doit d'exécuter le service de référentiel modèle.
3. Licence à associer au service de référentiel modèle.

4. Sélectionnez la base de données que vous souhaitez configurer pour le référentiel modèle à partir des options suivantes :
 - Oracle
 - SQL Server
 - DB2
 La valeur par défaut est Oracle.
5. Saisissez le nom d'utilisateur pour accéder à la base de données dans le paramètre **Database user ID** et appuyez sur **Entrée**. Le nom par défaut est **admin**.
6. Saisissez le mot de passe pour le nom d'utilisateur dans le paramètre **User password** et appuyez sur Entrée.
7. Appuyez sur **1** si la base de données est sécurisée avec SSL.
Si vous avez sélectionné l'option pour spécifier que SSL est activé sur la base de données, fournissez les paramètres suivants :

Paramètres de base de données sécurisée	Description
EncryptionMethod	Indique si les données sont cryptées lorsqu'elles sont transmises sur le réseau. Ce paramètre doit être défini pour SSL.
ValidateServerCertificate	Indique si Informatica valide le certificat envoyé par le serveur de base de données. Si ce paramètre est défini sur True, Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre HostNameInCertificate, Informatica valide également le nom d'hôte dans le certificat. Si ce paramètre est défini sur False, Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de truststore que vous spécifiez.
HostNameInCertificate	Nom d'hôte de la machine qui héberge la base de données sécurisée. Si vous spécifiez un nom d'hôte, Informatica valide le nom d'hôte inclus dans la chaîne de connexion avec le nom d'hôte dans le certificat SSL.
cryptoProtocolVersion	Indique le protocole cryptographique à utiliser pour la connexion à une base de données sécurisée. Vous pouvez définir le paramètre sur cryptoProtocolVersion=TLSv1.1 ou cryptoProtocolVersion=TLSv1.2 selon le protocole cryptographique utilisé par le serveur de base de données.
TrustStore	Chemin et nom du fichier truststore contenant le certificat SSL de la base de données. Si vous n'incluez pas le chemin du fichier truststore, Informatica recherche ce fichier dans le répertoire par défaut suivant : <Répertoire d'installation Informatica>/tomcat/bin
TrustStorePassword	Mot de passe du fichier truststore de la base de données sécurisée.

8. Appuyez sur **1** pour spécifier l'URL JDBC pour la connexion à la base de données.
9. Spécifiez l'adresse de la base de données dans le format suivant pour le paramètre **Database address** :
<Nom de domaine complet de l'hôte>:<port>
10. Spécifiez le nom du service de la base de données dans le format suivant pour le paramètre **Database service name** : <Nom de domaine complet du service>

11. Appuyez sur **1** pour spécifier que vous désirez configurer les paramètres JDBC.
12. Spécifiez les valeurs requises pour les paramètres ou appuyez sur **Entrée** pour appliquer les valeurs par défaut. Appuyez sur **Entrée** pour conserver les valeurs par défaut.
Utilisez la syntaxe suivante pour la chaîne de connexion du type de base de données sélectionné :

Type de base de données	Syntaxe de la chaîne de connexion
IBM DB2	<code>jdbc:informatica:db2:// <nom_hôte>:<numéro_port>;DatabaseName=<nom_basededonnées>;BatchPerformanceWorkaround=true;DynamicSections=3000</code>
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server qui utilise l'instance par défaut <code>jdbc:informatica:sqlserver:// <nom_hôte>:<numéro_port>;DatabaseName=<nom_basededonnées>;SnapshotSerializable=true</code> - Microsoft SQL Server qui utilise une instance nommée <code>jdbc:informatica:sqlserver://<nom_hôte> \<nom_instance_nommée>;DatabaseName=<nom_basededonnées>;SnapshotSerializable=true</code>
Oracle	<code>jdbc:informatica:oracle:// <nom_hôte>:<numéro_port>;SID=<nom_basededonnées>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true</code>

Le programme d'installation valide le nom du nœud et la licence, puis crée le service de référentiel modèle. Le programme d'installation passe à la création du service d'intégration de données.

Création du service d'intégration de données

Fournissez les informations suivantes pour le service d'intégration de données :

1. Nom du service d'intégration de données.
2. Nom du nœud sur lequel doit d'exécuter le service d'intégration de données.
3. Licence à associer au service d'intégration de données.
4. Le nom du service de référentiel modèle que vous voulez associer au service d'intégration de données.
5. Spécifiez le protocole que vous souhaitez utiliser pour le service à partir des options suivantes :
 - http
 - https
 - http&https

Si vous sélectionnez **https** ou **http&https** comme protocole pour le service, fournissez les informations suivantes :

 1. Port HTTPS. La valeur par défaut est 18095.
 2. Spécifiez le certificat SSL que vous désirez utiliser pour sécuriser le service d'intégration de données. Vous pouvez utiliser les certificats SSL par défaut dans les keystore et truststore par défaut ou utiliser des certificats SSL personnalisés. Si vous choisissez des certificats SSL personnalisés, spécifiez le chemin qui inclut le nom des fichiers keystore et truststore et les mots de passe pour accéder à ces fichiers.
6. Appuyez sur **1** si vous désirez que le service d'intégration de données utilise le moteur Spark pour exécuter des mappages Sqoop ou traiter des transformations Java.

Le programme d'installation valide le nom du nœud et la licence, puis crée et active le Service d'intégration de données. Le programme d'installation passe à la création de l'entrepôt de profilage.

Configurer l'entrepôt de profilage

Fournissez les informations suivantes pour configurer la base de données pour l'entrepôt de profilage :

1. Nom du Service d'intégration de données que vous désirez associer à l'entrepôt de profilage.
2. Sélectionnez la base de données que vous souhaitez configurer pour l'entrepôt de profilage à partir des options suivantes :
 - Oracle
 - SQL Server
 - DB2

La valeur par défaut est Oracle.

3. Saisissez le nom d'utilisateur pour accéder à la base de données dans le paramètre **Database user ID** et appuyez sur **Entrée**. Le nom par défaut est **admin**.
4. Saisissez le mot de passe pour le nom d'utilisateur dans le paramètre **User password** et appuyez sur **Entrée**.
5. Appuyez sur **1** si la base de données est sécurisée avec SSL.
Si vous avez sélectionné l'option pour spécifier que SSL est activé sur la base de données, fournissez les paramètres suivants :

Paramètres de base de données sécurisée	Description
EncryptionMethod	Indique si les données sont cryptées lorsqu'elles sont transmises sur le réseau. Ce paramètre doit être défini pour SSL.
ValidateServerCertificate	Indique si Informatica valide le certificat envoyé par le serveur de base de données. Si ce paramètre est défini sur True, Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre HostNameInCertificate, Informatica valide également le nom d'hôte dans le certificat. Si ce paramètre est défini sur False, Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de truststore que vous spécifiez.
HostNameInCertificate	Nom d'hôte de la machine qui héberge la base de données sécurisée. Si vous spécifiez un nom d'hôte, Informatica valide le nom d'hôte inclus dans la chaîne de connexion avec le nom d'hôte dans le certificat SSL.
cryptoProtocolVersion	Indique le protocole cryptographique à utiliser pour la connexion à une base de données sécurisée. Vous pouvez définir le paramètre sur cryptoProtocolVersion=TLSv1.1 ou cryptoProtocolVersion=TLSv1.2 selon le protocole cryptographique utilisé par le serveur de base de données.
TrustStore	Chemin et nom du fichier truststore contenant le certificat SSL de la base de données. Si vous n'incluez pas le chemin du fichier truststore, Informatica recherche ce fichier dans le répertoire par défaut suivant : <Répertoire d'installation Informatica>/tomcat/bin
TrustStorePassword	Mot de passe du fichier truststore de la base de données sécurisée.

6. Appuyez sur **1** pour spécifier l'URL JDBC pour la connexion à la base de données.

7. Spécifiez l'adresse de la base de données dans le format suivant pour le paramètre **Database address** :
<Nom de domaine complet de l'hôte>:<port>
8. Spécifiez le nom du service de la base de données dans le format suivant pour le paramètre **Database service name** :<Nom de domaine complet du service>
9. Appuyez sur **1** pour spécifier que vous désirez configurer les paramètres JDBC.
10. Spécifiez les valeurs requises pour les paramètres ou appuyez sur **Entrée** pour appliquer les valeurs par défaut. Appuyez sur **Entrée** pour conserver les valeurs par défaut.
Utilisez la syntaxe suivante pour la chaîne de connexion du type de base de données sélectionné :

Type de base de données	Syntaxe de la chaîne de connexion
IBM DB2	<code>jdbc:informatica:db2:// <nom_hôte>:<numéro_port>;DatabaseName=<nom_basededonnées>;BatchPerformanceWorkaround=true;DynamicSections=3000</code>
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server qui utilise l'instance par défaut <code>jdbc:informatica:sqlserver:// <nom_hôte>:<numéro_port>;DatabaseName=<nom_basededonnées>;SnapshotSerializable=true</code> - Microsoft SQL Server qui utilise une instance nommée <code>jdbc:informatica:sqlserver://<nom_hôte>\<nom_instance nommée>;DatabaseName=<nom_basededonnées>;SnapshotSerializable=true</code>
Oracle	<code>jdbc:informatica:oracle:// <nom_hôte>:<numéro_port>;SID=<nom_basededonnées>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true</code>

Le programme d'installation crée l'entrepôt de profilage de données et passe à la création du service de gestion de contenu.

Création du service de gestion de contenu

Fournissez les informations suivantes pour créer le service de gestion de contenu :

1. Nom du service de référentiel modèle que vous souhaitez associer au service.
2. Nom du service d'intégration de données que vous souhaitez associer au service.
3. Nom du nœud sur lequel doit d'exécuter le service de gestion de contenu.
4. Licence à associer au service de gestion de contenu.
5. Nom du service de gestion de contenu.
6. Spécifiez le protocole que vous souhaitez utiliser pour le service à partir des options suivantes :
 - http
 - https

Si vous sélectionnez **https** comme protocole pour le service, fournissez les informations suivantes :

1. Port HTTPS. La valeur par défaut est 17466.
2. Spécifiez le certificat SSL que vous désirez utiliser pour sécuriser le service de gestion de contenu. Vous pouvez utiliser les certificats SSL par défaut dans le keystore par défaut ou utiliser des certificats SSL personnalisés. Si vous choisissez des certificats SSL personnalisés, spécifiez le chemin qui inclut le nom du fichier keystore et le mot de passe pour accéder à ce fichier.

7. Effectuez les étapes suivantes pour configurer la base de données pour le service de gestion de contenu :
8. Sélectionnez la base de données que vous souhaitez configurer pour le service de gestion de contenu à partir des options suivantes :
 - Oracle
 - SQL Server
 - DB2
 La valeur par défaut est Oracle.
9. Saisissez le nom d'utilisateur pour accéder à la base de données dans le paramètre **Database user ID** et appuyez sur **Entrée**. Le nom par défaut est **admin**.
10. Saisissez le mot de passe pour le nom d'utilisateur dans le paramètre **User password** et appuyez sur Entrée.
11. Appuyez sur **1** si la base de données est sécurisée avec SSL.
Si vous avez sélectionné l'option pour spécifier que SSL est activé sur la base de données, fournissez les paramètres suivants :

Paramètres de base de données sécurisée	Description
EncryptionMethod	Indique si les données sont cryptées lorsqu'elles sont transmises sur le réseau. Ce paramètre doit être défini pour SSL.
ValidateServerCertificate	Indique si Informatica valide le certificat envoyé par le serveur de base de données. Si ce paramètre est défini sur True, Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre HostNameInCertificate, Informatica valide également le nom d'hôte dans le certificat. Si ce paramètre est défini sur False, Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de truststore que vous spécifiez.
HostNameInCertificate	Nom d'hôte de la machine qui héberge la base de données sécurisée. Si vous spécifiez un nom d'hôte, Informatica valide le nom d'hôte inclus dans la chaîne de connexion avec le nom d'hôte dans le certificat SSL.
cryptoProtocolVersion	Indique le protocole cryptographique à utiliser pour la connexion à une base de données sécurisée. Vous pouvez définir le paramètre sur cryptoProtocolVersion=TLSv1.1 ou cryptoProtocolVersion=TLSv1.2 selon le protocole cryptographique utilisé par le serveur de base de données.
TrustStore	Chemin et nom du fichier truststore contenant le certificat SSL de la base de données. Si vous n'incluez pas le chemin du fichier truststore, Informatica recherche ce fichier dans le répertoire par défaut suivant : <Répertoire d'installation Informatica>/tomcat/bin
TrustStorePassword	Mot de passe du fichier truststore de la base de données sécurisée.

12. Appuyez sur **1** pour spécifier l'URL JDBC pour la connexion à la base de données.

13. Spécifiez l'adresse de la base de données dans le format suivant pour le paramètre **Database address** :
<Nom de domaine complet de l'hôte>:<port>
14. Spécifiez le nom du service de la base de données dans le format suivant pour le paramètre **Database service name** :<Nom de domaine complet du service>
15. Appuyez sur **1** pour spécifier que vous désirez configurer les paramètres JDBC.
16. Spécifiez les valeurs requises pour les paramètres ou appuyez sur **Entrée** pour appliquer les valeurs par défaut. Appuyez sur **Entrée** pour conserver les valeurs par défaut.
Utilisez la syntaxe suivante pour la chaîne de connexion du type de base de données sélectionné :

Type de base de données	Syntaxe de la chaîne de connexion
IBM DB2	<code>jdbc:informatica:db2:// <nom_hôte>:<numéro_port>;DatabaseName=<nom_basededonnées>;BatchPerformanceWorkaround=true;DynamicSections=3000</code>
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server qui utilise l'instance par défaut <code>jdbc:informatica:sqlserver:// <nom_hôte>:<numéro_port>;DatabaseName=<nom_basededonnées>;SnapshotSerializable=true</code> - Microsoft SQL Server qui utilise une instance nommée <code>jdbc:informatica:sqlserver://<nom_hôte> \<nom_instance_nommée>;DatabaseName=<nom_basededonnées>;SnapshotSerializable=true</code>
Oracle	<code>jdbc:informatica:oracle:// <nom_hôte>:<numéro_port>;SID=<nom_basededonnées>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true</code>

Le programme d'installation crée et active le service de gestion de contenu et passe à la configuration du cluster et des options du service d'application.

Configuration du cluster et des options du service d'application

Effectuez les étapes suivantes pour configurer le cluster et les options du service d'application :

1. Appuyez sur **1** si vous désirez que le programme d'installation configure Apache ZooKeeper, YARN et HDFS en fonction des propriétés que vous fournissez.
2. Sélectionnez le type de cluster parmi les options suivantes :
 - Hortonworks
 - Cloudera
 - Azure HDInsight
3. Spécifiez si le cluster utilise l'authentification Kerberos.
4. Spécifiez si le cluster est activé pour SSL.

Configuration du service de cluster Informatica

Si vous installez Enterprise Data Catalog sur un cluster incorporé, fournissez les informations suivantes pour configurer le service de cluster Informatica :

1. Nom du nœud sur lequel doit d'exécuter le service de cluster Informatica.
2. Licence à associer au service de cluster Informatica.
3. Nom d'utilisateur pour le serveur Apache Ambari. La valeur par défaut est root.

4. Nom du service de cluster Informatica.
5. Nom d'hôte pour la passerelle de cluster Informatica Hadoop.
6. Liste séparée par des virgules de nœuds Hadoop où sont exécutés les agents Apache Ambari.
7. Numéro de port du serveur Apache Ambari. La valeur par défaut est 9075.
8. Numéro de port de la passerelle de cluster Informatica Hadoop. La valeur par défaut est 8080.
9. Spécifiez si vous désirez changer le mot de passe par défaut pour Ambari.
10. Fournissez les propriétés suivantes si vous désirez activer SSL pour le cluster :
 - a. Port HTTPS du service de cluster Informatica. La valeur par défaut est 7500.
 - b. Appuyez sur **1** si vous désirez utiliser le keystore par défaut généré par le programme d'installation.
 - c. Si vous choisissez d'utiliser un fichier keystore généré par le programme d'installation, ce dernier crée un fichier keystore auto-signé nommé Default.keystore à l'emplacement suivant : <Répertoire d'installation Informatica>/tomcat/conf/ Ou sinon, vous pouvez utiliser un fichier keystore avec un certificat auto-signé ou un certificat signé par une autorité de certification. Si vous ne prévoyez pas d'utiliser le fichier keystore généré par le programme d'installation, vérifiez que vous fournissez les certificats SSL dans un format PEM et dans des fichiers keystore Java (JKS). Informatica requiert des noms de fichier de certificat SSL spécifiques pour le domaine Informatica. Vous devez utiliser les mêmes certificats SSL pour tous les nœuds du domaine. Stockez les fichiers truststore et keystore dans un répertoire accessible à tous les nœuds du domaine et spécifiez le même répertoire de fichiers keystore et truststore pour tous les nœuds d'un même domaine.
 - d. Spécifiez l'emplacement du fichier truststore accessible par tous les nœuds du domaine et appuyez sur **Entrée**. La valeur par défaut est /opt/ssl.
11. Appuyez sur **2** si vous désirez spécifier un répertoire pour stocker les fichiers journaux HDFS, YARN et ZooKeeper, ainsi que les répertoires de données.
12. Si vous avez sélectionné **2** à l'étape précédente, spécifiez le chemin d'accès au répertoire où vous désirez stocker les fichiers journaux et appuyez sur **Entrée**.
13. Le programme d'installation crée le service de cluster Informatica et passe à la création du service de catalogue.

Configuration du service de catalogue

Fournissez les informations suivantes pour configurer le service de catalogue :

1. Nom du service de catalogue.
2. Nom du service de référentiel modèle que vous désirez associer au service de catalogue.
3. Nom du nœud sur lequel doit s'exécuter le service de catalogue.
4. Dans le cas où Enterprise Data Catalog a été déployé sur un cluster incorporé, si vous avez sélectionné les options pour associer le service de cluster Informatica au service de catalogue, fournissez le nom du service de cluster Informatica.
5. La licence que vous désirez associer au service de catalogue.
6. L'URL de distribution Hadoop du cluster.
7. Nom d'utilisateur pour accéder à l'URL de distribution Hadoop du cluster. Le nom par défaut est admin.
8. Mot de passe pour accéder à l'URL de distribution Hadoop du cluster.

9. Spécifiez les propriétés suivantes si vous avez déployé Enterprise Data Catalog sur un cluster existant :

Propriété	Description
Nom du cluster.	Si vous avez sélectionné Cloudera comme type de cluster, vous pouvez donner un nom au cluster.
Nom du service HDFS pour la haute disponibilité	S'applique au cluster existant hautement disponible. Spécifiez le nom de service HDFS.
URI du planificateur du gestionnaire de ressources Yarn	Valeur de l'URI du planificateur du gestionnaire de ressources Yarn.

Remarque: Si vous sélectionnez ClouderaManager ou Hortonworks comme distribution Hadoop pour un cluster existant, Enterprise Data Catalog identifie automatiquement les propriétés suivantes pour le type de distribution Hadoop :

- URI du cluster ZooKeeper
 - URI du NameNode HDFS
 - URI du gestionnaire de ressources Yarn
 - URI HTTPS ou HTTP du gestionnaire de ressources Yarn
 - URI HTTP du serveur d'historique
 - Nom du service HDFS pour la haute disponibilité
 - URI du planificateur du gestionnaire de ressources Yarn
10. Si vous avez déployé Enterprise Data Catalog sur un cluster Azure HDInsight, spécifiez les propriétés suivantes pour le service de catalogue :

Propriété	Description
Type de cluster	Cluster externe
Distribution Hadoop	HDInsight
URL du cluster	Nom d'hôte complet permettant d'accéder au cluster.
Nom d'utilisateur de l'URL du cluster	Nom d'utilisateur permettant d'accéder au cluster.
Mot de passe de l'URL du cluster	Mot de passe pour le nom d'utilisateur de l'URL du cluster.

Après avoir créé le service de catalogue, configurez les propriétés personnalisées suivantes dans l'application Informatica Administrator du service de catalogue :

Propriété personnalisée	Description
LdmCustomOptions.deployment.azure.account.key	La clé pour authentifier le service de catalogue afin de se connecter au compte de stockage Azure. La valeur de la clé du compte de stockage Azure peut être chiffrée ou non chiffrée. Vous pouvez récupérer la valeur depuis la propriété <code>fs.azure.account.key.<nom du compte de stockage></code> dans le fichier <code>core-site.xml</code> présent dans le cluster Azure HDInsight.
LdmCustomOptions.deployment.azure.key.decryption.script.path	Si la clé spécifiée dans la propriété <code>LdmCustomOptions.deployment.azure.account.key</code> est au format chiffré, vous pouvez utiliser le script shell de déchiffrement pour déchiffrer la clé à l'aide du certificat de clé. Vous devez vérifier que vous copiez le script shell de déchiffrement et le fichier de certificat de clé sur la machine du domaine (même chemin que la machine du cluster) avant d'activer le service de catalogue. Assurez-vous de conserver le chemin dans la machine du cluster Azure HDInsight pour les fichiers copiés dans la machine du domaine. La valeur de la propriété est l'emplacement du script shell de déchiffrement. Par exemple, <code>/usr/lib/python2.7/dist-packages/hdinsight_common/decrypt.sh</code> . Le fichier de certificat de clé, <code>key_decryption_cert.prv</code> , est présent dans le répertoire <code>/usr/lib/hdinsight-common/certs/key_decryption_cert.prv</code> du cluster Azure HDInsight.
LdmCustomOptions.deployment.hdfs.default.fs	Adresse du compte de stockage WASB auquel le service de catalogue doit se connecter. L'adresse comprend le nom du conteneur de stockage WASB avec le nom du compte de stockage. La valeur de la propriété est l'adresse WASB complète avec les noms du conteneur et du compte de stockage. Vous pouvez récupérer la valeur de la propriété depuis la propriété <code>fs.defaultFS</code> dans le fichier <code>core-site.xml</code> présent dans le cluster Azure HDInsight.

11. Le nom du cluster de service.
12. Fournissez les propriétés suivantes si vous désirez activer un accès sécurisé au service de catalogue :
 - a. Fournissez le port HTTPS que vous désirez configurer pour le service de catalogue. La valeur par défaut est 9124.
 - b. Appuyez sur **1** si vous désirez utiliser le keystore par défaut généré par le programme d'installation, sinon appuyez sur **2** pour utiliser un fichier keystore personnalisé.
Si vous ne prévoyez pas d'utiliser le fichier keystore généré par le programme d'installation, vérifiez que vous fournissez les certificats SSL dans un format PEM et dans des fichiers keystore Java (JKS). Informatica requiert des noms de fichier de certificat SSL spécifiques pour le domaine Informatica. Vous devez utiliser les mêmes certificats SSL pour tous les nœuds du domaine. Stockez les fichiers truststore et keystore dans un répertoire accessible à tous les nœuds du domaine et spécifiez le même répertoire de fichiers keystore et truststore pour tous les nœuds d'un même domaine.

Si vous avez sélectionné l'option pour utiliser un fichier keystore personnalisé, fournissez les informations suivantes :

1. Chemin d'accès au fichier keystore.
 2. L'alias keystore.
 3. Mot de passe du fichier keystore.
 4. Mot de passe du keystore Solr.
13. Sélectionnez la taille du chargement de métadonnées que vous désirez introduire dans le catalogue à partir des options suivantes :
- démo
 - faible
 - moyenne
 - élevée

Installation d'Enterprise Data Catalog en mode silencieux

Pour installer Enterprise Data Catalog sans interaction utilisateur, effectuez l'installation en mode silencieux. Utilisez un fichier de propriétés pour spécifier les options d'installation. Le programme d'installation lit le fichier pour déterminer les options d'installation. Vous pouvez utiliser l'installation en mode silencieux pour installer les services Informatica sur plusieurs machines du réseau ou pour standardiser l'installation entre les machines.

Copiez les fichiers d'installation d'Enterprise Data Catalog sur le disque dur de la machine sur laquelle vous prévoyez d'installer Enterprise Data Catalog. Si vous l'installez sur une machine distante, vérifiez que vous pouvez accéder aux fichiers et les créer sur la machine distante.

Pour effectuer l'installation en mode silencieux, effectuez les tâches suivantes :

1. Configurer le fichier de propriétés de l'installation et spécifier les options d'installation dans ce fichier.
2. Exécuter le programme d'installation avec le fichier de propriétés de l'installation.
3. Sécuriser les mots de passe dans le fichier de propriétés de l'installation.

Configuration du fichier de propriétés

Informatica fournit un exemple de fichier de propriétés qui contient les paramètres requis par le programme d'installation d'Enterprise Data Catalog. Vous pouvez personnaliser l'exemple de fichier de propriétés pour spécifier les options pour votre installation. Ensuite, exécutez l'installation silencieuse.

L'exemple de fichier `SilentInput.properties` est stocké dans le répertoire racine du DVD ou l'emplacement de téléchargement du programme d'installation. Après avoir personnalisé le fichier, enregistrez à nouveau le fichier avec le nom du fichier `SilentInput.properties`.

1. Accédez au répertoire racine qui contient les fichiers d'installation.
2. Recherchez l'exemple de fichier `SilentInput.properties`.
3. Créez une copie de sauvegarde du fichier `SilentInput.properties`.

4. Utilisez un éditeur de texte pour ouvrir le fichier et modifier les valeurs des paramètres d'installation. Le tableau suivant décrit les paramètres d'installation que vous pouvez modifier :

Nom de la propriété	Description
RESUME_INSTALLATION	Définissez la propriété sur True si vous désirez reprendre l'installation à partir du point d'échec ou de sortie. La valeur par défaut est False.
LICENSE_KEY_LOC	Chemin absolu et nom du fichier de clé de licence.
USER_INSTALL_DIR	Répertoire dans lequel Enterprise Data Catalog est installé.
HTTPS_ENABLED	Indique s'il faut sécuriser la connexion à Informatica Administrator. Si la valeur est 0, le programme d'installation établit une connexion HTTP non sécurisée vers Informatica Administrator. Si la valeur est 1, le programme d'installation établit une connexion HTTPS sécurisée vers Informatica Administrator.
DEFAULT_HTTPS_ENABLED	Indique si le programme d'installation crée un fichier keystore. Si la valeur est 1, le programme d'installation crée un fichier keystore et l'utilise pour la connexion HTTPS. Si la valeur est 0, le programme d'installation utilise le fichier keystore que vous spécifiez.
CUSTOM_HTTPS_ENABLED	Indique si le programme d'installation utilise un fichier keystore existant. Si la valeur est 1, le programme d'installation utilise le fichier keystore que vous spécifiez. Si DEFAULT_HTTPS_ENABLED=1, vous devez définir ce paramètre à 0. Si DEFAULT_HTTPS_ENABLED=0, vous devez définir ce paramètre à 1.
KSTORE_PSSWD	Mot de passe en texte clair pour le fichier keystore.
KSTORE_FILE_LOCATION	Chemin absolu et nom du fichier keystore.
HTTPS_PORT	Numéro de port à utiliser pour la connexion sécurisée à Informatica Administrator. La valeur par défaut est 8443.
CREATE_DOMAIN	Indique s'il faut créer un domaine Informatica. Si la valeur est 1, le programme d'installation crée un nœud et un domaine Informatica. Si la valeur est 0, le programme d'installation crée un nœud et joint le nœud à un autre domaine créé dans une installation précédente.
KEY_DEST_LOCATION	Répertoire dans lequel stocker la clé de cryptage sur le nœud créé lors de l'installation.
PASS_PHRASE_PASSWD	Mot clé à utiliser pour créer une clé de cryptage personnalisée permettant de sécuriser les données sensibles du domaine. Le mot clé doit respecter les critères suivants : <ul style="list-style-type: none"> - Il comporte entre 8 et 20 caractères. - Il doit inclure au moins une lettre en majuscule. - Il doit inclure au moins une lettre en minuscule. - Il doit inclure au moins un chiffre. - Il ne doit pas contenir d'espaces.

Nom de la propriété	Description
JOIN_DOMAIN	Indique s'il faut joindre le nœud à un autre domaine créé dans une installation précédente. Si la valeur est 1, le programme d'installation crée un nœud et joint le nœud à un autre domaine. Si CREATE_DOMAIN=1, vous devez définir ce paramètre à 0. Si CREATE_DOMAIN=0, vous devez définir ce paramètre à 1.
KEY_SRC_LOCATION	Répertoire contenant la clé de cryptage sur le nœud principal de passerelle du domaine Informatica que vous voulez joindre.
SSL_ENABLED	Active ou désactive la communication sécurisée entre les services dans le domaine Informatica. Indique s'il faut définir des communications sécurisées entre les services dans un domaine. Si la valeur est True, les communications sécurisées entre les services du domaine sont définies. Vous pouvez définir cette propriété comme True si CREATE_DOMAIN=1. Vous devez définir cette propriété comme True si JOIN_DOMAIN=1.
SECURITY_DOMAIN_NAME	Nom du domaine de sécurité par défaut du domaine auquel vous joignez le nœud que vous créez. La propriété représente le nom LDAP d'un domaine activé pour Kerberos.
TLS_CUSTOM_SELECTION	Indique si vous souhaitez utiliser les certificats SSL que vous fournissez pour activer la communication sécurisée dans le domaine Informatica. Pour utiliser les certificats SSL que vous fournissez, définissez cette propriété sur la valeur True.
NODE_KEYSTORE_DIR	Obligatoire si la propriété TLS_CUSTOM_SELECTION est définie sur la valeur True. Répertoire contenant les fichiers keystore. Il doit contenir les fichiers infa_keystore.jks et infa_keystore.pem.
NODE_KEYSTORE_PASSWD	Obligatoire si la propriété TLS_CUSTOM_SELECTION est définie sur la valeur True. Mot de passe du fichier keystore infa_keystore.jks.
NODE_TRUSTSTORE_DIR	Obligatoire si la propriété TLS_CUSTOM_SELECTION est définie sur la valeur True. Répertoire contenant les fichiers truststore. Il doit contenir les fichiers infa_truststore.jks et infa_truststore.pem.
NODE_TRUSTSTORE_PASSWD	Obligatoire si la propriété TLS_CUSTOM_SELECTION est définie sur la valeur True. Mot de passe du fichier infa_truststore.jks.
SERVES_AS_GATEWAY	Indique s'il faut créer une passerelle ou un nœud de travail. Si la valeur est 1, le programme d'installation configure le nœud comme nœud de passerelle. Si la valeur est 0, le programme d'installation configure le nœud comme nœud de travail.
DB_TYPE	Base de données pour le référentiel de configuration du domaine. Entrez l'une des valeurs suivantes : - Oracle - MSSQLServer - DB2 - Sybase

Nom de la propriété	Description
DB_UNAME	Nom du compte utilisateur de la base de données pour le référentiel de configuration du domaine.
DB_PASSWD	Mot de passe du compte utilisateur de la base de données.
DB_SSL_ENABLED	Indique si la base de données du référentiel de configuration du domaine est sécurisée. Pour créer le référentiel de configuration du domaine dans une base de données sécurisée, définissez ce paramètre sur la valeur True. Si ce paramètre est défini sur la valeur True, vous devez fournir la chaîne de connexion JDBC sécurisée avec les paramètres de base de données sécurisée.
TRUSTSTORE_DB_FILE	Chemin d'accès et nom du fichier truststore de la base de données sécurisée.
TRUSTSTORE_DB_PASSWD	Mot de passe du fichier Truststore.
SQLSERVER_SCHEMA_NAME	Pour Microsoft SQL Server. Nom du schéma qui contiendra les tables de configuration du domaine. Si ce paramètre est vide, le programme d'installation crée les tables dans le schéma par défaut.
TRUSTED_CONNECTION	Pour Microsoft SQL Server. Indique s'il faut se connecter à Microsoft SQL Server via une connexion de confiance. Si l'option n'est pas sélectionnée, le programme d'installation utilise l'authentification de Microsoft SQL Server. Définissez ce paramètre sur 0 pour l'installation Linux.
DB2_TABLESPACE	Pour IBM DB2. Nom de l'espace de table dans lequel les tables sont créées. Spécifiez un espace de table qui correspond aux spécifications de pageSize de 32 768 octets. Dans une base de données à partition unique, si DB2_TABLESPACE est vide, le programme d'installation crée les tables dans l'espace de table par défaut. Dans une base de données à plusieurs partitions, définissez l'espace de table dans la partition de catalogue de la base de données.
DB_CUSTOM_STRING_SELECTION	Détermine s'il faut utiliser une URL JDBC ou une chaîne de connexion personnalisée pour se connecter à la base de données de configuration du domaine. Si la valeur est 0, le programme d'installation crée une URL JDBC à partir des propriétés de la base de données que vous fournissez. Si la valeur est 1, le programme d'installation utilise la chaîne de connexion personnalisée que vous fournissez. Si vous créez le référentiel de configuration du domaine sur une base de données sécurisée, définissez ce paramètre sur 1.
DB_SERVICENAME	Requis si DB_CUSTOM_STRING_SELECTION=0. Nom du service pour les bases de données Oracle et IBM DB2. Nom de la base de données pour Microsoft SQL Server et Sybase ASE.
DB_ADDRESS	Requis si DB_CUSTOM_STRING_SELECTION=0. Nom d'hôte et numéro de port pour l'instance de base de données au format <i>HostName:Port</i> .

Nom de la propriété	Description
ADVANCE_JDBC_PARAM	Vous pouvez définir ce paramètre si DB_CUSTOM_STRING_SELECTION=0. Paramètres facultatifs à inclure dans la chaîne de connexion de l'URL JDBC. Vérifiez que la chaîne de paramètre est valide. Le programme d'installation ne valide pas la chaîne de paramètre avant de l'ajouter à l'URL JDBC. Si ce paramètre est vide, le programme d'installation crée l'URL JDBC sans paramètres supplémentaires.
DB_CUSTOM_STRING	Requis si DB_CUSTOM_STRING_SELECTION=1. Chaîne de connexion JDBC personnalisée valide.
DOMAIN_NAME	Si vous créez un domaine, il s'agit du nom du domaine à créer. Si vous joignez un domaine, il s'agit du nom du domaine à joindre qui a été créé dans une installation précédente. Le nom de domaine par défaut est Domain_<MachineName>. Le nom ne doit pas dépasser 128 caractères et doit être en ASCII 7 bits uniquement. Il ne peut pas contenir d'espaces ni les caractères spéciaux suivants : ` % * + ; " ? , < > \ /
DOMAIN_HOST_NAME	Si vous créez un domaine, c'est le nom de la machine sur laquelle le nœud est créé. Le nom d'hôte du nœud ne peut pas contenir le caractère de soulignement (_). Si la machine a un nom de réseau unique, utilisez le nom d'hôte par défaut. Si la machine dispose de plusieurs noms de réseau, vous pouvez modifier le nom d'hôte par défaut pour utiliser un autre nom de réseau. Vous pouvez éventuellement utiliser l'adresse IP. Si vous effectuez une jointure de domaine, c'est le nom d'hôte de la machine qui héberge le nœud passerelle du domaine que voulez joindre. Remarque : n'utilisez pas localhost. Le nom d'hôte doit explicitement identifier la machine.
NODE_NAME	Requis si CREATE_DOMAIN=1. Nom du nœud à créer sur cette machine. Le nom du nœud n'est pas le nom d'hôte de la machine.
DOMAIN_PORT	Si vous créez un domaine, c'est le numéro de port du nœud à créer. Le numéro de port par défaut pour le nœud est 6005. Si le numéro de port par défaut n'est pas disponible sur la machine, le programme d'installation affiche le numéro de port suivant disponible. Si vous effectuez une jointure de domaine, c'est le numéro de port du nœud passerelle du domaine que voulez joindre.
DOMAIN_USER	Nom d'utilisateur de l'administrateur du domaine. Si vous créez un domaine, vous pouvez utiliser ce nom d'utilisateur pour vous connecter la première fois à Informatica Administrator. Utilisez les directives suivantes : <ul style="list-style-type: none"> - Le nom n'est pas sensible à la casse et ne doit pas dépasser 128 caractères. - Le nom ne doit pas contenir de tabulation, de caractère nouvelle ligne ou les caractères spéciaux suivants : % * + \ / ' . ? ; < > - Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Tous les autres caractères d'espacement sont interdits. Si vous effectuez une jointure de domaine, c'est le nom d'utilisateur pour la connexion au domaine que voulez joindre.

Nom de la propriété	Description
DOMAIN_PSSWD	Mot de passe de l'administrateur du domaine. Le mot de passe doit contenir plus de 2 caractères et ne doit pas dépasser 16 caractères.
DOMAIN_CNFRM_PSSWD	Entrez une nouvelle fois le mot de passe pour le confirmer.
JOIN_NODE_NAME	Requis si JOIN_DOMAIN=1. Nom de nœud que vous joignez au domaine. Le nom du nœud n'est pas le nom d'hôte de la machine.
JOIN_HOST_NAME	Requis si JOIN_DOMAIN=1. Nom d'hôte de la machine sur laquelle créer le nœud que vous joignez au domaine. Le nom d'hôte du nœud ne peut pas contenir le caractère de soulignement (_). Remarque : n'utilisez pas localhost. Le nom d'hôte doit explicitement identifier la machine.
JOIN_DOMAIN_PORT	Requis si JOIN_DOMAIN=1. Numéro de port du nœud de passerelle du domaine que voulez joindre.
ADVANCE_PORT_CONFIG	Indique s'il faut afficher la liste des numéros de port pour le domaine et les composants de nœud. Si la valeur est 0, le programme d'installation affecte les numéros de port par défaut au domaine et aux composants de nœud. Si la valeur est 1, vous pouvez définir les numéros de port pour le domaine et les composants de nœud.
MIN_PORT	Vous pouvez définir ce paramètre si ADVANCE_PORT_CONFIG=1. Plus petit numéro de port de la plage des numéros de port pouvant être attribués aux processus de service d'application exécutés sur ce nœud.
MAX_PORT	Vous pouvez définir ce paramètre si ADVANCE_PORT_CONFIG=1. Plus grand numéro de port de la plage des numéros de port pouvant être attribués aux processus de service d'application exécutés sur ce nœud.
TOMCAT_PORT	Vous pouvez définir ce paramètre si ADVANCE_PORT_CONFIG=1. Numéro de port utilisé par le Gestionnaire de service sur le nœud. Le gestionnaire de service écoute les demandes de connexions entrantes sur ce port. Les applications clientes utilisent ce port pour communiquer avec les services du domaine. Il s'agit du port que les programmes de ligne de commande Informatica utilisent pour communiquer avec le domaine. Ce port est également utilisé par le pilote JDBC/ODBC du service de données SQL. La valeur par défaut est 6006.
AC_PORT	Vous pouvez définir ce paramètre si CREATE_DOMAIN=1 et ADVANCE_PORT_CONFIG=1. Numéro de port utilisé par Informatica Administrator. La valeur par défaut est 6007.
SERVER_PORT	Vous pouvez définir ce paramètre si ADVANCE_PORT_CONFIG=1. Numéro de port qui contrôle l'arrêt du serveur pour le Gestionnaire de service du domaine. Le gestionnaire de service écoute les commandes d'arrêt sur ce port. La valeur par défaut est 6008.

Nom de la propriété	Description
AC_SHUTDWN_PORT	Vous pouvez définir ce paramètre si CREATE_DOMAIN=1 et ADVANCE_PORT_CONFIG=1. Numéro de port qui contrôle l'arrêt du serveur pour Informatica Administrator. Informatica Administrator écoute les demandes d'arrêt sur ce port. La valeur par défaut est 6009.
ENABLE_USAGE_COLLECTION	Active Informatica DiscoveryIQ, un outil d'utilisation du produit qui envoie des rapports de routine sur l'utilisation des données et les statistiques système à 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 savoir comment désactiver l'envoi de statistiques d'utilisation, consultez le Guide d'Informatica Administrator. Vous devez définir la valeur sur 1 pour appliquer le HotFix.

5. Vous pouvez éventuellement créer un service de référentiel modèle et un service d'intégration de données lors de l'installation. Le tableau suivant décrit les propriétés que vous devez définir si vous souhaitez créer un service de référentiel modèle et un service d'intégration de données lors de l'installation :

Propriété	Description
CREATE_SERVICES	Active la création d'un service de référentiel modèle et d'un service d'intégration de données lors de l'installation. Définissez la valeur sur 1 pour activer la création des services pendant l'installation. La valeur par défaut est 0.
KERBEROS_SECURITY_DOMAIN_NAME	Nom du domaine de sécurité Kerberos. Vous devez entrer le nom du domaine de sécurité Kerberos si l'authentification Kerberos est activée sur ce domaine.
KERBEROS_DOMAIN_PSSWD	Mot de passe du domaine de sécurité Kerberos. Vous devez entrer le mot de passe du domaine de sécurité Kerberos si l'authentification Kerberos est activée sur ce domaine.
MRS_DB_TYPE	Le type de base de données du référentiel modèle. Entrez l'une des valeurs suivantes : - Oracle - DB2 - MSSQLServer
MRS_DB_UNAME	Nom du compte utilisateur de base de données pour la base de données du référentiel modèle.
MRS_DB_PASSWD	Mot de passe du compte utilisateur de la base de données.

Propriété	Description
MRS_DB_SSL_ENABLED	Indique si la base de données devant accueillir la base de données du référentiel modèle est sécurisée. Pour créer la base de données du référentiel modèle dans une base de données sécurisée, définissez ce paramètre sur la valeur True. Si ce paramètre est défini sur la valeur True, vous devez fournir la chaîne de connexion JDBC sécurisée avec les paramètres de base de données sécurisée.
MRS_SSL_DEFAULT_STRING	Paramètres de sécurité pour la chaîne de connexion JDBC utilisée pour la Connexion de base de données du référentiel modèle. Par exemple : EncryptionMethod=SSL;HostNameInCertificate=;ValidateServerCertificate=
TRUSTSTORE_MRS_DB_FILE	Chemin et nom du fichier truststore de la base de données sécurisée du référentiel modèle.
TRUSTSTORE_MRS_DB_PASSWD	Mot de passe du fichier truststore de la base de données sécurisée du référentiel modèle.
MRS_SQLSERVER_SCHEMA_NAME	Pour Microsoft SQL Server. Nom du schéma qui contiendra les tables du référentiel modèle. Si ce paramètre est vide, le programme d'installation crée les tables dans le schéma par défaut.
MRS_DB2_TABLESPACE	Pour IBM DB2. Nom de l'espace de table dans lequel créer les tables pour le référentiel modèle. Spécifiez un espace de table qui correspond aux spécifications de pageSize de 32 768 octets. Dans une base de données à partition unique, si DB2_TABLESPACE est vide, le programme d'installation crée les tables dans l'espace de table par défaut. Dans une base de données à plusieurs partitions, définissez l'espace de table dans la partition de catalogue de la base de données.
MRS_DB_CUSTOM_STRING_SELECTION	Détermine si une URL JDBC ou une chaîne de connexion personnalisée doit être utilisée pour la Connexion de base de données du référentiel modèle. Si la valeur est 0, le programme d'installation crée une URL JDBC à partir des propriétés de la base de données que vous fournissez. Si la valeur est 1, le programme d'installation utilise la chaîne de connexion personnalisée que vous fournissez. Si vous créez la base de données du référentiel modèle sur une base de données sécurisée, définissez ce paramètre sur 1.
MRS_DB_SERVICENAME	Nom du service ou de la base de données pour la base de données du référentiel modèle. Requis si MRS_DB_CUSTOM_STRING_SELECTION=0. Si le référentiel modèle se trouve sur une base de données Oracle ou IBM DB2, définissez cette propriété sur le nom du service. Si le référentiel modèle se trouve sur une base de données Microsoft SQL Server ou Sybase ASE, définissez cette propriété sur le nom de la base de données.

Propriété	Description
MRS_DB_ADDRESS	Requis si MRS_DB_CUSTOM_STRING_SELECTION=0. Nom d'hôte et numéro de port de l'instance de la base de données au format <i>HostName:Port</i> .
MRS_ADVANCE_JDBC_PARAM	Vous pouvez définir ce paramètre si MRS_DB_CUSTOM_STRING_SELECTION=0. Paramètres facultatifs à inclure dans la chaîne de connexion de l'URL JDBC. Vérifiez que la chaîne de paramètre est valide. Le programme d'installation ne valide pas la chaîne de paramètre avant de l'ajouter à l'URL JDBC. Si ce paramètre est vide, le programme d'installation crée l'URL JDBC sans paramètres supplémentaires.
MRS_DB_CUSTOM_STRING	Requis si MRS_DB_CUSTOM_STRING_SELECTION=1. Chaîne de connexion JDBC personnalisée valide.
MRS_SERVICE_NAME	Nom du service de référentiel modèle.
MRS_KEYTAB_FILELOC	Requis si ENABLE_KERBEROS=1 et SPN_SHARE_LEVEL=PROCESS Répertoire où est stocké le fichier Keytab du service de référentiel modèle. Dans le domaine Informatica, le nom de tout fichier Keytab doit suivre un format défini par Informatica.
DIS_SERVICE_NAME	Nom du service d'intégration de données.
DIS_KEYTAB_FILELOC	Requis si ENABLE_KERBEROS=1 et SPN_SHARE_LEVEL=PROCESS Répertoire où est stocké le fichier Keytab du service d'intégration de données. Dans le domaine Informatica, le nom de tout fichier Keytab doit suivre un format défini par Informatica.
DIS_PROTOCOL_TYPE	Type de protocole HTTP du service d'intégration de données. Utilisez l'une des valeurs suivantes : - http - https - les deux
DIS_HTTP_PORT	Requis si DIS_PROTOCOL_TYPE est défini sur http ou sur both. Port HTTP du service d'intégration de données.
DIS_HTTPS_PORT	Requis si DIS_PROTOCOL_TYPE est défini sur https ou sur both. Port HTTPS du service d'intégration de données.

Propriété	Description
DIS_CUSTOM_SELECTION	Paramètre facultatif si vous définissez la valeur de DIS_PROTOCOL_TYPE sur https ou sur both. Si vous définissez cette propriété sur la valeur True, vous fournissez les certificats SSL pour sécuriser le service d'intégration de données. Vous devez fournir les fichiers keystore et truststore qui doivent être utilisés pour sécuriser le service d'intégration de données.
DIS_KEYSTORE_DIR	Requis si DIS_CUSTOM_SELECTION est défini sur la valeur True. Emplacement du fichier keystore du service d'intégration de données.
DIS_KEYSTORE_PASSWD	Requis si DIS_CUSTOM_SELECTION est défini sur la valeur True. Mot de passe du fichier keystore du service d'intégration de données.
DIS_TRUSTSTORE_DIR	Requis si DIS_CUSTOM_SELECTION est défini sur la valeur True. Emplacement du fichier truststore du service d'intégration de données.
DIS_TRUSTSTORE_PASSWD	Requis si DIS_CUSTOM_SELECTION est défini sur la valeur True. Mot de passe du fichier truststore du service d'intégration de données.

6. Le tableau suivant répertorie les paramètres d'Enterprise Data Catalog que vous pouvez configurer :

Propriété	Description
INSTALL_TYPE	Indiquez si vous souhaitez installer ou mettre à niveau Informatica : - Définissez INSTALL_TYPE=0 pour installer Informatica. - Définissez INSTALL_TYPE=1 pour mettre à niveau Informatica. Remarque: - Utilisez le fichier SilentInput_upgrade.properties pour mettre à niveau Informatica. - Utilisez le fichier SilentInput_upgrade_NewConfig.properties pour mettre à niveau Informatica vers une configuration de nœud différente.
INSTALL_LDM	Indiquez si vous souhaitez installer les services Informatica seuls ou avec Enterprise Data Catalog : - Définissez INSTALL_LDM=0 pour installer Informatica sans les services d'Enterprise Data Catalog. - Définissez INSTALL_LDM=1 pour installer Informatica avec les services d'Enterprise Data Catalog.

Propriété	Description
CLUSTER_HADOOP_DISTRIBUTION_TYPE	Définissez ce champ sur une des valeurs suivantes si vous avez spécifié CLUSTER_TYPE=2 : <ul style="list-style-type: none"> - Définissez ce champ sur <i>HortonWorks</i>, <i>ClouderaManager</i> ou <i>HDInsight</i> si vous connaissez l'URL, le nom d'utilisateur et le mot de passe du cluster. - Définissez cette valeur de champ sur <i>Autres</i> si vous ne connaissez pas l'URL, le nom d'utilisateur et le mot de passe du cluster.
KDC_TYPE	S'applique au cluster Hadoop intégré activé pour Kerberos géré par Informatica. Cette propriété fait référence au type de centre de distribution de clés du cluster Hadoop. Vous pouvez choisir un KDC MIT ou Microsoft Active Directory. Définissez cette propriété si CLUSTER_TYPE=1 et IS_CLUSTER_SECURE=true. Remarque: N'utilisez pas cette propriété si le cluster n'est pas activé pour Kerberos.
LDAP_URL	S'applique au cluster Hadoop intégré activé pour Kerberos géré par Informatica. Cette propriété indique que le KDC Microsoft Active Directory est utilisé pour l'authentification et représente l'URL de l'annuaire du serveur LDAP.
CONTAINER_DN	S'applique au cluster Hadoop intégré activé pour Kerberos géré par Informatica. Cette propriété indique que le KDC Microsoft Active Directory est utilisé pour l'authentification et représente le nom unique du conteneur auquel l'utilisateur appartient.
KDC_HOST	Nom de la machine hôte du KDC. Définissez cette propriété si vous avez configuré CLUSTER_TYPE=1 et IS_CLUSTER_SECURE=true. Si vous avez configuré CLUSTER_TYPE=2, n'utilisez pas la propriété.
IHS_REALM	Nom du domaine Kerberos sur la machine qui héberge le serveur KDC. Définissez cette propriété si vous avez configuré CLUSTER_TYPE=1 et IS_CLUSTER_SECURE=true. Si vous avez configuré CLUSTER_TYPE=2, n'utilisez pas la propriété.
IHS_ADMINISTRATOR_SERVER_HOST	Le nom de la machine du serveur administrateur qui héberge le serveur KDC. Définissez cette propriété si vous avez configuré CLUSTER_TYPE=1 et IS_CLUSTER_SECURE=true. Si vous avez configuré CLUSTER_TYPE=2, n'utilisez pas la propriété.
IHS_ADMINISTRATOR_PRINCIPAL	L'administrateur principal de Kerberos. Définissez cette propriété si vous avez configuré CLUSTER_TYPE=1 et IS_CLUSTER_SECURE=true. Si vous avez configuré CLUSTER_TYPE=2, n'utilisez pas la propriété.
IHS_ADMINISTRATOR_PASSWORD	Le mot de passe de l'administrateur de Kerberos. Définissez cette propriété si vous avez configuré CLUSTER_TYPE=1 et IS_CLUSTER_SECURE=true. Si vous avez configuré CLUSTER_TYPE=2, n'utilisez pas la propriété.

Propriété	Description
KERBEROS_CONF_FILE_LOC	Emplacement du fichier <code>krb5.conf</code> . Vous devez spécifier la propriété du cluster Hadoop incorporé activé pour Kerberos ou le cluster Hadoop existant activé pour Kerberos dans l'entreprise.
CATALOGE_SERVICE_KEYTAB_LOCATION	Emplacement du fichier keytab que vous avez spécifié pour le service de catalogue. Définissez cette propriété si vous aviez configuré les propriétés suivantes : <ul style="list-style-type: none"> - CLUSTER_TYPE=1 - IS_CLUSTER_SECURE=true - Si le service de catalogue est configuré dans un cluster Hadoop intégré Si vous aviez configuré CLUSTER_TYPE=2, n'utilisez pas la propriété.
CLUSTER_HADOOP_DISTRIBUTION_URL_USER	Le nom d'utilisateur pour accéder à l'URL de distribution Hadoop. Spécifiez la propriété si vous aviez configuré Cloudera Manager, HortonWorks ou HDInsight pour CLUSTER_HADOOP_DISTRIBUTION_TYPE
CLUSTER_HADOOP_DISTRIBUTION_URL_PASSWD	Le mot de passe du nom d'utilisateur utilisé pour accéder à l'URL de distribution Hadoop. Spécifiez la propriété si vous aviez configuré Cloudera Manager, HortonWorks ou HDInsight pour CLUSTER_HADOOP_DISTRIBUTION_TYPE
INFA_SERVICES_INSTALLED	Détermine s'il faut installer Enterprise Data Catalog avec ou sans Informatica. Définissez INFA_SERVICES_INSTALLED=true, si la version actuelle d'Informatica est déjà installée et que vous ne souhaitez installer qu'Enterprise Data Catalog. Définissez INFA_SERVICES_INSTALLED=false, si la version actuelle d'Informatica n'est pas installée et que vous souhaitez installer Enterprise Data Catalog.
CLUSTER_TYPE	Spécifiez 1 pour un cluster Hadoop incorporé. Le programme d'installation crée un service de cluster Informatica pour la configuration de l'hôte et de l'agent de serveur Ambari, puis crée un service de catalogue. Spécifiez 2 pour un cluster Hadoop existant. Le programme d'installation crée le service de catalogue.
ASSOCIATE_PROFILE_CONNECTION	Définissez la valeur sur 1 pour associer une connexion et une base de données de l'entrepôt de profils au service d'intégration de données. Définissez la valeur sur 0 si vous ne souhaitez pas associer la connexion et la base de données de l'entrepôt de profils au service d'intégration de données.
PWH_DB_TYPE	Représente le type de base de données pour la connexion de l'entrepôt de profils. Définissez la propriété sur un des types de bases de données suivants : Oracle ou DB2. Les options de types de bases de données répertoriées sont sensibles à la casse.
PWH_DB_UNAME	Représente le nom de compte utilisateur de base de données pour le référentiel de configuration du domaine.

Propriété	Description
PWH_DB_PASSWD	Représente le mot de passe de base de données pour le compte utilisateur de base de données.
PWH_SQLSERVER_SCHEMA_NAME	Représente le nom du schéma qui contient des tables de configuration du domaine. Définissez cette propriété si DB_TYPE=MSSQLServer. Si PWH_SQLSERVER_SCHEMA_NAME est vide, le programme d'installation crée les tables dans le schéma par défaut.
PWH_DB2_TABLESPACE	Représente le nom de l'espace de table dans lequel les tables doivent être créées. Définissez la propriété si DB_TYPE=DB2. Spécifiez un espace de table qui correspond à la configuration requise de pageSize de 32 768 octets. Dans une base de données à partition unique, si PWH_DB2_TABLESPACE est vide, le programme d'installation crée les tables dans l'espace de table par défaut. Dans une base de données à plusieurs partitions, définissez l'espace de table dans la partition de catalogue de la base de données.
PWH_DB_CUSTOM_STRING_SELECTION	Détermine s'il faut utiliser une URL JDBC ou une chaîne de connexion personnalisée pour se connecter à la base de données de configuration du domaine. Définissez PWH_DB_CUSTOM_STRING_SELECTION=1 si PWH_TRUSTED_CONNECTION=1. Fournissez la chaîne de connexion valide par défaut dans PWH_DB_CUSTOM_STRING. Si vous spécifiez 0, le programme d'installation crée une URL JDBC à partir des propriétés de la base de données que vous fournissez. Si vous spécifiez 1, le programme d'installation utilise la chaîne de connexion personnalisée que vous fournissez.
PWH_DB_SERVICENAME	Représente le nom de service ou de la base de données. Définissez la propriété si PWH_DB_CUSTOM_STRING_SELECTION=0. Définissez la propriété sur le nom de service pour les bases de données Oracle et IBM DB2. Définissez la propriété sur le nom des bases de données Microsoft SQL Server et Sybase ASE. Laissez la propriété vide si PWH_DB_CUSTOM_STRING_SELECTION=1.
PWH_DB_ADDRESS	Représente le nom d'hôte et le numéro de port de l'instance de base de données. Définissez la propriété si PWH_DB_CUSTOM_STRING_SELECTION=0. Définissez la propriété au format suivant : HostName:PortNumber. Laissez la propriété vide si PWH_DB_CUSTOM_STRING_SELECTION=1.
PWH_ADVANCE_JDBC_PARAM	Représente des paramètres supplémentaires dans la chaîne de connexion de l'URL JDBC. Si PWH_DB_CUSTOM_STRING_SELECTION=0, vous pouvez définir la propriété pour qu'elle comprenne les paramètres facultatifs dans la chaîne de connexion de l'URL JDBC. La chaîne de paramètre doit être valide. Si le paramètre est vide, le programme d'installation crée l'URL JDBC sans paramètres supplémentaires.

Propriété	Description
PWH_DB_CUSTOM_STRING	Représente une chaîne de connexion JDBC personnalisée valide. Définissez la propriété si PWH_DB_CUSTOM_STRING_SELECTION=1.
PWH_DATA_ACCESS_CONNECT_STRING	Fournissez cette chaîne de propriété si ASSOCIATE_PROFILE_CONNECTION=1
LOAD_DATA_DOMAIN	Définissez la valeur de cette propriété sur 1 pour créer le service de gestion de contenu avec la connexion de base de données intermédiaire, puis chargez les domaines de données étendus.
CMS_SERVICE_NAME	Nom du service de gestion de contenu. 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 contenir ni espaces ni l'un des caractères spéciaux suivants : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
CMS_PROTOCOL_TYPE	Spécifiez <code>http</code> ou <code>https</code> pour spécifier le type de protocole. Les options sont sensibles à la casse.
CMS_HTTP_PORT	Numéro de port HTTP pour le service.
CMS_HTTPS_PORT	Numéro de port HTTPS pour le service.
CMS_KEYSTORE_FILE	Chemin et nom du fichier keystore.
CMS_KEYSTORE_PASSWD	Mot de passe du fichier keystore.
CMS_DB_TYPE	Type de base de données pour la connexion à la base de données intermédiaire du service de gestion de contenu. Vous pouvez sélectionner <code>Oracle</code> ou <code>DB2</code> comme type de base de données. Les options de types de bases de données sont sensibles à la casse.
CMS_DB_UNAME	Le nom du compte utilisateur de la base de données pour le référentiel de configuration du domaine.
CMS_DB_PASSWD	Le mot de passe du compte utilisateur de la base de données.
CMS_SQLSERVER_SCHEMA_NAME	Le nom du schéma qui contient les tables de configuration du domaine. Si <code>CMS_SQLSERVER_SCHEMA_NAME</code> est vide, le programme d'installation crée les tables dans le schéma par défaut. Définissez la propriété si <code>DB_TYPE=MSSQLServer</code> .

Propriété	Description
CMS_DB2_TABLESPACE	Le nom de l'espace de table où les tables doivent être créées. Définissez la propriété si DB_TYPE=DB2. Spécifiez un espace de table qui correspond à la configuration requise de pageSize de 32 768 octets. Dans une base de données à partition unique, si CMS_DB2_TABLESPACE est vide, le programme d'installation crée les tables dans l'espace de table par défaut. Dans une base de données à plusieurs partitions, définissez l'espace de table dans la partition de catalogue de la base de données.
CMS_DB_CUSTOM_STRING_SELECTION	Détermine s'il faut utiliser une URL JDBC ou une chaîne de connexion personnalisée pour se connecter à la base de données de configuration du domaine. Définissez CMS_DB_CUSTOM_STRING_SELECTION=1 si CMS_TRUSTED_CONNECTION=1. Fournissez la chaîne de connexion valide par défaut dans CMS_DB_CUSTOM_STRING. Si vous spécifiez 0, le programme d'installation crée une URL JDBC à partir des propriétés de la base de données que vous fournissez. Si vous spécifiez 1, le programme d'installation utilise la chaîne de connexion personnalisée que vous fournissez.
CMS_DB_SERVICENAME	Représente le nom de service ou de la base de données. Définissez la propriété si CMS_DB_CUSTOM_STRING_SELECTION=0. Définissez la propriété sur le nom de service pour les bases de données Oracle et IBM DB2. Définissez la propriété sur le nom des bases de données Microsoft SQL Server et Sybase ASE. Laissez la propriété vide si CMS_DB_CUSTOM_STRING_SELECTION=1.
CMS_DB_ADDRESS	Représente le nom d'hôte et le numéro de port de l'instance de base de données. Définissez la propriété si CMS_DB_CUSTOM_STRING_SELECTION=0. Définissez la propriété au format : HostName:PortNumber. Laissez la propriété vide si CMS_DB_CUSTOM_STRING_SELECTION=1.
CMS_ADVANCE_JDBC_PARAM	Représente des paramètres supplémentaires dans la chaîne de connexion de l'URL JDBC. Si CMS_DB_CUSTOM_STRING_SELECTION=0, vous pouvez définir la propriété pour qu'elle comprenne les paramètres facultatifs dans la chaîne de connexion de l'URL JDBC. Assurez-vous que la chaîne de paramètre est valide. Si la propriété est vide, le programme d'installation crée l'URL JDBC sans paramètres supplémentaires.
CMS_DB_CUSTOM_STRING	Représente une chaîne de connexion JDBC personnalisée valide. Définissez la propriété si CMS_DB_CUSTOM_STRING_SELECTION=1.
CMS_DATA_ACCESS_CONNECT_STRING	Vous devez fournir cette propriété si LOAD_DATA_DOMAIN=1.

Propriété	Description
SERVICE_ENABLE_TLS	Définissez cette propriété sur <code>true</code> pour activer le service de Transport Layer Security (TLS). Vous pouvez laisser cette propriété vide si vous ne souhaitez pas activer TLS pour le service. Si <code>CLUSTER_TYPE=1</code> et <code>SERVICE_ENABLE_TLS=true</code> , le programme d'installation active à la fois le service de cluster Informatica et le service de catalogue pour Secure Sockets Layer (SSL). Si <code>CLUSTER_TYPE=2</code> et <code>SERVICE_ENABLE_TLS=true</code> , le programme d'installation active le service de catalogue pour SSL.
IS_CLUSTER_SSL_ENABLE	Définissez cette propriété sur <code>True</code> si vous possédez un cluster existant activé pour SSL. Si vous ne souhaitez pas activer SSL sur le cluster, laissez cette propriété vide.
IS_CLUSTER_HA_ENABLE	Définissez cette propriété sur <code>True</code> si vous possédez un cluster existant activé pour la haute disponibilité. Si vous ne voulez pas activer la haute disponibilité sur le cluster, laissez cette propriété vide.
IS_CLUSTER_SECURE	Définissez cette propriété sur <code>true</code> si vous avez besoin que le cluster soit activé pour Kerberos. Vous pouvez laisser cette propriété vide si vous ne souhaitez pas activer Kerberos pour le cluster.
GATEWAY_USERNAME	Spécifiez le nom d'utilisateur d'un cluster incorporé dans lequel vous vous connectez à d'autres hôtes à partir de l'hôte domaine Enterprise Data Catalog sans mot de passe SSH. Le nom d'utilisateur par défaut est <code>root</code> . Pour <code>CLUSTER_TYPE=2</code> , laissez cette propriété vide.
HADOOP_SERVICE_NAME	Spécifiez le nom du service de cluster Informatica si <code>CLUSTER_TYPE=1</code> . Laissez cette propriété vide pour <code>CLUSTER_TYPE=2</code> .
HADOOP_SERVICE_PORT	Spécifiez le port du service de cluster Informatica si <code>CLUSTER_TYPE=1</code> . Laissez cette propriété vide pour <code>CLUSTER_TYPE=2</code> . Laissez cette propriété vide si <code>SERVICE_ENABLE_TLS=true</code>
HADOOP_TLS_HTTPS_PORT	Spécifiez le port HTTPS pour le service de cluster Informatica si <code>SERVICE_ENABLE_TLS=true</code> . Laissez cette propriété vide pour <code>CLUSTER_TYPE=2</code> .
HADOOP_KEYSTORE_FILE	Chemin et nom du fichier keystore. Vous devez fournir ce paramètre si <code>SERVICE_ENABLE_TLS=true</code> . Laissez cette propriété vide pour <code>CLUSTER_TYPE=2</code> .
HADOOP_KEYSTORE_ALIAS	Spécifiez l'alias keystore si <code>SERVICE_ENABLE_TLS=true</code> et <code>SSL_ENABLED=true</code> . Laissez cette propriété vide pour <code>CLUSTER_TYPE=2</code> .
HADOOP_KEYSTORE_PASSWD	Spécifiez le mot de passe du fichier keystore si <code>SERVICE_ENABLE_TLS=true</code> . Laissez cette propriété vide pour <code>CLUSTER_TYPE=2</code> .

Propriété	Description
HADOOP_TRUSTSTORE_FILE	Spécifiez l'emplacement du fichier truststore si SSL_ENABLED=true. Laissez cette propriété vide pour CLUSTER_TYPE=2. L'emplacement doit être un emplacement commun présent dans tous les nœuds Hadoop où vous pouvez copier le fichier truststore après l'exportation et l'importation de HADOOP_KEYSTORE_FILE. Définissez cette propriété si le domaine est activé pour SSL.
HADOOP_GATEWAY_HOST	Spécifiez le paramètre de l'hôte de passerelle où le serveur Ambari est installé si CLUSTER_TYPE=1. Laissez cette propriété vide pour CLUSTER_TYPE=2.
HADOOP_NODES	Spécifiez le nom d'hôte de l'agent Ambari séparé par des virgules où l'agent Ambari est installé. Vous devez spécifier cette propriété si CLUSTER_TYPE=1. Laissez cette propriété vide pour CLUSTER_TYPE=2.
HADOOP_GATEWAY_PORT	Spécifiez le port pour connecter le serveur Ambari si CLUSTER_TYPE=1. Laissez cette propriété vide pour CLUSTER_TYPE=2.
CATALOGUE_SERVICE_NAME	Nom du service de catalogue. Vous devez spécifier ce paramètre pour les clusters incorporés et existants.
CATALOGUE_SERVICE_PORT	Le port du service de catalogue. Spécifiez la propriété pour les clusters incorporés et existants. Laissez cette propriété vide pour SERVICE_ENABLE_TLS=true.
CATALOGUE_SERVICE_TLS_HTTPS_PORT	Le port HTTPS du service de cluster Informatica. Spécifiez la propriété si SERVICE_ENABLE_TLS=true pour le cluster existant.
CATALOGUE_SERVICE_KEYSTORE_FILE	Nom de fichier et chemin du fichier keystore du service de catalogue. Vous devez spécifier ce paramètre si SERVICE_ENABLE_TLS=true.
CATALOGUE_SERVICE_KEYSTORE_ALIAS	Spécifiez la propriété de l'alias keystore si SERVICE_ENABLE_TLS=true et SSL_ENABLED=true.
CATALOGUE_SERVICE_KEYSTORE_PASSWD	Spécifiez le mot de passe du fichier keystore si SERVICE_ENABLE_TLS=true.
DOMAIN_KEYSTORE_ALIAS	Spécifiez l'alias keystore de domaine si SERVICE_ENABLE_TLS=true et SSL_ENABLED=true. Vous devez spécifier cette propriété si le domaine est créé en mode SSL et si TLS_CUSTOM_SELECTION=true.
CATALOGUE_SERVICE_SOLR_KEYSTORE_FILE	Nom de fichier et chemin du fichier keystore SOLR pour le service de catalogue. Vous devez spécifier cette propriété si IS_CLUSTER_SSL_ENABLE=true. Assurez-vous que le chemin du fichier pointe vers le cluster et non vers le domaine. Définissez cette propriété si le cluster est activé pour SSL ou Kerberos ou SSL et Kerberos.

Propriété	Description
CATALOGUE_SERVICE_SOLR_KEYSTORE_PASSWD	Mot de passe du fichier keystore SOLR. Vous devez spécifier cette propriété si IS_CLUSTER_SSL_ENABLE=true.
YARN_RESOURCE_MANAGER_URI	L'URI du gestionnaire de ressource YARN. Vous devez spécifier cette propriété si CLUSTER_TYPE=2. Veuillez à spécifier la propriété au format suivant : hostname:port. Laissez cette propriété vide pour CLUSTER_TYPE=1.
YARN_RESOURCE_MANAGER_HTTP_URI	L'URI HTTP du gestionnaire de ressource YARN. Vous devez spécifier cette propriété si CLUSTER_TYPE=2. Veuillez à spécifier la propriété au format suivant : hostname:port. Laissez cette propriété vide pour CLUSTER_TYPE=1.
YARN_RESOURCE_MANAGER_SCHEDULER_URI	L'URI du planificateur du gestionnaire de ressource YARN. Vous devez spécifier ce paramètre si CLUSTER_TYPE=2. Veuillez à spécifier la propriété au format suivant : hostname:port. Laissez cette propriété vide pour CLUSTER_TYPE=1.
ZOOKEEPER_URI	L'URI de ZooKeeper. Spécifiez cette propriété si CLUSTER_TYPE=2. Vous devez spécifier cette propriété au format suivant : zookeeperhost:clientport. Laissez cette propriété vide pour CLUSTER_TYPE=1.
HDFS_HOST_NAME	L'URI du namenode HDFS. Spécifiez ce paramètre si CLUSTER_TYPE=2. Vous devez spécifier cette propriété au format suivant : hostname:port. Laissez cette propriété vide pour CLUSTER_TYPE=1.
SERVICE_CLUSTER_NAME	Nom du cluster de service HDFS. Vous devez spécifier cette propriété si CLUSTER_TYPE=2. La valeur par défaut est DOMAIN_NAME_CATALOGUE_SERVICE_NAME. Laissez cette propriété vide pour CLUSTER_TYPE=1.
HDFS_SERVICE_NAME_HA	Le nom du service HDFS si le cluster est activé pour la haute disponibilité. Vous devez spécifier cette propriété si CLUSTER_TYPE=2 et si IS_CLUSTER_HA_ENABLE=true. Laissez cette propriété vide pour CLUSTER_TYPE=1.
IS_CLUSTER_SECURE	Spécifiez si le cluster est sécurisé ou non. Vous devez configurer cette propriété si CLUSTER_TYPE=2 et si IS_CLUSTER_SECURE=true pour un cluster activé pour Kerberos. Laissez cette propriété vide pour CLUSTER_TYPE=1.
HDFS_SERVICE_PRINCIPAL	Le principal de service pour HDFS. Vous devez spécifier cette propriété si CLUSTER_TYPE=2 et si IS_CLUSTER_SECURE=true pour un cluster activé pour Kerberos. Laissez cette propriété vide pour CLUSTER_TYPE=1.

Propriété	Description
YARN_SERVICE_PRINCIPAL	Le principal de service pour YARN. Vous devez spécifier cette propriété si CLUSTER_TYPE=2 et si IS_CLUSTER_SECURE=true pour un cluster activé pour Kerberos. Laissez cette propriété vide pour CLUSTER_TYPE=1.
KDC_DOMAIN_NAME	Le nom de domaine du centre de distribution de clés Kerberos (KDC). Vous devez spécifier cette propriété si CLUSTER_TYPE=2 et si IS_CLUSTER_SECURE=true pour un cluster activé pour Kerberos. Laissez cette propriété vide pour CLUSTER_TYPE=1.
KDC_KEYTAB_LOCATION	L'emplacement du centre de distribution de clés Kerberos (KDC). Vous devez spécifier ce paramètre si CLUSTER_TYPE=2 et si IS_CLUSTER_SECURE=true pour un cluster activé pour Kerberos. Laissez cette propriété vide pour CLUSTER_TYPE=1.
HISTORY_SERVER_HTTP_URI	L'URI HTTP du serveur d'historique. Vous devez spécifier ce paramètre si CLUSTER_TYPE=2. Laissez cette propriété vide pour CLUSTER_TYPE=1.

7. Enregistrez le fichier de propriétés sous le nom `SilentInput.properties`.

Exécution du programme d'installation silencieux

Après avoir configuré le fichier de propriétés, ouvrez une invite de commande pour démarrer l'installation silencieuse.

1. Ouvrez un shell Linux.
2. Allez à la racine du répertoire qui contient les fichiers d'installation.
3. Vérifiez que le répertoire contient le fichier `SilentInput.properties` que vous avez modifié et réenregistré.
4. Exécutez `silentInstall.sh` pour démarrer l'installation silencieuse.

Le programme d'installation silencieuse s'exécute en arrière-plan. Le processus peut prendre du temps. L'installation silencieuse est terminée lorsque `Informatica_<Version>_Services_InstallLog.log` est créé dans le répertoire d'installation.

L'installation silencieuse échoue si vous n'avez pas configuré le fichier de propriétés correctement ou si le répertoire d'installation n'est pas disponible. Consultez les fichiers journaux de l'installation et corrigez les erreurs. Relancez ensuite l'installation silencieuse.

Installation des services d'application Enterprise Data Catalog en mode silencieux

Si vous n'avez pas installé les services d'application d'Enterprise Data Catalog lorsque vous installez Enterprise Data Catalog, vous pouvez utiliser le programme d'installation pour installer les services d'application. Pour installer les services d'application d'Enterprise Data Catalog sans interaction utilisateur, installez-les en mode silencieux. Utilisez un fichier de propriétés pour spécifier les options d'installation. Le

programme d'installation lit le fichier pour déterminer les options d'installation. Vous pouvez utiliser l'installation en mode silencieux pour installer les services Informatica sur plusieurs machines du réseau ou pour standardiser l'installation entre les machines.

Pour installer les services d'application en mode silencieux, effectuez les tâches suivantes :

1. Configurez le fichier de propriétés de l'installation et spécifiez les options d'installation du service d'application dans ce fichier.
2. Exécutez le programme d'installation avec le fichier de propriétés de l'installation.
3. Sécuriser les mots de passe dans le fichier de propriétés de l'installation.

Configuration du fichier de propriétés

Effectuez les étapes suivantes pour configurer le fichier `SilentInput_configure.properties` :

1. Accédez au répertoire racine qui contient les fichiers d'installation.
2. Recherchez le fichier `SilentInput_configure.properties`.
3. Créez une copie de sauvegarde du fichier `SilentInput_configure.properties`.
4. Utilisez un éditeur de texte pour ouvrir le fichier et spécifiez les valeurs des paramètres de service d'application.

Pour plus d'informations concernant les paramètres de service d'application, consultez la rubrique ["Création des services d'application Enterprise Data Catalog à l'aide du programme d'installation" à la page 96.](#)

5. Enregistrez le fichier.

Exécution du programme d'installation silencieuse pour installer les services

Après avoir configuré le fichier de propriétés, ouvrez une invite de commande pour démarrer l'installation silencieuse.

1. Ouvrez un shell Linux.
2. Accédez au répertoire racine qui contient les fichiers d'installation.
3. Vérifiez que le répertoire contient le fichier `SilentInput_configure.properties` que vous avez modifié et enregistré.
4. Exécutez `silentinstallConfig.sh` pour démarrer l'installation silencieuse.

Le programme d'installation silencieuse s'exécute en arrière-plan. Le processus peut prendre du temps. L'installation en mode silencieux est terminée lorsque le fichier `Informatica_<Version>_Services_InstallLog.log` est créé dans le répertoire d'installation.

L'installation silencieuse échoue si vous n'avez pas configuré le fichier de propriétés correctement ou si le répertoire d'installation n'est pas disponible. Consultez les fichiers journaux de l'installation et corrigez les erreurs. Relancez ensuite l'installation silencieuse.

Sécurisation des mots de passe dans le fichier de propriétés

Après avoir exécuté le programme d'installation silencieuse, vérifiez que les mots de passe dans le fichier de propriétés sont sécurisés.

Lorsque vous configurez le fichier de propriétés pour une installation silencieuse, vous entrez des mots de passe en texte brut. Après avoir exécuté le programme d'installation silencieuse, utilisez l'une des méthodes suivantes pour sécuriser les mots de passe :

- Supprimez les mots de passe du fichier de propriétés.
- Supprimez le fichier de propriétés.
- Stockez le fichier de propriétés dans un emplacement sécurisé.

Partie IV : Après l'installation d'Enterprise Data Catalog

Cette partie contient les chapitres suivants :

- [Configuration du domaine, 129](#)
- [Préparation de la création des services d'application, 134](#)
- [Créer les services d'application, 140](#)
- [Configuration de l'authentification unique avec l'authentification SAML, 159](#)

CHAPITRE 6

Configuration du domaine

Ce chapitre comprend les rubriques suivantes :

- [Présentation de la configuration du domaine, 129](#)
- [Vérification de la compatibilité de la page de code, 129](#)
- [Configuration des variables d'environnement, 130](#)
- [Privilèges du service de catalogue, 132](#)

Présentation de la configuration du domaine

Après avoir installé les services Informatica et avant de créer les services d'application, effectuez la configuration des services du domaine.

La configuration du domaine inclut des tâches telles que la vérification des pages de code, la configuration des variables d'environnement du domaine et la configuration du pare-feu.

Vérification de la compatibilité de la page de code

Les pages de code des services d'applications doivent être compatibles avec celles du domaine.

Vérifiez et configurez les paramètres régionaux et les pages de code :

Vérifiez que la base de données de configuration du domaine est compatible avec les pages de code des services d'applications que vous créez dans le domaine.

Le gestionnaire de service synchronise la liste des utilisateurs du domaine avec la liste des utilisateurs et des groupes de chaque service d'application. Si un nom d'utilisateur du domaine contient des caractères que la page de code du service d'application ne reconnaît pas, les caractères ne sont pas convertis correctement et des incohérences se produisent.

Vérifiez que les paramètres régionaux des machines qui accèdent à l'outil Administrator tool et aux outils clients Informatica sont compatibles avec les pages de code des référentiels du domaine.

Si le paramètre régional n'est pas compatible avec la page de code du référentiel, vous ne pouvez pas créer de service d'application.

Configurer les variables d'environnement régionales sur Linux

Vérifiez que le paramètre régional est compatible avec la page de code pour le référentiel. Si le paramètre régional n'est pas compatible avec la page de code du référentiel, vous ne pouvez pas créer de service d'application.

Utilisez LANG, LC_CTYPE ou LC_ALL pour définir la page de code Linux.

Utilisez la commande suivante pour vérifier que la valeur de la variable d'environnement régionale est compatible avec les paramètres de langue de la machine et le type de page de code à utiliser pour le référentiel :

```
locale -a
```

La commande renvoie les langues installées dans le système d'exploitation Linux et les paramètres régionaux existants.

Définissez les variables d'environnement régionales suivantes :

Paramètre régional sous Linux

Linux permet à différentes valeurs régionales de représenter le même paramètre régional. Par exemple, "utf8," "UTF-8," "UTF8," et "utf-8" représentent le même paramètre régional sur une machine Linux. Informatica exige que vous utilisiez une valeur spécifique pour chaque paramètre régional sur une machine Linux. Assurez-vous de définir de manière appropriée la variable d'environnement LANG pour toutes les machines Linux.

Paramètre régional pour les clients de base de données Oracle

Pour les clients de base de données Oracle, définissez NLS_LANG sur le paramètre régional que vous voulez que le client et le serveur de base de données utilisent avec le nom de connexion. Un paramètre régional comprend la langue, le territoire et le jeu de caractères. La valeur de NLS_LANG dépend de la configuration. Par exemple, si la valeur est american_america.UTF8, définissez la variable dans un shell C à l'aide de la commande suivante :

```
setenv NLS_LANG american_america.UTF8
```

Configuration des variables d'environnement

Enterprise Data Catalog utilise des variables d'environnement pour stocker les informations sur la configuration lors de l'exécution des services d'application et de la connexion aux clients. Configurez les variables d'environnement pour répondre aux prérequis d'Informatica.

Des variables d'environnement incorrectement configurées peuvent empêcher le domaine ou les nœuds Informatica de démarrer ou peuvent entraîner des problèmes de connexion entre les clients Informatica et le domaine.

Pour configurer des variables d'environnement sous Linux, connectez-vous avec le compte utilisateur système que vous avez utilisé pour installer Enterprise Data Catalog.

Configurer les variables d'environnement d'Enterprise Data Catalog

Vous pouvez configurer les variables d'environnement d'Enterprise Data Catalog pour stocker les paramètres de mémoire, de domaine et d'emplacement.

Définissez les variables d'environnement suivantes :

INFA_JAVA_OPTS

Par défaut, Informatica utilise un maximum de 512 Mo de mémoire système.

Si le domaine comporte plus de 1 000 utilisateurs, mettez à jour la taille maximum des segments de mémoire selon le nombre d'utilisateurs dans le domaine.

Vous pouvez utiliser la variable d'environnement INFA_JAVA_OPTS pour configurer la quantité de mémoire système utilisée par Enterprise Data Catalog. Par exemple, pour configurer 1 Go de mémoire système pour le démon Informatica sous Linux dans un shell C, utilisez la commande suivante :

```
setenv INFA_JAVA_OPTS "-Xmx1024m"
```

Redémarrez le nœud pour appliquer les modifications.

INFA_DOMAINS_FILE

Le programme d'installation crée un fichier `domains.infa` dans le répertoire d'installation d'Enterprise Data Catalog. Le fichier `domains.infa` contient les informations de connectivité pour les nœuds de passerelle dans un domaine, dont les noms de domaines, les noms d'hôtes de domaines et les numéros de ports d'hôtes de domaines.

Définissez la valeur de la variable INFA_DOMAINS_FILE sur le chemin d'accès et le nom du fichier `domains.infa`.

Configurez la variable INFA_DOMAINS_FILE sur la machine où vous installez les services d'Enterprise Data Catalog.

INFA_HOME

Utilisez INFA_HOME pour désigner le répertoire d'installation d'Enterprise Data Catalog. Si vous modifiez la structure du répertoire d'Enterprise Data Catalog, vous devez définir la variable d'environnement sur l'emplacement du répertoire d'installation d'Enterprise Data Catalog ou du répertoire dans lequel se trouvent les fichiers installés d'Enterprise Data Catalog.

Par exemple, vous utilisez un lien symbolique sous Linux pour tous les répertoires d'Enterprise Data Catalog. Pour configurer INFA_HOME de sorte que toute application ou tout service d'Enterprise Data Catalog puisse localiser les autres composants d'Enterprise Data Catalog qu'il doit exécuter, définissez INFA_HOME sur l'emplacement du répertoire d'installation d'Enterprise Data Catalog.

INFA_TRUSTSTORE

Si vous activez la communication sécurisée pour le domaine, définissez la variable INFA_TRUSTSTORE avec le répertoire qui contient les fichiers `truststore` des certificats SSL. Le répertoire doit contenir les fichiers `truststore` nommés `infa_truststore.jks` et `infa_truststore.pem`.

Vous devez définir la variable INFA_TRUSTSTORE si vous utilisez le certificat SSL fourni par Informatica ou un certificat que vous indiquez.

INFA_TRUSTSTORE_PASSWORD

Si vous activez la communication sécurisée pour le domaine et que vous spécifiez le certificat SSL à utiliser, définissez la variable INFA_TRUSTSTORE_PASSWORD avec le mot de passe du fichier `infa_truststore.jks` qui contient le certificat SSL. Le mot de passe doit être chiffré. Utilisez le programme de ligne de commande `pmpasswd` pour chiffrer le mot de passe.

Remarque: Veillez à configurer les variables INFA_TRUSTSTORE et INFA_TRUSTSTORE_PASSWORD dans tous les nœuds du cluster.

Configurer les variables d'environnement de chemin de bibliothèque sous Linux

Configurez les variables d'environnement de chemin de bibliothèque sur les machines qui exécutent les processus du service d'intégration de données. Le nom des variables et les prérequis dépendent de la plateforme et de la base de données.

Configurez la variable d'environnement LD_LIBRARY_PATH.

Le tableau suivant décrit les valeurs que vous définissez pour LD_LIBRARY_PATH pour les différentes bases de données :

Base de données	Valeur
Oracle	<DatabasePath>/lib
IBM DB2	<DatabasePath>/lib
Sybase ASE	"\${SYBASE_OCS}/lib:\${SYBASE_ASE}/lib:\${LD_LIBRARY_PATH}"
ODBC	<CLOSEDODBCHOME>/lib

Privilèges du service de catalogue

Les privilèges du service de catalogue déterminent les actions que les utilisateurs peuvent effectuer sur Catalog Administrator et Enterprise Data Catalog.

Le tableau suivant répertorie les privilèges requis dans le groupe Privilèges du catalogue et les actions que les utilisateurs peuvent effectuer :

Nom du privilège	Description
Gestion de catalogue : vue Catalogue	Les utilisateurs peuvent effectuer les actions suivantes : <ul style="list-style-type: none">- Afficher les attributs personnalisés- Rechercher les ressources de données- Filtrer les ressources de données à l'aide de filtres de recherche- Afficher la présentation des ressources de données- Afficher le lignage des ressources de données- Afficher les relations des ressources de données
Gestion de catalogue : modification du catalogue	Les utilisateurs peuvent effectuer les actions suivantes : <ul style="list-style-type: none">- Modifier les attributs personnalisés- Configurer les filtres de recherche- Afficher les filtres de recherche
Gestion de ressource : Admin - Afficher la ressource	Les utilisateurs peuvent effectuer les actions suivantes : <ul style="list-style-type: none">- Afficher la ressource- Afficher la planification

Nom du privilège	Description
Gestion de ressource : Admin - Modifier le profilage	Les utilisateurs peuvent effectuer les actions suivantes : <ul style="list-style-type: none"> - Afficher la ressource - Afficher la planification - Mettre à jour les paramètres du profil - Créer une configuration de profilage global - Mettre à jour la configuration de profilage global - Supprimer la configuration de profilage global - Afficher la configuration de profilage global
Gestion de ressource : Admin - Modifier la ressource	Les utilisateurs peuvent effectuer les actions suivantes : <ul style="list-style-type: none"> - Créer une ressource - Mettre à jour la ressource - Afficher la ressource - Supprimer la ressource - Purger la ressource - Modifier les paramètres de profilage - Créer une planification - Mettre à jour la planification - Supprimer la planification - Afficher la planification - Attribuer la planification à la ressource - Purger la planification - Attribuer la connexion - Annuler l'attribution de la connexion
Admin - Créer un attribut	Les utilisateurs peuvent effectuer les actions suivantes : <ul style="list-style-type: none"> - Mettre à jour l'attribut système - Créer un attribut personnalisé - Mettre à jour l'attribut personnalisé - Supprimer l'attribut personnalisé
Admin - Surveillance	Les utilisateurs peuvent effectuer les actions suivantes : <ul style="list-style-type: none"> - Afficher la tâche de surveillance - Explorer la tâche de surveillance - Reprendre la tâche de surveillance - Interrompre la tâche de surveillance - Annuler la tâche de surveillance - Activer la notification par e-mail

Le tableau suivant répertorie le privilège requis et l'action que les utilisateurs peuvent effectuer avec le privilège dans le groupe Privilèges de l'API :

Nom du privilège	Description
Privilège de l'API REST	Les utilisateurs peuvent effectuer les fonctions d'Enterprise Data Catalog à l'aide des API REST.

CHAPITRE 7

Préparation de la création des services d'application

Ce chapitre comprend les rubriques suivantes :

- [Préparation de la création des services d'application - Présentation, 134](#)
- [Connexion à Informatica Administrator, 134](#)
- [Création de connexions, 135](#)

Préparation de la création des services d'application - Présentation

Avant de créer un service d'application, vérifiez l'installation et la configuration sur les nœuds.

Connectez-vous à l'outil Informatica Administrator et créez des connexions aux bases de données accessibles aux services d'application via la connectivité de cluster.

Connexion à Informatica Administrator

Vous devez disposer d'un compte utilisateur pour vous connecter à l'application Web Informatica Administrator.

Dans Microsoft Internet Explorer et Google Chrome, ajoutez l'URL de l'application Web Informatica à la liste des sites de confiance. Si vous utilisez Chrome version 41 ou ultérieure, vous devez également définir les stratégies AuthServerWhitelist et AuthNegotiateDelegateWhitelist.

1. Démarrez un navigateur Microsoft Internet Explorer ou Google Chrome.
2. Dans le champ **Adresse**, saisissez l'URL de l'outil Administrator tool :
 - Si l'outil Administrator tool n'est pas configuré pour utiliser une connexion sécurisée, entrez l'URL suivante :

```
http://<fully qualified hostname>:<http port>/administrator/
```
 - Si l'outil Administrator tool est configuré pour utiliser une connexion sécurisée, entrez l'URL suivante :

```
https://<fully qualified hostname>:<http port>/administrator/
```

Le nom d'hôte et le port dans l'URL correspondent à ceux du nœud maître de passerelle. Si vous avez configuré une communication sécurisée pour le domaine, vous devez utiliser HTTPS dans l'URL pour pouvoir accéder à l'outil Administrator tool.

3. Saisissez le nom d'utilisateur, le mot de passe et le domaine de sécurité de votre compte utilisateur, puis cliquez sur **Connexion**.

Le champ **Domaine de sécurité** s'affiche lorsque le domaine Informatica contient un domaine de sécurité LDAP. Si vous ne connaissez pas le domaine de sécurité auquel appartient votre compte utilisateur, contactez l'administrateur de domaine Informatica.

Remarque: Si vous vous connectez pour la première fois avec le nom d'utilisateur et le mot de passe fournis par l'administrateur du domaine, modifiez votre mot de passe pour maintenir la sécurité.

Création de connexions

Dans l'outil Administrator tool, créez des connexions aux bases de données utilisées par les services d'application. Vous devez spécifier les détails de connexion durant la configuration du service d'application.

Lorsque vous créez la Connexion de base de données, spécifiez les propriétés de la connexion et testez la connexion.

Le tableau suivant décrit les connexions de base de données que vous devez créer avant de créer les services d'application associés :

Connexion de base de données	Description
Base de données du cache d'objet de données	Pour accéder au cache d'objet de données, créez la connexion du cache d'objet de données pour le service d'intégration de données.
Base de données du flux de travail	Pour stocker les métadonnées d'exécution d'un flux de travail, créez la connexion à la base de données du flux de travail pour le service d'intégration de données.
Base de données de l'entrepôt de profilage	Pour créer et exécuter des profils et des fiches d'évaluation, créez la connexion de base de données de l'entrepôt de profilage pour le service d'intégration de données. Utilisez cette instance du service d'intégration de données lorsque vous configurez les propriétés d'exécution du service Analyst. Remarque: Pour utiliser la base de données Microsoft SQL Server en tant qu'entrepôt de profilage, choisissez ODBC comme type de fournisseur et désactivez l'option Utiliser DSN dans la boîte de dialogue Propriétés de connexion Microsoft SQL Server lorsque vous configurez la connexion Microsoft SQL Server.
Entrepôt de données de référence	Pour stocker les données de table de référence, créez la connexion de l'entrepôt de données de référence pour le service de gestion de contenu.

Propriétés de la connexion IBM DB2

Utilisez une connexion DB2 pour LUW pour accéder aux tables dans une base de données DB2 pour LUW.

Le tableau suivant décrit les propriétés de la connexion de DB2 pour LUW :

Propriété	Description
Nom d'utilisateur	Nom d'utilisateur de la base de données.
Mot de passe	Mot de passe pour le nom d'utilisateur.
Chaîne de connexion pour l'accès aux métadonnées	Chaîne de connexion pour importer des objets de données physiques. Utilisez la chaîne de connexion suivante : <code>jdbc:informatica:db2://<host>:50000;databaseName=<dbname></code>
Chaîne de connexion pour l'accès aux données	Chaîne de connexion pour prévisualiser les données et exécuter les mappages. Entrez <code>dbname</code> depuis l'alias configuré dans le client DB2.
Page de code	Page de code de la base de données.
Environnement SQL	Facultatif. Entrez les commandes SQL pour paramétrer l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute l'environnement de connexion SQL à chaque connexion à la base de données.
Transaction SQL	Facultatif. Entrez les commandes SQL pour paramétrer l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de transaction au début de chaque transaction.
Période de nouvelle tentative	Cette propriété est réservée à une utilisation ultérieure.
Espace de table	Nom d'espace de table de la base de données DB2 pour LUW.
Caractère identificateur SQL	Le type de caractère utilisé pour identifier des caractères spéciaux et des mots clés SQL réservés, tels que WHERE. Le service d'intégration de données place le caractère sélectionné autour des caractères spéciaux et mots clés SQL réservés. Le service d'intégration de données utilise également ce caractère pour la propriété de prise en charge des identifiants à casse mixte.
Prise en charge des identifiants à casse mixte	Lorsque cette option est activée, le service d'intégration de données place les caractères identifiants autour des noms de table, de vue, de schéma, de synonyme et de colonne lors de la génération et de l'exécution de SQL par rapport à ces objets dans la connexion. Utilisez-la si les objets comportent une casse mixte ou des noms en minuscules. Par défaut, cette option n'est pas sélectionnée.

Propriétés de connexion Microsoft SQL Server

Utilisez une connexion Microsoft SQL Server pour accéder aux tables d'une base de données Microsoft SQL Server.

Le tableau suivant décrit les propriétés de la connexion Microsoft SQL Server :

Propriété	Description
Nom d'utilisateur	Nom de l'utilisateur de la base de données.
Mot de passe	Mot de passe pour le nom d'utilisateur.
Utiliser une connexion approuvée	Facultatif. Lorsque cette option est activée, le service d'intégration de données utilise l'authentification Windows pour accéder à la base de données Microsoft SQL Server. Le nom de l'utilisateur qui démarre le service d'intégration de données doit être celui d'un utilisateur Windows valide ayant accès à la base de données Microsoft SQL Server.
Chaîne de connexion pour l'accès aux métadonnées	Chaîne de connexion pour importer des objets de données physiques. Utilisez la chaîne de connexion suivante : <code>jdbc:informatica:sqlserver:// <host>:<port>;databaseName=<dbname></code>
Chaîne de connexion pour l'accès aux données	Chaîne de connexion qui permet de prévisualiser les données et d'exécuter les mappages. Entrez <code><ServerName>@<DBName></code>
Nom de domaine	Facultatif. Nom du domaine où Microsoft SQL Server est en cours d'exécution.
Taille du paquet	Obligatoire. Optimisation de la connexion ODBC de Microsoft SQL Server. Augmentez la taille du paquet pour augmenter les performances. La valeur par défaut est 0.
Page de code	Page de code de la base de données.
Nom du propriétaire	Nom du propriétaire du schéma. Spécifiez les connexions à la base de données de l'entrepôt de profilage ou à la base de données du cache d'objets de données.
Nom du schéma	Nom du schéma dans la base de données. Spécifiez les connexions à l'entrepôt de profilage, à la base de données temporaire ou à la base de données du cache d'objets de données. Vous devez indiquer le nom du schéma de l'entrepôt de profilage et de la base de données temporaire s'il est différent du nom d'utilisateur de la base de données. Vous devez spécifier le nom du schéma de la base de données du cache d'objet de données s'il est différent du nom d'utilisateur de la base de données et que vous gérez le cache avec un outil externe.
Environnement SQL	Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de connexion à chaque connexion à la base de données.
Transaction SQL	Facultatif. Commandes SQL permettant de définir l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de transaction au début de chaque transaction.

Propriété	Description
Période de nouvelle tentative	Cette propriété est réservée à une utilisation ultérieure.
Caractère identificateur SQL	Type de caractère servant à identifier les caractères spéciaux et les mots clés SQL réservés, tels que WHERE. Le service d'intégration de données place le caractère sélectionné autour des caractères spéciaux et des mots clés SQL réservés. Le service d'intégration de données utilise également ce caractère pour la propriété de prise en charge des identifiants à casse mixte.
Prise en charge des identifiants à casse mixte	Lorsque cette option est activée, le service d'intégration de données place les caractères identifiants autour des noms de table, de vue, de schéma, de synonyme et de colonne lors de la génération et de l'exécution de SQL par rapport à ces objets dans la connexion. Utilisez-la si les objets comportent une casse mixte ou des noms en minuscules. Par défaut, cette option n'est pas sélectionnée.

Remarque: Lorsque vous utilisez une connexion Microsoft SQL Server pour accéder aux tables d'une base de données Microsoft SQL Server, l'outil Developer n'affiche pas les synonymes des tables.

Propriétés de connexion Oracle

Utilisez une connexion Oracle pour accéder aux tables dans une base de données Oracle.

Le tableau suivant décrit les propriétés de la connexion Oracle :

Propriété	Description
Nom d'utilisateur	Nom d'utilisateur de la base de données.
Mot de passe	Mot de passe pour le nom d'utilisateur.
Chaîne de connexion pour l'accès aux métadonnées	Chaîne de connexion pour importer des objets de données physiques. Utilisez la chaîne de connexion suivante : jdbc:informatica:oracle://<host>:1521;SID=<sid>
Chaîne de connexion pour l'accès aux données	Chaîne de connexion pour prévisualiser les données et exécuter les mappages. Entrez <code>dbname.world</code> à partir de l'entrée TNSNAMES.
Page de code	Page de code de la base de données.
Environnement SQL	Facultatif. Entrez les commandes SQL pour paramétrer l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute l'environnement de connexion SQL à chaque connexion à la base de données.
Transaction SQL	Facultatif. Entrez les commandes SQL pour paramétrer l'environnement de base de données lorsque vous vous connectez à la base de données. Le service d'intégration de données exécute le SQL de l'environnement de transaction au début de chaque transaction.
Période de nouvelle tentative	Cette propriété est réservée à une utilisation ultérieure.
Mode parallèle	Facultatif. Active le traitement parallèle lors du chargement des données dans une table en mode groupé. Cette option est désactivée par défaut.

Propriété	Description
Caractère identificateur SQL	Le type de caractère utilisé pour identifier des caractères spéciaux et des mots clés SQL réservés, tels que WHERE. Le service d'intégration de données place le caractère sélectionné autour des caractères spéciaux et mots clés SQL réservés. Le service d'intégration de données utilise également ce caractère pour la propriété de prise en charge des identifiants à casse mixte.
Prise en charge des identifiants à casse mixte	Lorsque cette option est activée, le service d'intégration de données place les caractères identifiants autour des noms de table, de vue, de schéma, de synonyme et de colonne lors de la génération et de l'exécution de SQL par rapport à ces objets dans la connexion. Utilisez-la si les objets comportent une casse mixte ou des noms en minuscules. Par défaut, cette option n'est pas sélectionnée.

Création d'une connexion

Dans l'outil Administrator tool, vous pouvez créer des connexions de base de données relationnelle, de médias sociaux et de systèmes fichiers.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Gérer**.
2. Cliquez sur la vue **Connexions**.
3. Dans le navigateur, sélectionnez le domaine.
4. Dans le navigateur, cliquez sur **Actions > Nouveau > Connexion**.
La boîte de dialogue **Nouvelle connexion** s'affiche.
5. Dans la boîte de dialogue **Nouvelle connexion**, sélectionnez le type de connexion, puis cliquez sur **OK**.
L'assistant **Nouvelle connexion** s'affiche.
6. Entrez les propriétés de la connexion.
Les propriétés de la connexion que vous entrez dépendent du type de connexion. Cliquez sur **Suivant** pour accéder à la page suivante de l'assistant **Nouvelle connexion**.
7. Une fois les propriétés de la connexion saisies, vous pouvez cliquer sur **Tester la connexion** pour tester la connexion.
8. Cliquez sur **Terminer**.

CHAPITRE 8

Créer les services d'application

Ce chapitre comprend les rubriques suivantes :

- [Créer des services d'applications - Présentation, 140](#)
- [Vérification des prérequis du service d'application, 140](#)
- [Dépendances des services d'application, 142](#)
- [Créer et configurer le service de référentiel modèle, 142](#)
- [Créer et configurer le service d'intégration de données, 147](#)
- [Création d'un service de catalogue, 150](#)
- [Créer et configurer le service de gestion de contenu, 156](#)

Créer des services d'applications - Présentation

Si vous avez choisi de ne pas créer de services d'applications lorsque vous avez installé Enterprise Data Catalog, utilisez l'outil Informatica Administrator pour créer les services d'applications dans l'ordre requis.

Certains services d'applications sont interdépendants. Lorsque vous créez ces services d'applications dépendants, vous devez fournir le nom des autres services d'applications en cours d'exécution. Vérifiez les dépendances des services d'applications pour déterminer l'ordre dans lequel vous devez créer les services. Par exemple, vous devez créer le service de référentiel modèle et le service d'intégration de données avant de créer le service de catalogue.

Avant de créer les services d'applications, vérifiez que vous avez effectué les tâches prérequis dont le processus d'installation et de configuration a besoin. Après avoir créé chaque service d'application, vérifiez les prochaines tâches à effectuer.

Vérification des prérequis du service d'application

Avant de créer un service d'application, assurez-vous d'avoir effectué les tâches prérequis suivantes :

Configurez la base de données.

Configurez les bases de données suivantes :

- Référentiel modèle pour le service de référentiel modèle.

- Base de données de cache d'objets de données, destinée à mettre en cache les objets de données logiques et les tables virtuelles.
- Entrepôt de profilage permettant d'enregistrer les statistiques de profilage et de qualité des données.
- Entrepôt de données de référence destiné à stocker les données de référence pour le service de gestion de contenu.

Installez le logiciel client de base de données sur les machines du service.

Installez et configurez le logiciel client de base de données natif associé aux sources de données relationnelles et aux bases de données du référentiel sur la machine sur laquelle le service d'intégration de données est en cours d'exécution.

Configurez les variables d'environnement client de la base de données sous Linux.

Vous devez configurer les variables d'environnement client de la base de données sur les machines qui exécutent le service d'intégration de données.

Créez un fichier keytab pour le service.

Si vous définissez le niveau du principal de service au niveau du processus, créez un fichier keytab unique pour les services suivants :

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

Remarque: Le nom du service que vous créez doit correspondre au nom du service figurant dans le nom du fichier keytab.

Configurez les fichiers keystore.

Pour configurer une connexion sécurisée à l'application cliente, créez un fichier keystore pour le service de catalogue.

Déterminez la page de code à utiliser pour le référentiel.

Vérifiez que la base de données de configuration du domaine est compatible avec les pages de code des services d'applications que vous créez dans le domaine.

Configurez les variables d'environnement des paramètres régionaux sous Linux.

Vérifiez que les paramètres régionaux des machines qui accèdent à l'outil Informatica Administrator tool et aux outils Enterprise Data Catalog sont compatibles avec les pages de code des référentiels du domaine.

Configuration des variables d'environnement de chemin de bibliothèque sous Linux.

Configurez les variables d'environnement de chemin de bibliothèque sur les machines qui exécutent le service d'intégration de données.

Créez des connexions aux bases de données auxquelles les services d'applications accèdent via une connectivité de cluster.

Dans l'outil Informatica Administrator tool, créez des connexions aux bases de données suivantes :

- Entrepôt de données de référence
- Base de données du cache d'objet de données
- Base de données de l'entrepôt de profilage

Dépendances des services d'application

Un service d'application dépendant requiert un ou plusieurs autres services d'application. Avant de créer un service dépendant, vous devez créer tous les services d'application dont il a besoin.

Par exemple, le service d'intégration de données dépend du service de référentiel modèle. Lorsque vous créez un service d'intégration de données, l'outil Informatica Administrator vous demande d'indiquer le nom d'un service de référentiel modèle. Par conséquent, vous devez créer un service de référentiel modèle avant de créer un service d'intégration de données.

Les services qui accèdent aux objets du référentiel modèle peuvent dépendre les uns des autres. Les dépendances du service d'application déterminent l'ordre dans lequel vous devez créer les services.

Services qui accèdent à des objets du référentiel modèle

Créez les services d'application qui accèdent aux objets du référentiel modèle dans l'ordre suivant :

1. Service de référentiel modèle.
Le service de référentiel modèle n'a pas de dépendances vis-à-vis d'un service d'application.
2. Service d'intégration de données.
Le service d'intégration de données dépend du service de référentiel modèle.
3. Service de catalogue.
Le service de catalogue dépend du service de référentiel modèle et du service d'intégration de données.
4. Service de gestion de contenu.
Le service de gestion de contenu dépend du service de référentiel modèle et du service d'intégration de données.

Créer et configurer le service de référentiel modèle

Le service de référentiel modèle est un service d'application qui gère le référentiel modèle. Le référentiel modèle stocke les métadonnées créées par les outils d'Enterprise Data Catalog et les services d'application dans une base de données relationnelle pour permettre la collaboration entre les outils et les services. Le référentiel modèle stocke également les informations sur la configuration des ressources et les domaines de données.

Lorsque vous accédez à un objet de référentiel modèle dans les outils d'Enterprise Data Catalog ou le service d'intégration de données, le client ou le service envoie une demande au service de référentiel modèle. Le processus du service de référentiel modèle extrait, insère et met à jour les métadonnées stockées dans les tables de base de données du référentiel modèle.

Créer le service de référentiel modèle

Utilisez l'assistant de création de service dans l'outil Administrator tool pour créer le service.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Gérer**.
2. Cliquez sur **Actions > Nouveau > Service de référentiel modèle**.
La boîte de dialogue **Nouveau service de référentiel modèle** s'affiche.

3. Dans la page **Nouveau service de référentiel modèle - Étape 1 sur 2**, entrez les propriétés suivantes :

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 contenir ni espaces ni l'un des caractères spéciaux suivants : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Description	Description du service. La description ne peut pas dépasser 765 caractères.
Emplacement	Domaine et dossier où le service est créé. Cliquez sur Parcourir pour choisir un autre dossier. Vous pouvez déplacer le service après l'avoir créé.
Licence	Objet de licence permettant d'utiliser le service.
Nœud	Nœud sur lequel le service s'exécute.
Nœuds de sauvegarde	Si votre licence comprend la haute disponibilité, il s'agit des nœuds sur lesquels le service peut s'exécuter si le nœud principal est indisponible.

4. Cliquez sur **Suivant**.

La page **Nouveau service de référentiel modèle - Étape 2 sur 2** s'affiche.

5. Entrez les propriétés suivantes de la base de données du référentiel modèle :

Propriété	Description
Type de base de données	Type de base de données du référentiel.
Nom d'utilisateur	Nom d'utilisateur de la base de données du référentiel.
Mot de passe	Mot de passe de la base de données du référentiel pour l'utilisateur de la base de données.
Schéma de base de données	Disponible pour Microsoft SQL Server. Nom du schéma qui contiendra les tables du référentiel modèle.
Espace de table de base de données	Disponible pour IBM DB2. Nom de l'espace de table dans lequel les tables sont créées. Pour une base de données IBM DB2 à partitions multiples, l'espace de table doit s'étendre sur un seul nœud et une seule partition.

6. Entrez la chaîne de connexion JDBC que le service utilise pour se connecter à la base de données du référentiel modèle.

Utilisez la syntaxe suivante pour la chaîne de connexion au type de base de données sélectionné :

Type de base de données	Syntaxe de la chaîne de connexion
IBM DB2	<code>jdbc:informatica:db2:// <host_name>:<port_number>;DatabaseName=<database_name>;BatchPerformanceWorkaround=true;DynamicSections=3000</code>
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server qui utilise l'instance par défaut <code>jdbc:informatica:sqlserver:// <host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true</code> - Microsoft SQL Server qui utilise une instance nommée <code>jdbc:informatica:sqlserver://<host_name> \<named_instance_name>;DatabaseName=<database_name>;SnapshotSerializable=true</code>
Oracle	<code>jdbc:informatica:oracle:// <host_name>:<port_number>;SID=<database_name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true</code>

7. Si la base de données du référentiel modèle est sécurisée avec le protocole SSL, vous devez entrer les paramètres de la base de données sécurisée dans le champ **Paramètres JDBC sécurisés**.

Entrez les paramètres sous la forme `nom=valeur` en les séparant par un point-virgule (;). Par exemple :

`param1=value1;param2=value2`

Entrez les paramètres de la base de données sécurisée suivants :

Paramètres de base de données sécurisée	Description
EncryptionMethod	Requis. Indique si les données sont cryptées lorsqu'elles sont transmises sur le réseau. Ce paramètre doit être défini sur SSL.
ValidateServerCertificate	Facultatif. Indique si Informatica valide le certificat envoyé par le serveur de base de données. Si ce paramètre est défini sur True, Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre HostNameInCertificate, Informatica valide également le nom d'hôte dans le certificat. Si ce paramètre est défini sur False, Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de truststore que vous spécifiez.
HostNameInCertificate	Facultatif. Nom d'hôte de la machine qui héberge la base de données sécurisée. Si vous spécifiez un nom d'hôte, Informatica valide le nom d'hôte inclus dans la chaîne de connexion avec le nom d'hôte dans le certificat SSL.
cryptoProtocolVersion	Requis. Indique le protocole cryptographique à utiliser pour la connexion à une base de données sécurisée. Vous pouvez définir le paramètre sur <code>cryptoProtocolVersion=TLSv1.1</code> ou <code>cryptoProtocolVersion=TLSv1.2</code> en fonction du protocole cryptographique utilisé par le serveur de base de données.

Paramètres de base de données sécurisée	Description
TrustStore	Requis. Chemin et nom du fichier truststore contenant le certificat SSL de la base de données. Si vous n'incluez pas le chemin du fichier truststore, Informatica recherche ce fichier dans le répertoire par défaut suivant : <Répertoire d'installation Informatica>/tomcat/bin
TrustStorePassword	Requis. Mot de passe du fichier truststore de la base de données sécurisée.

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

8. Cliquez sur **Tester la connexion** pour vérifier que vous pouvez vous connecter à la base de données.
9. Sélectionnez **Aucun contenu n'est disponible dans la chaîne de connexion indiquée. Créez un contenu**.
10. Cliquez sur **Terminer**.

Le domaine crée le service de référentiel modèle, crée du contenu pour le référentiel modèle dans la base de données spécifiée et active le service.

Remarque: Lorsque vous mettez à niveau les propriétés du service de référentiel modèle, vous devez le redémarrer ainsi que le service de catalogue pour que les modifications soient appliquées.

Après avoir créé le service via l'assistant, vous pouvez modifier les propriétés ou configurer d'autres propriétés.

Après la création du service de référentiel modèle

Après avoir créé le service de référentiel modèle, effectuez les tâches suivantes :

- Créer l'utilisateur du référentiel modèle.
- Créer les autres services d'application.

Créer l'utilisateur du référentiel modèle

Le domaine utilise un compte utilisateur pour authentifier d'autres services d'application qui effectuent des demandes dans le service de référentiel modèle. Vous devez créer un compte utilisateur et affecter l'utilisateur au rôle Administrateur pour le service de référentiel modèle.

Lorsque vous créez un service d'application qui dépend du service de référentiel modèle, vous indiquez le nom du service de référentiel modèle et celui de l'utilisateur de ce référentiel modèle.

1. Dans l'outil Administrator, cliquez sur l'onglet **Sécurité**.
2. Dans le menu Actions de sécurité, cliquez sur **Créer un utilisateur** pour créer un compte utilisateur natif.

Remarque: Si vous configurez l'authentification LDAP dans le domaine, vous pouvez utiliser un compte utilisateur LDAP pour l'utilisateur du référentiel modèle.

- Entrez les propriétés suivantes de l'utilisateur :

Propriété	Description
Nom de connexion	Nom de connexion du compte utilisateur. Le nom de connexion d'un compte utilisateur doit être unique dans le domaine de sécurité auquel il appartient. Le nom n'est pas sensible à la casse et ne doit pas dépasser 128 caractères. Les tabulations, retours à la ligne et caractères spéciaux suivants ne sont pas admis : , + " \ < > ; / * % ? & Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Tous les autres caractères d'espacement sont interdits.
Mot de passe	Mot de passe du compte utilisateur. Le mot de passe peut comprendre de 1 à 80 caractères.
Confirmer le mot de passe	Entrez à nouveau le mot de passe pour le confirmer. Vous devez saisir à nouveau le mot de passe. Ne faites pas de copier-coller du mot de passe.
Nom complet	Nom complet du compte utilisateur. Le nom complet ne peut pas inclure les caractères spéciaux suivants : < > "
Description	Description du compte utilisateur. La description ne peut pas dépasser 765 caractères, ni inclure les caractères spéciaux suivants : < > "

- Cliquez sur **OK**.
Les propriétés de l'utilisateur s'affichent.
- Cliquez sur l'onglet **Privilèges**.
- Cliquez sur **Éditer**.
La boîte de dialogue **Modifier les rôles et les privilèges** s'ouvre.
- Dans l'onglet **Rôles**, développez le service de référentiel modèle.
- Sous **Rôles définis par le système**, sélectionnez Administrateur et cliquez sur **OK**.

Créer d'autres services

Après avoir créé le service de référentiel modèle, créez les services d'application qui en dépendent.

Créez les services dépendants dans l'ordre suivant :

- Service d'intégration de données
- Service de cluster Informatica si vous avez choisi l'option de cluster Hadoop incorporé pour l'installation d'Enterprise Information Catalog.
- Service de catalogue
- Service de gestion de contenu

Créer et configurer le service d'intégration de données

Le service d'intégration de données est un service d'application qui effectue des tâches d'intégration de données pour les outils d'Enterprise Data Catalog, tels qu'Informatica Administrator, l'outil de recherche Enterprise Data Catalog et Informatica Catalog Administrator.

Lorsque vous exécutez des analyses sur les ressources et que vous affichez les statistiques de métadonnées et de profilage dans Enterprise Data Catalog, l'outil client envoie des demandes au service d'intégration de données pour effectuer les tâches d'intégration de données.

Créer le service d'intégration de données

Utilisez l'assistant de création de service dans l'outil Administrator tool pour créer le service.

Avant de créer le service d'intégration de données, vérifiez que vous avez créé et activé le service de référentiel modèle. Vous devez également vérifier que vous avez créé un utilisateur de référentiel modèle que le service d'intégration de données peut utiliser pour accéder au service de référentiel modèle.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Gérer**.
2. Cliquez sur la vue **Services et nœuds**.
3. Dans le navigateur de domaine, sélectionnez le domaine.
4. Cliquez sur **Actions > Nouveau > Service d'intégration de données**.
L'assistant **Nouveau service d'intégration de données** s'affiche.
5. Sur la page **Nouveau service d'intégration de données - Étape 1 sur 14**, entrez les propriétés suivantes :

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 contenir ni espaces ni l'un des caractères spéciaux suivants : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Description	Description du service. La description ne peut pas dépasser 765 caractères.
Emplacement	Domaine et dossier où le service est créé. Cliquez sur Parcourir pour choisir un autre dossier. Vous pouvez déplacer le service après l'avoir créé.
Licence	Objet de licence permettant d'utiliser le service.
Attribuer	Sélectionnez Nœud pour configurer le service afin qu'il s'exécute sur un nœud. Si votre licence inclut une grille, vous pouvez créer une grille et attribuer le service à exécuter sur la grille après l'avoir créé.
Nœud	Nœud sur lequel le service s'exécute.
Nœuds de sauvegarde	Si votre licence comprend la haute disponibilité, il s'agit des nœuds sur lesquels le service peut s'exécuter si le nœud principal est indisponible.

Propriété	Description
Service de référentiel modèle	Service de référentiel modèle à associer au service.
Nom d'utilisateur	Nom d'utilisateur employé par le service pour accéder au service de référentiel modèle. Entrez l'utilisateur du référentiel modèle que vous avez créé.
Mot de passe	Mot de passe de l'utilisateur du référentiel modèle.
Domaine de sécurité	Domaine de sécurité LDAP de l'utilisateur du référentiel modèle. Le champ apparaît lorsque le domaine Informatica contient un domaine de sécurité LDAP. Non disponible pour un domaine avec l'authentification Kerberos.

6. Cliquez sur **Suivant**.

La page **Nouveau service d'intégration de données - Étape 2 sur 14** s'affiche.

7. Entrez le numéro de port HTTP à utiliser pour le service d'intégration de données.
8. Acceptez les valeurs par défaut pour les autres propriétés de sécurité. Vous pouvez configurer les propriétés de sécurité après avoir créé le service d'intégration de données.
9. Sélectionnez **Activer le service**.

Le service de référentiel modèle doit être en cours d'exécution pour que vous puissiez activer le service d'intégration de données.

10. Vérifiez que l'option **Aller jusqu'à la page de configuration des plug-ins** n'est pas sélectionnée.

11. Cliquez sur **Suivant**.

La page **Nouveau service d'intégration de données - Étape 3 sur 14** s'affiche.

12. Définissez la propriété **Lancer les options de tâches** sur l'une des valeurs suivantes :

- Dans le processus de service. Sélectionnez cette valeur lorsque vous exécutez des tâches de service de données SQL et de service Web. L'exécution des tâches de service de données SQL et de service Web dans le processus de service offre généralement de meilleurs résultats.
- Dans les processus locaux distincts. Sélectionnez cette valeur lorsque vous exécutez des tâches de mappage, de profil et de flux de travail. L'exécution des tâches dans des processus locaux distincts permet une plus grande stabilité, car l'interruption inattendue d'une tâche n'affecte pas toutes les autres tâches.

Si vous configurez le service d'intégration de données de façon à ce qu'il s'exécute sur une grille après sa création, vous pouvez le configurer pour qu'il exécute les tâches dans des processus distants séparés.

13. Acceptez les valeurs par défaut pour les autres options d'exécution et cliquez sur **Suivant**.

La page **Nouveau service d'intégration de données - Étape 4 sur 14** s'affiche.

14. Si vous avez créé la base de données du cache d'objet de données pour le service d'intégration de données, cliquez sur **Sélectionner** pour sélectionner la connexion de cache. Sélectionnez la connexion de cache d'objet de données que vous avez créée pour le service afin d'accéder à la base de données.

15. Acceptez les valeurs par défaut pour les autres propriétés figurant sur cette page et cliquez sur **Suivant**.

La page **Nouveau service d'intégration de données - Étape 5 sur 14** s'affiche.

16. Pour des performances optimales, activez les modules du service d'intégration de données que vous prévoyez d'utiliser.

Le tableau suivant répertorie les modules du service d'intégration de données que vous pouvez activer :

Module	Description
Module de service Web	Exécute des mappages d'opérations de service Web.
Module de service de mappage	Exécute les mappages et les aperçus.
Module de service de profilage	Exécute les profils et les fiches d'évaluation.
Module de service SQL	Exécute les requêtes SQL à partir d'un outil client tiers pour un service de données SQL.
Module Service d'orchestration du flux de travail	Exécute les flux de travail.

17. Cliquez sur **Suivant**.

La page **Nouveau service d'intégration de données - Étape 6 sur 14** s'affiche.

Vous pouvez configurer les propriétés du serveur proxy HTTP pour rediriger les demandes HTTP vers le service d'intégration de données. Vous pouvez configurer les propriétés de configuration HTTP pour filtrer les machines clientes des services Web qui peuvent envoyer des demandes au service d'intégration de données. Vous pouvez configurer ces propriétés après avoir créé le service.

18. Acceptez les valeurs par défaut pour le serveur proxy HTTP et les propriétés de configuration HTTP, puis cliquez sur **Suivant**.

La page **Nouveau service d'intégration de données - Étape 7 sur 14** s'affiche.

Le service d'intégration de données utilise les propriétés du cache de l'ensemble de résultats pour exploiter les résultats mis en cache pour les requêtes de service de données SQL et les demandes de service Web. Vous pouvez configurer les propriétés après avoir créé le service.

19. Acceptez les valeurs par défaut pour les propriétés du cache de l'ensemble de résultats et cliquez sur **Suivant**.

La page **Nouveau service d'intégration de données - Étape 8 sur 14** s'affiche.

20. Si vous avez créé la base de données de l'entrepôt de profilage pour le service d'intégration de données, sélectionnez le module de service de profilage.

21. Si vous avez créé la base de données du flux de travail pour le service d'intégration de données, sélectionnez le module Service d'orchestration du flux de travail.

22. Vérifiez que les autres modules ne sont pas sélectionnés.

Vous pourrez configurer les propriétés des autres modules après avoir créé le service.

23. Cliquez sur **Suivant**.

La page **Nouveau service d'intégration de données - Étape 11 sur 14** s'affiche.

24. Si vous avez créé la base de données de l'entrepôt de profilage pour le service d'intégration de données, cliquez sur **Sélectionner** pour sélectionner la connexion de base de données. Sélectionnez la connexion d'entrepôt de profilage que vous avez créée pour le service afin d'accéder à la base de données.

25. Indiquez s'il existe ou non du contenu dans la base de données de l'entrepôt de profilage.

Si vous avez créé une nouvelle base de données d'entrepôt de profilage, sélectionnez **Aucun contenu n'est disponible dans la chaîne de connexion indiquée**.

26. Cliquez sur **Suivant**.

La page **Nouveau service d'intégration de données - Étape 12 sur 14** s'affiche.

27. Acceptez les valeurs par défaut pour les propriétés avancées de profilage et cliquez sur **Suivant**.
La page **Nouveau service d'intégration de données - Étape 14 sur 14** s'affiche.
28. Si vous avez créé la base de données du flux de travail pour le service d'intégration de données, cliquez sur **Sélectionner** pour sélectionner la connexion à la base de données. Sélectionnez la connexion à la base de données du flux de travail que vous avez créée pour permettre au service d'accéder à la base de données.
29. Cliquez sur **Terminer**.
Le domaine crée et active le service d'intégration de données.
Après avoir créé le service via l'assistant, vous pouvez modifier les propriétés ou configurer d'autres propriétés.

Après la création du service d'intégration de données

Après avoir créé le service d'intégration de données, effectuez les tâches suivantes :

- Vérifier la configuration du fichier hôte sous Linux.
- Créer les autres services d'application.

Vérification de la configuration du fichier d'hôte sous Linux

Si vous avez configuré le service d'intégration de données sous Linux pour lancer les tâches sous forme de processus distincts, vérifiez que le fichier d'hôte du nœud qui exécute le service contient une entrée localhost. Dans le cas contraire, les tâches échouent lorsque la propriété **Lancer les tâches comme des processus séparés** du service d'intégration de données est activée.

Créer d'autres services

Après avoir créé le service d'intégration de données, créez les services d'application qui en dépendent.

Créez les services dépendants dans l'ordre suivant :

1. Service de cluster Informatica si vous choisissez le cluster Hadoop incorporé pour le déploiement d'Enterprise Data Catalog.
2. Service de catalogue.
3. Service de gestion de contenu.

Création d'un service de catalogue

Créez un service de catalogue pour exécuter l'application Enterprise Data Catalog et gérer les connexions entre les composants d'Enterprise Data Catalog. Vous pouvez configurer les propriétés générales, du service d'application et de sécurité du service de catalogue.

Si vous prévoyez de déployer Enterprise Data Catalog sur plusieurs nœuds, veillez à configurer le service de cluster Informatica et le service de catalogue sur des nœuds distincts.

Remarque: Le service de catalogue dispose des mêmes privilèges que le compte utilisateur qui le crée. Vérifiez que le compte d'utilisateur ne dispose pas de privilèges pour lire ou modifier des fichiers sensibles sur le système.

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 catalogue**.
La boîte de dialogue **Nouveau service de catalogue - Étape 1 sur 4** s'affiche.
3. Configurez les propriétés générales dans la boîte de dialogue.

Le tableau suivant décrit les propriétés :

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'espace. Les caractères qui composent le nom doivent être compatibles avec la page de code du référentiel modèle que vous associez au service de catalogue. Le nom ne peut pas contenir les caractères spéciaux suivants : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Description	Description du service. La description ne peut pas dépasser 765 caractères.
Emplacement	Domaine dans lequel le service s'exécute
Licence	Licence à attribuer au service de catalogue. Sélectionnez la licence que vous avez installée avec Informatica.
Nœud	Nœud du domaine Informatica sur lequel est exécuté le service de catalogue. Si vous modifiez le nœud, vous devez recycler le service de catalogue.
Nœuds de sauvegarde	Si votre licence comprend la haute disponibilité, il s'agit des nœuds sur lesquels le service peut s'exécuter si le nœud principal est indisponible.

4. Cliquez sur **Suivant**.
La boîte de dialogue **Nouveau service de catalogue - Étape 2 sur 4** s'affiche.
5. Configurez les propriétés du service d'application dans la boîte de dialogue.

Le tableau suivant décrit les propriétés :

Propriété	Description
Service de référentiel modèle	Service de référentiel modèle à associer au service de catalogue. Le service de référentiel modèle gère le référentiel modèle qu'Enterprise Data Catalog utilise. Si vous mettez à jour la propriété pour spécifier un service de référentiel modèle différent, recyclez le service de catalogue.
Nom d'utilisateur	Nom d'utilisateur de la base de données du référentiel modèle.
Mot de passe	Version cryptée du mot de passe de la base de données du référentiel modèle.
Domaine de sécurité	Nom du domaine de sécurité qui inclut le Nom d'utilisateur .

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

7. Configurez les propriétés de sécurité dans la boîte de dialogue.

Le tableau suivant décrit les propriétés :

Propriété	Description
Port HTTP	Numéro de port HTTP unique utilisé pour chaque processus de service d'intégration de données. La valeur par défaut est 8085.
Activer le protocole TLS	Indique que le service de catalogue doit utiliser HTTPS. Si vous n'avez pas configuré le service d'intégration de données pour utiliser HTTPS, le service de catalogue ne démarre pas.
Port HTTPS	Numéro de port de la connexion HTTPS.
Fichier keystore	Chemin d'accès 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). Lorsque l'application Enterprise Data Catalog crée le service de catalogue, elle exporte le keystore dans un certificat et stocke le certificat dans le répertoire keystore. Veillez à configurer les autorisations de lecture et d'écriture dans le répertoire d'Enterprise Data Catalog pour stocker le certificat.
Mot de passe keystore	Mot de passe du fichier keystore. Requis si vous sélectionnez Activer TLS (Transport Layer Security).
Protocole SSL	Protocole Secure Sockets Layer à utiliser.

8. Cliquez sur **Suivant**.

La boîte de dialogue **Nouveau service de catalogue - Étape 4 sur 4** s'affiche.

9. Configurez les propriétés du cluster Hadoop dans la boîte de dialogue.

Le tableau suivant décrit les propriétés :

Propriété	Description
Type de cluster	<p>Sélectionnez l'une des options suivantes pour indiquer le type de déploiement d'Enterprise Data Catalog :</p> <ul style="list-style-type: none"> - Cluster externe. Déployez Enterprise Data Catalog dans un cluster Hadoop existant sur Hortonworks, ClouderaManager ou Azure HDInsight. - Cluster interne. Déployez Enterprise Data Catalog dans le cluster Hadoop intégré sur Hortonworks.
Distribution Hadoop	<p>Applicable si vous sélectionnez l'option Cluster externe pour Type de cluster. Sélectionnez une des options suivantes pour spécifier la distribution Hadoop :</p> <ul style="list-style-type: none"> - ClouderaManager. Utilisez cette option si vous souhaitez utiliser une distribution Hadoop de ClouderaManager. - Hortonworks. Utilisez cette option si vous souhaitez utiliser une distribution Hadoop de Hortonworks. <p>Remarque: Si vous sélectionnez ClouderaManager ou Hortonworks comme distribution Hadoop, Enterprise Data Catalog identifie automatiquement les propriétés suivantes pour le type de distribution Hadoop :</p> <ul style="list-style-type: none"> - URI du cluster ZooKeeper - URI du NameNode HDFS - URI du gestionnaire de ressources Yarn - URI HTTPS ou HTTP du gestionnaire de ressources Yarn - URI HTTP du serveur d'historique - Nom du service HDFS pour la haute disponibilité - URI du planificateur du gestionnaire de ressources Yarn <p>- HDInsight. Utilisez cette option si vous souhaitez utiliser une distribution Hadoop de d'Azure HDInsight.</p> <p>- Autres. Utilisez cette option si vous souhaitez spécifier manuellement toutes les propriétés d'une distribution Hadoop de ClouderaManager, HortonWorks ou Azure HDInsight. Veuillez à configurer les options personnalisées suivantes pour le service de catalogue :</p> <ul style="list-style-type: none"> - LdmCustomOptions.yarn-site.yarn.application.classpath - LdmCustomOptions.yarn-site.yarn.nodemanager.webapp.address - LdmCustomOptions.yarn-site.yarn.nodemanager.webapp.https.address <p>Remarque: Si vous sélectionnez ClouderaManager ou Hortonworks, configurez les propriétés suivantes avec les autres propriétés requises :</p> <ul style="list-style-type: none"> - URL du cluster. L'URL du cluster pour accéder à la distribution Hadoop sélectionnée. - Nom d'utilisateur de l'URL du cluster. Le nom d'utilisateur pour accéder à l'URL du cluster. - Mot de passe de l'URL du cluster. Le mot de passe associé au nom d'utilisateur de l'URL du cluster.
URI du cluster ZooKeeper	S'applique au cluster existant. Plusieurs adresses ZooKeeper dans une liste séparée par des virgules.
URI du NameNode HDFS	<p>S'applique au cluster existant. L'URI pour accéder à HDFS.</p> <p>Utilisez le format suivant pour spécifier l'URI du NameNode dans la distribution Cloudera : <Hostname>:<Port></p> <p>Où</p> <ul style="list-style-type: none"> - <host name> est le nom d'hôte ou l'adresse IP du NameNode. - <port number> est le numéro de port sur lequel le NameNode écoute les appels de procédure distante (RPC).

Propriété	Description
URI du gestionnaire de ressources Yarn	S'applique au cluster existant. Service au sein d'Hadoop qui envoie les tâches MapReduce aux nœuds spécifiques dans la grappe. Utiliser le format suivant :<Hostname>:<Port> Où - <host name> est le nom ou l'adresse IP du gestionnaire de ressources Yarn. - <port number> est le numéro de port sur lequel le gestionnaire de ressources Yarn écoute les appels de procédure distante (RPC).
URI HTTPS ou HTTP du gestionnaire de ressources Yarn	S'applique au cluster existant. Valeur d'URI https ou http pour le gestionnaire de ressources Yarn.
URI HTTP du serveur d'historique	S'applique au cluster existant. Spécifiez une valeur pour générer des fichiers journaux d'allocation YARN pour les analyseurs. Catalog Administrator affiche l'URL des journaux dans le cadre de la surveillance des tâches.
Nom du service HDFS pour la haute disponibilité	S'applique au cluster haute disponibilité existant. Spécifiez le nom de service HDFS.
URI du planificateur du gestionnaire de ressource Yarn	S'applique au cluster existant. Valeur de l'URI du planificateur du gestionnaire de ressources Yarn.
Nom du cluster de service	S'applique à la fois aux clusters intégrés et existants. Nom du cluster de service. Assurez-vous d'avoir un répertoire /Informatica/LDM/<ServiceClusterName> dans HDFS. Remarque: Si vous ne spécifiez pas un nom de cluster de service, Enterprise Data Catalog considère DomainName_CatalogServiceName comme la valeur par défaut. Le répertoire /Informatica/LDM/<DomainName>_<CatalogServiceName> doit alors se trouver dans HDFS. Sinon, le service de catalogue pourrait échouer.
Type de chargement	Sélectionnez l'une des options suivantes pour spécifier la taille de données que vous prévoyez de charger dans le catalogue : - démo - faible - moyenne - élevée Pour plus d'informations sur les valeurs de paramètres taille de données, types de charges et réglage des performances, consultez l'article de procédure <i>Réglage des performances d'Enterprise Data Catalog</i> .
Activer l'authentification Kerberos	Sélectionnez cette option pour activer l'authentification Kerberos du cluster existant.
Nom de principal du service HDFS	S'applique à l'authentification Kerberos. Nom de principal du service HDFS.
Nom de principal du service YARN	S'applique à l'authentification Kerberos. Nom de principal du service YARN.

Propriété	Description
Emplacement keytab du service	S'applique à l'authentification Kerberos. Chemin d'accès au fichier keytab.
Nom du domaine Kerberos	S'applique à l'authentification Kerberos. Nom du domaine Kerberos.
Activer SSL du cluster	Sélectionnez cette option pour activer l'authentification SSL pour une communication sécurisée dans le cluster existant.
Keystore Solr	S'applique à l'authentification SSL. Chemin d'accès au fichier keystore Solr.
Mot de passe du keystore Solr	S'applique à l'authentification SSL. Mot de passe du fichier keystore Solr.
Recevoir des alertes par e-mail	S'applique à la fois aux clusters intégrés et existants. Choisissez de recevoir des notifications par e-mail sur l'état du service de catalogue. Remarque: Si vous sélectionnez cette option, vous devez activer le service de messagerie. Pour plus d'informations sur l'activation du service de messagerie, consultez le guide <i>Administrator Reference for Enterprise Data Catalog</i> .
Activer le service de catalogue	S'applique à la fois aux clusters intégrés et existants. Sélectionnez cette option pour activer le service de catalogue.
Service de cluster Informatica	S'applique au cluster intégré. Nom du service de cluster Informatica, qui est un service d'application qu'Enterprise Data Catalog utilise dans le déploiement de cluster intégré.

10. Cliquez sur **Terminer**.

- Assurez-vous que le fichier `krb5.conf` se trouve dans tous les nœuds de cluster et les machines du domaine dans le répertoire `/etc`.
- Si vous n'avez pas choisi d'activer le service de catalogue auparavant, vous devez le réinitialiser pour le démarrer.

Configuration du service de catalogue pour Azure HDInsight

Procédez comme suit pour configurer le service de catalogue d'un cluster HDInsight Azure :

1. Spécifiez les propriétés et valeurs suivantes dans la boîte de dialogue **Boîte de dialogue Nouveau service de catalogue - Étape 4 sur 4** :

Propriété	Description
Type de cluster	Cluster externe
Distribution Hadoop	HDInsight
URL du cluster	Nom d'hôte complet permettant d'accéder au cluster.
Nom d'utilisateur de l'URL du cluster	Nom d'utilisateur permettant d'accéder au cluster

Propriété	Description
Mot de passe de l'URL du cluster	Mot de passe pour le nom d'utilisateur de l'URL du cluster.

2. Après avoir créé le service de catalogue, configurez les propriétés personnalisées suivantes dans l'application Informatica Administrator du service de catalogue :

Propriété personnalisée	Description
LdmCustomOptions.deployment.azure.account.key	La clé pour authentifier le service de catalogue afin de se connecter au compte de stockage Azure. La valeur de la clé du compte de stockage Azure peut être chiffrée ou non chiffrée. Vous pouvez récupérer la valeur depuis la propriété <code>fs.azure.account.key.<storage account name></code> dans le fichier <code>core-site.xml</code> présent dans le cluster Azure HDInsight.
LdmCustomOptions.deployment.azure.key.decryption.script.path	Si la clé spécifiée dans la propriété <code>LdmCustomOptions.deployment.azure.account.key</code> est au format chiffré, vous pouvez utiliser le script shell de déchiffrement pour déchiffrer la clé à l'aide du certificat de clé. Vous devez vérifier que vous copiez le script shell de déchiffrement et le fichier de certificat de clé sur la machine du domaine (même chemin que la machine du cluster) avant d'activer le service de catalogue. Assurez-vous de conserver le chemin dans la machine du cluster Azure HDInsight pour les fichiers copiés dans la machine du domaine. La valeur de la propriété est l'emplacement du script shell de déchiffrement. Par exemple, <code>/usr/lib/python2.7/dist-packages/hdinsight_common/decrypt.sh</code> . Le fichier de certificat de clé, <code>key_decryption_cert.prv</code> , est présent dans le répertoire <code>/usr/lib/hdinsight-common/certs/key_decryption_cert.prv</code> du cluster Azure HDInsight.
LdmCustomOptions.deployment.hdfs.default.fs	Adresse du compte de stockage WASB auquel le service de catalogue doit se connecter. L'adresse comprend le nom du conteneur de stockage WASB avec le nom du compte de stockage. La valeur de la propriété est l'adresse WASB complète avec les noms du conteneur et du compte de stockage. Vous pouvez récupérer la valeur de la propriété depuis la propriété <code>fs.defaultFS</code> dans le fichier <code>core-site.xml</code> présent dans le cluster Azure HDInsight.

Créer et configurer le service de gestion de contenu

Le service de gestion de contenu est un service d'application qui gère les données de référence. Un objet de données de référence contient un ensemble de valeurs de données dans lequel vous pouvez lancer une recherche tout en effectuant des opérations de qualité des données sur les données source. Le service de gestion de contenu compile également les spécifications de règles dans des mapplets. Un objet de spécification de règle décrit les spécifications de données d'une règle métier en termes logiques.

Le service de gestion de contenu utilise le service d'intégration de données pour exécuter des mappages en vue de transférer des données entre les tables de référence et les sources de données externes. Le service

de gestion de contenu fournit également des transformations, des spécifications de mappage et des spécifications de règles avec les types de données de référence suivants :

- Données de référence d'adresse
- Populations d'identités
- Modèles probabilistes et modèles classificateurs
- Tables de référence

Créer le service de gestion de contenu

Utilisez l'assistant de création de service dans l'outil Administrator tool pour créer le service.

Avant de créer le service de gestion de contenu, vérifiez que vous avez créé et activé le service de référentiel modèle et le service d'intégration de données. Vous devez également vérifier que vous avez créé un utilisateur de référentiel modèle que le service de gestion de contenu peut utiliser pour accéder au service de référentiel modèle.

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Gérer**.
2. Cliquez sur **Actions > Nouveau > Service de gestion de contenu**.
La boîte de dialogue **Nouveau service de gestion de contenu** s'affiche.
3. Sur la page **Nouveau service de gestion de contenu - Étape 1 de 2**, entrez les propriétés suivantes :

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 contenir ni espaces ni l'un des caractères spéciaux suivants : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Description	Description du service. La description ne peut pas dépasser 765 caractères.
Emplacement	Domaine et dossier où le service est créé. Cliquez sur Parcourir pour choisir un autre dossier. Vous pouvez déplacer le service après l'avoir créé.
Licence	Objet de licence permettant d'utiliser le service.
Nœud	Nœud sur lequel le service s'exécute.
Port HTTP	Numéro de port HTTP à utiliser pour le service de gestion de contenu.
Service d'intégration de données	Service d'intégration de données à associer au service. Le service d'intégration de données et le service de gestion de contenu doivent s'exécuter sur le même nœud.
Service de référentiel modèle	Service de référentiel modèle à associer au service.
Nom d'utilisateur	Nom d'utilisateur employé par le service pour accéder au service de référentiel modèle. Entrez l'utilisateur du référentiel modèle que vous avez créé.
Mot de passe	Mot de passe de l'utilisateur du référentiel modèle.

Propriété	Description
Domaine de sécurité	Domaine de sécurité LDAP de l'utilisateur du référentiel modèle. Le champ apparaît lorsque le domaine Informatica contient un domaine de sécurité LDAP. Non disponible pour un domaine avec l'authentification Kerberos.
Emplacement des données de référence	Connexion à l'entrepôt de données de référence que vous avez créée pour permettre au service de gestion de contenu d'accéder à l'entrepôt de données de référence. Cliquez sur Sélectionner pour sélectionner la connexion.

4. Cliquez sur **Suivant**.

La boîte de dialogue **Nouveau service de gestion de contenu - Étape 2 de 2** s'affiche.

5. Acceptez les valeurs par défaut pour les propriétés de sécurité.
6. Sélectionner **Activer le service**.

Le service de référentiel modèle et le service d'intégration de données doivent être en cours d'exécution pour que vous puissiez activer le service de gestion de contenu.

7. Cliquez sur **Terminer**.

Le domaine crée et active le service de gestion de contenu.

Après avoir créé le service via l'assistant, vous pouvez modifier les propriétés ou configurer d'autres propriétés.

CHAPITRE 9

Configuration de l'authentification unique avec l'authentification SAML

- [Présentation de l'authentification unique utilisant l'authentification SAML, 159](#)

Présentation de l'authentification unique utilisant l'authentification SAML

Vous pouvez activer l'authentification unique pour les applications d'Enterprise Data Catalog utilisant l'authentification SAML.

Si vous avez activé l'authentification SAML lorsque vous avez installé Enterprise Data Catalog, vous pouvez activer l'authentification SAML à l'aide de l'une des méthodes suivantes :

- OKTA avec Active Directory
- Services de fédération Active Directory (AD FS) avec Active Directory

Vous devez effectuer l'une des étapes suivantes en fonction de la méthode d'authentification SAML que vous choisissez d'implémenter :

- Configuration du paramètre d'URL Relaystate par défaut dans OKTA.
- Configuration des points de terminaison d'URL des applications d'Enterprise Data Catalog dans AD FS.

Si vous n'aviez pas activé l'authentification SAML lorsque vous avez installé Enterprise Data Catalog, suivez les instructions répertoriées dans la section *Authentification unique basée sur SAML pour les applications Web d'Informatica* du *Guide de sécurité d'Informatica 10.2.1*.

Configuration du paramètre d'URL Relaystate par défaut dans OKTA.

Si vous prévoyez d'utiliser l'authentification SAML à l'aide d'OKTA et d'Active Directory, veillez à configurer le paramètre d'URL RelayState par défaut dans OKTA au format suivant :

```
namespaceINFA_SAML_IDP_DATA_VALUE_SEPERATOR<namespace-  
value>INFA_SAML_IDP_DATA_SEPERATORdef_webapp_urlINFA_SAML_IDP_DATA_VALUE_SEPERATOR/<app-  
context>/INFA_SAML_IDP_DATA_SEPERATORrequested_urlINFA_SAML_IDP_DATA_VALUE_SEPERATOR/  
<app-context>/INFA_SAML_IDP_DATA_SEPERATOR
```

Le tableau suivant répertorie les propriétés et les valeurs que vous devez remplacer dans l'URL RelayState :

Propriété	Valeur
<namespace-value>	Remplacez par l'espace de noms configuré pour OKTA.
<app-context>	Idmadmin

Configuration des points de terminaison d'URL des applications d'Enterprise Data Catalog dans les services de fédération Active Directory (AD FS)

Si vous prévoyez d'utiliser l'authentification SAML à l'aide d'AD FS et d'Active Directory, vous devez ajouter des URL pour accéder aux applications suivantes d'Informatica en tant que points de terminaison dans AD FS :

- Informatica Administrator
- Outil Analyst tool
- Catalog Administrator
- Enterprise Data Catalog

Pour obtenir les étapes d'ajout des URL à AD FS, consultez la section *Ajouter des URL d'applications Web d'Informatica à AD FS* dans le *Guide de sécurité d'Informatica 10.2.1*.

Partie V : Désinstallation

- [Désinstallation, 162](#)

CHAPITRE 10

Désinstallation

Ce chapitre comprend les rubriques suivantes :

- [Présentation de la désinstallation, 162](#)
- [Règles et instructions pour la désinstallation, 162](#)
- [Désinstallation d'Enterprise Data Catalog, 163](#)

Présentation de la désinstallation

Désinstallez Enterprise Data Catalog pour supprimer les fichiers correspondants.

Le processus de désinstallation d'Enterprise Data Catalog supprime tous les fichiers correspondants et efface toutes les configurations correspondantes. Le processus de désinstallation ne supprime pas les fichiers qui ne sont pas installés avec Enterprise Data Catalog. Par exemple, le processus d'installation crée des répertoires temporaires. Le programme de désinstallation ne conserve pas la trace de ces répertoires et ne peut donc pas les supprimer. Vous devez supprimer manuellement ces répertoires par une désinstallation propre.

Lorsque vous installez Enterprise Data Catalog, le programme d'installation crée un programme de désinstallation. Celui-ci est stocké dans le répertoire de désinstallation dans le répertoire d'installation.

Pour désinstaller Enterprise Data Catalog, utilisez la ligne de commande.

Règles et instructions pour la désinstallation

Utilisez les règles et instructions suivantes lorsque vous désinstallez des composants d'Enterprise Data Catalog :

- Le mode de désinstallation d'Enterprise Data Catalog dépend du mode que vous utilisez pour installer Enterprise Data Catalog. Par exemple, vous installez Enterprise Data Catalog en mode console. Lors de l'exécution du programme de désinstallation, il fonctionne en mode console.
- La désinstallation d'Enterprise Data Catalog n'affecte pas les référentiels correspondants. Le programme de désinstallation supprime les fichiers d'Enterprise Data Catalog. Il ne supprime pas les référentiels de la base de données. Si vous devez déplacer les référentiels, vous pouvez les sauvegarder et les restaurer vers une autre base de données.
- La désinstallation d'Enterprise Data Catalog ne supprime pas les tables de métadonnées de la base de données de configuration de domaine. Si vous installez à nouveau Enterprise Data Catalog à l'aide de la

base de données de configuration du domaine et du compte utilisateur identiques, vous devez supprimer manuellement les tables ou choisir de les remplacer. Vous pouvez utiliser la commande `infasetup BackupDomain` pour sauvegarder la base de données de configuration du domaine avant de remplacer les tables de métadonnées. Pour supprimer manuellement les tables de métadonnées, utilisez la commande `infasetup DeleteDomain` avant d'exécuter le programme de désinstallation.

- La désinstallation d'Enterprise Data Catalog supprime tous les fichiers d'installation et sous-répertoires du répertoire d'installation d'Enterprise Data Catalog. Avant de désinstaller Enterprise Data Catalog, arrêtez tous les services et processus d'Enterprise Data Catalog et vérifiez que tous les fichiers du répertoire d'installation sont fermés. Une fois le processus de désinstallation terminé, le programme de désinstallation affiche le nom des fichiers et répertoires qui n'ont pas été supprimés.
- L'installation d'Enterprise Data Catalog crée le dossier suivant pour les bibliothèques et les fichiers requis par les adaptateurs de tiers générés à l'aide des API d'Informatica Development Platform :
<Répertoire d'installation d'Enterprise Data Catalog>/services/shared/extensions
La désinstallation d'Enterprise Data Catalog supprime ce dossier et les sous-dossiers créés en dessous.

Désinstallation d'Enterprise Data Catalog

Vous pouvez désinstaller Enterprise Data Catalog en mode console ou en mode silencieux sous Linux.

Désinstallation d'Enterprise Data Catalog en mode silencieux

Avant d'exécuter le programme de désinstallation, arrêtez tous les services et processus Enterprise Data Catalog et vérifiez que tous les fichiers du répertoire d'installation sont fermés. Le processus de désinstallation ne peut pas supprimer des fichiers qui sont ouverts ou utilisés par un service ou un processus en cours d'exécution.

1. Accédez au répertoire suivant :

```
<Enterprise Data Catalog installation directory>/Uninstaller
```

2. Tapez la commande suivante pour exécuter le programme de désinstallation en mode silencieux :

```
./uninstaller
```

Si vous avez installé Enterprise Data Catalog en mode silencieux, le programme de désinstallation se lance en mode silencieux. Le programme de désinstallation en mode silencieux s'exécute en tâche de fond. Le processus peut prendre du temps. La désinstallation en mode silencieux échoue si le répertoire d'installation n'est pas accessible.

Partie VI : Dépannage

- [Dépannage, 165](#)

CHAPITRE 11

Dépannage

Ce chapitre comprend les rubriques suivantes :

- [Présentation du dépannage, 165](#)
- [Dépannage à l'aide des fichiers journaux d'installation, 165](#)
- [Dépannage des domaines et des nœuds, 167](#)
- [Dépannage des problèmes courants de déploiement des clusters, 169](#)
- [Dépannage du déploiement de clusters existants, 175](#)
- [Dépannage du déploiement de clusters incorporés, 176](#)
- [Dépannage des problèmes liés au services d'application, 180](#)

Présentation du dépannage

Ce chapitre consacré au dépannage fournit des informations sur le processus d'installation d'Informatica ainsi que sur les causes et résolutions des erreurs pouvant se produire pendant l'installation. Le chapitre fournit également quelques conseils utiles basés sur des scénarios en temps réel décrivant les problèmes et les solutions pour le déploiement de clusters incorporés, existants et communs.

Dépannage à l'aide des fichiers journaux d'installation

Vous pouvez utiliser les fichiers journaux suivants pour dépanner une installation Informatica :

Fichiers journaux d'installation

Le programme d'installation produit des fichiers journaux pendant et après l'installation. Vous pouvez utiliser ces journaux pour obtenir plus d'informations sur les tâches effectuées par le programme d'installation et sur les erreurs survenues pendant l'installation. Les fichiers journaux d'installation comprennent les journaux suivants :

- Journaux de débogage
- Journaux d'installation des fichiers

Fichiers journaux du gestionnaire de service

Fichiers journaux générés lors du démarrage du gestionnaire de service sur un nœud.

Fichiers journaux de débogage

Le programme d'installation écrit les actions et les erreurs dans le fichier journal de débogage. Le nom du fichier journal dépend du composant Informatica que vous installez.

Le tableau suivant décrit les propriétés du fichier journal de débogage :

Propriété	Description
Nom du fichier journal	<ul style="list-style-type: none">- Informatica_<Version>_Services.log- Informatica_<Version>_Client.log- Informatica_<Version>_Services_Upgrade.log- Informatica_<Version>_Client_Upgrade.log
Emplacement	Répertoire d'installation
Utilisation	Obtenir plus d'informations sur les actions effectuées par le programme d'installation et obtenir des informations sur les erreurs d'installation. Le programme d'installation écrit des informations dans ce fichier pendant l'installation. Si le programme d'installation génère une erreur, vous pouvez utiliser ce journal pour dépanner l'erreur.
Contenu	Résumé détaillé de chaque action effectuée par le programme d'installation, les informations que vous avez saisies dans l'installation, chaque commande et ligne de commande utilisée par le programme d'installation et le code d'erreur renvoyé par la commande.

Le journal de débogage contient la sortie des commandes infacmd et infasetup utilisées pour créer le domaine, le nœud et les services d'application. Il contient aussi des informations sur le démarrage des services d'application.

Fichier journal d'installation

Le fichier journal d'installation contient les informations sur les fichiers installés.

Le tableau suivant décrit les propriétés du fichier journal d'installation :

Propriété	Description
Nom du fichier journal	<ul style="list-style-type: none">- Informatica_<Version>_Services_InstallLog.log- Informatica_<Version>_Client_InstallLog.log
Emplacement	Répertoire d'installation
Utilisation	Obtenir les informations sur les fichiers installés et les entrées de registre créées.
Contenu	Répertoires créés, nom des fichiers installés et des commandes exécutées et statut de chaque fichier installé.

Fichiers journaux de Service Manager

Le programme d'installation démarre le service Informatica. Le service Informatica démarre Service Manager pour le nœud. Service Manager génère les fichiers journaux qui indiquent l'état de démarrage d'un nœud. Utilisez ces fichiers pour résoudre les problèmes quand le service Informatica ne peut pas démarrer et que vous ne pouvez pas vous connecter à Informatica Administrator. Les fichiers journaux de Service Manager sont créés sur chaque nœud.

Le tableau suivant décrit les fichiers générés par Service Manager :

Propriété	Description
catalina.out	Événements de journal de la machine virtuelle Java (JVM) qui exécute le gestionnaire de service. Par exemple, un port est disponible pendant l'installation, mais est utilisé lorsque le gestionnaire de service démarre. Utilisez ce journal pour obtenir plus d'informations sur le port indisponible lors du démarrage du gestionnaire de service. Le fichier catalina.out se trouve dans le répertoire suivant : <répertoire d'installation d'Informatica>/logs/<nom du nœud>/catalina.out
node.log	Événements de journal générés lors du démarrage du gestionnaire de service sur un nœud. Vous pouvez utiliser ce journal pour obtenir davantage d'informations sur l'échec du démarrage du gestionnaire de service pour un nœud. Par exemple, si le gestionnaire de service ne peut pas se connecter à la base de données de configuration du domaine au bout de 30 secondes, il ne peut pas démarrer. Le fichier node.log se trouve dans le répertoire /tomcat/logs.

Remarque: Service Manager utilise également node.log pour consigner les événements quand Log Manager est indisponible. Par exemple, si la machine où Service Manager s'exécute ne dispose pas suffisamment d'espace disque disponible pour enregistrer les fichiers d'événements du journal, Log Manager est indisponible.

Dépannage des domaines et des nœuds

Le programme d'installation peut générer des erreurs lors de la création et de la configuration des domaines et des nœuds pendant l'installation d'Informatica.

Vous pouvez rencontrer des erreurs avec les tâches d'installation suivantes :

- Ajout de la base de données de configuration du domaine
- Ajout ou jointure d'un domaine
- Démarrage d'Informatica
- Ping sur le domaine
- Ajout d'une licence

Création du référentiel de configuration de domaine

Si vous créez un domaine, le programme d'installation crée un référentiel de configuration de domaine pour stocker les métadonnées du domaine. Le programme d'installation utilise les options que vous avez entrées lors de l'installation pour ajouter les métadonnées de configuration au référentiel de configuration du domaine. Le programme d'installation utilise JDBC pour communiquer avec la base de données. Il n'est pas nécessaire de configurer la connectivité ODBC ou native sur la machine où vous avez installé les services d'Enterprise Data Catalog.

Le programme d'installation crée et place une table dans la base de données du référentiel de configuration du domaine pour vérifier les informations de connexion. Le compte utilisateur de la base de données doit avoir les privilèges de création sur la base de données. Chaque domaine doit avoir un référentiel de configuration de domaine séparé.

Création ou jointure d'un domaine

Le programme d'installation effectue différentes tâches selon que vous créez un domaine ou que vous le joignez :

- **Création d'un domaine.** Le programme d'installation exécute la commande `infasetup DefineDomain` pour créer le domaine et le nœud de passerelle du domaine sur la machine actuelle selon les informations entrées dans la fenêtre Configurer le domaine.
- **Jointure d'un domaine.** Le programme d'installation exécute la commande `infasetup DefineWorkerNode` pour créer un nœud sur la machine actuelle, et exécute la commande `infacmd AddDomainNode` pour ajouter le nœud au domaine. Le programme d'installation utilise les informations que vous entrez dans la fenêtre Configurer le domaine pour exécuter les commandes.

Les commandes `infasetup` et `infacmd` échouent si le nœud de passerelle n'est pas disponible. Si le nœud de passerelle n'est pas disponible, vous ne pouvez pas vous connecter à Informatica Administrator.

Par exemple, la commande `DefineDomain` échoue si vous cliquez sur Tester la connexion et que le test de connexion réussisse mais que la base de données ne soit plus disponible avant que vous ne cliquiez sur Suivant. La commande `DefineDomain` peut également échouer si le nom d'hôte ou l'adresse IP n'appartient pas à la machine actuelle. Vérifiez que la base de données pour la configuration du domaine est disponible et que le nom d'hôte est correct et réessayez.

Si la commande `AddDomainNode` échoue, vérifiez que le service Informatica est exécuté sur le nœud de passerelle et réessayez.

Exécution d'une ressource

La valeur de compteur d'exécution est négative lorsque vous exécutez une ressource.

Ce problème se produit lorsque l'heure de l'horloge système du service de catalogue Informatica et l'heure de la machine du nœud de service ne sont pas synchronisées. Pour résoudre ce problème, assurez-vous que l'heure de l'horloge système du service de catalogue Informatica et l'heure de la machine du nœud de service sont synchronisées.

Démarrage d'Enterprise Data Catalog

Le programme d'installation exécute `infaservice` pour démarrer le service Informatica. Pour résoudre les problèmes en cas d'échec de démarrage d'Enterprise Data Catalog, utilisez les informations dans le journal de débogage de l'installation et dans les fichiers journaux `node.log` et `catalina.out` du gestionnaire de service pour identifier la cause de l'erreur.

Si vous créez un domaine, connectez-vous à Informatica Administrator après le démarrage du service Informatica pour vérifier que le domaine est disponible. Si vous joignez un domaine, connectez-vous à Informatica Administrator après le démarrage du service Informatica pour vérifier que le nœud a été correctement créé et démarré.

Enterprise Data Catalog peut ne pas démarrer pour les raisons suivantes :

- **La mémoire système de Service Manager est insuffisante.** Il est possible que l'environnement d'exécution Java (JRE) qui démarre Informatica et exécute le gestionnaire de service ne dispose pas suffisamment de mémoire système pour démarrer. Définissez la variable d'environnement `INFA_JAVA_OPTS` pour configurer la quantité de mémoire système utilisée par Enterprise Data Catalog. Sous Linux, vous pouvez définir la configuration de la mémoire lors du démarrage d'Informatica.
- **La base de données de configuration de domaine n'est pas disponible.** Enterprise Data Catalog ne parvient pas à démarrer sur un nœud si le gestionnaire de service d'un nœud de passerelle ne peut pas se

connecter à la base de données de configuration de domaine dans les 30 secondes. Vérifiez que le référentiel de configuration du domaine est disponible.

- **Certains des dossiers du répertoire d'installation d'Informatica ne disposent pas des autorisations d'exécution appropriées.** Accordez l'autorisation d'exécuter sur le répertoire d'installation d'Informatica.
- **Échec de résolution de localhost.** Si vous utilisez un cluster incorporé et que localhost ne se résout pas correctement, le service de cluster Informatica peut échouer. Vous devez vérifier que localhost se résout correctement.

Ping sur le domaine

Le programme d'installation exécute la commande Ping *infacmd* pour vérifier que le domaine est disponible avant qu'il ne poursuive l'installation. Le domaine doit être disponible pour que les objets de licence soient ajoutés au domaine. Si la commande Ping échoue, démarrez Enterprise Data Catalog sur le nœud de passerelle.

Ajout d'une licence

Le programme d'installation exécute la commande AddLicense *infacmd* pour lire le fichier de clé de licence Informatica et créer un objet de licence dans le domaine. Pour exécuter les services d'application dans Informatica Administrator, un objet de licence valide doit exister dans le domaine.

Si vous utilisez une licence incrémentielle et effectuez une jointure de domaine, le numéro de série de la licence incrémentielle doit correspondre au numéro de série d'un objet de licence existant dans le domaine. Si les numéros de série ne correspondent pas, la commande AddLicense échoue.

Vous pouvez obtenir plus d'informations sur le contenu du fichier de clé de licence utilisé pour l'installation, y compris le numéro de série, la version, la date d'expiration, les systèmes d'exploitation et les options de connectivité dans le journal de débogage de l'installation. Vous pouvez obtenir plus d'informations sur les licences existantes pour le domaine dans Informatica Administrator.

Dépannage des problèmes courants de déploiement des clusters

Échec de l'ingestion avec le message d'erreur `org.apache.zookeeper KeeperException$AuthFailedException: KeeperErrorCode = AuthFailed`.

Ajoutez les lignes suivantes au fichier `/etc/krb5.conf` pour tous les clusters :

- `[libdefaults]`
- `kdc_timeout=60000`
- `max_retries = 6`

Échec de l'ingestion avec le message d'erreur `org.apache.zookeeper KeeperException$SessionExpiredException: KeeperErrorCode = Session expired`.

Définissez les propriétés personnalisées suivantes pour le service de catalogue à l'aide d'Informatica Administrator :

- `LdmCustomOptions.hclient.hbase.client.scanner.timeout.period = 900000`

- `LdmCustomOptions.hclient.hbase.rpc.timeout = 900000`
- `LdmCustomOptions.zkclient.zookeeper.session.timeout = 90000`

Échec de l'exécution de l'analyseur dans un cluster configuré pour la haute disponibilité.

Assurez-vous que tous les services de cluster tels que HDFS, YARN, ZooKeeper dans le cluster sont configurés pour la haute disponibilité.

Le compteur de connexions du client Apache Zookeeper est bas et le message d'erreur suivant s'affiche dans le fichier journal de Zookeeper : *"Too many connections from /<ipaddress>- max is 60."* Il est possible que vous rencontriez également des échecs du service d'ingestion avec le message d'erreur suivant dans les fichiers journaux : *"Unexpected error, closing socket connection and attempting reconnect java.io.IOException: Connection reset by peer."*

Apache Zookeeper est une application partagée et nécessite plusieurs connexions ouvertes et configurées. Remplacez la valeur du paramètre `maxclientCnxns` par la valeur recommandée en fonction de la charge du cluster et démarrez le cluster entier à nouveau.

Le service de catalogue ne parvient pas à démarrer après avoir redémarré le service de cluster Informatica.

Vous devez redémarrer manuellement le service de catalogue en même temps que le service de cluster Informatica.

Un des composants de cluster ne parvient pas à démarrer avec le message d'erreur suivant dans le fichier journal : *"Caused by: java.lang.NumberFormatException: For input string: "0LdmCustomOptions.HbaseMasterProperties."*

Ce problème peut se produire en raison de paramètres incorrects de propriétés personnalisées pour le service de catalogue, qui ont été configurés dans Informatica Administrator. Vérifiez que chaque propriété personnalisée à mettre à jour est définie en tant que paramètre `LdmCustomOptions` dans Informatica Administrator. Vous pouvez ensuite démarrer le service de catalogue à nouveau pour afficher le cluster.

Le service de catalogue ne parvient pas à répondre avec le message d'erreur suivant dans le fichier journal :

"Connection timed out for connection string () and timeout () / elapsed () org.apache.curator.CuratorConnectionLossException: KeeperErrorCode = ConnectionLoss at org.apache.curator.ConnectionState.checkTimeouts(ConnectionState.java:197)".* Il est possible que le fichier journal du client d'ingestion ou de HBase contienne le message d'erreur suivant : *"Possibly transient ZooKeeper, quorum=..., exception=org.apache.zookeeper.KeeperException ConnectionLossException: KeeperErrorCode = ConnectionLoss for /hbase/meta-region-server."

Ce problème pourrait se produire en raison de l'incapacité du service de catalogue à accéder aux composants du cluster de base, tels qu'Apache Zookeeper. Les problèmes de Zookeeper peuvent se produire en raison de problèmes de disques temporaires. Corrigez les problèmes de disques et vérifiez qu'Apache Zookeeper est opérationnel.

Le fichier journal d'Apache Zookeeper affiche le message d'erreur suivant en raison de la latence de disque élevée : *"fsync-ing the write ahead log in SyncThread:3 took 25115ms which will adversely affect operation latency."*

Il est recommandé d'allouer un disque dédié, et non une partition de disque, à Apache Zookeeper, car il doit fournir des garanties de haute cohérence à son client. Vérifiez d'avoir alloué le nombre recommandé de disques durs pour la taille de la charge de travail. Vous devez également pointer le répertoire de données Zookeeper vers son disque dédié.

Certains des membres du quorum de l'ensemble Apache Zookeeper ne sont pas accessibles, et le fichier journal affiche les messages d'avertissement semblables au suivant : *"[QuorumPeer[myid=3]/0:0:0:0:0:0:2181:QuorumCnxManager@383] - Cannot open channel to 2 at election address 10.65.144.18:3888 java.net.ConnectException: Connection refused at java.net.PlainSocketImpl.socketConnect(Native Method)"*

Vérifiez que les hôtes Zookeeper sont accessibles sur le réseau. Il est important que la mémoire des membres du quorum Zookeeper soit suffisante. Vérifiez que les nœuds répondent aux prérequis recommandés de mémoire. Vérifiez que seuls les processus liés au service de catalogue sont exécutés sur le même hôte.

Plusieurs membres de quorum Apache Zookeeper affichent des messages de fin de session sur le client, tels que le suivant : "Caught end of stream exception EndOfStreamException: Unable to read additional data from client sessionid 0x0, likely client has closed socket, Processed session termination for sessionid."

Surveillez l'utilisation des segments de mémoire pour les membres du quorum Zookeeper. Vous pouvez envisager d'augmenter les segments de mémoire de Zookeeper et de démarrer le cluster entier à nouveau.

Le service d'ingestion ne parvient pas à démarrer, et le fichier journal affiche le message d'erreur suivant : "Initial job has not accepted any resources; check your cluster UI to ensure that workers are registered and have sufficient memory".

Cette erreur indique une quantité insuffisante de mémoire ou de cœurs du processeur dans le cluster entier. Vérifiez que le cluster possède les ressources suffisantes pour lancer de nouvelles applications.

Le service de catalogue ne parvient pas à démarrer après avoir modifié la propriété personnalisée

`LdmCustomOptions.loadType` dans Informatica Administrator et le fichier journal contient le message d'erreur suivant : **"Caused by: org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'hbaseGraphFactory': Invocation of init method failed; nested exception is com.thinkaurelius.titan.core.TitanConfigurationException: Local settings present for one or more globally managed options: [cluster.max-partitions]. These options are controlled through the ManagementSystem interface; local settings have no effect."**

Vous devez sauvegarder toutes les données avant de modifier la propriété personnalisée du type de charge, modifier le paramètre du type de charge, démarrer le cluster à nouveau, puis charger les données sauvegardées.

Échec du service de catalogue ou du service d'ingestion en raison de l'indisponibilité de certaines tables de base de données HBase avec le message d'erreur suivant dans les fichiers journaux : "Caused by: com.thinkaurelius.titan.diskstorage.TemporaryBackendException: Temporary failure in storage backend at com.thinkaurelius.titan.diskstorage.hbase.HBaseStoreManager.ensureTableExists (HBaseStoreManager.java:754) Caused by: org.apache.hadoop.hbase.TableNotFoundException: Idmns:titan_db."

Cette erreur se produit en raison d'un nettoyage inapproprié des données relatives au service de catalogue ou au service d'ingestion. Si vous avez modifié le type de charge à l'aide de la propriété personnalisée `LdmCustomOptions.loadType` dans Informatica Administrator, vérifiez que vous avez sauvegardé toutes les données liées au service, supprimé entièrement les données, puis que vous les avez rechargées.

Échec du service de catalogue ou du service d'ingestion en raison de la présence de certaines tables de base de données HBase avec le message d'erreur suivant dans les fichiers journaux : "Caused by: org.apache.hadoop.hbase.ipc.RemoteWithExtrasException (org.apache.hadoop.hbase.TableExistsException): org.apache.hadoop.hbase.TableExistsException: Idmns:exDocStore at org.apache.hadoop.hbase.master.procedure.CreateTableProcedure.prepareCreate."

Cette erreur se produit en raison d'un nettoyage inapproprié des données relatives au service de catalogue ou au service d'ingestion. Si vous avez modifié le type de charge à l'aide de la propriété personnalisée `LdmCustomOptions.loadType` dans Informatica Administrator, vérifiez que vous avez sauvegardé toutes les données liées au service, supprimé entièrement les données, puis que vous les avez rechargées.

Échec du service de catalogue ou du service d'ingestion en raison de certaines tables de base de données HBase avec le message d'erreur suivant dans les fichiers journaux : "Caused by: org.apache.hadoop.hbase.TableNotEnabledException: Idmns:DataDomain_stage is disabled at org.apache.hadoop.hbase.client.HConnectionManager \$HConnectionImplementation.relocateRegion(HConnectionManager.java:1139)."

Cette erreur se produit en raison d'un nettoyage inapproprié des données relatives au service de catalogue ou au service d'ingestion. Si vous avez modifié le type de charge à l'aide de la propriété personnalisée `LdmCustomOptions.loadType` dans Informatica Administrator, vérifiez que vous avez sauvegardé toutes les données liées au service, supprimé entièrement les données, puis que vous les avez rechargées.

Échec du service de catalogue ou du service d'ingestion avec l'une des erreurs suivantes dans les fichiers journaux : le fichier journal HBase contient le message d'erreur "*Caused by: com.thinkaurelius.titan.diskstorage.TemporaryBackendException: Temporary failure in storage backend Caused by: org.apache.hadoop.hbase.client.RetriesExhaustedException: Failed after attempts=4, exceptions: failed on local exception: java.io.IOException: Connection reset by peer This server is in the failed servers list.*" Il est possible que le fichier journal du service d'ingestion contienne le message d'erreur "*Caused by: org.apache.spark.SparkException: Job aborted due to stage failure: Task 0 in stage 9468.0 failed 4 times, most recent failure: Lost task 0.3 in stage 9468.0 (TID 12018): org.apache.hadoop.hbase.client.RetriesExhaustedException: Failed after attempts=4, exceptions: This server is in the failed servers list.*"

L'erreur pourrait se produire lorsque le serveur HBase n'est pas accessible en raison de facteurs, tels que le partitionnement du réseau, l'indisponibilité du serveur de région HBase due à la charge de travail, ou de ses activités de nettoyage internes, telles que la répartition et les compactages de données. Vous pouvez essayer de redémarrer le service de catalogue avec une mémoire accrue pour HBase.

Il est possible que les serveurs HBase échouent si Apache Zookeeper ou HDFS n'est pas accessible. Le service de catalogue essaie de démarrer automatiquement les instances HBase jusqu'au nombre configuré de tentatives, sauf si l'erreur est fatale. Dans de tels cas, vous devrez peut-être redémarrer manuellement le service de catalogue.

L'application Apache YARN s'arrête par intermittence et les nœuds de cluster ne sont pas utilisés pour soumettre les applications de cluster. Le fichier journal du gestionnaire de ressource YARN contient le message d'erreur suivant : "*Node irl66dsg04.xxx.com:8041 reported UNHEALTHY with details: 1/1 log-dirs are bad: /var/log/hadoop-yarn/container, Node Transitioned from RUNNING to UNHEALTHY, Container Transitioned from RUNNING to KILLED, Removed node irl66dsg04.xxx.com:8041 cluster capacity: <memory:184320, vCores:96>*"

Vérifiez l'espace disque de / `partition` sur le disque dur en utilisant les commandes, telles que `df`. Apache YARN considère un nœud comme étant défectueux et termine les applications de nœud si l'utilisation de l'espace disque est supérieure à 80 %. Supprimez les données inutiles de la partition '/'. Si vous possédez plusieurs disques, pointez / `partition` sur un disque non chargé d'autres affectations.

Le serveur de la région HBase s'arrête avec un message d'erreur semblable au suivant dans le fichier journal : "*Sleeper: Slept 15559ms instead of 3000ms, this is likely due to a long garbage collecting pause and it's usually bad. HeapMemoryManager: heapOccupancyPercent 0.9935025 is above heap occupancy alarm watermark (0.95). JvmPauseMonitor: Detected pause in JVM or host machine (eg GC): pause of approximately 3733ms. GC pool 'ParNew' had collection(s): count=1 time=4075ms.*"

Cette erreur se produit en raison de problèmes de mémoire HBase. Vérifiez que vous avez configuré le type approprié de charge de travail ou de jeu de données pour votre charge de travail d'Enterprise Data Catalog en utilisant la propriété personnalisée `LdmCustomOptions.loadType` dans Informatica Administrator. Parfois, vous devrez peut-être augmenter manuellement les paramètres des segments HBase à l'aide d'Informatica Administrator, puis redémarrer le service de catalogue.

Échec du service d'ingestion avec des problèmes de mémoire, et le fichier journal du service d'ingestion contient des messages d'erreur semblables au suivant : "*TaskSetManager: Lost task 1.0 in stage 18.0 (TID 39, INVRLX65CMD03.informatica.com): org.apache.spark.util.TaskCompletionListenerException: GC overhead limit exceeded at org.apache.spark.TaskContextImpl.markTaskCompleted(TaskContextImpl.scala:83) at org.apache.spark.scheduler.Task.run(Task.scala:72)*"

Cette erreur se produit en raison de la mémoire HBase réduite. Vérifiez que vous avez configuré le type approprié de charge de travail ou de jeu de données pour votre charge de travail d'Enterprise Data Catalog en utilisant la propriété personnalisée `LdmCustomOptions.loadType` dans Informatica Administrator. Dans certains cas, vous devrez peut-être augmenter manuellement les paramètres des segments HBase à l'aide d'Informatica Administrator, puis redémarrer le service de catalogue.

Échec du service d'ingestion avec le message d'erreur suivant dans le fichier journal : "*ERROR executor.CoarseGrainedExecutorBackend: RECEIVED SIGNAL 15: SIGTERM spark.TaskContextImpl: Error in*

TaskCompletionListener java.io.IOException: Filesystem closed at org.apache.hadoop.hdfs.DFSClient.checkOpen(DFSClient.java:761)"

Cette erreur indique que le système de fichiers Hadoop n'est pas accessible. Utilisez l'interface utilisateur d'Apache Ambari pour vérifier que HDFS est opérationnel.

Échec d'un nœud de données HDFS avec un message d'erreur semblable au suivant: " BlockStateChange: BLOCK NameSystem.addToCorruptReplicasMap: blk_1073876841 added as corrupt on 10.65.145.216:50010 by irlcmg07.informatica.com/10.65.145.216 because reported RWR replica with genstamp 136273 does not match COMPLETE block's genstamp in block map 138353."

Cette erreur se produit généralement dans un déploiement à nœud unique, car les données ne sont pas répliquées. Il est possible que le problème se produise en raison de la corruption de données dans certains blocs de données HDFS. La corruption de données peut se produire en raison d'un volume de disque ou d'un disque corrompu dont la mémoire est saturée.

Si vous possédez plus d'un répertoire de disque configuré pour HDFS, vous pouvez essayer de modifier la valeur de `dfs.datanode.failed.volumes.tolerated` à partir de 0. Une valeur de 0 entraîne l'arrêt du nœud de données, même avec un minimum d'un volume de disque qui contient des données corrompues.

Où puis-je trouver tous les fichiers journaux liés au service de cluster Informatica et comment puis-je les utiliser pour effectuer le dépannage ?

Vous pouvez trouver les détails des problèmes liés au service de cluster Informatica en procédant comme suit :

1. Ouvrez et vérifiez le fichier journal du service de cluster Informatica à l'emplacement suivant :
<Install Directory>/logs/<Infomatica Cluster Service Node Name>/services/InfahadoopService/<Infomatica Cluster Service Name>.
2. Ouvrez et vérifiez le fichier journal du serveur Apache Ambari sur l'hôte du serveur Ambari à l'emplacement suivant : /var/log/ambari-server
3. Ouvrez et vérifiez le fichier journal de l'agent Apache Ambari sur l'hôte de l'agent Ambari à l'emplacement suivant : /var/log/ambari-agent.
4. Si vous ne pouvez pas résoudre le problème en suivant les étapes précédentes, procédez comme suit :
 - a. Lancez l'application Apache Ambari à l'aide de l'URL `http://<ambari-server host>:8080/` .
 - b. Cliquez sur **ops** en haut de l'application pour vérifier les demandes en échec :



- c. Enregistrez le nom de l'hôte sur lequel la demande a échoué et le composant Hadoop lié à la demande ayant échoué.
- d. Connectez-vous à l'hôte où la demande a échoué.
- e. Vérifiez le fichier journal du composant Hadoop spécifique lié à la demande ayant échoué aux emplacements suivants :

Nom du composant	Emplacement du fichier journal
NameNode	/var/log/hadoop/hdfs ou /var/log/hadoop-hdfs
SecondaryNameNode	/var/log/hadoop/hdfs ou /var/log/hadoop-hdfs

Nom du composant	Emplacement du fichier journal
JournalNode	/var/log/hadoop/hdfs ou /var/log/hadoop-hdfs
ZKFC	/var/log/hadoop/hdfs ou /var/log/hadoop-hdfs
DataNode	/var/log/hadoop/hdfs ou /var/log/hadoop-hdfs
HistoryServer	/var/log/hadoop/mapreduce ou /var/log/hadoop-mapreduce
MetricsCollector	/var/log/ambari-metrics-collector
MetricsMonitor	/var/log/ambari-metrics-monitor
AppTimelineServer	/var/log/hadoop-yarn ou /var/log/hadoop/yarn
ResourceManager	/var/log/hadoop-yarn ou /var/log/hadoop/yarn
NodeManager	/var/log/hadoop-yarn ou /var/log/hadoop/yarn
ZookeeperServer	/var/log/zookeeper

Remarque: S'il existe des services Hadoop en cours d'exécution qui n'ont pas été arrêtés lorsque vous avez arrêté le service de cluster Informatica précédemment, il est possible que le texte `java.net.BindException: Address already in use` s'affiche dans le fichier journal. Vous devez alors arrêter ces processus sur les ports mentionnés dans l'exception.

Où puis-je trouver tous les fichiers journaux des applications Apache YARN, telles que Solr, HBase, et le service d'ingestion ?

Vous pouvez procéder comme suit pour afficher les fichiers journaux :

1. Connectez-vous à l'interface utilisateur d'Apache Ambari, puis cliquez sur l'onglet **Service** en haut de la page pour ouvrir la page suivante :



2. Cliquez sur **Liens rapides > ResourceManager UI** pour ouvrir la page suivante qui répertorie toutes les applications :



Vous pouvez afficher les différentes applications lancées par ce service de catalogue sur Apache YARN. La colonne État indique l'état actuel des applications.

3. Cliquez sur le lien sous la colonne **ID** pour ouvrir la page suivante :

Application Metrics			
Total Resource Preempted: <memory.0, vCores.0>			
Total Number of Non-AM Containers Preempted: 0			
Total Number of AM Containers Preempted: 0			
Resource Preempted from Current Attempt: <memory.0, vCores.0>			
Number of Non-AM Containers Preempted from Current Attempt: 0			
Aggregate Resource Allocation: 2054819277 MB-seconds, 1720005 vcore-seconds			
ApplicationMaster			
Attempt Number	Start Time	Node	Logs
1	Fri Dec 11 04:09:52 +0530 2015	inkr65dsg110.informatica.com:8042	logs

4. Pour afficher le fichier journal, cliquez sur **journaux**.

Échec du service d'ingestion avec le message d'erreur suivant :

" **java.io.IOException: Connection reset by peer.**" lors de l'exécution de tâches dans une séquence.

Ce problème se produit en raison du nombre limité de connexions du client Zookeeper autorisées pour Enterprise Data Catalog. Vous pouvez passer la valeur de connexion du client Zookeeper sur 0, ce qui indique un nombre illimité de connexions.

Échec de l'installation d'Apache Ambari lorsque le référentiel yum est configuré pour télécharger Apache Ambari depuis un répertoire personnalisé.

Ce problème se produit lorsque vous avez configuré un référentiel personnalisé pour télécharger Apache Ambari. Pour résoudre ce problème, assurez-vous d'avoir mis à jour les fichiers yum.conf et .repo dans le répertoire `/etc/yum.repos.d/` pour pointer vers l'emplacement où se trouvent les fichiers d'installation d'Apache Ambari.

Une ressource PowerCenter ne peut pas se connecter au domaine Informatica activé pour SSL.

Ce problème se produit généralement lorsque vous n'importez pas le certificat de sécurité dans le truststore local. Vous pouvez importer le certificat de sécurité dans le truststore local pour résoudre ce problème.

Le service de catalogue ne peut pas être activé

Ce problème peut se produire si vous avez activé l'option Recevoir les alertes par e-mail pour le service de catalogue et si le service de messagerie est dans l'état désactivé. Assurez-vous d'avoir activé le service de messagerie.

Pour plus d'informations sur l'activation du service de messagerie, consultez le guide *Administrator Reference for Enterprise Data Catalog*.

Dépannage du déploiement de clusters existants

Échec de l'ingestion de métadonnées dans le catalogue.

Vérifiez que les fichiers de script du programme d'installation d'Enterprise Data Catalog qui lancent les tâches Solr et d'ingestion sont copiés vers l'hôte cible du cluster existant.

Puis-je implémenter la sécurité Kerberos si j'installe Enterprise Data Catalog sur un cluster existant ?

Oui. Enterprise Data Catalog prend en charge l'authentification réseau Kerberos sur un cluster existant.

Le service de catalogue s'est arrêté de façon inattendue et le message d'erreur dans le fichier journal se lit comme suit : « **GSSException: No valid credentials provided (Mechanism level: Server not found in Kerberos database)** ». Comment résoudre le problème ?

Vérifiez que tous les nœuds de cluster du domaine `/etc/hosts` possèdent des noms d'hôtes complets et corrigez les noms d'hôtes incorrects.

J'ai un environnement de cluster Cloudera version 4 et je ne parviens pas à installer Enterprise Data Catalog sur le cluster.

Enterprise Data Catalog prend en charge Cloudera version 5.8 ou ultérieure ou HortonWorks version 2.5 pour le déploiement de cluster Hadoop existant. Mettez à niveau la version Cloudera vers 5.8 ou ultérieure.

J'ai ajouté quelques hôtes contenant des services de haute disponibilité au cluster à l'aide de CDH Manager. Cependant, je ne vois pas les nœuds activés.

Si vous avez ajouté des nœuds à un cluster existant, assurez-vous de les avoir ajoutés à la liste des nœuds Hadoop dans Informatica Administrator et redémarrez le service de catalogue.

Je rencontre des problèmes avec la disponibilité du centre de distribution Kerberos (KDC) et je vois des messages similaires à ceux qui suivent : « (java.security.PrivilegedActionException: javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided (Mechanism level: Connection reset)]) occurred when evaluating Zookeeper Quorum Member's received SASL token. Zookeeper Client will go to AUTH_FAILED state. » Comment résoudre les problèmes ?

Un cluster compatible Kerberos requiert un KDC hautement disponible. Assurez-vous d'avoir activé la haute disponibilité pour KDC.

Le service d'ingestion est interrompu par le fil Apache en raison de problèmes généraux de mémoire avec des erreurs semblables à celles qui suivent : « Container killed by YARN for exceeding memory limits. 10.0 GB of 10 GB physical memory used. Consider boosting spark.yarn.executor.memoryOverhead. » Comment puis-je résoudre les erreurs ?

Le problème se produit en raison de vérifications de la mémoire Apache YARN. Il est recommandé que les deux propriétés suivantes aient la valeur False :

- yarn.nodemanager.pmem-check-enabled
- yarn.nodemanager.vmem-check-enabled

Après avoir brusquement arrêté un domaine et un service de catalogue, vous voyez que l'application YARN continue à s'exécuter.

Si vous n'arrêtez pas le domaine correctement, il est possible que les applications YARN pour HBase, Solr et Spark continuent à s'exécuter. Vous devez arrêter manuellement ces applications YARN avant de redémarrer le domaine et les services d'applications.

Dépannage du déploiement de clusters incorporés

Je vois des échecs de haute disponibilité dans le cluster incorporé.

La haute disponibilité est possible en cas de première installation d'Enterprise Data Catalog sur plus de deux nœuds. Vérifiez que le nombre de nœuds de cluster d'Enterprise Data Catalog n'est pas inférieur à trois. Si vous utilisez un nœud unique pour Enterprise Data Catalog pendant l'installation ou que vous ajoutez successivement plusieurs modes après l'installation, vous ne pourrez pas implémenter la haute disponibilité. Si l'un des hôtes hautement disponibles s'arrête ou est inaccessible, Enterprise Data Catalog peut continuer à s'exécuter, mais il est possible que le cluster ne soit pas hautement disponible. Vous devez alors configurer le nœud qui a été arrêté ou qui est inaccessible de façon à rendre le cluster hautement disponible.

Lorsqu'Oracle et le service de cluster Informatica s'exécutent sur la même machine, le service de cluster Informatica ne démarre pas.

Vérifiez si Oracle est en cours d'exécution sur le port 8080. Le port 8080 est réservé à Apache Ambari. Si Oracle et le service de cluster Informatica sont exécutés sur la même machine, assurez-vous d'exécuter Oracle sur un autre port.

L'outil Apache Ambari ne fonctionne pas après avoir installé Enterprise Data Catalog sur un cluster Hadoop incorporé.

- Le nom d'hôte Ambari que vous spécifiez pendant l'installation est sensible à la casse. Vérifiez que le nom d'hôte répond aux exigences. Informatica recommande d'utiliser des minuscules pour les noms d'hôtes.

Exécutez la commande suivante pour vérifier que le nom d'hôte est correctement configuré :

```
#hostname -f
```

La commande renvoie le nom de domaine complet que vous avez configuré.

- Si vous avez installé Enterprise Data Catalog sur Red Hat Enterprise Linux (RHEL) version 6.5 ou ultérieure, vérifiez que tous les référentiels du système d'exploitation de base sont disponibles. Le programme d'installation d'Enterprise Data Catalog extrait de nombreux packages des référentiels du système d'exploitation de base. Par exemple, les hôtes doivent pouvoir accéder au référentiel `rhel-6-server-optional-rpms` de Red Hat Enterprise Linux pour que l'installation soit effectuée. Si vous ne disposez pas de l'ensemble complet des référentiels du système d'exploitation de base, vous pouvez rencontrer des problèmes d'installation.
- Vérifiez la version de Python installée. Enterprise Data Catalog prend en charge Python version 2.6.8-0.15.1 ou antérieure. La version Python 2.7.9 ou ultérieure n'est pas prise en charge.
- Avant d'installer Enterprise Data Catalog, vérifiez que les ports 8080, 8440 et 8411 ne sont pas utilisés. Apache Ambari utilise ces ports pendant l'installation.

Le service de cluster Informatica ne répond pas.

Assurez-vous de ne pas avoir d'autorisations `777` dans le répertoire `/var`. Toutefois, vous devez disposer de l'autorisation d'écriture dans le répertoire `/var`.

Le serveur Ambari de la base de données PostgreSQL par défaut s'arrête ou vous souhaitez déplacer le serveur Ambari d'un hôte vers un autre.

Vous pouvez effectuer les étapes suivantes pour configurer le serveur Ambari sur un nouvel hôte :

1. Désactivez le service de cluster Informatica à l'aide d'Informatica Administrator.
2. Redémarrez l'instance PostgreSQL sur l'hôte du serveur Ambari. Sauvegardez les bases de données PostgreSQL `ambarirca` et `ambari`.

Remarque: Pour en savoir plus sur la sauvegarde des bases de données PostgreSQL, reportez-vous à la section *Déplacement du serveur Ambari* dans la documentation de HortonWorks.

3. Mettez à jour la valeur du nom d'hôte du serveur Ambari du service de cluster Informatica avec le nouveau nom d'hôte du serveur Ambari. Pour mettre à jour le nom d'hôte dans Informatica Administrator, sélectionnez le service de catalogue, puis, dans le champ **Service de cluster Informatica** sous **Options du cluster Hadoop**, entrez le nom d'hôte.
4. Activez le service de cluster Informatica. Cette action installe le serveur Ambari sur le nouvel hôte de passerelle Hadoop que vous avez fourni et met à jour l'agent Ambari avec le nouvel hôte de serveur Ambari.
5. Désactivez le service de cluster Informatica.
6. Supprimez les deux bases de données `ambarirca` et `ambari` de l'instance PostgreSQL sur le nouvel hôte de passerelle Hadoop.
7. Restaurez les deux bases de données `ambarirca` et `ambari` à partir de la sauvegarde de l'hôte de passerelle Hadoop précédent.

Remarque: Pour en savoir plus sur la restauration des bases de données PostgreSQL à partir d'une sauvegarde, reportez-vous à la section *Déplacement du serveur Ambari* dans la documentation de HortonWorks.

8. Activez le service de cluster Informatica.

Le serveur Apache Ambari ne parvient pas à démarrer et le message d'erreur suivant s'affiche dans le fichier journal

correspondant : About to start PostgreSQLERROR: Exiting with exit code 1.REASON: Unable to start PostgreSQL server. Exiting

Ajoutez `127.0.0.1 localhost localhost.localdomain` au fichier `/etc/hosts`.

Je vois que le cluster n'est pas hautement disponible.

Vérifiez que tous les nœuds qui hébergent des composants de haute disponibilité sont bien en cours d'exécution. Si l'un des nœuds qui héberge des composants de haute disponibilité s'arrête, le cluster cesse d'être hautement disponible. Assurez-vous de configurer le nœud qui s'était arrêté.

Lorsque l'un des nœuds esclaves du cluster est inaccessible, je ne peux pas activer le service de cluster Informatica.

Si l'un des nœuds esclaves est inaccessible en raison d'une défaillance inattendue, vous devez supprimer l'hôte de la liste des agents Apache Ambari dans Informatica Administrator, ou reconfigurer le nœud esclave avant de recycler le service de cluster d'Informatica.

J'ai supprimé un service de catalogue existant et en ai activé un nouveau. Cependant, je suis incapable d'accéder aux données du catalogue et de les utiliser.

Si vous souhaitez pointer un nouveau service de catalogue vers les données existantes du catalogue, assurez-vous de spécifier pour le nouveau service de catalogue le même nom de cluster de service que celui que vous avez utilisé pour le service de catalogue supprimé. Spécifiez le nom du cluster de service dans Informatica Administrator sous la section **Options du cluster Hadoop** dans l'onglet **Propriétés**.

Après avoir ajouté quelques nœuds à un cluster incorporé existant, Apache Ambari Metrics System ne démarre pas.

Cet échec peut se produire parce que certaines machines, en particulier les machines virtuelles, ne disposent pas des packages système requis. Veillez à ce que les nouveaux hôtes que vous ajoutez répondent aux prérequis pour le déploiement du cluster incorporé d'Enterprise Data Catalog. Reportez-vous aux sections *Prérequis* et *Préparation de l'environnement de cluster Hadoop incorporé* du chapitre *Méthodes de déploiement* de ce guide.

Échec de l'agent Apache Ambari avec l'un des messages d'erreur suivants dans le fichier journal de l'agent Ambari :

```
NetUtil.py:67 - SSLERROR: Failed to connect. Please check openssl library versions or INFO
2014-04-02 04:25:22,669 NetUtil.py:55 - Failed to connect to https://{ambari-server}:8440/
cert/ca due to [Errno 1] _ssl.c:492: error:100AE081:elliptic curve
routines:EC_GROUP_new_by_curve_name:unknown group
```

Une des conditions préalables pour que l'agent Apache Ambari fonctionne correctement est d'avoir une version 1.0.1e ou ultérieure d'OpenSSL. Vous pouvez effectuer les étapes suivantes :

1. Vérifiez la version de la bibliothèque OpenSSL installée sur vos hôtes à l'aide de la commande suivante :

```
rpm -qa | grep openssl
```
2. Si la sortie de la commande précédente lit `openssl-1.0.1e-15.x86_64 (1.0.1 Build 15)`, vous devez mettre à niveau la bibliothèque OpenSSL. Pour mettre à niveau la bibliothèque OpenSSL, exécutez la commande suivante :

```
yum upgrade openssl
```
3. Vérifiez que la nouvelle version d'OpenSSL est installée en utilisant la commande `rpm`.
4. Redémarrez les agents Apache Ambari et cliquez sur **Réessayer > Échec** dans l'interface utilisateur de l'assistant.

Lorsque vous installez Enterprise Data Catalog sur un cluster incorporé, le programme d'installation ne crée pas le service de cluster Informatica en raison de problèmes d'autorisation.

Si l'utilisateur racine ne dispose pas de l'autorisation requise pour ajouter des utilisateurs sous le répertoire de base de l'utilisateur, le fichier journal des tâches affiche le message d'erreur suivant :

```
Execution of 'useradd -m -G hadoop -g hadoop mapred' returned 12. useradd: cannot create directory /home/mapred
```

Vous pouvez alors modifier le répertoire d'accueil de l'utilisateur de la machine virtuelle en répertoire pour lequel l'utilisateur racine dispose de l'autorisation de création :

```
sudo vim /etc/default/useradd
```

Passez le répertoire de base en HOME=/export/home.

Échec du serveur de chronologie d'application Apache Ambari avec le message d'erreur suivant : ps -p 'hadoop-yarn/yarn/yarn-yarn-timelineserver.pid' failed: <https://issues.apache.org/jira/browse/AMBARI-4825>

Ce problème peut se produire parce que plusieurs terminaux sont actifs. Utilisez les commandes w, whoami et kill pour vérifier et fermer tous les terminaux excepté celui qui est pertinent. Vous pouvez ensuite redémarrer le cluster YARN.

L'installation du serveur Apache Ambari échoue sur certaines machines hôtes et l'erreur suivante apparaît dans les fichiers journaux du serveur Ambari : Ambari-server status Traceback (most recent call last) File "/usr/sbin/ambari-server.py", line 26, in <module> from ambari_commons.exceptions import FatalException, NonFatalException ImportError: No module named ambari_commons.exceptions.

Ce problème se produit lorsque vous essayez d'installer un serveur Ambari sur un hôte unique qui dispose d'un agent Ambari d'une installation précédente. Le lien /usr/lib/python2.6/site-packages/ambari_commons doit pointer vers /usr/lib/ambari-server/lib/ambari_commons au lieu de /usr/lib/ambari-agent/lib/ambari_commons.

Lorsque vous ajoutez uniquement deux nœuds au cluster, l'installation du cluster échoue avec le code d'erreur suivant 00030: Cannot create a cluster with 2 hosts. Minimum 3 hosts are required for creating the High Availability cluster.

Vous ne pouvez pas créer de cluster avec seulement deux nœuds. Vous devez fournir au moins trois nœuds pour un cluster à haute disponibilité et un hôte pour un cluster qui n'est pas de haute disponibilité. Vous pouvez ajouter des nœuds à un cluster à nœud unique existant déjà configuré. Toutefois, vous ne pouvez pas configurer le cluster en tant que cluster à haute disponibilité.

Lorsque vous créez un cluster, la vérification de la configuration système minimale requise échoue avec l'un des codes d'erreur suivants : 00026, 00027 ou 00028.

Si vous disposez d'un cluster à nœud unique, la machine hôte doit respecter les critères de configuration minimale pour les nœuds principaux. Si vous disposez d'un cluster à haute disponibilité, au moins trois des machines hôtes doivent satisfaire aux critères de configuration minimale pour les nœuds principaux. Les machines hôtes restantes doivent satisfaire aux critères de configuration minimale pour les nœuds esclaves.

Vous ne pouvez pas supprimer un nœud du cluster et vous voyez l'un des codes d'erreur suivants dans le fichier journal : 00035 ou 00036.

Le code d'erreur 00035 indique que lors de la suppression du nœud, le nombre de nœuds de données en direct dans le cluster se réduit à moins de trois. Le nombre minimal de nœuds en direct requis dans le cluster est de trois. Le code d'erreur 0036 indique qu'il y a eu une tentative de suppression d'un nœud qui héberge les services principaux. Vous ne pouvez pas supprimer un nœud qui héberge les services principaux.

Le nœud de données HDFS affiche des erreurs indiquant fréquemment des opérations inconnues avec les erreurs suivantes dans les fichiers journaux du nœud de données : DataXceiver error processing unknown operation

```
src: /127.0.0.1:33349 dst: /127.0.0.1:50010 java.io.EOFException at
java.io.DataInputStream.readShort DataInputStream.java:315) at
org.apache.hadoop.hdfs.protocol.datatransfer.Receiver.readOp Receiver.java:58)
```

Apache Ambari ouvre une connexion de socket au nœud de données HDFS chaque minute pour le surveiller. Vous pouvez ignorer ces erreurs, car elles n'affectent pas les opérations de cluster.

Le domaine Informatica, le service d'intégration de données et le service de gestion de contenu sont sécurisés à l'aide du protocole SSL. Si je change les paramètres du service de catalogue de façon à activer le mode SSL, le service ne parvient pas à démarrer. Comment résoudre le problème ?

Après avoir configuré le domaine Informatica, le service d'intégration de données et le service de gestion de contenu de façon à les sécuriser avec le protocole SSL à l'aide du programme d'installation LDM, effectuez les opérations suivantes :

1. Exportez le certificat keystore du service de catalogue.
2. Importez le certificat keystore dans le fichier truststore Informatica.
3. Placez le fichier truststore Informatica sur tous les nœuds Hadoop. Assurez-vous de suivre la même structure de répertoire pour le fichier truststore sur toutes les machines hôtes.
4. Dans Informatica Administrator, spécifiez l'emplacement du fichier truststore Informatica commun dans le champ **Emplacement du fichier truststore du domaine** de la section **Options avancées** du service de cluster Informatica.
5. Dans la boîte de dialogue **Modifier les propriétés de sécurité** de l'onglet **Processus** du service de cluster Informatica, sélectionnez **Activer TLS (Transport Layer Security)** et spécifiez le chemin d'accès au fichier keystore mentionné à l'étape 1.
6. Activez le service de cluster Informatica. Si le service est déjà activé, désactivez-le en mode **Complet**, puis réactivez le service.
7. Accédez à la section Propriétés de sécurité du service de catalogue et spécifiez le chemin d'accès au fichier keystore mentionné à l'étape 1.
8. Activez le service de catalogue.

Je ne trouve pas les fichiers Apache Ambari dans le programme d'installation pour créer le service de cluster Informatica sur le cluster incorporé.

Si vous choisissez de créer le service de cluster Informatica sur le cluster incorporé, vous pouvez copier les fichiers ambaribinaries.tar.gz dans le répertoire `Installer/services/InfaHadoopService/Binaries`.

Dépannage des problèmes liés au services d'application

Le service de catalogue ne parvient pas à démarrer lorsqu'il est configuré sur NFS (Network File System).

Montez et configurez le système de fichiers local pour le service de catalogue.

ANNEXE A

Démarrage et arrêt des services d'Enterprise Data Catalog

Cette annexe comprend les rubriques suivantes :

- [Démarrage et arrêt des services d'Enterprise Data Catalog sous Linux, 181](#)
- [Arrêt des services d'Enterprise Data Catalog dans l'outil Administrator tool, 181](#)
- [Règles et instructions de démarrage et d'arrêt d'Enterprise Data Catalog, 182](#)

Démarrage et arrêt des services d'Enterprise Data Catalog sous Linux

Sous Linux, exécutez `infaservice.sh` pour démarrer et arrêter le démon d'Enterprise Data Catalog. Les `infaservice.sh` est installé dans le répertoire suivant :

```
<Enterprise Data Catalog installation directory>/tomcat/bin
```

1. Accédez au répertoire dans lequel se trouve `infaservice.sh`.
2. À l'invite de commande, tapez la commande suivante pour démarrer le démon :

```
infaservice.sh startup
```

Entrez la commande suivante pour arrêter le daemon :

```
infaservice.sh shutdown
```

Remarque: Si vous utilisez un lien symbolique pour spécifier l'emplacement de `infaservice.sh`, définissez la variable d'environnement `INFA_HOME` sur l'emplacement du répertoire d'installation d'Enterprise Data Catalog.

Arrêt des services d'Enterprise Data Catalog dans l'outil Administrator tool

Lorsque vous arrêtez un nœud à l'aide d'Informatica Administrator, vous arrêtez le service de catalogue sur ce nœud.

Vous pouvez abandonner les processus en cours d'exécution ou leur permettre de se terminer avant que le service ne s'arrête. Si vous arrêtez un nœud et abandonnez les processus du service de référentiel en cours

d'exécution sur ce nœud, vous risquez de perdre les modifications qui n'ont pas encore été enregistrées dans le référentiel. Si vous abandonnez un nœud exécutant les processus de service d'intégration, les flux de travail sont également abandonnés.

1. Connectez-vous à Informatica Administrator.
2. Dans le navigateur, sélectionnez le nœud à arrêter.
3. Dans le menu **Actions** de l'onglet Domaine, sélectionnez **Arrêter le nœud**.

Règles et instructions de démarrage et d'arrêt d'Enterprise Data Catalog

Prenez en compte les règles et instructions suivantes lorsque vous démarrez et arrêtez Enterprise Data Catalog sur un nœud :

- Lors de l'arrêt d'un nœud, ce dernier n'est plus disponible au domaine. Si vous arrêtez un nœud de passerelle et que le domaine n'en comprenne pas d'autres, le domaine n'est plus disponible.
- Lorsque vous démarrez Enterprise Data Catalog, vérifiez que le port utilisé par le service sur le nœud est disponible. Par exemple, si vous arrêtez Enterprise Data Catalog sur un nœud, vérifiez que le port n'est pas utilisé par tout autre processus sur la machine avant de redémarrer Enterprise Data Catalog. Si le port n'est pas disponible, Enterprise Data Catalog ne parvient pas à démarrer.
- Si vous n'utilisez pas Informatica Administrator pour arrêter un nœud, tous les processus en cours d'exécution sur le nœud seront abandonnés. Pour attendre la fin de l'exécution de tous les processus avant d'arrêter un nœud, utilisez Informatica Administrator.
- Si deux nœuds figurent dans un domaine avec un nœud configuré comme nœud principal pour un service d'applications et l'autre nœud configuré comme nœud de sauvegarde, démarrez Enterprise Data Catalog sur le nœud principal avant de démarrer le nœud de sauvegarde. Sinon, le service d'applications s'exécutera sur le nœud de sauvegarde, et non sur le nœud principal.

ANNEXE B

Supprimer l'accès sudo après la création d'un cluster incorporé

- [Suppression de l'accès sudo après la création d'un cluster incorporé, 183](#)

Suppression de l'accès sudo après la création d'un cluster incorporé

Vous pouvez gérer un cluster incorporé sans fournir d'accès sudo aux comptes utilisateur. Vous pouvez réduire les menaces de sécurité dans votre entreprise en restreignant l'accès sudo aux comptes utilisateur. Si vous accordez un accès sudo à un compte utilisateur, vous pouvez utiliser le compte utilisateur pour exécuter des programmes ou des applications avec les privilèges de sécurité d'un autre utilisateur. Les privilèges de sécurité peuvent être ceux d'un utilisateur qui a un accès racine ou des privilèges de super-utilisateur.

Prérequis

Les prérequis pour créer un cluster incorporé sans fournir d'accès sudo aux comptes utilisateur sont les suivants :

- Si vous créez un cluster incorporé pour la première fois, supprimez le contenu du répertoire /<Répertoire_installation>/tomcat/temp/<nom-cluster>/temp.
- Si le cluster incorporé est créé et que le cluster existe, avant de démarrer le service de cluster Informatica, vérifiez que le serveur et les agents Ambari sont en cours d'exécution.

Exécution d'un cluster incorporé sans accès sudo

1. Créez un service de cluster Informatica en utilisant un compte qui ne possède pas de privilèges racine.
Remarque: Vérifiez que le service de cluster Informatica ne démarre pas.
2. Fournissez un accès sudo au compte utilisateur qui a été utilisé pour créer le service de cluster Informatica.
3. Ajoutez les propriétés personnalisées **lcsCustomOptions.ihs.gateway.user.sudo.enabled** pour le service de cluster Informatica et définissez la valeur de la propriété sur **False**.
4. Lancez Informatica Administrator et démarrez ensuite le service de cluster Informatica pour créer le cluster incorporé sur les nœuds requis.

5. Après avoir créé le cluster incorporé sur tous les nœuds, révoquez l'accès sudo pour le compte utilisateur.

Forum Aux Questions (FAQ)

Est-ce que le cluster incorporé fonctionne toujours si je crée le cluster, révoque l'accès sudo pour le compte utilisateur et désactive le service de cluster Informatica ?

Le cluster incorporé continue de fonctionner en arrière-plan.

Est-ce que le service de cluster Informatica surveille le cluster incorporé et démarre les services configurés pour s'exécuter sur le cluster si je démarre le service de cluster Informatica ?

Après avoir démarré le service, le cluster incorporé s'exécute, le service surveille le cluster et démarre les services configurés pour s'exécuter sur le cluster.

J'ai configuré l'accès sudo pour un compte utilisateur sur tous les nœuds et utilisé le compte pour arrêter le cluster incorporé. Est-ce que le service de cluster Informatica continue de fonctionner ?

Le cluster incorporé et le service de cluster Informatica sont arrêtés.

Sans accès sudo, puis-je démarrer et arrêter le service de cluster Informatica ?

Vous ne pouvez pas démarrer ou arrêter le service de cluster Informatica sans accès sudo. Vous pouvez accorder un accès sudo à l'administrateur pour le cluster de machines afin de démarrer ou arrêter le service à l'aide des commandes suivantes :

- `sudo ambari-server*`
- `sudo ambari-agent*`

ANNEXE C

Configurer un répertoire journal personnalisé pour Ambari

- [Configuration d'un répertoire journal personnalisé pour Ambari, 185](#)

Configuration d'un répertoire journal personnalisé pour Ambari

Les fichiers journaux Ambari sont stockés par défaut dans le répertoire `/var/log`. Vous pouvez configurer un répertoire personnalisé pour les fichiers journaux Ambari.

Pour spécifier un répertoire personnalisé pour stocker les fichiers journaux Ambari, effectuez les étapes suivantes :

1. Connectez-vous à Informatica Administrator.
2. Cliquez sur le service de cluster Informatica que vous avez configuré et cliquez sur **Modifier**.
3. Ajoutez la propriété personnalisée `IcsCustomOptions.ihs.hadoop.dir` pour le service de cluster Informatica et spécifiez le répertoire personnalisé dans la zone de texte **Valeur** pour la propriété.
4. Cliquez sur **Terminer**.

ANNEXE D

Configurer Enterprise Data Catalog pour un cluster avec WANdisco Fusion activé

- [Configuration d'Enterprise Data Catalog pour un cluster avec WANdisco Fusion activé, 186](#)

Configuration d'Enterprise Data Catalog pour un cluster avec WANdisco Fusion activé

Vous pouvez déployer Enterprise Data Catalog sur un cluster existant où WANdisco Fusion est activé. Les entreprises utilisent WANdisco Fusion pour répliquer et transférer des données entre des clusters Hadoop. Enterprise Data Catalog prend en charge les clusters Hadoop Cloudera et Hortonworks avec WANdisco Fusion.

Prérequis

Créez un répertoire avec l'autorisation `read` sur la machine où s'exécute le Domaine Informatica et copiez les fichiers JAR suivants à partir du cluster Hadoop vers le répertoire :

- Pour un cluster Cloudera Hadoop :
 - `hadoop-yarn-api-<version>-cdh<version>.jar`
 - `hadoop-yarn-common-<version>-cdh<version>.jar`
 - `hadoop-yarn-client-<version>-cdh<version>.jar`
- Pour un cluster Hortonworks Hadoop :
 - `hadoop-yarn-api-<version>-hdp<version>.jar`
 - `hadoop-yarn-common-<version>-hdp<version>.jar`
 - `hadoop-yarn-client-<version>-hdp<version>.jar`

Vous pouvez copier les fichiers `hadoop-yarn-api-<version>-<type cluster hadoop> <version>.jar`, `hadoop-yarn-common-<version>-<type cluster hadoop><version>.jar` et `hadoop-yarn-client-<version>-<type cluster hadoop><version>.jar` à partir de la machine où vous avez installé le cluster Hadoop.

- Copiez tous les fichiers JAR à partir de la machine où vous avez installé le client WANdisco Fusion vers le répertoire que vous avez créé. L'emplacement par défaut à partir duquel vous pouvez copier les fichiers JAR fusion est `/opt/wandisco/fusion/client/lib` sur la machine où vous avez installé le client WANdisco Fusion.
- Assurez-vous que les **Plugins** listés dans l'interface WANdisco Fusion ont le statut **Actif**.
- Si vous prévoyez d'exécuter un profilage sur le moteur Blaze pour des ressources, en fonction du type de cluster Hadoop que vous utilisez, assurez-vous de copier les fichiers suivants dans le répertoire `<INFA_HOME>/services/shared/hadoop/<version-distribution>/lib` :
 - Copiez tous les fichiers JAR à partir des chemins d'accès des bibliothèques du client fusion. Le chemin d'accès par défaut est `/opt/wandisco/fusion/client/lib`
 - Les fichiers suivants à partir de la machine où vous avez installé le cluster Hadoop :
 - `hadoop-yarn-api-<version>-<type cluster hadoop> <version>.jar`
 - `hadoop-yarn-common-<version>-<type cluster hadoop><version>.jar`
 - `hadoop-yarn-client-<version>-<type cluster hadoop><version>.jar`

Remarque: Assurez-vous de configurer l'autorisation `read` pour le répertoire où les fichiers JAR sont présents.

Pour déployer Enterprise Data Catalog sur un cluster existant avec WANdisco Fusion activé, effectuez les étapes suivantes :

1. Connectez-vous à Informatica Administrator.
2. Sélectionnez le service de catalogue que vous avez configuré et cliquez sur **Modifier**.
3. Ajoutez les propriétés personnalisées suivantes pour le service de catalogue :
 - `LdmCustomOptions.deployment.is.wandisco.cluster`. Définissez la valeur sur **True** dans la zone de texte **Valeur**. La valeur par défaut est **False**.
 - `LdmCustomOptions.ldm.extra.jars.location`. Spécifiez le chemin d'accès au répertoire qui inclut les fichiers JAR dans la zone de texte **Valeur**.
4. Cliquez sur **Terminer**.

Si vous aviez créé le service de catalogue à l'aide du programme d'installation, le service est créé mais il ne démarre pas. Vous devez utiliser Informatica Administrator pour configurer les propriétés `LdmCustomOptions.ldm.extra.jars.location` et `LdmCustomOptions.deployment.is.wandisco.cluster` pour le service de catalogue et démarrer ensuite le service.

ANNEXE E

Configurer Informatica Custom Service Descriptor

Cette annexe comprend les rubriques suivantes :

- [Présentation, 188](#)
- [Prérequis, 189](#)
- [Création du service Informatica Custom Service Descriptor, 189](#)
- [Foire aux questions, 191](#)

Présentation

Enterprise Data Catalog fournit un Custom Service Descriptor (CSD) que vous pouvez utiliser pour créer un service Informatica basé sur CSD sur un cluster existant Cloudera Hadoop avec Kerberos activé.

Lorsque vous déployez Enterprise Data Catalog sur un cluster existant Cloudera Hadoop avec Kerberos activé, il est nécessaire de fusionner les keytabs de nom d'hôte et les keytabs HTTP pour tous les nœuds où Cloudera NodeManager s'exécute. Vous devez ensuite fournir le keytab fusionné dans la propriété **Service Keytab Location** lorsque vous configurez le service de catalogue pour authentifier l'accès client à Enterprise Data Catalog.

Un CSD consiste en un fichier JAR qui définit le service que vous voulez créer sur un cluster Cloudera Hadoop qui prend en charge les services basés sur CSD. Après avoir créé le service Informatica basé sur CSD, nommé service Informatica Data Catalog dans le service Cloudera et Configuration Manager (SCM), vous pouvez accéder au service à partir de Cloudera Manager. Vous pouvez utiliser le service Informatica Data Catalog pour copier le keytab HTTP de chaque nœud sur un emplacement de disque virtuel spécifié sur ce nœud. Vous pouvez spécifier l'emplacement du disque virtuel lorsque vous configurez le service Informatica Data Catalog. Le service de catalogue récupère les serveurs principaux HTTP à partir du keytab HTTP à l'emplacement du disque virtuel.

Les avantages liés à l'utilisation du service Informatica Data Catalog sont les suivants :

- Les emplacements de disque virtuel sont des emplacements de stockage temporaires en mémoire qui évitent les failles de sécurité.
- Vous pouvez éviter tous les risques de sécurité associés à l'utilisation d'un keytab HTTP puisque le keytab stocké sur un emplacement de disque virtuel n'est accessible que par des applications Informatica.
- Vous pouvez vous passer des étapes nécessitant la copie des serveurs principaux HTTP de chaque nœud et la fusion des keytabs de nom d'hôte et du keytab HTTP.

Prérequis

Assurez-vous que les conditions préalables suivantes sont remplies sur tous les nœuds de cluster Cloudera Hadoop :

- Assurez-vous que l'administrateur du service Cloudera et Configuration Manager (SCM) soit propriétaire du répertoire où vous stockez le keytab HTTP. Vous pouvez utiliser la commande `chown cloudera-scm:cloudera-scm <Répertoire>` pour assigner la propriété du répertoire. Autrement, vous pouvez aussi faire en sorte que le répertoire où vous stockez le keytab HTTP pour chaque nœud possède les autorisations `read, write et execute`.
- Le service Informatica Data Catalog utilise le port 8080 par défaut sur chaque nœud. Si vous prévoyez d'utiliser ce port pour le service, assurez-vous qu'il soit libre sur chaque nœud. Vous pouvez modifier le port lorsque vous créez ou activez le service Informatica basé sur CSD.
- Assurez-vous que l'utilisateur du cluster de service est ajouté au groupe Cloudera SCM. Utilisez la commande `usermod -G cloudera-scm <Utilisateur_Scm>` pour ajouter l'utilisateur du cluster de service au groupe Cloudera SCM.

Création du service Informatica Custom Service Descriptor

Vous pouvez utiliser le fichier `INFORMATICA_DATA_CATALOG-1.0.jar` pour créer le service de catalogue de données Informatica dans un cluster Cloudera Hadoop. Copiez le fichier JAR à partir de `$INFA_HOME/services/CatalogService/ClouderaKeytabUtility/`.

Effectuez les étapes suivantes pour créer le service de catalogue de données Informatica :

1. Copiez `INFORMATICA_DATA_CATALOG-1.0.jar` vers le répertoire `/opt/cloudera/csd` sur la machine où est installé le service Cloudera et Configuration Manager (SCM).
2. Redémarrez le serveur Cloudera SCM.
3. Ouvrez l'interface utilisateur Cloudera SCM.

Remarque: Si les services de gestion Cloudera sont en cours d'exécution, redémarrez les services.

4. Si vous avez créé le cluster, sélectionnez l'option pour ajouter le service **Catalogue de données Informatica** à partir de l'interface utilisateur Cloudera SCM. Si vous êtes en train de créer un cluster, sélectionnez le service **Catalogue de données Informatica** lorsque vous sélectionnez la liste des services à installer. Consultez l'image suivante pour référence :

Service Type	Description
ADLS Connector	The ADLS Connector service provides key management for accessing Azure Data Lake Stores from CDH services.
Accumulo	The Apache Accumulo sorted, distributed key/value store is a robust, scalable, high performance data storage and retrieval system. This service only works with releases based on Apache Accumulo 1.6 or later.
Echo	The echo service
Flume	Flume collects and aggregates data from almost any source into a persistent store such as HDFS.
HBase	Apache HBase provides random, real-time, read/write access to large data sets (requires HDFS and ZooKeeper).
HDFS	Apache Hadoop Distributed File System (HDFS) is the primary storage system used by Hadoop applications. HDFS creates multiple replicas of data blocks and distributes them on compute hosts throughout a cluster to enable reliable, extremely rapid computations.
Hive	Hive is a data warehouse system that offers a SQL-like language called HiveQL.
Hue	Hue is a graphical user interface to work with the Cloudera Distribution Including Apache Hadoop (requires HDFS, MapReduce, and Hive).
Impala	Impala provides a real-time SQL query interface for data stored in HDFS and HBase. Impala requires the Hive service and shares the Hive Metastore with Hue.
Informatica Data Catalog	Informatica Enterprise Data Catalog Service to get http keytabs

Back Continue

- Lorsque vous configurez le service dans l'assistant d'ajout de service, sélectionnez les nœuds dans le cluster où Cloudera NodeManager s'exécute comme montré sur l'image suivante :

cloudera MANAGER Support ▾ admin ▾

Add Informatica Data Catalog Service to Cluster 1

Customize Role Assignments for Informatica Data Catalog

You can customize the role assignments for your new service here, but note that if assignments are made incorrectly, such as assigning too many roles to a single host, performance will suffer.

You can also view the role assignments by host. [View By Host](#)

Informatica Server × 1 New
vats001.informatica.com ▾

Back 1 2 3 4 Continue

- Spécifiez le port pour le service. La valeur par défaut est 8080.
- Spécifiez l'emplacement du disque virtuel sur les nœuds où vous désirez stocker le keytab HTTP comme montré sur l'image suivante :

cloudera MANAGER Support ▾ admin ▾

Add Informatica Data Catalog Service to Cluster 1

Review Changes

Directory
Directory: Informatica Server Default Group

Missing required value: Directory

Webserver port
Service_Port: Informatica Server Default Group

Back 1 2 3 4 Continue

8. Cliquez sur **Continuer** et terminez l'assistant d'ajout de service pour ajouter le service de catalogue de données Informatica.

Remarque: Lorsque vous démarrez le service de catalogue de données Informatica, le service copie le keytab HTTP vers l'emplacement de disque virtuel spécifié.

Foire aux questions

Quels sont les prérequis pour régénérer un keytab HTTP ?

Effectuez les étapes suivantes avant de régénérer un keytab HTTP :

1. Arrêtez le service de catalogue.
Cloudera Manager vous invite à arrêter tous les services qui nécessitent des keytabs HTTP. Ces services incluent le service NodeManager, le service ResourceManager et le service Informatica.
2. Arrêtez les services qui nécessitent des keytabs HTTP.
3. Régénérez les principaux utilisateurs du nom du cluster de services pour tous les services, y compris le service de catalogue.
4. Démarrez les services que vous avez arrêtés.

Comment configurer un disque virtuel sur un nœud ?

Ajoutez l'entrée `tmpfs <répertoire disque virtuel> tmpfs nodev,nosuid,noexec,nodiratime,size=<taille disque virtuel> 0 0` d'emplacement de montage dans le fichier `/etc/fstab`. Par exemple, si vous devez spécifier `/mnt/ramdiskdir` en tant que répertoire de disque virtuel et que vous voulez configurer 512 Mo comme taille du disque virtuel, ajoutez l'entrée de montage suivante : `tmpfs /mnt/ramdiskdir tmpfs nodev,nosuid,noexec,nodiratime,size=512M 0 0`

Remarque: Si vous redémarrez la machine, le répertoire du disque virtuel est conservé mais les données dans le répertoire sont supprimées.

Si vous désirez configurer un disque virtuel temporaire, utilisez la commande suivante : `mount -t tmpfs -o size=<taille disque virtuel> tmpfs <répertoire disque virtuel>`

Ai-je besoin d'ajouter l'utilisateur du nom du cluster de services au groupe Cloudera SCM ?

Cloudera Manager exécute le service CSD avec les privilèges d'un utilisateur Cloudera SCM. Les privilèges de l'utilisateur Cloudera SCM sont également utilisés pour générer le keytab spnego. Un utilisateur Cloudera SCM peut ne pas avoir d'autorisations suffisantes pour accorder des autorisations de propriété pour un keytab à un utilisateur de cluster de services. Les autorisations par défaut configurées pour un keytab sont `640` ce qui accorde au propriétaire du keytab uniquement des autorisations de lecture et d'écriture et des autorisations de lecture pour le groupe. Pour accorder un accès restreint similaire à celui de l'utilisateur Cloudera SCM à l'utilisateur du cluster de services, vous pouvez ajouter le nom d'utilisateur du cluster de services dans le groupe Cloudera SCM.

ANNEXE F

Créer des utilisateurs et des groupes d'utilisateurs personnalisés pour les services déployés dans un cluster incorporé

Cette annexe comprend les rubriques suivantes :

- [Présentation, 192](#)
- [Prérequis, 193](#)
- [Création d'utilisateurs et de groupes d'utilisateurs personnalisés pour les services déployés dans un cluster incorporé, 193](#)

Présentation

Vous pouvez créer des noms d'utilisateur et des groupes d'utilisateurs personnalisés pour les services tels que HDFS et YARN lorsque vous déployez Enterprise Data Catalog sur un cluster Hadoop incorporé.

Ambari utilise des noms d'utilisateur tels que hdfs, zookeeper, yarn et postgres pour les services par défaut. Vous pouvez configurer des noms d'utilisateur et des groupes d'utilisateurs personnalisés pour Ambari en ajoutant des propriétés personnalisées dans le service de cluster Informatica.

Remarque: Assurez-vous d'ajouter toutes les propriétés personnalisées lorsque vous créez le service de cluster Informatica.

Les propriétés personnalisées que vous pouvez configurer pour les noms d'utilisateur et les groupes d'utilisateurs sont les suivantes :

Nom d'utilisateur	Propriété personnalisée
hdfs	lcsCustomOptions.ihssecurity.hdfs.user
yarn	lcsCustomOptions.ihssecurity.yarn.user

Nom d'utilisateur	Propriété personnalisée
mapred	lcsCustomOptions.ihssecurity.mapred.user
zookeeper	lcsCustomOptions.ihssecurity.zookeeper.user
ams	lcsCustomOptions.ihssecurity.ams.user
smoke	lcsCustomOptions.ihssecurity.smoke.user

Groupe d'utilisateurs	Propriété personnalisée
proxy user	lcsCustomOptions.ihssecurity.proxyuser.group
hadoop	lcsCustomOptions.ihssecurity.hadoop.group

Prérequis

Assurez-vous que les conditions préalables suivantes sont remplies avant de créer des noms d'utilisateur ou des groupes d'utilisateurs personnalisés pour les services :

- Assurez-vous de spécifier des propriétés personnalisées pour tous les noms d'utilisateur et tous les groupes d'utilisateurs.
- Avant d'activer le service de cluster Informatica, assurez-vous que tous les utilisateurs et les groupes d'utilisateurs personnalisés existent dans LDAP. Si vous désirez utiliser des utilisateurs et des groupes d'utilisateurs personnalisés gérés localement, assurez-vous qu'ils existent sur la machine locale.
- Assurez-vous de gérer toutes les tâches associées à la création et à la gestion des utilisateurs et des groupes d'utilisateurs personnalisés. Ces tâches incluent l'ajout d'utilisateurs personnalisés dans les groupes d'utilisateurs requis et la création de répertoires de base.
- Assurez-vous d'inclure le nom d'utilisateur smoke dans les groupes d'utilisateurs suivants :
 - proxy user
 - hadoop

Création d'utilisateurs et de groupes d'utilisateurs personnalisés pour les services déployés dans un cluster incorporé

Effectuez les étapes suivantes pour configurer les noms d'utilisateur et les groupes d'utilisateurs personnalisés :

1. Connectez-vous à Informatica Administrator.
2. Effectuez les étapes de création de service de cluster Informatica telles qu'elles sont listées dans la section *Création d'un service de cluster Informatica*.

3. Ajoutez toutes les propriétés personnalisées et spécifiez les noms d'utilisateur et les groupes d'utilisateurs personnalisés comme valeurs pour les propriétés personnalisées dans le service de cluster Informatica.
4. Cliquez sur **Terminer**.

ANNEXE G

Configurer des ports personnalisés pour les applications Hadoop

Cette annexe comprend les rubriques suivantes :

- [Présentation, 195](#)
- [Configuration de ports personnalisés pour les applications Hadoop, 197](#)

Présentation

Vous pouvez spécifier des ports personnalisés pour les applications Hadoop lorsque vous créez ou modifiez le service de cluster Informatica.

En fonction de la taille de données que vous spécifiez dans la propriété **Load Type** lorsque vous créez le service de cluster Informatica, vous pouvez ajouter les propriétés de l'application Hadoop et les ports personnalisés dans le fichier `LowLoad.properties`, `MediumLoad.properties` ou `HighLoad.properties` présent dans le répertoire `<INFA_HOME>/services/InfaHadoopService/Binaries`. Vous pouvez ensuite activer ou recycler le service de cluster Informatica pour implémenter les modifications de port personnalisé.

Remarque: Assurez-vous de ne supprimer aucune ligne existante du fichier `<Type charge>.properties`. `<Type charge>` correspond à `LowLoad`, `MediumLoad` ou `HighLoad`.

Les ports personnalisés que vous pouvez configurer pour les applications Hadoop sont les suivants :

Propriété de l'application Hadoop	Valeur du port par défaut
<code>zoo.cfg.clientPort</code>	2181
<code>yarn-site.yarn.resourcemanager.webapp.address</code>	8046
<code>yarn-site.yarn.resourcemanager.webapp.https.address</code>	8088
<code>yarn-site.yarn.resourcemanager.address</code>	8032
<code>yarn-site.yarn.resourcemanager.resource-tracker.address</code>	8025

Propriété de l'application Hadoop	Valeur du port par défaut
yarn-site.yarn.resourcemanager.scheduler.address	8030
yarn-site.yarn.resourcemanager.admin.address	8141
yarn-site.yarn.nodemanager.address	45454
yarn-site.yarn.nodemanager.webapp.address	8042
yarn-site.yarn.timeline-service.address	10200
yarn-site.yarn.timeline-service.webapp.address	8188
yarn-site.yarn.timeline-service.webapp.https.address	8190
hdfs-site.dfs.namenode.http-address	50070
hdfs-site.dfs.namenode.https-address	50470
hdfs-site.dfs.namenode.rpc-address	8020
hdfs-site.dfs.datanode.address	50010
hdfs-site.dfs.datanode.http.address	50075
hdfs-site.dfs.datanode.https.address	50475
hdfs-site.dfs.journalnode.rpc-address	8485
hdfs-site.dfs.journalnode.http-address	8480
hdfs-site.dfs.journalnode.https-address	8481
hdfs-site.dfs.datanode.ipc.address	8010
mapred-site.mapreduce.jobhistory.address	10020
mapred-site.mapreduce.jobhistory.webapp.address	19888

Remarque: Pour un cluster incorporé où Kerberos n'est pas activé, configurez les ports dans l'intervalle de 1024 à 65535

Configurer les ports d'application pour un cluster incorporé avec Kerberos activé

Vous pouvez configurer des ports personnalisés pour les propriétés de l'application Hadoop suivantes si le cluster incorporé est activé pour Kerberos :

- Assurez-vous que vous configurez les valeurs dans l'intervalle de 0 à 1023 si vous voulez fournir des valeurs personnalisées pour les propriétés de l'application Hadoop suivantes :

- `dfs.datanode.address`
- `dfs.datanode.http.address`

Remarque: Si le cluster incorporé n'est pas activé pour Kerberos, vous pouvez configurer les valeurs dans l'intervalle de 0 à 1023 pour les propriétés de l'application Hadoop suivantes :

- `hdfs-site.dfs.datanode.address` 1019 par défaut.

- `hdfs-site.dfs.datanode.http.address` 1022 par défaut.

Configuration de ports personnalisés pour les applications Hadoop

Effectuez les étapes suivantes pour configurer les noms d'utilisateur et les groupes d'utilisateurs personnalisés :

1. Connectez-vous à Informatica Administrator.
2. Ouvrez le fichier `<Type de charge>.properties` à partir du répertoire suivant : `<INFA_HOME>/services/InfaHadoopService/Binaries`
3. Ajoutez le port personnalisé pour l'application Hadoop dans le format suivant : `<Propriété>=${(host)}:<port>` dans le fichier `custom.properties.<taille>`. Par exemple, pour spécifier un port personnalisé pour `yarn-site.yarn.resourcemanager.webapp.address`, ajoutez la ligne suivante dans le fichier : `yarn-site.yarn.resourcemanager.webapp.address=${host}:<numéro port personnalisé>`. Remplacez `<numéro port personnalisé>` par le numéro de port requis.
4. Enregistrez le fichier `custom.properties.<taille>`.
5. Cliquez sur **Terminer**.
6. Désactivez et réactivez le service de cluster Informatica pour implémenter les modifications. Si vous modifiez un service de cluster Informatica existant, vous pouvez recycler le service de cluster Informatica pour implémenter les modifications. Si vous désirez recycler le service, assurez-vous que les numéros de port pour les propriétés d'application Hadoop suivantes correspondent aux numéros de port configurés pour les propriétés listées dans la colonne *Propriété de l'application Hadoop dépendante*.

Propriété de l'application Hadoop	Propriété de l'application Hadoop dépendante
<code>yarn-site.yarn.log.server.url</code>	<code>mapred-site.mapreduce.jobhistory.webapp.address</code>
<code>yarn-site.yarn.log.server.web-service.url</code>	<code>yarn-site.yarn.timeline-service.webapp.address</code>
<code>hdfs-site.dfs.namenode.shared.edits.dir</code>	<code>hdfs-site.dfs.journalnode.rpc.address</code>

Par exemple, si vous aviez configuré le numéro de port 8189 pour `mapred-site.mapreduce.jobhistory.webapp.address`, assurez-vous de spécifier le même numéro de port pour `yarn-site.yarn.log.server.url`.

INDEX

A

- AddLicense (infacmd)
 - dépannage [169](#)
- authentification
 - Kerberos [64](#)
- authentification Kerberos
 - cluster existant [64](#)
- authentification utilisateur
 - présentation [22](#)

B

- base de données, préparations
 - référentiels [37](#)
- bases de données
 - Référentiel de l'analyseur de données [38](#)

C

- cache d'objet de données
 - Configuration requise pour la base de données Oracle [42](#)
 - spécifications de la base de données [41](#)
 - spécifications de la base de données IBM DB2 [42](#)
 - spécifications de la base de données Microsoft SQL Server [42](#)
- catalina.out
 - dépannage de l'installation [166](#)
- clé de chiffrement
 - présentation [22](#)
 - stockage des données sécurisé [22](#)
- clés de licence
 - présentation [22](#)
- clients
 - présentation [23](#)
- cluster Hadoop existant
 - préparation [64](#)
- cluster Hadoop intégré
 - préparation [60](#)
- compatibilité de la page de code
 - paramètre régional [129](#)
 - services d'applications [129](#)
- comptes d'utilisateur de la base de données.
 - directives de configuration [38](#)
- comptes utilisateur
 - Référentiel modèle [145](#)
- configuration
 - domaines [129](#)
 - variables d'environnement [130](#)
 - variables d'environnement sous Linux [132](#)
- configuration requise pour l'installation
 - configuration requise pour les services d'applications [31](#)
 - espace disque [28](#)
 - spécifications de la base de données [30](#)
 - spécifications de port [29](#)

- configuration requise pour la base de données
 - entrepôt de profilage [45](#)
- configuration requise pour la base de données IBM DB2
 - entrepôt de profilage [46](#)
- configuration requise pour la base de données Microsoft SQL Server
 - entrepôt de profilage [46](#)
 - référentiel de configuration du domaine [40](#)
 - Référentiel modèle [45](#)
- configuration requise pour la base de données Oracle
 - cache d'objet de données [42](#)
 - entrepôt de données de référence [48](#)
- Configuration requise pour la base de données Oracle
 - Référentiel modèle [45](#)
- configuration système minimale
 - requis [28](#)
- configuration système minimale requise
 - nœuds [31](#)
- configuration système requise
 - services d'applications [31](#)
- connexions
 - création de connexions à la base de données [135](#)
 - création de connexions de bases de données [139](#)
 - propriétés IBM DB2 [136](#)
 - propriétés Microsoft SQL Server [137](#)
 - propriétés Oracle [138](#)
 - connexions à la base de données
 - création [135](#)

D

- dépannage
 - création de domaines [168](#)
 - Exécution d'une ressource [168](#)
 - jointure de domaines [168](#)
 - licences [169](#)
 - ping sur les domaines [169](#)
 - référentiel de configuration du domaine [167](#)
 - services Informatica [168](#)
- dépannage de la jointure des domaines [168](#)
- désinstallation
 - règles et instructions [162](#)
- domaines
 - authentification utilisateur [22](#)
 - configuration [129](#)
 - conventions de dénomination [32](#)
 - Gestionnaire de service [21](#)
 - nœuds [20](#)
 - planification [24](#)
 - ports [29](#)
 - présentation [19](#)
 - sécurité [23](#)
 - services d'application [22](#)
 - domaines de sécurité
 - SSL [64](#)

E

- Enterprise Data Catalog
 - déploiement de Hadoop incorporé [49](#)
 - déploiement Hadoop existant [63](#)
 - désinstallation [163](#)
 - installation [13](#)
 - installation en mode console [70](#)
 - installation en mode silencieux [107](#), [126](#)
 - présentation du déploiement [49](#)
 - services [15](#), [16](#)
- entrepôt de données de référence
 - configuration requise pour la base de données Oracle [48](#)
 - spécifications de la base de données [47](#)
 - spécifications de la base de données IBM DB2 [47](#)
 - spécifications de la base de données Microsoft SQL Server [48](#)
- entrepôt de profilage
 - configuration requise pour la base de données [45](#)
 - configuration requise pour la base de données IBM DB2 [46](#)
 - spécifications de la base de données Microsoft SQL Server [46](#)
 - spécifications de la base de données Oracle [46](#)
- espace disque requis
 - configuration requise pour l'installation [28](#)

F

- fichier d'hôte
 - Service d'intégration de données [150](#)
- fichiers journaux
 - catalina.out [166](#)
 - installation [165](#)
 - journaux d'installation [166](#)
 - journaux de débogage [166](#)
 - node.log [166](#)
 - types [165](#)

G

- gestion des clusters
 - présentation [60](#)
- Gestionnaire de service
 - présentation [21](#)

I

- infacmd
 - ping sur objets [169](#)
- Informatica Administrator
 - connexion [134](#)
- installation
 - processus [14](#)

J

- journaux d'installation
 - descriptions [166](#)
- journaux de débogage
 - dépannage de l'installation [166](#)

L

- LANG
 - variables d'environnement [130](#)

- LC_ALL
 - variables d'environnement [130](#)
- LC_CTYPE
 - variables d'environnement [130](#)
- licences
 - ajout [169](#)
 - présentation [22](#)
- Linux
 - chemins de bibliothèque [132](#)
 - démarrage et arrêt des services d'Enterprise Data Catalog [181](#)
 - installation des services d'Enterprise Data Catalog en mode console [70](#)
 - variables d'environnement [130](#)
- localhost
 - Service d'intégration de données [150](#)

M

- mode console
 - installation des services d'Enterprise Data Catalog [70](#)
- mode silencieux
 - Enterprise Data Catalog [107](#)
 - Installation d'Enterprise Data Catalog [126](#)

N

- node.log
 - dépannage de l'installation [166](#)
- nœud unique
 - installation [19](#)
- nœuds
 - conventions de dénomination [32](#)
 - de travail [20](#)
 - dépannage [168](#)
 - Gestionnaire de service [21](#)
 - passerelles [20](#)
 - présentation [20](#)
 - rôle de calcul [20](#)
 - rôle de service [20](#)
 - rôles [20](#)
 - services d'application [22](#)
- nœuds de passerelle
 - création lors de l'installation [20](#)
- nœuds de travail
 - création lors de l'installation [20](#)
- nœuds multiples
 - installation [19](#)

O

- objets de domaine
 - conventions de dénomination [32](#)

P

- Ping (infacmd)
 - dépannage [169](#)
- ports
 - domaines [29](#)
 - services d'applications [29](#)
 - spécifications [29](#)
- prérequis
 - services d'applications [140](#)

- prérequis de la base de données IBM DB2
 - base de données du référentiel modèle [38, 43](#)
 - référentiel du domaine [38, 43](#)
- privilèges
 - Service de catalogue [132](#)

R

- référentiel de configuration du domaine
 - configuration requise [30](#)
 - configuration requise de la base de données Microsoft SQL Server [40](#)
 - dépannage [167](#)
 - préparation des bases de données [38](#)
 - prérequis de la base de données IBM DB2 [38, 43](#)
 - spécifications de la base de données Oracle [40](#)
- Référentiel de l'analyseur de données
 - spécifications de la base de données Sybase ASE [41](#)
- référentiel modèle
 - spécifications de la base de données [43](#)
- Référentiel modèle
 - Configuration requise pour la base de données Oracle [45](#)
 - prérequis de la base de données IBM DB2 [38, 43](#)
 - spécifications de la base de données Microsoft SQL Server [45](#)
 - utilisateurs [145](#)
- référentiels
 - préparation des bases de données [37](#)
- rôle de calcul
 - nœuds [20](#)
- rôle de service
 - nœuds [20](#)

S

- sécurité
 - domaines [23](#)
 - stockage des données [22](#)
- sécurité de domaine
 - présentation [23](#)
- serveur Enterprise Data Catalog
 - désinstallation [162](#)
- Service d'intégration de données
 - après la création [150](#)
 - configuration [147](#)
 - configuration du fichier d'hôte [150](#)
 - création [147](#)
 - présentation [25](#)
 - service dépendant [142](#)
 - services associés [25](#)
- Service de catalogue
 - création [150](#)
 - présentation [26](#)
 - privilèges [132](#)
 - service dépendant [142](#)
 - services associés [26](#)
- Service de cluster Informatica
 - création [57](#)
 - flux de travail [56](#)
 - présentation [27, 56](#)
- Service de gestion de contenu
 - bases de données requises [28](#)
 - configuration [156](#)
 - création [156, 157](#)
 - présentation [27](#)
 - service dépendant [142](#)
 - services associés [27](#)

- Service de référentiel modèle
 - après la création [145](#)
 - bases de données requises [26](#)
 - configuration [142](#)
 - création [142](#)
 - présentation [26](#)
- Service Manager
 - fichiers journaux [166](#)
- services
 - Gestionnaire de service [21](#)
 - services d'application [22](#)
- services d'application
 - dépendances [142](#)
 - préparation de la création [134](#)
 - présentation [22](#)
- services d'applications
 - configuration requise pour l'installation [31](#)
 - conventions de dénomination [32](#)
 - ports [29](#)
 - prérequis [140](#)
- Services d'Enterprise Data Catalog
 - démarrage et arrêt sous Linux [181](#)
- services dépendants
 - présentation [142](#)
- services Informatica
 - dépannage [168](#)
- services système
 - présentation [22](#)
- spécifications de la base de données
 - cache d'objet de données [41](#)
 - configuration requise pour l'installation [30](#)
 - entrepôt de données de référence [47](#)
 - référentiel modèle [43](#)
- spécifications de la base de données IBM DB2
 - cache d'objet de données [42](#)
 - entrepôt de données de référence [47](#)
- spécifications de la base de données Microsoft SQL Server
 - cache d'objet de données [42](#)
 - entrepôt de données de référence [48](#)
- spécifications de la base de données Oracle
 - entrepôt de profilage [46](#)
 - référentiel de configuration du domaine [40](#)
- spécifications de la base de données Sybase ASE
 - Référentiel de l'analyseur de données [41](#)
- spécifications de port
 - configuration requise pour l'installation [29](#)
- spécifications pour l'installation
 - spécifications système minimales [28](#)
- spécifications système
 - spécifications minimales pour l'installation [28](#)

V

- variables d'environnement
 - configuration [130](#)
 - Linux [130](#)
- variables d'environnement
 - chemins de bibliothèque sous Linux [132](#)
 - configuration sous Linux [132](#)
 - LANG [130](#)
 - LANG_C [130](#)
 - LC_ALL [130](#)
 - LC_CTYPE [130](#)
 - paramètre régional [130](#)
- variables d'environnement régionales
 - configuration [130](#)