



Informatica®
10.5.6

Installation pour Enterprise Data Catalog

© Copyright Informatica LLC 1998, 2024

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

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

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.

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 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.

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

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

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

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

Date de publication: 2024-07-10

Sommaire

Préface.....	11
Ressources Informatica.	11
Informatica Network.	11
Base de connaissances Informatica.	11
Documentation Informatica.	12
Matrices de disponibilité des produits Informatica.	12
Informatica Velocity.	12
Informatica Marketplace.	12
Support client international Informatica.	12
 Partie I: Installation : mise en route.....	 13
 Chapitre 1: Installation : mise en route.	 14
Liste de contrôle pour la mise en route	14
Présentation de l'installation.	14
Installation d'installation.	15
Planifier l'option d'installation.	16
Planifier les composants d'installation.	17
Nœuds.	18
Gestionnaire de service.	18
Services d'application.	18
Bases de données.	18
Authentification utilisateur.	19
Stockage des données sécurisé.	20
Sécurité de domaine.	20
Outils client Informatica.	20
 Partie II: Avant l'installation des services.....	 22
 Chapitre 2: Avant l'installation des services sous UNIX ou Linux.	 23
Avant de commencer Liste de contrôle	23
Lire les notes de publication.	24
Vérifier la configuration système requise.	24
Vérifier l'espace disque temporaire et les autorisations.	25
Vérifier les exigences de dimensionnement.	25
Vérifier les spécifications de correctif sur UNIX ou Linux.	27
Vérifications des spécifications de port	28
Vérifier la configuration requise des packages de distribution(Linux et UNIX).	29
Vérifier la limite du descripteur de fichier.	30
Sauvegarder les fichiers Data Transformation.	31

Examiner les variables d'environnement.	31
Créer un compte d'utilisateur système.	32
Configurer un fichier keystore.	33
Télécharger et extraire les fichiers du programme d'installation.	34
Vérifier la signature de code du programme d'installation.	35
Vérifier la somme de contrôle du package d'installation sur UNIX et Linux.	36
Préparer l'installation des fichiers binaires pour les ressources d'Informatica Platform.	36
Vérification de la clé de licence.	36
Préparer l'importation du cluster.	37

Chapitre 3: Préparer les services d'application et les bases de données. . . . 38

Liste de contrôle pour préparer les services d'application	38
Préparer les services d'application et les bases de données - Présentation.	39
Configurer les comptes de l'utilisateur de la base de données.	39
Identifier les services d'application par produit.	40
Spécifications de la base de données du référentiel de configuration du domaine.	41
Spécifications de la base de données IBM DB2.	41
Configuration requise pour la base de données Microsoft SQL Server.	42
Configuration requise de Microsoft Azure SQL Database	42
Configuration requise pour la base de données Oracle.	43
Configuration requise pour la base de données PostgreSQL	43
Spécifications de la base de données Sybase.	43
Service Analyst	45
Effectuer les tâches prérequis.	45
Service de catalogue.	46
Service de gestion de contenu.	47
Spécifications de l'entrepôt de données de référence.	47
Service d'intégration de données.	49
Spécifications de la base de données du cache d'objet de données.	50
Configuration requise pour l'entrepôt de profilage profilage.	51
Configuration requise pour la base de données de flux de travail.	53
Service de cluster Informatica.	56
Service d'accès aux métadonnées.	56
Service de référentiel modèle.	57
Configuration requise pour la base de données du référentiel modèle.	58
Spécifications de la base de données IBM DB2.	58
Configuration requise de Microsoft Azure SQL Database.	59
Configuration requise de la base de données Microsoft SQL Server.	60
Configuration requise pour la base de données Oracle.	60
Exigences de la base de données PostgreSQL.	60
Service de référentiel modèle de surveillance.	61
Service de recherche.	62
Configuration de la connectivité native sur les machines du service.	62

Installer le logiciel client de base de données.	63
Configurer les variables d'environnement client de la base de données.	63
Chapitre 4: Préparer le déploiement d'Enterprise Data Catalog.	66
Liste de contrôle pour préparer le déploiement d'Enterprise Data Catalog.	66
Planification du déploiement.	67
Service de cluster Informatica et services associés.	67
Prérequis courants du système d'exploitation.	67
Prérequis du système d'exploitation pour Red Hat Enterprise Linux.	72
Prérequis du système d'exploitation pour SUSE Linux Enterprise Server	72
Prérequis du nœud.	73
Chapitre 5: Enregistrer des informations pour les invites du programme d'installation.	74
Liste de contrôle pour enregistrer les invites du programme d'installation.	74
Enregistrer des informations pour les invites du programme d'installation - Présentation.	75
Domaine.	76
Nœuds.	77
Packages de distribution.	77
Services d'application.	77
Bases de données	78
Chaîne de connexion à une base de données sécurisée.	80
Configuration de cluster.	82
Stockage des données sécurisé.	84
Chapitre 6: Configurer les certificats SSL personnalisés.	85
Configurer les certificats SSL personnalisésPrésentation.	85
Générer des certificats SSL personnalisés signés par une autorité de certification (CA).	86
Valider les certificats signés par une autorité de certification (CA).	90
Générer des certificats SSL personnalisés auto-signés.	91
Chapitre 7: Présentation du programme d'installation des services.	94
Tâches du programme d'installation des services.	94
Sécuriser les fichiers et les répertoires.	94
Utilitaires de pré-installation.	95
Exécuter l'outil Pre-Installation System Check (i10Pi) en mode console.	95
Exécuter l'outil Pre-Installation System Check (i10Pi) en mode silencieux.	99
Partie III: Exécuter le programme d'installation des services.	100
Chapitre 8: Installer Enterprise Data Catalog avec des services Informatica 101	
Installer Enterprise Data Catalog avec des services Informatica - Présentation.	101
Installer en créant un domaine.	101

Installer en joignant un domaine.	116
---	-----

Chapitre 9: Créer un domaine avec des produits Catalog et Data Engineering. 128

Commencer l'installation.	128
Exécuter le programme d'installation.	128
Bienvenue - Accepter les conditions générales.	129
Choisissez l'option d'installation.	129
Adapter les services d'application.	129
Spécifier le répertoire d'installation.	130
Préparer l'utilitaire de pré-validation.	131
Configurer le domaine.	134
Configurer les options du domaine.	135
Configurer la sécurité du domaine.	138
Configurer les détails du référentiel du domaine.	139
Sécurité du domaine - Clé de chiffrement.	144
Configurer le domaine et le nœud.	145
Configurer la base de données du référentiel modèle.	151
Configurer la base de données du référentiel modèle de surveillance.	154
Configurer les paramètres du service d'intégration de données.	159
Créer la configuration du cluster.	161
Configurer Enterprise Data Catalog.	163
Configurer les détails de la base de données de l'entrepôt de profilage.	163
Configurer les paramètres et la base de données du service de gestion de contenu.	166
Créer et configurer le service de cluster Informatica.	169
Créer et configurer le service de catalogue.	170
Configurer le référentiel MetaDex.	172

Chapitre 10: Joindre un domaine avec des produits Catalog et Data Engineering. 175

Commencer l'installation.	175
Exécuter le programme d'installation.	175
Bienvenue - Accepter les conditions générales.	176
Choisissez l'option d'installation.	176
Adapter les services d'application.	176
Spécifier le répertoire d'installation.	177
Configurer le domaine.	178
Configurer le domaine.	178
Sécurité de domaine.	180
Configurer le référentiel du domaine.	181
Sécurité du domaine - Clé de chiffrement.	182
Configurer le domaine et le nœud.	182

Chapitre 11: Installer les fichiers binaires d'Enterprise Data Catalog. 185

Présentation de l'installation des fichiers binaires d'Enterprise Data Catalog.	185
Installation des fichiers binaires pour Enterprise Data Catalog	185
Lorsque vous installez les fichiers binaires d'Enterprise Data Catalog.	186
Création de services pour Enterprise Data Catalog.	187
Spécification des détails du domaine Informatica.	188
Création du service de référentiel modèle.	188
Création du service d'intégration de données.	190
Configuration de l'entrepôt de profilage.	191
Création du service de gestion de contenu.	192
Configuration des options du cluster et du service d'application.	194
Création du service de cluster Informatica.	194
Création du service de catalogue.	197
Configuration du référentiel MetaDex.	198

Chapitre 12: Exécuter le programme d'installation silencieuse. 201

Présentation du programme d'installation silencieuse d'Enterprise Data Catalog.	201
Installation en mode silencieux.	201
Configurer le fichier de propriétés.	202
Exécuter le programme d'installation.	202
Installer les services d'application Enterprise Data Catalog en mode silencieux.	203
Configurer le fichier de propriétés.	203
Exécuter le programme d'installation pour installer les services.	203
Chiffrement des mots de passe dans le fichier des propriétés.	204

Chapitre 13: Dépannage 205

Présentation du dépannage de l'installation.	205
Reprise d'un processus d'installation ayant échoué.	205
Avant de reprendre le programme d'installation.	206
Reprendre le programme d'installation.	206
Dépannage à l'aide des fichiers journaux d'installation.	206
Fichiers journaux de débogage.	207
Fichier journal d'installation.	207
Fichiers journaux du gestionnaire de service.	208
Dépannage des domaines et des nœuds.	208
Création du référentiel de configuration de domaine.	208
Création ou jonction d'un domaine.	209
Démarrage d'Informatica.	209
Ping sur le domaine.	210
Ajout d'une licence.	210
Dépannage d'Informatica Developer.	210

Partie IV: Après l'installation des services.....	211
Chapitre 14: Configuration du domaine.....	212
Liste de contrôle pour la configuration du domaine.....	212
Présentation de la configuration du domaine.....	213
Intégrer le domaine à l'environnement Hadoop ou Databricks.....	213
Vérification des paramètres régionaux et de la compatibilité des pages de code.....	213
Configurer des variables d'environnement régionales.....	214
Configurer les variables d'environnement sur UNIX ou Linux.....	215
Configuration des variables d'environnement Informatica.....	215
Configurer des variables d'environnement de chemin de bibliothèque.....	216
Chapitre 15: Préparation de la création des services d'application.....	218
Liste de contrôle pour préparer la création de services d'application.....	218
Créer des répertoires pour le service Analyst.....	219
Création d'un keystore pour une connexion sécurisée à un service d'application Web.....	219
Connexion à Informatica Administrator.....	220
Création de connexions.....	221
Propriétés de la connexion IBM DB2.....	221
Propriétés de connexion à la base de données Microsoft Azure SQL.....	222
Propriétés de connexion Microsoft SQL Server.....	223
Propriétés de connexion Oracle.....	224
Propriétés de connexion PostgreSQL.....	225
Création d'une connexion.....	226
Chapitre 16: Créer et configurer des services d'application.....	228
Liste de contrôle pour créer et configurer des services d'application.....	228
Créer et configurer les services d'application - Présentation.....	229
Créer et configurer le service de référentiel modèle.....	229
Créer le service de référentiel modèle.....	229
Après la création du service de référentiel modèle.....	232
Créer et configurer le service d'intégration de données.....	234
Créer le service d'intégration de données.....	234
Après la création du service d'intégration de données.....	237
Créer et configurer le service de gestion de contenu.....	237
Créer le service de gestion de contenu.....	238
Créer et configurer le service Analyst.....	239
Créer le service Analyst.....	239
Après la création du service Analyst.....	242
Créer et configurer le service de cluster Informatica.....	242
Après la création du service de cluster Informatica.....	244
Créer et configurer le service de catalogue.....	247

Créer et configurer le service d'accès aux métadonnées.	251
Configurer le référentiel MetaDex.	252
Configurer l'accès au service de catalogue.	254
Partie V: Installation du client Informatica.	256
Chapitre 17: Installer Informatica Developer	257
Avant l'installation Informatica Developer.	257
Vérifier la somme de contrôle du package d'installation	257
Vérifier les spécifications système.	258
Vérifier la configuration requise de tiers pour Informatica Developer.	258
Installer l'outil Developer tool.	258
Après l'installation d'Informatica Developer.	259
Installation des langues.	259
Configuration du client pour un domaine sécurisé.	260
Configuration du répertoire d'espace de travail de l'outil Developer.	260
Démarrage de l'outil Developer.	261
Chapitre 18: Installer en mode silencieux	263
Présentation de l'installation en mode silencieux.	263
Configurer le fichier de propriétés.	263
Exécuter le programme d'installation silencieuse.	264
Partie VI: Désinstallation.	265
Chapitre 19: Désinstallation.	266
Désinstallation d'Informatica - Présentation.	266
Règles et instructions pour la désinstallation.	266
Désinstallation du serveur Informatica en mode console.	267
Désinstallation du serveur Informatica en mode silencieux.	268
Annexe A: Démarrage et arrêt des services Informatica.	269
Démarrage et arrêt des services Informatica - Présentation	269
Démarrage et arrêt des services Informatica à partir de la console.	269
Arrêt d'Informatica dans Informatica Administrator.	270
Règles et instructions pour démarrer ou arrêter Informatica.	270
Annexe B: Gestion des packages de distribution.	271
Présentation de la gestion des packages de distribution.	271
Avant de commencer.	272
Installer ou supprimer des packages de distribution en mode console.	272
Installer ou supprimer des packages de distribution en mode silencieux.	273
Après l'installation.	274

Annexe C: Connexion à des bases de données sous UNIX ou Linux..... 275

Présentation de la connexion à des bases de données sous UNIX ou Linux.	275
Connexion à une base de données universelle IBM DB2.	276
Configuration de la connectivité native.	276
Connexion à une base de données Microsoft SQL Server.	278
Configuration de l'authentification SSL via ODBC.	278
Connexion à une base de données Oracle.	279
Configuration de la connectivité native.	279
Connexion à une base de données Sybase ASE.	281
Configuration de la connectivité native.	281
Connexion à une base de données Teradata.	283
Configuration de la connectivité ODBC.	283
Connexion à une source de données JDBC.	286
Connexion à une source de données ODBC.	286
Exemple de fichier odbc.ini.	288

Index..... 295

Préface

Pour installer Enterprise Data Catalog, suivez les instructions du *Guide d'installation pour Enterprise Data Catalog*. Vous pouvez installer les services et les clients Informatica sur une ou plusieurs machines. Ce guide comprend les tâches prérequis et post-requis et les étapes d'installation des clients et des services Informatica pour le domaine Informatica. Les tâches prérequis comprennent la planification de l'environnement, la configuration des bases de données et la vérification de la configuration système requise. Les tâches post-requis comprennent les services d'application supplémentaires et la configuration des variables d'environnement.

Ressources Informatica

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

Informatica Network

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

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

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

Base de connaissances Informatica

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

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

Documentation Informatica

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

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

Matrices de disponibilité des produits Informatica

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

Informatica Velocity

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

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

Informatica Marketplace

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

Support client international Informatica

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

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

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

Partie I : Installation : mise en route

- [Installation : mise en route, 14](#)

CHAPITRE 1

Installation : mise en route

Ce chapitre comprend les rubriques suivantes :

- [Liste de contrôle pour la mise en route , 14](#)
- [Présentation de l'installation, 14](#)
- [Installation d'installation, 15](#)
- [Planifier l'option d'installation, 16](#)
- [Planifier les composants d'installation, 17](#)

Liste de contrôle pour la mise en route

Ce chapitre contient des concepts de haut niveau et des informations de planification relatives à l'installation. Utilisez cette liste de contrôle pour le suivi des tâches préliminaires

- ☐ Comprendre les concepts de haut niveau :
 - Description et processus du programme d'installation.
 - Terminologie et composants du domaine Informatica.
- ☐ Démarrer la planification de haut niveau :
 - Options d'installation. Examinez les options d'installation pour connaître le produit et les options d'installation.
 - Composants d'installation. Consultez la description des composants d'installation et les notes de planification.

Présentation de l'installation

Bienvenue dans le programme d'installation des services de domaine et des clients Informatica. Les services de domaine Informatica comportent les services de base pour la prise en charge des services de domaine et d'application. Les clients Informatica comprennent à la fois des applications clientes lourdes et Web.

Lorsque vous installez les services Informatica, vous êtes invité à créer ou à joindre un domaine. Le domaine est un groupe de nœuds qui représentent les machines sur lesquelles les services d'application sont exécutés. La première fois que vous exécutez le programme d'installation, vous devez créer le domaine. Si vous effectuez l'installation sur une seule machine, vous devez créer un domaine Informatica et un nœud de passerelle sur la machine. Si vous effectuez une installation sur plusieurs machines, vous devez créer un

domaine Informatica et un nœud de passerelle lors de la première installation. Lors de l'installation sur les machines supplémentaires, vous créez des nœuds de travail ou de passerelle que vous associez au domaine.

Lorsque vous exécutez le programme d'installation, il installe des fichiers pour les services. Vous pouvez éventuellement créer des services d'application pendant le processus d'installation, ou vous pouvez créer manuellement des services d'application lorsque l'installation est terminée.

Si d'autres produits Informatica sont installés sur votre ordinateur, vérifiez que la version installée est compatible avec celle du produit que vous installez.

Installation d'installation

L'installation des services de domaine Informatica et des clients Informatica se divise en plusieurs étapes.

Le processus d'installation varie en fonction des produits que vous installez. Tenez compte des tâches de haut niveau suivantes du processus d'installation :

Effectuer les tâches de pré-installation.

1. Planifiez l'installation d'Informatica. Déterminez les produits que vous souhaitez exécuter dans votre environnement. Si vous créez un domaine, tenez compte du nombre de nœuds dans le domaine, des services d'application qui seront exécutés sur chaque nœud, de la configuration système requise et du type d'authentification utilisateur que le domaine utilisera.
2. Préparez les bases de données requises pour les référentiels, les entrepôts et les catalogues. Vérifiez les spécifications de base de données et configurez les bases de données.
3. Configurez les machines de manière à répondre aux exigences système afin de vous assurer que vous pouvez installer et exécuter correctement les services Informatica.
4. Déterminez les exigences de sécurité pour le domaine, les services et les bases de données.

Exécutez le programme d'installation.

Lorsque vous exécutez le programme d'installation, vous pouvez faire votre choix entre différentes options, en fonction de vos besoins.

Terminez la configuration.

1. Vérifiez la compatibilité de la page de code.
2. Configurez les variables d'environnement
3. Terminez les tâches requises par le type d'authentification utilisateur utilisé par le domaine.
4. Configurez éventuellement une communication sécurisée pour le domaine.
5. Créez et configurez des services d'application.
6. Configurez les connexions requises par les services d'application.
7. Créez les utilisateurs et les connexions requis par les services d'application.

Installez les outils client Informatica.

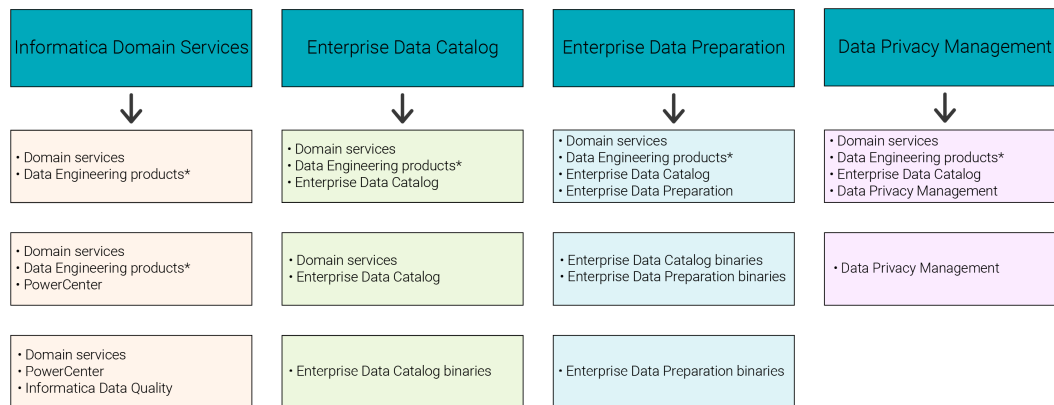
1. Vérifiez que la configuration requise pour l'installation et que les logiciels tiers requis sont conformes pour les clients.
2. Utilisez le programme d'installation client pour installer les clients sur les machines Windows.
3. Configurez les variables d'environnement requises, et installez éventuellement des langues supplémentaires.

Planifier l'option d'installation

Avant de commencer la planification et la préparation de l'installation, déterminez le type d'installation que vous souhaitez exécuter.

Lorsque vous exécutez le programme d'installation, vous pouvez choisir parmi les options du panneau Bienvenue en fonction du ou des produits que vous souhaitez installer. Le panneau Composants s'affiche en fonction de votre sélection de produits afin que vous puissiez choisir les composants du produit.

L'image suivante montre les produits que vous pouvez installer en fonction des options d'installation :



*Data Engineering products include Data Engineering Integration, Data Engineering Quality, and Data Engineering Streaming.

Tenez compte des différentes options disponibles lorsque vous exécutez le programme d'installation :

Services de domaine Informatica

Pour installer les services de domaine Informatica, vous pouvez sélectionner l'option d'installation 1 dans le panneau Composants pour installer et configurer les services de domaine Informatica.

Avec l'installation des services de domaine Informatica, effectuez l'installation à partir de l'une des options de produit suivantes :

- Uniquement les produits Data Engineering pour Integration, Quality et Streaming
- Les produits traditionnels et les produits Data Engineering susmentionnés
- Uniquement les produits traditionnels, tels que PowerCenter et Informatica Data Quality.

Lorsque vous installez des services de domaine Informatica, vous pouvez choisir de créer un domaine ou de le joindre. Test Data Management est installé avec les produits traditionnels et Data Engineering.

Enterprise Data Catalog

Pour installer Enterprise Data Catalog, vous pouvez sélectionner l'option d'installation 2 dans le panneau Composants pour installer et configurer Enterprise Data Catalog.

Lorsque vous installez Enterprise Data Catalog, choisissez l'une des options suivantes :

- Services de domaine, produits Data Engineering et Enterprise Data Catalog.
- Services de domaine et Enterprise Data Catalog.
- Uniquement les fichiers binaires d'Enterprise Data Catalog dans un domaine existant. Après avoir installé les fichiers binaires, vous pouvez réexécuter le programme d'installation pour configurer les services.

Enterprise Data Preparation

Pour installer Enterprise Data Preparation, vous pouvez sélectionner l'option d'installation 3 suivante dans le panneau Composants pour installer et configurer Enterprise Data Preparation.

Lorsque vous installez Enterprise Data Preparation, choisissez l'une des options suivantes :

- Produits Data Engineering, Enterprise Data Catalog et Enterprise Data Preparation.
- Fichiers binaires d'Enterprise Data Catalog et d'Enterprise Data Preparation dans un domaine existant. Après avoir installé les fichiers binaires, vous pouvez réexécuter le programme d'installation pour configurer les services.
- Uniquement les fichiers binaires d'Enterprise Data Preparation dans un domaine existant avec Enterprise Data Catalog. Après avoir installé les fichiers binaires, vous pouvez réexécuter le programme d'installation pour configurer les services.

Data Privacy Management

Pour installer Data Privacy Management, vous pouvez sélectionner l'option d'installation 4 suivante dans le panneau Composants pour installer et configurer Data Privacy Management.

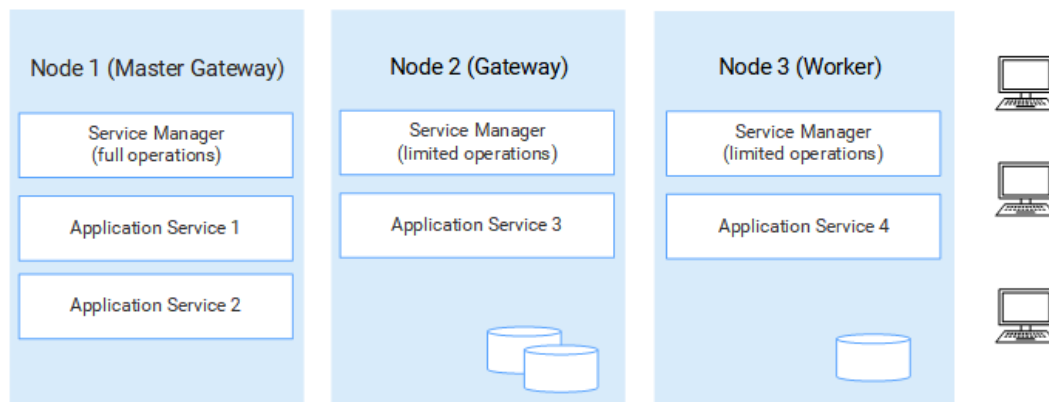
Lorsque vous installez Data Privacy Management, choisissez l'une des options suivantes :

- Les produits Data Engineering, Enterprise Data Catalog et Data Privacy Management.
- Data Privacy Management dans un domaine existant avec Enterprise Data Catalog.

Planifier les composants d'installation

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 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 et certains services requièrent des bases de données pour écrire des métadonnées et des résultats d'exécution.

L'image suivante présente une architecture de haut niveau d'un domaine sur plusieurs nœuds :



Nœuds

La première fois que vous installez les services de domaine, vous créez le domaine Informatica ainsi qu'un nœud de passerelle. Lorsque vous installez les services de domaine sur d'autres machines, vous créez des nœuds supplémentaires que vous associez au domaine.

Le domaine comprend les types de nœuds suivants :

- **Nœud de passerelle.** Un nœud de passerelle correspond à un nœud configuré pour servir de passerelle dans le domaine. Un nœud de passerelle peut exécuter des services d'application, et il peut servir de nœud principal de passerelle. Le nœud principal de passerelle est le point d'entrée du domaine. Vous pouvez configurer plusieurs nœuds en tant que nœud de passerelle, mais seul le nœud de passerelle agit en tant que nœud principal de passerelle à un moment donné.
- **Nœud de travail** Un nœud de travail correspond à tout nœud que vous ne configurez pas pour qu'il serve de passerelle au domaine. Un nœud de travail peut exécuter des services d'application, mais il ne peut pas servir de passerelle.

Lorsque vous planifiez l'installation : vous devez planifier le nombre et le type de nœuds dont vous avez besoin en fonction de vos besoins de service et de traitement. Si vous disposez d'une haute disponibilité, il est conseillé de créer plusieurs nœuds de passerelle pour les fonctionnalités de failover.

Gestionnaire de service

Le gestionnaire de service est un service qui gère toutes les opérations du domaine. Le gestionnaire de service s'exécute sur chaque nœud du domaine et exécute des fonctions de domaine, telles que l'authentification, la journalisation et la gestion des services d'application. Le gestionnaire de service sur un nœud de passerelle effectue plus de tâches que le gestionnaire de service sur un nœud de travail.

Lorsque vous planifiez l'installation : notez que la fonctionnalité gestionnaire de service est associée au type de nœud.

Services d'application

Les services d'application représentent des fonctionnalités basées sur le serveur. Un service d'application peut être obligatoire ou facultatif et peut nécessiter l'accès à une base de données.

Lorsque vous exécutez le programme d'installation, vous pouvez choisir de créer certains services. Une fois l'installation terminée, vous créez d'autres services d'application à partir de la clé de licence générée pour votre organisation.

Lorsque vous planifiez l'installation : 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.

Bases de données

Certains services d'application requièrent des bases de données pour stocker des métadonnées et pour écrire des résultats d'exécution. Vous devez créer des bases de données pour les services d'application dans le domaine.

Vous pouvez créer les bases de données suivantes :

Base de données du référentiel de configuration de domaine

Le référentiel de configuration de domaine stocke les informations de configuration et d'utilisateur d'un domaine.

Base de données du référentiel de l'analyse des actifs de données

Le référentiel de l'analyse des actifs de données stocke les informations analytiques collectées à partir du catalogue. Vous pouvez afficher des rapports et des données statistiques dans l'onglet Analyse d'Enterprise Data Catalog.

Base de données pour 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. Configurez un service de gestion de contenu pour identifier l'entrepôt de données de référence et le référentiel modèle.

Base de données du cache des objets de données

Le cache des objets de données stocke les objets de données logiques et les tables virtuelles mis en cache pour le service d'intégration de données. 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.

Base de données de l'entrepôt de profilage

L'entrepôt de profilage stocke les résultats du profilage et de la fiche d'évaluation. Vous devez disposer d'un entrepôt de profilage pour effectuer le profilage et la découverte de données.

Base de données de flux de travail

La base de données de flux de travail stocke les métadonnées d'exécution pour les flux de travail utilisant le service d'intégration de données.

Base de données du référentiel modèle

Le référentiel modèle stocke des données et des métadonnées des services et des clients Informatica. Les outils client Informatica, tels que l'outil Analyst tool et l'outil Developer tool, stockent les données dans le référentiel modèle.

Base de données du référentiel modèle de surveillance

Le référentiel modèle de surveillance stocke les statistiques des travaux ad hoc, des applications, des objets de données logiques, des services de données SQL, des services Web et des flux de travail créés par les clients Informatica et les services d'application.

Lorsque vous planifiez l'installation : vous devez créer des bases de données et des utilisateurs de base de données requis par les services d'application.

Authentification utilisateur

Lorsque vous exécutez le programme d'installation, vous pouvez choisir l'authentification à utiliser pour le domaine.

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

- Native. Les comptes d'utilisateurs natifs sont stockés dans le domaine et peuvent uniquement être utilisés dans ce domaine. L'authentification native est définie par défaut.
- LDAP. Les comptes utilisateurs LDAP sont stockés dans un service d'annuaire LDAP et partagés par des applications de l'entreprise. Vous pouvez configurer l'authentification LDAP après avoir exécuté le programme d'installation.
- SAML. Vous pouvez configurer l'authentification SAML (Security Assertion Markup Language) pour les outils Administrator tool, Analyst tool et Monitoring tool. Vous pouvez configurer l'authentification SAML après avoir exécuté le programme d'installation.

Lorsque vous planifiez l'installation: Vous devez planifier le type d'authentification que vous souhaitez utiliser dans le domaine.

Stockage des données sécurisé

Informatica chiffre les données sensibles avant de les stocker dans les référentiels Informatica.

Lorsque vous créez un domaine, vous devez spécifier le répertoire de clé de chiffrement. Le programme d'installation génère un fichier de clé de chiffrement nommé siteKey et le stocke dans un répertoire par défaut ou dans le répertoire que vous spécifiez. Tous les nœuds du domaine doivent utiliser la même clé de chiffrement.

Important: Le programme d'installation génère également une clé de site unique. En cas de perte de la clé de site, vous ne pouvez plus la régénérer. Veillez à enregistrer une copie de cette clé et de ne pas partager la clé de site unique avec d'autres.

Sécurité de domaine

Lorsque vous créez un domaine, vous pouvez activer des options pour configurer la sécurité du domaine.

Vous pouvez configurer une communication sécurisée pour les composants de domaine suivants :

- Outil Administrator tool. Configurez une connexion HTTPS sécurisée pour l'outil Administrator tool. Pendant l'installation, vous pouvez fournir le fichier keystore à utiliser pour la connexion HTTPS.
- Gestionnaire de service. Configurez une connexion sécurisée entre le gestionnaire de service et d'autres services de domaine. Pendant l'installation, vous pouvez fournir des fichiers keystore et truststore contenant des certificats SSL que vous souhaitez utiliser.
- Référentiel de configuration du domaine. Vous pouvez sécuriser le référentiel de configuration du domaine avec le protocole SSL. Pendant l'installation, vous pouvez fournir le fichier truststore contenant le certificat SSL que vous souhaitez utiliser.

Lorsque vous planifiez l'installation: , déterminez le niveau de sécurité que vous souhaitez configurer pour les composants de domaine. Si vous décidez de configurer la sécurité du domaine, vous devez connaître l'emplacement et le mot de passe des fichiers keystore et truststore.

Outils client Informatica

Les clients Informatica vous permettent d'accéder aux fonctionnalités Informatica sous-jacentes du domaine. Les clients font des demandes au gestionnaire de service et aux services d'application.

Les clients Informatica comprennent à la fois des applications clientes lourdes et des applications clientes légère ou Web que vous utilisez pour accéder aux services et aux référentiels du domaine.

Le tableau suivant décrit les outils clients des produits Data Engineering :

Client Informatica	Description
Informatica Developer (outil Developer tool)	Application cliente lourde pour créer et exécuter des objets de données, des mappages, des profils et des flux de travail.
Informatica Administrator (outil Administrator tool)	Application Web qui sert à gérer le domaine et les services d'application.

Client Informatica	Description
Informatica Analyst (outil Analyst tool)	Application Web pour analyser, nettoyer, intégrer et normaliser les données dans une entreprise.
Informatica Mass Ingestion (outil d'ingestion de masse)	Application Web pour créer, déployer, exécuter et surveiller les spécifications d'ingestion de masse.

Lorsque vous planifiez l'installation : déterminez le nombre d'instances de l'outil Developer tool que vous souhaitez installer. Vous n'avez pas besoin de planifier les applications client Web.

Le tableau suivant décrit les outils clients d'Enterprise Data Catalog :

Client Informatica	Description
Informatica Developer (outil Developer tool)	Application cliente lourde, qui sert à créer, importer et exporter des domaines de données.
Informatica Administrator (outil Administrator tool)	Application Web qui sert à gérer le domaine et les services d'application.
Informatica Catalog Administrator	Application Web qui permet d'administrer les ressources, les analyseurs, les planifications, les attributs et les connexions.
Enterprise Data Catalog	Application Web qui affiche une vue complète des métadonnées provenant des ressources de données configurées.

Lorsque vous planifiez l'installation : Déterminez le nombre d'instances de l'outil Developer tool que vous souhaitez installer. Vous n'avez pas besoin de planifier les applications Web clientes.

Partie II : Avant l'installation des services

Cette partie contient les chapitres suivants :

- [Avant l'installation des services sous UNIX ou Linux, 23](#)
- [Préparer les services d'application et les bases de données, 38](#)
- [Préparer le déploiement d'Enterprise Data Catalog, 66](#)
- [Enregistrer des informations pour les invites du programme d'installation, 74](#)
- [Configurer les certificats SSL personnalisés, 85](#)
- [Présentation du programme d'installation des services, 94](#)

CHAPITRE 2

Avant l'installation des services sous UNIX ou Linux

Ce chapitre comprend les rubriques suivantes :

- [Avant de commencer Liste de contrôle , 23](#)
- [Lire les notes de publication, 24](#)
- [Vérifier la configuration système requise, 24](#)
- [Sauvegarder les fichiers Data Transformation, 31](#)
- [Examiner les variables d'environnement, 31](#)
- [Créer un compte d'utilisateur système, 32](#)
- [Configurer un fichier keystore, 33](#)
- [Télécharger et extraire les fichiers du programme d'installation, 34](#)
- [Préparer l'installation des fichiers binaires pour les ressources d'Informatica Platform, 36](#)
- [Vérification de la clé de licence, 36](#)
- [Préparer l'importation du cluster, 37](#)

Avant de commencer Liste de contrôle

Ce chapitre présente les tâches préliminaires que vous devez effectuer. Utilisez cette liste de contrôle pour le suivi des tâches préliminaires avant de préparer les services.

- ☐ Lisez les notes de publication Informatica relatives aux mises à jour pour le processus d'installation et de mise à niveau.
- ☐ Vérifiez la configuration système requise :
 - Vérifiez les exigences de dimensionnement en fonction de vos besoins de traitement et d'accès concurrentiel.
 - Consultez les spécifications des correctifs pour vérifier que la machine dispose des correctifs et des bibliothèques requis pour le système d'exploitation.
 - Vérifiez que les numéros de port à utiliser pour les processus de service d'application sont disponibles sur les machines sur lesquelles vous installez les services Informatica.
 - Examinez la configuration requise de distribution pour intégrer le domaine Informatica à l'environnement Hadoop ou Databricks.

- Vérifiez que le système d'exploitation respecte la limite du descripteur de fichier.
- ☐ Sauvegardez les fichiers Data Transformation créés dans une installation précédente.
- ☐ Examinez les variables d'environnement système.
- ☐ Créez un compte utilisateur système pour exécuter le programme d'installation.
- ☐ Configurez les fichiers keystore et truststore si vous voulez configurer une communication sécurisée pour le domaine et une connexion sécurisée aux applications Web clientes.
- ☐ Extrayez les fichiers du programme d'installation :
 - Vérifiez la signature du code d'installation.
 - Vérifiez l'intégrité du package d'installation avec la somme de contrôle.
- ☐ Vérifiez la clé de licence.

Lire les notes de publication

Lisez les notes de publication pour connaître les mises à jour apportées au processus d'installation et de mise à niveau. Vous trouverez également des informations sur les problèmes connus et résolus de la version.

Recherchez les notes de publication sur le [documentation portal](#) d'Informatica.

Vérifier 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 exigences du produit et les plates-formes prises en charge, reportez-vous à la [Product Availability Matrix](#).

Configuration système requise d'Enterprise Data Catalog

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

La configuration système requise diffère en fonction des conditions suivantes :

Si le domaine Informatica, les nœuds de données et les nœuds de traitement se trouvent sur la même machine avec deux millions d'actifs dans le catalogue

La configuration mémoire minimale requise pour le système d'exploitation Linux est de 56 Go de RAM. L'espace disque minimal requis est de 185 Go. Le nombre de cœurs de processeur requis est de 24.

Si le domaine Informatica, les nœuds de données et les nœuds de traitement se trouvent sur des machines différentes

La configuration minimale requise de la mémoire 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 125 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.

Configuration requise pour le serveur de base de données du référentiel d'analyse des actifs de données

La configuration système minimale requise pour la machine qui héberge la base de données du référentiel d'analyse des actifs de données est basée sur le nombre d'actifs dans le catalogue et du type de base de données. Pour plus d'informations sur la configuration matérielle requise telles que le nombre de cœurs de processeur et la mémoire, reportez-vous à la section Paramètres de réglage des performances pour l'analyse des actifs de données du *Guide de réglage des performances d'Enterprise Data Catalog*.

Configuration requise de MetaDex

Avant de générer des visualisations PNG, effectuez les étapes suivantes pour installer les bibliothèques supplémentaires et recréer le cache des polices sur la machine :

1. Exécuter la commande suivante :

```
# install required fonts
sudo yum install fontconfig dejavu-sans-fonts dejavu-serif-fonts
```

pour installer les bibliothèques suivantes :

- fontconfig
- dejavu-sans-fonts
- dejavu-serif-fonts

2. Exécuter la commande suivante :

```
# rebuild fonts cache
fc-cache -f -v
```

pour recréer le cache des polices.

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

Vérifier l'espace disque temporaire et les autorisations

Assurez-vous que votre environnement présente la configuration minimale requise en matière d'espace disque disponible, d'autorisations pour les fichiers temporaires et d'outils client Informatica.

Espace disque pour les fichiers temporaires

Le programme d'installation écrit des fichiers temporaires sur le disque dur. Vérifiez que vous disposez de suffisamment d'espace (1 Go) 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.

Autorisations d'accès aux fichiers temporaires

Assurez-vous d'avoir les autorisations de lecture, d'écriture et d'exécution dans le répertoire `/tmp`.

Pour obtenir plus d'informations sur les exigences du produit et les plates-formes prises en charge, reportez-vous à la [Product Availability Matrix](#).

Vérifier les exigences de dimensionnement

Allouez des ressources pour l'installation et le déploiement de services en fonction du type de déploiement attendu de votre environnement.

Avant d'allouer des ressources, vous devez identifier le type de déploiement en fonction de vos besoins pour le volume de traitement et le niveau d'accès concurrentiel. En fonction du type de déploiement, vous pouvez allouer des ressources à l'espace disque, aux cœurs et à la mémoire vive. Vous pouvez également choisir d'adapter les services lorsque vous exécutez le programme d'installation.

Déterminer le type de déploiement d'installation et de services

Le tableau suivant décrit l'environnement des différents types de déploiement :

Type de déploiement	Description de l'environnement
Sandbox	Utilisé pour la preuve de concepts ou comme sandbox avec un minimum d'utilisateurs.
De base	Utilisé pour le traitement à faible volume avec de faibles niveaux d'accès concurrentiel.
Standard	Utilisé pour le traitement à volume élevé avec de faibles niveaux d'accès concurrentiel.
Avancé	Utilisé pour le traitement à volume élevé avec des niveaux élevés d'accès concurrentiel.

Identifier les exigences de dimensionnement

Le tableau suivant fournit la configuration requise minimale de dimensionnement pour le nœud de domaine Informatica :

Type de déploiement	Espace disque par nœud	Total des cœurs virtuels	RAM par nœud
Sandbox	140 Go	16	32 Go
De base	140 Go	24	64 Go
Standard	140 Go	48	64 Go
Avancé	140 Go	96	128 Go

Pour plus d'informations sur les recommandations de dimensionnement pour les nœuds de cluster sur lesquels vous avez déployé Enterprise Data Catalog, consultez le Guide de réglage des performances d'Enterprise Data Catalog.

Les exigences de dimensionnement tiennent compte des facteurs suivants :

- Espace disque nécessaire à l'extraction du programme d'installation
- Espace disque temporaire nécessaire à l'exécution du programme d'installation
- Espace disque nécessaire à l'installation des services et des composants
- Espace disque requis pour les répertoires de journalisation
- Configuration minimale pour exécuter les services d'application

Les numéros de tailles ne tiennent pas compte des exigences de traitement de données opérationnelles et de mise en cache des objets pour le mode natif d'exécution.

Remarque: Pour les déploiements dans le nuage, choisissez des machines dont la configuration est la plus proche des exigences de tailles.

Adapter les services lors de l'installation

Lorsque vous exécutez le programme d'installation, vous pouvez choisir d'adapter les services en fonction des dimensions du déploiement. Si vous créez un service de référentiel modèle, un service d'intégration de données ou un service de gestion de contenu pendant l'installation, le programme d'installation peut adapter

les services en fonction du type de déploiement que vous entrez. Le programme d'installation configure des propriétés telles que la taille maximale des segments de mémoire et la taille du pool d'exécution.

Vous pouvez adapter les services à tout moment après les avoir installés à l'aide de la commande `infacmd autotune`. Lorsque vous exécutez la commande, vous pouvez adapter des propriétés pour d'autres services ainsi que les propriétés du moteur d'exécution Hadoop.

Vérifier les spécifications de correctif sur UNIX ou Linux

Avant d'installer les services Informatica, vérifiez que la machine dispose des correctifs et des bibliothèques requis pour le système d'exploitation.

Enterprise Data Catalog sur Linux

Le tableau suivant répertorie les correctifs et les bibliothèques requis par les services Informatica pour Enterprise Data Catalog sur Linux :

Plate-forme	Système d'exploitation	Correctif du système d'exploitation
AWS Linux	Linux 2 - 2023.4.20240416	Tous les packages suivants : <ul style="list-style-type: none">- <code>e2fsprogs-libs-1.42.9-12.amzn2.0.2.x86_64</code>- <code>keyutils-libs-1.5.8-3.amzn2.0.2.x86_64</code>- <code>libselinux-2.5-12.amzn2.0.2.x86_64</code>- <code>libsepol-2.5-8.1.amzn2.0.2.x86_64</code>
Ubuntu	20.04.1	Tous les packages suivants : <ul style="list-style-type: none">- <code>e2fsprogs/focal,now 1.45.5-2ubuntu1 amd64</code> [installé]- <code>libkeyutils1/focal,now 1.6-6ubuntu1 amd64</code> [installé, automatique]- <code>libselinux1/focal,now 3.0-1build2 amd64</code> [installé, automatique]- <code>libsepol1/focal,now 3.0-1 amd64</code> [installé, automatique]
Ubuntu	22.04	Tous les packages suivants : <ul style="list-style-type: none">- <code>e2fsprogs/focal,now 1.46.5-2ubuntu1.1 amd64</code> [installé]- <code>libkeyutils1/focal,now 1.6.1-2ubuntu3 amd64</code> [installé, automatique]- <code>libselinux1/focal,now 3.3-1build2 amd64</code> [installé, automatique]- <code>libsepol1/focal,now 2.7-1ubuntu0.1 amd64</code> [installé, automatique]
Linux-x64	Red Hat Enterprise Linux 7.3	Tous les packages suivants, où <version> correspond à une version du package : <ul style="list-style-type: none">- <code>e2fsprogs-libs-<version>.el7</code>- <code>keyutils-libs-<version>.el7</code>- <code>libselinux-<version>.el7</code>- <code>libsepol-<version>.el7</code>
Linux-x64	Red Hat Enterprise Linux 8	Tous les packages suivants, où <version> correspond à une version du package : <ul style="list-style-type: none">- <code>e2fsprogs-libs-<version>.el8</code>- <code>keyutils-libs-<version>.el8</code>- <code>libselinux-<version>.el8</code>- <code>libsepol-<version>.el8</code> <p>Remarque: OpenSSL 3.0 n'est pas pris en charge. Si la machine sur laquelle le service PostgreSQL s'exécute est compatible FIPS, vérifiez que <code>compat-openssl10</code> est installé. Vérifiez que la variable <code>\$PATH</code> pointe vers le répertoire <code>/usr/bin</code> pour utiliser la version correcte de Linux OpenSSL.</p>

Plate-forme	Système d'exploitation	Correctif du système d'exploitation
Linux-x64	SUSE Linux Enterprise Server 12	Service Pack 5
Linux-x64	SUSE Linux Enterprise Server 15	Service Pack 5

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'application.

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 ports sont disponibles sur les machines sur lesquelles vous exécutez le programme d'installation.

Remarque: Les services et nœuds peuvent ne pas démarrer en cas de conflit de ports.

Le tableau suivant décrit les spécifications de port pour l'installation :

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 dans le 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 d'arrêt d'Informatica Administrator	Numéro de port qui contrôle l'arrêt du serveur pour Informatica Administrator. Informatica Administrator écoute les commandes d'arrêt sur ce port. La valeur par défaut est 6009.
Numéro de port minimal	Numéro de port le plus faible dans la plage des numéros de port qui peut être attribué 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 ports dynamiques pouvant être attribués aux processus de service d'application exécutés sur ce nœud. Le numéro par défaut est 6114.

Port	Description
Plage de ports dynamiques pour les services d'application	<p>Plage de numéros de port qui peuvent être attribués 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'application 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>
Ports statiques des services d'application	<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 catalogue. La valeur par défaut est de 9085 pour HTTP. - 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. - Service de cluster Informatica. La valeur par défaut est de 9075 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.

Vérifier la configuration requise des packages de distribution(Linux et UNIX)

Vous pouvez utiliser des packages de distribution tiers pour intégrer le domaine Informatica à l'environnement Hadoop ou Databricks.

Le domaine et le client Informatica nécessitent les packages de distribution pour traiter des fichiers complexes dans le domaine Informatica, ou pour se connecter à l'environnement Hadoop ou Databricks lorsque vous les traitez dans le domaine Informatica, ou pour transférer le traitement vers l'environnement Hadoop ou Databricks.

Si vous avez besoin d'un package de distribution, vous pouvez l'installer via le programme d'installation ou via Integration Package Manager (le gestionnaire de packages) à tout moment.

Traiter dans le domaine Informatica

Vous pouvez utiliser le package de distribution Cloudera CDP Private Cloud pour traiter des fichiers complexes dans le domaine Informatica ou pour vous connecter à l'environnement Hadoop ou Databricks, mais les traiter dans le domaine Informatica. Cependant, vous pouvez utiliser un autre package de distribution en fonction de vos besoins.

Les adaptateurs suivants nécessitent des packages de distribution pour le traitement dans le domaine Informatica :

- PowerExchange for Amazon S3
- PowerExchange for Google Cloud Storage
- PowerExchange for Google Cloud Storage pour PowerCenter
- PowerExchange for Hadoop for PowerCenter
- PowerExchange for HBase
- PowerExchange for HDFS
- PowerExchange for Hive
- PowerExchange for JDBC V2
- PowerExchange for Kafka pour PowerCenter
- PowerExchange for MapR-DB
- PowerExchange for Microsoft Azure Blob Storage
- PowerExchange for Microsoft Azure Data Lake Storage Gen1
- PowerExchange for Microsoft Azure Data Lake Storage Gen2

Traiter avec l'environnement Hadoop ou Databricks

Lorsque vous transférez le traitement vers l'environnement Hadoop ou Databricks, le client et le domaine Informatica nécessitent des packages de distribution. Pour plus d'informations sur les packages de distribution pris en charge, reportez-vous à la [Product Availability Matrix](#).

Vérifier la limite du descripteur de fichier

Vérifiez que le système d'exploitation répond aux exigences du descripteur de fichier.

Les processus de service Informatica peuvent utiliser un grand nombre de fichiers. Pour éviter les erreurs dues à un grand nombre de fichiers et de processus, vous pouvez modifier les paramètres système à l'aide de la commande `limit` si vous utilisez un shell C, ou de la commande `ulimit` si vous utilisez un shell Bash.

Répertorier les paramètres du système d'exploitation

Pour obtenir une liste des paramètres du système d'exploitation, y compris la limite de descripteur de fichier, exécutez la commande suivante :

Dans un shell C, exécutez `limit`

Dans un shell Bash, exécutez `ulimit -a`

Définir la limite de descripteur de fichier

Les processus de service Informatica peuvent utiliser un grand nombre de fichiers. Définissez la limite des descripteurs de fichier par processus à 16 000 ou plus. La limite recommandée est de 32 000 descripteurs de fichier par processus.

Pour modifier les paramètres système, exécutez la commande `limit` ou `ulimit` avec la valeur et l'indicateur pertinents. Par exemple, pour définir la limite du descripteur de fichier, exécutez la commande suivante :

Dans un shell C, exécutez `limit -h filesize <valeur>`

Dans un shell Bash, exécutez `ulimit -n <valeur>`

Définir le nombre maximal de processus utilisateur

Les services Informatica utilisent un grand nombre de processus utilisateur. Utilisez la commande `ulimit -u` pour régler le nombre maximal de processus utilisateur sur un niveau suffisamment haut pour convenir à tous les processus requis par le moteur Blaze.

Pour définir le nombre maximal de processus utilisateur, exécutez la commande suivante :

Dans un shell C, exécutez `limit -u processes <valeur>`

Dans un shell Bash, exécutez `ulimit -u valeur`

Sauvegarder les fichiers Data Transformation

Avant l'installation, vous devez sauvegarder les fichiers Data Transformation créés dans les versions précédentes. Une fois l'installation terminée, copiez les fichiers dans les nouveaux répertoires d'installation pour obtenir le même référentiel et les mêmes composants globaux personnalisés que dans la version précédente.

Le tableau suivant répertorie les fichiers ou répertoires à sauvegarder.

Fichier ou répertoire	Emplacement par défaut
Référentiel	<répertoire d'installation Informatica>\DataTransformation\ServiceDB
Répertoire des composants globaux personnalisés (fichiers TGP)	<répertoire d'installation Informatica>\DataTransformation\autoInclude\user
Répertoire des composants globaux personnalisés (fichiers DLL et JAR)	<répertoire d'installation Informatica>\DataTransformation\externLibs\user
Fichier de configuration	<répertoire d'installation Informatica>\DataTransformation\CMConfig.xml
Fichier de licence	<répertoire d'installation Informatica>\DataTransformation\CDELICENSE.cfg

Ne copiez pas les fichiers de bibliothèque Data Transformation. Réinstallez plutôt les bibliothèques Data Transformation.

Examiner les variables d'environnement

Configurer les variables d'environnement pour l'installation d'Informatica.

Le tableau suivant décrit les variables d'environnement à examiner :

Variable	Description
IATEMPDIR	<p>Emplacement des fichiers temporaires créés pendant l'installation. Informatica requiert 1Go d'espace sur le disque pour les fichiers temporaires.</p> <p>Configurez la variable d'environnement si vous ne souhaitez pas créer de fichiers temporaires dans le répertoire /tmp.</p> <p>Pour modifier le répertoire /tmp par défaut, vous devez définir les variables d'environnement IATEMPDIR et _JAVA_OPTIONS sur le nouveau répertoire.</p> <p>Par exemple, définissez la variable pour exporter IATEMPDIR=/home/user.</p> <p>Remarque: Annulez la définition de la variable IATEMPDIR après l'installation.</p>
_JAVA_OPTIONS	<p>Configurez la variable d'environnement pour modifier le répertoire temporaire.</p> <p>Pour modifier le répertoire /tmp par défaut, vous devez définir les variables d'environnement IATEMPDIR et _JAVA_OPTIONS sur le nouveau répertoire.</p> <p>Par exemple, définissez la variable pour exporter _JAVA_OPTIONS=-Djava.io.tmpdir=/home/user.</p> <p>Remarque: Annulez la définition de la variable _JAVA_OPTIONS après l'installation.</p>
LANG et LC_ALL	<p>Modifiez les paramètres régionaux pour définir le codage de caractères approprié pour la session de terminal. Par exemple, définissez le codage sur <code>Latin1</code> ou <code>ISO-8859-1</code> pour le français, sur <code>EUC-JP</code> ou <code>Shift JIS</code> pour le japonais, ou sur <code>UTF-8</code> pour le chinois ou le coréen. Le codage de caractères détermine les types de caractères qui s'affichent dans le terminal UNIX.</p>
DISPLAY	<p>Effacez la variable d'environnement DISPLAY avant d'exécuter le programme d'installation. L'installation peut échouer si la variable d'environnement DISPLAY a une valeur.</p>
SKIP_VENDOR_CHECK	<p>Configurez la variable d'environnement pour supprimer l'invite sudo du programme d'installation sous Linux ou AIX.</p> <p>Définissez la variable d'environnement sur true pour supprimer l'invite sudo de l'installation du serveur Informatica sous Linux ou AIX.</p> <p>Remarque: Si vous ne disposez pas des privilèges sudo, définissez la variable d'environnement sur true avant d'exécuter le programme d'installation. Si vous disposez de privilèges sudo, vous n'avez pas besoin de définir la variable d'environnement.</p>

Remarque: Assurez-vous que l'indicateur NOEXEC n'est pas défini pour le système de fichiers monté dans le répertoire /tmp.

Créer un compte d'utilisateur système

Créez un compte utilisateur spécifiquement conçu pour exécuter le service Informatica.

Vérifiez que le compte utilisateur que vous utilisez pour installer Informatica dispose d'une autorisation d'accès en écriture sur le répertoire d'installation.

Vérifiez que le compte utilisateur qui installe le service Informatica ne dispose pas de privilèges et d'autorisations pour accéder aux fichiers sensibles sur la machine sur laquelle vous installez les services Informatica.

Configurer un fichier keystore

Lorsque vous installez les services Informatica, vous pouvez configurer une communication sécurisée pour le domaine et une connexion sécurisée à Informatica Administrator (l'outil Administrator). Si vous configurez ces options de sécurité, vous devez paramétrer les fichiers keystore et truststore.

Avant d'installer les services Informatica, configurez les fichiers pour une communication sécurisée dans le domaine Informatica ou pour une connexion sécurisée à l'outil Administrator tool. Pour créer les fichiers requis, vous pouvez utiliser les programmes suivants :

keytool

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

OpenSSL

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

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

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

Pour un niveau de sécurité accru, envoyez votre CSR à une autorité de certification pour obtenir un certificat signé.

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

Communication sécurisée dans le domaine Informatica

Avant d'activer la communication sécurisée dans le domaine Informatica, vérifiez que les conditions suivantes sont remplies :

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

Note that RSA encryption requires more than 512 bits.

You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into keystores.

You must have a keystore in PEM format named `infa_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

The keystore files must contain the root and intermediate SSL certificates.

Remarque: The password for the keystore in JKS format must be the same as the private key pass phrase used to generate the SSL certificate.

You imported the certificate into truststores.

You must have a truststore in PEM format named `infa_truststore.pem` and a truststore in JKS format named `infa_truststore.jks`.

The truststore files must contain the root, intermediate, and end user SSL certificates.

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

Les keystores et truststores doivent se trouver dans un répertoire accessible au programme d'installation.

The keystore type used for the Administrator tool determines the keystore types for the Content Management Service.

If you used the default keystore certificate for the Administrator tool, you can use either the default or a custom keystore certificate for the Content Management Service.

If you used a custom keystore certificate for the Administrator tool, you must use a custom keystore certificate for the Content Management Service.

Pour plus d'informations sur la création d'un keystore et d'un truststore personnalisés, consultez la section [Informatica How-To Library article "How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain"](#).

Connexion sécurisée à l'outil Administrator tool

Avant de sécuriser la connexion à l'outil Administrator tool, vérifiez que les conditions suivantes sont remplies :

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

Note that RSA encryption requires more than 512 bits.

You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into a keystore in JKS format.

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

Le keystore se trouve dans le répertoire approprié.

Le keystore doit se trouver dans un répertoire accessible au programme d'installation.

Télécharger et extraire les fichiers du programme d'installation

Les fichiers d'installation sont distribués sous forme de fichiers compressés. Vous pouvez obtenir le fichier d'installation d'Informatica et les packages de distribution à partir du lien FTP contenu dans votre e-mail de confirmation de commande.

Téléchargez le fichier TAR d'installation d'Informatica et les fichiers ZIP des packages de distribution requis sur le site de téléchargement de logiciels électroniques d'Informatica. Vous pouvez les télécharger dans un répertoire local ou un lecteur réseau partagé mappé sur votre machine.

Pour télécharger d'autres fichiers et utilitaires compressés, envoyez une demande d'expédition auprès du support client international Informatica.

Extrayez les fichiers du programme d'installation Informatica dans un répertoire situé sur votre machine. L'utilisateur qui exécute le programme d'installation doit disposer d'autorisations de lecture et d'écriture sur le répertoire qui contient les fichiers du programme d'installation et d'autorisations d'exécution sur le fichier exécutable.

Remarque: Veillez à extraire les fichiers du programme d'installation dans un répertoire local, car vous ne pouvez pas exécuter le programme d'installation à partir d'un fichier mappé.

Copiez les fichiers ZIP des packages de distribution à l'emplacement suivant : `<Informatica installer files>/source`

Remarque: Le programme d'installation échoue si les fichiers ZIP des packages de distribution ne sont pas disponibles dans le répertoire source.

Vérifier la signature de code du programme d'installation

Vous pouvez vérifier la signature du code logiciel d'Informatica.

Informatica utilise une signature numérique basée sur certificat pour signer le code logiciel d'Informatica. La signature de code permet de valider son authenticité et garantit l'absence de modifications ou de corruptions du code après sa signature par Informatica. Vous pouvez déterminer la fiabilité du logiciel en fonction de la présence ou de l'absence de la signature de code.

Vous pouvez demander un certificat de signature de code qui contient des informations qui identifient pleinement Informatica LLC et une autorité de certification (CA) qui émet le certificat. Le certificat numérique lie l'identité d'Informatica à une clé publique et à une clé privée.

La signature numérique du logiciel commence par la création d'un hachage cryptographique ou d'un condensé. La correspondance du condensé avec les données d'origine est de type un-à-un. Utilisez le condensé, car il n'y a aucune suggestion sur le mode de recréation des données d'origine. Même une modification mineure des données d'origine entraîne celle de la valeur de hachage. Informatica utilise sa clé privée pour signer le condensé ou génère une signature sous la forme d'une chaîne de bits. Les algorithmes de signature numérique correcte permettent à un utilisateur ayant une clé publique de vérifier le créateur de la signature.

Vérifier l'authenticité du code signé

Après qu'Informatica signe le pack de logiciel, vous pouvez contacter le support client international Informatica pour accéder au certificat de signature de code. Informatica livre le programme d'installation avec le fichier de signature qui contient le hachage du fichier binaire du programme d'installation chiffré avec la clé privée d'Informatica. Vous pouvez valider l'intégrité des fichiers binaires signés numériquement à l'aide d'outils disponibles, tels qu'OpenSSL.

Par exemple, pour vérifier l'authentification du package et confirmer la sécurité du code, entrez les commandes OpenSSL suivantes :

```
openssl base64 -d -in $signature -out /tmp/sign.sha256
openssl dgst -sha256 -verify <(openssl x509 -in <cert> -pubkey -noout) -signature /tmp/
sign.sha256 <file>
```

où `<signature>` est le fichier contenant la signature en Base64, `<cert>` est le certificat de signature de code et `<file>` est le fichier à vérifier.

En fonction du résultat de ce processus de vérification, OpenSSL affiche un message de succès ou d'échec selon que le code du programme d'installation est reconnu comme authentique ou non. Veuillez noter que la vérification du programme d'installation peut prendre environ deux minutes.

Vérifier la somme de contrôle du package d'installation sur UNIX et Linux

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

Vérifiez la somme de contrôle des fichiers du programme d'installation spécifiques par rapport à la somme de contrôle des fichiers d'installation téléchargés depuis le site de téléchargement de logiciels électroniques Informatica.

Le tableau suivant répertorie la somme de contrôle et la taille de fichier pour le programme d'installation des services Informatica pour UNIX et Linux :

Fichier	Valeur de la somme de contrôle	Taille du fichier
informatica_1056_server_linux-x64.tar	2774164387	12477583360

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

Préparer l'installation des fichiers binaires pour les ressources d'Informatica Platform

Pour exécuter les ressources Informatica Platform, téléchargez et installez les fichiers binaires.

Informatica fournit des fichiers ZIP contenant les fichiers binaires du scanner et les fichiers binaires complémentaires du scanner. Le fichier ScannerBinaries.zip comprend les fichiers binaires de ressources Informatica Platform pour la version 10.5.6 et le fichier ExtendedScannerBinaries.zip comprend les fichiers binaires de ressources Informatica Platform à partir des versions précédentes.

Effectuez les étapes suivantes pour préparer les fichiers binaires pour les ressources d'Informatica Platform :

1. Téléchargez les fichiers binaires du scanner à partir du site de téléchargement de logiciels électroniques Informatica.
2. Copiez le fichier ZIP à l'emplacement suivant : `<Installer directory>/source`

Vérification de la clé de licence

Avant d'installer le logiciel, vérifiez que vous disposez de la clé de licence.

Lorsque vous téléchargez les fichiers d'installation depuis le site Electronic Software Download (ESD), la clé de licence se trouve dans un courriel d'Informatica. Copiez le fichier de clé de licence dans un répertoire accessible par le compte d'utilisateur qui installe le produit.

Contactez le Support client international Informatica si vous n'avez pas de clé de licence ou si vous avez une clé de licence incrémentielle et que vous voulez créer un domaine.

Préparer l'importation du cluster

Lorsque vous exécutez le programme d'installation, vous pouvez choisir de configurer le cluster. La configuration de cluster permet au service d'intégration de données de transmettre la logique de mappage au cluster. Pour intégrer le domaine Informatica au cluster non natif, vous devez importer une configuration de cluster. Vous pouvez importer les informations de cluster directement depuis le cluster ou depuis un fichier d'archive.

Vous pouvez importer les informations de cluster depuis un fichier d'archive de tout cluster pris en charge dans le domaine. Votre administrateur préférera peut-être vous fournir le fichier d'archive pour protéger les informations de connexion sensibles au cluster. Le format du fichier d'archive peut être .zip ou .tar. Veillez à stocker le fichier d'archive localement.

Préparer le fichier d'archive pour l'environnement Hadoop

Pour importer la configuration de cluster depuis Amazon EMR, MapR ou Google Dataproc, vous devez le faire depuis un fichier d'archive. Le contenu du fichier d'archive de la configuration de cluster Hadoop peut être le suivant selon la distribution :

- core-site.xml
- hbase-site.xml. est requis uniquement si vous accédez aux sources et aux cibles HBase.
- hdfs-site.xml
- hive-site.xml
- mapred-site.xml ou tez-site.xml. Incluez le fichier mapred-site.xml ou le fichier tez-site.xml en fonction du type d'exécution Hive utilisé pour le cluster Hadoop.
- yarn-site.xml

Remarque: Lorsque vous configurez un cluster de cloud public CDP, le fichier hbase-site.xml se trouve sur le cluster Data Lake. Les autres fichiers se trouvent sur le cluster Data Hub.

Préparer le fichier d'archive pour l'environnement Databricks

Pour créer le fichier .xml pour l'importation, vous devez vous procurer les informations requises auprès de l'administrateur Databricks. Vous pouvez fournir n'importe quel nom pour le fichier et le stocker localement.

Le tableau suivant décrit les propriétés du cluster pour le configurer dans le fichier d'importation pour l'environnement Databricks :

Nom de la propriété	Description
cluster_name	Nom du cluster Databricks.
cluster_ID	ID du cluster Databricks.
base URL	URL d'accès au cluster Databricks.
accesstoken	ID de jeton créé dans Databricks requis pour l'authentification.

Vous pouvez inclure éventuellement d'autres propriétés spécifiques à l'environnement Databricks. Lorsque vous finalisez le fichier .xml, compressez-le dans un fichier .zip ou .tar pour l'importation.

CHAPITRE 3

Préparer les services d'application et les bases de données

Ce chapitre comprend les rubriques suivantes :

- [Liste de contrôle pour préparer les services d'application , 38](#)
- [Préparer les services d'application et les bases de données - Présentation, 39](#)
- [Configurer les comptes de l'utilisateur de la base de données, 39](#)
- [Identifier les services d'application par produit, 40](#)
- [Spécifications de la base de données du référentiel de configuration du domaine, 41](#)
- [Service Analyst , 45](#)
- [Effectuer les tâches prérequis, 45](#)
- [Service de catalogue, 46](#)
- [Service de gestion de contenu, 47](#)
- [Service d'intégration de données, 49](#)
- [Service de cluster Informatica, 56](#)
- [Service d'accès aux métadonnées, 56](#)
- [Service de référentiel modèle, 57](#)
- [Service de référentiel modèle de surveillance, 61](#)
- [Service de recherche, 62](#)
- [Configuration de la connectivité native sur les machines du service, 62](#)

Liste de contrôle pour préparer les services d'application

Ce chapitre contient des informations sur les services d'application et les bases de données de l'environnement Informatica. Utilisez cette liste de contrôle pour le suivi de la planification des services et de la préparation des bases de données.

- ☐ Identifiez les services d'application dont vous avez besoin dans votre environnement.

- ☐ Identifiez les services d'application que le programme d'installation doit créer.
- ☐ Préparez des bases de données pour les services :
 - Créez la base de données.
 - Créez un utilisateur pour la base de données.
 - Créez des variables d'environnement.
 - Configurez la connectivité.

Préparer les services d'application et les bases de données - Présentation

Lorsque vous planifiez les services d'application, vous devez tenir compte des services associés qui se connectent au service d'application. Vous devez également planifier les bases de données relationnelles nécessaires aux services d'application.

Le programme d'installation vous invite à la création éventuelle de services pendant l'installation. Les propriétés de certains services requièrent des informations sur la base de données. Si vous souhaitez que le programme d'installation crée un service qui requiert une base de données, vous devez préparer la base de données avant d'exécuter le programme d'installation. Pour préparer les bases de données, vérifiez les exigences de la base de données, configurez la base de données et paramétrez un compte utilisateur. Les exigences de la base de données dépendent des services d'application que vous créez.

Si vous ne créez pas de services lors de l'installation, vous pouvez les créer manuellement après l'installation.

Configurer les comptes de l'utilisateur de la base de données

Définissez une base de données et un compte d'utilisateur pour les bases de données du référentiel.

Utilisez les règles et les directives suivantes lorsque vous configurez les comptes de l'utilisateur :

- 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.

Identifier les services d'application par produit

Chaque service d'application propose des fonctionnalités différentes dans le domaine Informatica. Vous devez créer les services d'application en fonction de la clé de licence générée pour votre organisation.

Le tableau suivant répertorie les services d'application que chaque produit utilise :

Produit	Services d'application
Enterprise Data Catalog	<ul style="list-style-type: none">- Service Analyst- Service de catalogue*- Service de gestion de contenu*- Service d'intégration de données*- Service d'accès aux métadonnées*- Service de référentiel modèle*- Service de référentiel modèle de surveillance*- Service de cluster Informatica*- Service de recherche
Data Engineering Integration	<ul style="list-style-type: none">- Service Analyst- Service d'intégration de données*- Service d'ingestion de masse- Service d'accès aux métadonnées*- Service de référentiel modèle*- Service de référentiel modèle de surveillance*
Data Engineering Quality	<ul style="list-style-type: none">- Service Analyst- Service de gestion de contenu*- Service d'intégration de données*- Service d'ingestion de masse- Service d'accès aux métadonnées*- Service de référentiel modèle*- Service de référentiel modèle de surveillance*- Service de recherche
Data Engineering Streaming	<ul style="list-style-type: none">- Service Analyst- Service d'intégration de données*- Service d'ingestion de masse- Service d'accès aux métadonnées*- Service de référentiel modèle*- Service de référentiel modèle de surveillance*
<i>* Vous pouvez créer ces services lorsque vous installez le produit.</i>	

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 du domaine.

Vous devez configurer une base de données et un compte d'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 Informatica, vous fournissez les informations de la base de données et du compte d'utilisateur pour le référentiel de configuration du domaine. Le programme d'installation d'Informatica utilise JDBC pour communiquer avec le référentiel de configuration du domaine.

The domain configuration repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL
- Sybase ASE

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

Spécifications de la base de données IBM DB2

Use the following guidelines when you set up the repository on IBM DB2:

- If the repository is in an IBM DB2 database, verify that IBM DB2 Version 10.5 is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
 - DB2_SKIPINSERTED
 - DB2_EVALUNCOMMITTED
 - DB2_SKIPDELETED
 - AUTO_RUNSTATS
- On the database, set the configuration parameters.

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

Paramètre	Valeur
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.

In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

In a multi-partition database, specify a non-partitioned tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.

- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.
- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.

- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.

The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

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 de Microsoft Azure SQL Database

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 :

- 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 la base de données PostgreSQL

Utilisez les directives suivantes lors de la configuration de la base de données sur PostgreSQL :

- Vérifiez que le compte utilisateur de la base de données dispose des privilèges CONNECT, CREATE TABLE et CREATE VIEW.
- Spécifiez le nom du schéma de la base de données lorsque vous utilisez PostgreSQL comme base de données.
- Assurez-vous que l'espace disque de PostgreSQL est suffisant pour les fichiers de données. Par défaut, ceux-ci se trouvent à l'emplacement suivant :
 <PostgreSQL installation directory>/data
- Dans la base de données, définissez les paramètres de configuration.

Le tableau suivant répertorie les valeurs minimales et recommandées pour les paramètres de configuration :

Paramètre	Valeur minimale	Valeur recommandée
max_connections	200	4000
shared_buffers	2 Go	16 Go
max_locks_per_transaction	1024	1024
max_wal_size	1 Go	8 Go
checkpoint_timeout	5 minutes	30 minutes

Spécifications de la base de données Sybase

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 16 K minimum. Vous devez définir la taille de page sur 16 K car ceci est une configuration unique qui ne pourra pas être changée par la suite.

- Définissez la configuration du verrouillage de base de données pour utiliser le verrouillage au niveau des lignes :
Le tableau suivant décrit la configuration du verrouillage de base de données que vous devez définir :

Configuration de la base de données	Procédure de système Sybase	Valeur
Schéma de verrouillage	sp_configure "lock scheme"	0, datarows

- Définissez l'option de base de données Sybase « ddl in tran » sur TRUE.
- Définissez « autoriser les nulls par défaut » sur TRUE.
- Activez l'option de base de données Sybase select into/bulkcopy/plsort.
- Activez le privilège « Sélectionner » pour la table système sysobjects.
- Créez le script de connexion suivant pour désactiver la troncation VARCHAR par défaut :

```
create procedure dbo.sp_string_rtrunc_proc as set string_rtruncation on
sp_modifylogin "user_name", "login script", sp_string_rtrunc_proc
```

Le script de connexion est exécuté chaque fois que l'utilisateur se connecte à l'instance Sybase. La procédure stockée définit le paramètre au niveau de la session. La procédure système sp_modifylogin met à jour « user_name » selon la procédure qui est stockée et désignée comme son « script de connexion ». L'utilisateur doit être autorisé à appeler la procédure stockée.

- Vérifiez que l'utilisateur de la base de données dispose des privilèges CREATE DEFAULT, CREATE PROCEDURE, CREATE RULE, CREATE TABLE et CREATE VIEW.
- Définissez les configurations de la base de données sur les valeurs initiales recommandées.
Le tableau suivant répertorie les paramètres de configuration mémoire de la base de données que vous devez définir :

Configuration de la base de données	Procédure de système Sybase	Valeur
Quantité maximum de mémoire physique totale	sp_configure "max memory"	2097151
Taille de cache de la procédure	sp_configure "procedure cache size"	500000
Nombre d'objets ouverts	sp_configure "number of open objects"	5000
Nombre d'index ouverts	sp_configure "number of open indexes"	5000
Nombre de partitions ouvertes	sp_configure "number of open partitions"	5000
Mémoire du segment par utilisateur	sp_configure "heap memory per user"	49152
Nombre de verrous	sp_configure "number of locks"	100000

Service Analyst

Le service Analyst exécute l'outil Analyst tool. Il gère les connexions entre les composants de service et l'utilisateur qui ont accès à l'outil Analyst tool. Lorsque vous créez le service, vous devez y associer d'autres services d'application.

Le tableau suivant résume certaines dépendances associées au service Analyst :

Dépendance	Résumé
Produits	Les produits suivants utilisent le service Analyst : <ul style="list-style-type: none">- Data Engineering Integration- Data Engineering Quality- Data Engineering Streaming- Enterprise Data Catalog- Informatica Data Quality- PowerCenter- Test Data Management
Services	Le service Analyst requiert une association directe avec les services suivants : <ul style="list-style-type: none">- Service d'intégration de données- Service de référentiel modèle
Bases de données	Aucune de base de données n'est associée au service Analyst.
Programme d'installation	Vous ne pouvez pas créer le service Analyst pendant l'installation.

Effectuer les tâches prérequis

L'installation d'Enterprise Data Catalog comprend plusieurs phases.

Lorsque vous prévoyez d'installer Enterprise Data Catalog, vous devez prendre en compte les dépendances de chaque produit. Vous devez également planifier les bases de données relationnelles nécessaires à chaque produit.

Reportez-vous à la liste de services suivante et vérifiez la configuration requise associée aux services :

Service de cluster Informatica

Le service de cluster Informatica est un service d'application qui exécute et gère les nœuds et les services associés à Enterprise Data Catalog. Pour plus d'informations, reportez-vous à la section ["Service de cluster Informatica" à la page 56](#).

Service de catalogue

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. Pour plus d'informations, reportez-vous à la section ["Service de catalogue" à la page 46](#).

Service d'intégration de données

Le service d'intégration de données reçoit les demandes des outils clients Informatica pour exécuter des tâches d'intégration, de profil et de préparation de données. Il écrit des résultats dans différentes bases de données et écrit des métadonnées au moment de l'exécution dans le référentiel modèle. Vous devez

également préparer les bases de données associées au service. Pour plus d'informations, reportez-vous à la section ["Service d'intégration de données" à la page 49](#).

Service de référentiel modèle

Le service de référentiel modèle gère le référentiel modèle. Il reçoit des clients Informatica et des services d'application des demandes de stockage des métadonnées ou d'accès à celles-ci dans le référentiel modèle. Vous devez également préparer la base de données du référentiel modèle. Pour plus d'informations, reportez-vous à la section ["Service de référentiel modèle" à la page 57](#).

Service de catalogue

Le service de catalogue est un service d'application qui exécute Enterprise Data Catalog dans le domaine Informatica. Il 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.

Le tableau suivant récapitule les dépendances pour les produits, services et bases de données associés au service de catalogue :

Dépendance	Résumé
Produits	Les produits suivants utilisent le service de catalogue : <ul style="list-style-type: none">- Enterprise Data Catalog- Enterprise Data Preparation- Data Privacy Management
Services	Le service de catalogue dépend des services suivants : <ul style="list-style-type: none">- Service de gestion de contenu- Service d'intégration de données- Service de cluster Informatica- Service de référentiel modèle- Service Analyst
Bases de données	Si vous souhaitez activer l'analyse des actifs de données pour le service de catalogue, vous pouvez sélectionner l'une des bases de données suivantes pour le référentiel de l'analyse des actifs de données : <ul style="list-style-type: none">- Oracle- SQL Server- PostgreSQL Configurez l'analyse des actifs de données pour le service de catalogue si vous souhaitez activer l'analyse de flux de données. Si vous souhaitez l'activer pour une ressource PowerCenter, créez un utilisateur de base de données en lecture seule sur la base de données du référentiel PowerCenter.
Programme d'installation	Vous pouvez créer le service de catalogue lorsque vous installez Enterprise Data Catalog.

Service de gestion de contenu

Le service de gestion de contenu gère les données de référence pour les domaines de données qui utilisent des tables de référence. Il 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. Lorsque vous créez le service, vous devez y associer d'autres services d'application.

Le tableau suivant récapitule les dépendances pour les produits, services et bases de données associés au service de gestion de contenu :

Dépendance	Résumé
Produits	Les produits suivants utilisent le service de gestion de contenu : <ul style="list-style-type: none">- Data Engineering Quality- Data Privacy Management- Enterprise Data Catalog- Enterprise Data Preparation- Informatica Data Quality- Test Data Management
Services	Le service de gestion de contenu requiert une association directe avec les services suivants : <ul style="list-style-type: none">- Service de référentiel modèle- Service d'intégration de données
Bases de données	Le service de gestion de contenu utilise la base de données suivante : <ul style="list-style-type: none">- 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.
Programme d'installation	Vous pouvez créer le service de gestion de contenu lorsque vous exécutez le programme d'installation. Remarque: Vous devez créer le service de gestion de contenu sur le même nœud que le service d'intégration de données.

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.

The reference data warehouse supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL, using a JDBC driver

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.

Configuration requise pour la base de données IBM DB2

Use the following guidelines when you set up the repository on IBM DB2:

- Verify that the database user account has CREATETAB and CONNECT privileges.
- Vérifiez que l'utilisateur de la base de données dispose des privilèges SELECT sur les tables SYSCAT.DBAUTH et SYSCAT.DBTAUTH.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespacespace parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespacespace.

Configuration requise de Microsoft Azure SQL Database

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 DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName 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=[DatabaseName]
```

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

- 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 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.

Configuration requise de la base de données PostgreSQL

Utilisez les directives suivantes lors de la configuration de la base de données sur PostgreSQL :

- Utilisez une connexion JDBC pour vous connecter à la base de données PostgreSQL.

Informatica installe un pilote JDBC DataDirect pour PostgreSQL que vous pouvez utiliser pour vous connecter à la base de données. Recherchez le pilote dans le répertoire d'installation `clients/DeveloperClient/infacmd` et copiez le pilote dans le répertoire `clients/externaljdbcjars`.
- Spécifiez le nom du schéma de la base de données. Vous devez définir le nom de schéma.

Si la base de données utilise le nom de schéma PostgreSQL par défaut `public`, vous pouvez spécifier `public` comme nom de schéma.
- Vérifiez que l'utilisateur de la base de données dispose des privilèges `CONNECT` et `CREATE TABLE`.

Service d'intégration de données

Le service d'intégration de données reçoit les demandes des outils clients Informatica pour exécuter des tâches d'intégration, de profil et de préparation de données. Il écrit des résultats dans différentes bases de

données et écrit des métadonnées au moment de l'exécution dans le référentiel modèle. Lorsque vous créez le service, vous devez lui associer un autre service d'application.

Le tableau suivant récapitule les dépendances pour les produits, services et bases de données associés au service d'intégration de données :

Dépendance	Résumé
Produits	Les produits suivants utilisent le service d'intégration de données : <ul style="list-style-type: none">- Data Engineering Integration- Data Engineering Quality- Data Engineering Streaming- Data Privacy Management- Enterprise Data Catalog- Enterprise Data Preparation- Informatica Data Quality- PowerCenter- Test Data Management
Services	Le service d'intégration de données requiert une association directe avec le service suivant : <ul style="list-style-type: none">- Service de référentiel modèle
Bases de données	Le service d'intégration de données utilise les bases de données suivantes : <ul style="list-style-type: none">- Cache d'objet de données. Met en cache des objets de données logiques et des tables virtuelles.- Entrepôt de profilage. Stocke les informations de profilage, telles que les résultats de profils et de fiches d'évaluation.- Base de données de flux de travail. Stocke les métadonnées d'exécution des flux de travail.
Programme d'installation	Vous pouvez créer le service d'intégration de données lorsque vous exécutez le programme d'installation.

Règles et instructions

Tenez compte des règles et directives suivantes pour la création d'un service d'intégration de données :

Si vous prévoyez d'utiliser des profils de système d'exploitation pour Data Engineering Integration, vous devez créer un service d'intégration de données dédié pour Enterprise Data Catalog. Enterprise Data Catalog ne prend pas en charge les profils de système d'exploitation.

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.

The data object cache database supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- 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

Use the following guidelines when you set up the repository on IBM DB2:

- Verify that the database user account has CREATETAB and CONNECT privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

Configuration requise pour 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 de Microsoft Azure SQL Database

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 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.

The profiling warehouse supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server

- Oracle
- PostgreSQL

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 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

Use the following guidelines when you set up the repository on IBM DB2:

- Le compte d'utilisateur de la base de données doit avoir les privilèges CREATETAB, CONNECT, CREATE VIEW et CREATE FUNCTION.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

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.

Oracle Database Requirements

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.

- Set the following parameters to the Informatica recommended values:

Parameter	Recommended Value
open_cursors	4000
Sessions	1000 You can use the following expression to determine the default session value: $(1.5 * PROCESSES) + 22$ Remarque: If the session value is lower than the default value, the Oracle database uses the default session value.
Processes	1000

Configuration requise pour la base de données de flux de travail

Le service d'intégration de données stocke les métadonnées d'exécution de flux de travail dans la base de données de flux de travail. Avant de créer la base de données de flux de travail, configurez-lui une base de données et un compte utilisateur de base de données.

Vous devez spécifier la connexion à la base de données de flux de travail lorsque vous créez le service d'intégration de données.

The workflow database supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL

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

Use the following guidelines when you set up the repository on IBM DB2:

- Verify that the database user account has CREATETAB and CONNECT privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.
- Définissez les paramètres de pooling de connexions.

Le tableau suivant présente les paramètres de pooling de connexions que vous devez définir :

Paramètre	Valeur
Taille maximale du pool de connexions	128
Taille minimale du pool de connexions	0
Durée maximale d'inactivité	120 secondes

Configuration requise de Microsoft Azure SQL Database

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 DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName 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=[DatabaseName]
```

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

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

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`.
- Définissez les paramètres de pooling de connexions.

Le tableau suivant présente les paramètres de pooling de connexions que vous devez définir :

Paramètre	Valeur
Taille maximale du pool de connexions	128
Taille minimale du pool de connexions	0
Durée maximale d'inactivité	120 secondes

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 TABLE
 - ALTER VIEW
 - CREATE SEQUENCE
 - CREATE SESSION
 - CREATE SYNONYM
 - CREATE TABLE
 - CREATE VIEW
 - DROP TABLE
 - DROP 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.
- Définissez les paramètres de pooling de connexions.

Le tableau suivant présente les paramètres de pooling de connexions que vous devez définir :

Paramètre	Valeur
Taille maximale du pool de connexions	128
Taille minimale du pool de connexions	0
Durée maximale d'inactivité	120 secondes

Configuration requise de la base de données PostgreSQL

Utilisez les directives suivantes lors de la configuration de la base de données sur PostgreSQL :

- Utilisez une connexion JDBC pour vous connecter à la base de données PostgreSQL.
- Vérifiez que le compte utilisateur de la base de données dispose des privilèges CONNECT, CREATE TABLE et CREATE VIEW.
- Spécifiez le nom du schéma de la base de données lorsque vous utilisez PostgreSQL comme base de données.
- Assurez-vous que l'espace disque de PostgreSQL est suffisant pour les fichiers de données. Par défaut, ceux-ci se trouvent à l'emplacement suivant :
<PostgreSQL installation directory>/data
- Dans la base de données, définissez les paramètres de configuration.

Le tableau suivant répertorie les valeurs minimales et recommandées pour les paramètres de configuration :

Paramètre	Valeur minimale	Valeur recommandée
max_connections	200	4000
shared_buffers	2 Go	16 Go
max_locks_per_transaction	1024	1024
max_wal_size	1 Go	8 Go
checkpoint_timeout	5 minutes	30 minutes

Service de cluster Informatica

Le service de cluster Informatica exécute et gère Enterprise Data Catalog et les services associés.

Le tableau suivant récapitule les dépendances pour les produits, services et bases de données associés au service de cluster Informatica :

Dépendance	Résumé
Produits	Les produits suivants utilisent le service de cluster Informatica : <ul style="list-style-type: none"> - Data Privacy Management - Enterprise Data Catalog - Enterprise Data Preparation
Services	Celui-ci doit être associé au service de catalogue.
Bases de données	MongoDB comme magasin de métadonnées.
Programme d'installation	Vous pouvez créer le service de cluster Informatica lorsque vous installez Enterprise Data Catalog.

Service d'accès aux métadonnées

Le service d'accès aux métadonnées est un service d'application qui permet à l'outil Developer tool d'accéder à l'environnement Hadoop pour importer et prévisualiser des métadonnées. Si le domaine utilise une

authentification non-Kerberos, vous pouvez créer et configurer le service d'accès aux métadonnées. Si le domaine utilise l'authentification Kerberos, ne choisissez pas de créer le service d'accès aux métadonnées.

Le tableau suivant récapitule les dépendances des produits, services et bases de données associés au service d'accès aux métadonnées, ainsi que les restrictions du programme d'installation :

Dépendance	Résumé
Produits	Les produits suivants utilisent le service d'accès aux métadonnées : <ul style="list-style-type: none"> - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming - Enterprise Data Catalog - Enterprise Data Preparation
Services	Le service d'accès aux métadonnées ne requiert pas d'association avec un autre service d'application.
Bases de données	Le service d'accès aux métadonnées n'a pas de base de données associée.
Programme d'installation	Vous pouvez créer le service d'accès aux métadonnées lorsque vous exécutez le programme d'installation.

Service de référentiel modèle

Le service de référentiel modèle gère le référentiel modèle. Il reçoit les demandes des clients Informatica et des services d'application pour stocker les métadonnées ou y accéder dans le référentiel modèle.

Le tableau suivant récapitule les dépendances pour les produits, services et bases de données associés au service de référentiel modèle.

Dépendance	Résumé
Produits	Les produits suivants utilisent le service de référentiel modèle : <ul style="list-style-type: none"> - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming - Data Privacy Management - Enterprise Data Catalog - Enterprise Data Preparation - Informatica Data Quality - PowerCenter - Test Data Management
Services	Le service de référentiel modèle ne requiert pas d'association avec un autre service d'application.
Bases de données	Le service de référentiel modèle utilise la base de données suivante : <ul style="list-style-type: none"> - Référentiel modèle. Stocke les métadonnées créées par les clients Informatica et les services d'application.
Programme d'installation	Vous pouvez créer le service de référentiel modèle lorsque vous exécutez le programme d'installation.

Configuration requise pour la base de données du référentiel modèle

Les services et les clients Informatica stockent les données et les métadonnées dans le référentiel modèle. Configurez un référentiel modèle de surveillance afin de stocker des statistiques de tâches ad hoc, les applications, les objets de données logiques, les services de données SQL, les services Web et les flux de travail. Avant de créer le service de référentiel modèle, définissez les bases de données et le compte d'utilisateur pour le référentiel modèle. Il est recommandé d'utiliser une configuration de base de données différente pour le référentiel modèle et le référentiel modèle de surveillance.

The Model repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- PostgreSQL

Lorsque vous configurez Microsoft SQL Server, vous pouvez choisir de configurer Microsoft Azure SQL Database comme référentiel modèle.

Si vous avez spécifié les informations d'identification de Windows NT pour la base de données du référentiel modèle sur Microsoft SQL Server, vous devez également spécifier la syntaxe de la chaîne de connexion pour inclure la méthode d'authentification NTLM.

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 des bases de données, reportez-vous à la documentation de votre système de base de données.

Spécifications de la base de données IBM DB2

Use the following guidelines when you set up the repository on IBM DB2:

- Spécifiez le nom de l'espace de table lorsque vous utilisez IBM DB2 comme base de données de référentiel modèle.
- If the repository is in an IBM DB2 database, verify that IBM DB2 Version 10.5 is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
 - DB2_SKIPINSERTED
 - DB2_EVALUNCOMMITTED
 - DB2_SKIPDELETED
 - AUTO_RUNSTATS
- On the database, set the configuration parameters.

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

Paramètre	Valeur
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.
In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.
In a multi-partition database, specify a non-partitioned tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.
- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.
The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

Configuration requise de Microsoft Azure SQL Database

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 DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName 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=[DatabaseName]
```

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

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

Remarque: Les instructions pour configurer le référentiel pour Azure SQL Database avec authentification Active Directory sont les mêmes.

Configuration requise de 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 DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName 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=[DatabaseName]
```

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

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

Remarque: Les instructions pour configurer les référentiels pour Microsoft Azure SQL Database et Azure SQL Database avec authentification Active Directory sont les mêmes.

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.
- Vous pouvez configurer Oracle Real Application Cluster (RAC) pour spécifier une connexion à un service Oracle activé avec l'équilibrage de charge et la haute disponibilité. Le service de référentiel modèle est résilient au basculement de base de données dans la configuration d'Oracle RAC. Vous ne pouvez pas effectuer d'opérations d'administrateur pour le domaine Informatica et le service de référentiel modèle.

Exigences de la base de données PostgreSQL

Utilisez les directives suivantes lors de la configuration de la base de données sur PostgreSQL :

- Vérifiez que le compte utilisateur de la base de données dispose des privilèges CONNECT, CREATE TABLE et CREATE VIEW.
- Spécifiez le nom du schéma de la base de données lorsque vous utilisez PostgreSQL comme base de données.
- Assurez-vous que l'espace disque de PostgreSQL est suffisant pour les fichiers de données. Par défaut, ceux-ci se trouvent à l'emplacement suivant :

<PostgreSQL installation directory>/data

- Dans la base de données, définissez les paramètres de configuration.

Le tableau suivant répertorie les valeurs minimales et recommandées pour les paramètres de configuration :

Paramètre	Valeur minimale	Valeur recommandée
max_connections	200	4000
shared_buffers	2 Go	16 Go
max_locks_per_transaction	1024	1024
max_wal_size	1 Go	8 Go
checkpoint_timeout	5 minutes	30 minutes

Service de référentiel modèle de surveillance

Le service de référentiel modèle de surveillance est un service de référentiel modèle qui surveille les statistiques pour les tâches relatives au service d'intégration de données. La configuration du service de référentiel modèle de surveillance s'effectue dans les propriétés du domaine.

Remarque: Si vous souhaitez générer des statistiques de surveillance, vous devez créer un service de référentiel modèle dédié à la surveillance. Vous ne pouvez pas stocker les statistiques de surveillance d'exécution dans le même référentiel que celui dans lequel vous stockez des métadonnées d'objet.

Le tableau suivant récapitule les dépendances pour les produits, services et bases de données associés au service de référentiel modèle de surveillance :

Dépendance	Résumé
Produits	Les produits suivants utilisent le service de référentiel modèle de surveillance : <ul style="list-style-type: none">- Data Engineering Integration- Data Engineering Quality- Data Engineering Streaming- Data Privacy Management- Enterprise Data Catalog- Enterprise Data Preparation- Informatica Data Quality- PowerCenter- Test Data Management
Services	Le service de référentiel modèle de surveillance ne nécessite aucune association avec un autre service d'application.
Bases de données	Le service de référentiel modèle de surveillance utilise la base de données suivante : <ul style="list-style-type: none">- Référentiel modèle. Stocke les statistiques de surveillance d'exécution, que vous pouvez afficher dans l'outil Administrator tool.
Programme d'installation	Vous pouvez créer le service de référentiel modèle de surveillance lorsque vous exécutez le programme d'installation.

Service de recherche

Le service de recherche gère les recherches dans l'outil Analyst et retourne les résultats de la recherche à partir du référentiel modèle. Lorsque vous créez le service, vous devez lui associer un autre service d'application.

Le tableau suivant récapitule les dépendances pour les produits, services et bases de données associés au service de recherche :

Dépendance	Résumé
Produits	Les produits suivants utilisent le service de recherche : <ul style="list-style-type: none">- Data Engineering Integration- Data Engineering Quality- Data Engineering Streaming- Enterprise Data Catalog- Enterprise Data Preparation- Informatica Data Quality- PowerCenter
Services	Le service de recherche nécessite une association directe avec le service suivant : <ul style="list-style-type: none">- Service de référentiel modèle
Bases de données	Le service de recherche n'est associé à aucune base de données.
Programme d'installation	Vous ne pouvez pas créer le service de recherche lorsque vous exécutez le programme d'installation.

Configuration de la connectivité native sur les machines du service

Pour établir la connectivité native entre un service d'application et une base de données, installez le logiciel client de base de données pour la base de données à laquelle vous voulez accéder.

Les pilotes natifs sont emballés avec le serveur de base de données et le logiciel client. Configurez la connectivité sur les machines qui doivent accéder aux bases de données. Pour assurer la compatibilité entre le service d'application et la base de données, utilisez les bibliothèques clients de la base de données appropriées et installez un logiciel client qui est compatible avec la version de la base de données.

Le service d'intégration de données utilise les pilotes de base de données natifs pour se connecter aux bases de données suivantes :

- Bases de données source et cible. Lit les données de bases de données source et écrit des données dans des bases de données cible.
- Base de données du cache d'objet de données. Stocke le cache d'objet de données.
- Bases de données de profilage source. Lit les données de bases de données relationnelles source pour exécuter des profils sur les sources.
- Entrepôt de profilage. Écrit les résultats du profilage dans l'entrepôt de profilage.
- Tables de référence. Exécute les mappages pour transférer les données entre les tables de référence et les sources de données externes.

Lorsque le service d'intégration de données s'exécute sur un seul nœud ou sur les nœuds principal et de sauvegarde, installez le logiciel client de base de données et configurez la connectivité sur les machines où le service d'intégration de données s'exécute.

Lorsque le service d'intégration de données s'exécute sur une grille, installez le logiciel client de base de données et configurez la connectivité sur chaque machine qui représente un nœud doté du rôle de calcul ou un nœud doté des rôles de service et de calcul.

Installer le logiciel client de base de données

Vous devez installer les clients de bases de données sur les machine requises en fonction des types de bases de données accessibles aux services d'application.

Pour assurer la compatibilité entre le service d'application et la base de données, utilisez les bibliothèques de client de base de données appropriées et installez un logiciel client qui est compatible avec la version de la base de données.

Installez le logiciel client de base de données suivant selon le type de base de données accessible au service d'application :

IBM DB2 Client Application Enabler (CAE)

Configurez la connectivité sur les machines requises en vous connectant à la machine en tant qu'utilisateur démarrant les services Informatica.

Microsoft SQL Server 2014 Native Client

Téléchargez le client à partir du site Web Microsoft suivant :
<http://www.microsoft.com/en-in/download/details.aspx?id=42295>.

Client Oracle

Installez des versions compatibles du client Oracle et serveur de base de données Oracle. Vous devez aussi installer la même version du client Oracle sur toutes les machines qui le requièrent. Pour vérifier la compatibilité, contactez Oracle.

Sybase Open Client (OCS)

Installez une version d'Open Client compatible avec le serveur de base de données Sybase ASE. Vous devez aussi installer la même version d'Open Client sur les machines hébergeant la base de données Sybase ASE et Informatica. Pour vérifier la compatibilité, contactez Sybase.

Configurer les variables d'environnement client de la base de données

Configurez les variables d'environnement client de la base de données sur les machines qui exécutent les processus de service d'intégration de données.

Quand vous avez configuré les variables d'environnement de la base de données, vous pouvez tester la connexion à la base de données à partir du client de base de données.

Base de données Oracle

Le tableau suivant répertorie les variables d'environnement de base de données que vous devez définir pour la base de données Oracle avec `sqlplus` comme utilitaire de base de données :

Variable d'environnement	Valeur
ORACLE_HOME	<Client InstallDatabasePath>
PATH	<DatabasePath>/bin et USER_INSTALL_DIR/server/bin:\$PATH
LD_LIBRARY_PATH	\$Oracle_HOME/lib et USER_INSTALL_DIR/server/bin:\$LD_LIBRARY_PATH
TNS_ADMIN	Définissez cette valeur sur l'emplacement du fichier tnsnames.ora : \$ORACLE_HOME/network/admin
INFA_TRUSTSTORE	Pour le domaine SSL par défaut, ajoutez la valeur à USER_INSTALL_DIR/services/shared/security Pour le domaine SSL personnalisé, définissez INFA_TRUSTSTORE et INFA_TRUSTSTORE_PASSWORD

Base de données IBM DB2

Le tableau suivant répertorie les variables d'environnement de base de données que vous devez définir pour la base de données IBM DB2 avec `db2connect` comme utilitaire de base de données :

Variable d'environnement	Valeur
DB2DIR	<database path>
DB2INSTANCE	<DB2InstanceName>
PATH	<database path>/bin

Base de données Sybase ASE

Le tableau suivant répertorie les variables d'environnement de base de données que vous devez définir pour la base de données Sybase ASE avec `isql` comme utilitaire de base de données :

Variable d'environnement	Valeur
SYBASE15	<<database path>/sybase<version> >
SYBASE_ASE	\${SYBASE15}/ASE-<version>
SYBASE_OCS	\${SYBASE15}/OCS-<version>
PATH	\${SYBASE_ASE}/bin:\${SYBASE_OCS}/bin:\$PATH

Base de données PostgreSQL

Le tableau suivant répertorie les variables d'environnement de base de données que vous devez définir pour la base de données PostgreSQL :

Variable d'environnement	Valeur
PGSERVICEFILE	Définissez cette valeur sur l'emplacement du fichier pg_service.conf : <i><pg_service.conf file directory>/pg_service.conf</i>
PGHOME	<i>/usr/pgsql-10</i>
PATH	<i>\$PGHOME:\${PATH}</i>
LD_LIBRARY_PATH	<i>\$PGHOME/lib:\${LD_LIBRARY_PATH}</i>
INFA_TRUSTSTORE	Pour le domaine SSL par défaut, ajoutez cette valeur à <i><InstallationDirectory>/services/shared/security</i> Pour le domaine SSL personnalisé, définissez INFA_TRUSTSTORE et INFA_TRUSTSTORE_PASSWORD
POSTGRES_ODBC	Définissez cette valeur sur 1 pour la connexion PostgreSQL ODBC. Vous pouvez la définir pour tous les référentiels du domaine ou pour tout référentiel PostgreSQL utilisant une connexion ODBC.

Base de données Microsoft SQL Server

Le tableau suivant répertorie les variables d'environnement de base de données que vous devez définir pour la base de données Microsoft SQL Server :

Variable d'environnement	Valeur
ODBCHOME	<i>USER_INSTALL_DIR/ODBC7.1</i>
ODBCINI	<i>\$ODBCHOME/odbc.ini</i>
ODBCINST	<i>\$ODBCHOME/odbcinst.ini</i>
PATH	<i>/opt/mssql-tools/bin:\$PATH\$PATHUSER_INSTALL_DIR/ODBC7.1:\$PATHUSER_INSTALL_DIR/server/bin:\$PATH</i>
LD_LIBRARY_PATH	<i>\$ODBCHOME/lib</i>
INFA_TRUSTSTORE	<i>USER_INSTALL_DIR/server/bin:\$LD_LIBRARY_PATH</i> Pour le domaine SSL par défaut, ajoutez la valeur à <i>USER_INSTALL_DIR/services/shared/security</i> Pour le domaine SSL personnalisé, définissez INFA_TRUSTSTORE et INFA_TRUSTSTORE_PASSWORD

CHAPITRE 4

Préparer le déploiement d'Enterprise Data Catalog

Ce chapitre comprend les rubriques suivantes :

- [Liste de contrôle pour préparer le déploiement d'Enterprise Data Catalog, 66](#)
- [Planification du déploiement, 67](#)
- [Service de cluster Informatica et services associés, 67](#)
- [Prérequis courants du système d'exploitation, 67](#)
- [Prérequis du système d'exploitation pour Red Hat Enterprise Linux, 72](#)
- [Prérequis du système d'exploitation pour SUSE Linux Enterprise Server , 72](#)
- [Prérequis du nœud, 73](#)

Liste de contrôle pour préparer le déploiement d'Enterprise Data Catalog

Vous pouvez déployer Enterprise Data Catalog sur un seul nœud de données ou sinon sur trois ou six nœuds de données dans un cluster.

Ce chapitre contient les tâches que vous devez effectuer avant de déployer Enterprise Data Catalog.

Effectuez les tâches suivantes :

- ☐ Comprendre le déploiement d'Enterprise Data Catalog et le service de cluster Informatica qui exécute et gère Enterprise Data Catalog.
- ☐ Comprendre les services associés au service de cluster Informatica.
- ☐ Effectuez les tâches prérequis et préparez l'environnement.

Planification du déploiement

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

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

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

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

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

Service de cluster Informatica et services associés

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

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

Prérequis courants du système d'exploitation

Vous pouvez installer Enterprise Data Catalog sur une machine qui s'exécute sur Red Hat Enterprise Linux Server ou sur SUSE Linux Enterprise Server. Les prérequis de cette section sont communs à Red Hat Enterprise Linux et à SUSE Linux Enterprise Server.

Prérequis de configuration du système d'exploitation

Veillez à vérifier les prérequis suivants du système d'exploitation :

- Vérifiez que Bash est le shell par défaut.
- Vérifiez que ntpd ou chronyd est synchronisé entre le nœud de domaine Informatica et les nœuds de cluster.
- Vérifiez que le référentiel de base Linux est configuré et fonctionnel.
- Définissez la limite souple et la limite stricte pour le nombre maximal de processus utilisateur et de descripteurs de fichiers sur au moins 65 000 pour les machines sur lesquelles vous prévoyez d'héberger le domaine Informatica.
- Définissez la limite souple et la limite stricte pour le descripteur de fichier ouvert sur au moins 65 000 pour les machines sur lesquelles vous déployez le service de cluster Informatica.
- Définissez UMASK sur 022 (0022).
- Définissez la valeur du paramètre MaxStartups dans le fichier de configuration du serveur SSH sur 30:30:100.

Prérequis d'applications et d'utilitaires

Vérifiez que les applications et les utilitaires suivants sont installés :

- JDK 1.8
- Shell Bash
- xz-libs
- systemctl
- rsync
- netstat
- YUM
- Zypper
- scp
- curl
- rpm
- zip
- unzip
- tar
- wget
- libcurl
- nslookup
- md5sum
- ping
- ifconfig
- cksum
- dnsdomainname

- OpenSSL version 1.0.1e-30.el6_6.5.x86_64 ou versions ultérieures.

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

Si la machine sur laquelle le service PostgreSQL s'exécute est compatible FIPS, vérifiez que `compat-openssl10` est installé.

Prérequis de répertoires

Configurez les prérequis de répertoires suivants :

Répertoire racine (/)

Le répertoire racine (/) doit disposer d'au moins 10 Go d'espace disque libre. Si vous prévoyez de créer le répertoire de données pour le service de cluster Informatica dans le répertoire racine, vérifiez que celui-ci dispose d'au moins 50 Go d'espace disque disponible supplémentaire. Pour configurer un répertoire distinct pour les fichiers journaux du service de cluster Informatica, vérifiez que le répertoire dispose d'au moins 50 Go d'espace disque libre.

Si vous configurez le répertoire `workingDir` sur /, confirmez que le système de fichiers monté dans les répertoires `/tmp` et `/var` dispose de l'indicateur `EXEC` défini.

Si `workingDir` n'est pas configuré sur /, confirmez si le répertoire `workingDir` dispose des autorisations `read`, `write` et `execute` configurées. Confirmez que l'indicateur `EXEC` est défini pour le répertoire.

Les autorisations de lecture, d'écriture et d'exécution ne doivent pas être configurées dans le répertoire.

Répertoire /var

Le répertoire ne doit pas disposer de l'autorisation d'écriture pour tous.

Le répertoire doit disposer d'au moins 2 Go d'espace disque libre.

Les autorisations de lecture, d'écriture et d'exécution ne doivent pas être configurées dans le répertoire.

Répertoire /tmp

Les autorisations de lecture, d'écriture et d'exécution doivent être configurées dans le répertoire.

Répertoire /usr

Le répertoire doit disposer d'au moins 2 Go d'espace disque libre.

Répertoire personnalisé

Vérifiez qu'au moins 60 Go d'espace disque libre est disponible dans tout répertoire personnalisé que vous prévoyez de configurer.

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

Prérequis de DNS

Vérifiez les prérequis de DNS suivants dans le fichier `/etc/hosts` pour tous les nœuds du cluster :

- Une entrée pour l'adresse de bouclage `127.0.0.1 localhost localhost.domain.com` dans le fichier.
- Chaque machine du cluster inclut l'entrée `127.0.0.1 localhost localhost.localdomain` dans le fichier.
- Le fichier comprend 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.

Prérequis de comptes utilisateur

Vérifiez les prérequis suivants pour tous les comptes utilisateur :

- Créez un compte d'utilisateur sans privilèges racine et assurez-vous que l'utilisateur dispose des privilèges sudo.

Remarque: Les services associés au service de cluster Informatica tels qu'Apache Solr, PostgreSQL et Nomad nécessitent un utilisateur non racine disposant de privilèges sudo pour exécuter les services. Sudo permet à un utilisateur d'exécuter des programmes ou des commandes avec des privilèges élevés pendant une période spécifique. Enterprise Data Catalog nécessite un utilisateur non-racine avec des autorisations sudo pour exécuter certaines commandes lors de l'exécution de tâches administratives telles que l'installation, la mise à niveau et la surveillance du statut des services.

- Mettez à jour le fichier sudoers. Certaines commandes nécessitent des privilèges sudo pour l'utilisateur de la passerelle lorsque vous activez le service de cluster Informatica pour la première fois. Assurez-vous que l'utilisateur dispose des privilèges sudo pour les commandes `mkdir`, `chown`, `chmod`, `echo`, `systemctl`, `cp`, `mv`, `sysctl`, `rm`, `sshd`.

Remarque: Vous devez configurer les autorisations sudo pour les commandes si vous prévoyez de modifier les propriétés du service de cluster Informatica ou de remplacer les certificats SSL configurés pour le service de cluster Informatica.

Pour configurer les privilèges sudo pour les commandes, vous devez ajouter les commandes au fichier `/etc/sudoers`, comme illustré dans l'exemple suivant : `%<Gateway user name> ALL = (ALL) NOPASSWD: /bin/mkdir, /bin/chown, /bin/chmod, /bin/echo, /bin/systemctl, /bin/cp, /bin/mv, /usr/sbin/sysctl, /bin/rm, /usr/sbin/sshd`.

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

- Ajoutez les entrées suivantes dans le fichier `/etc/security/limits.d/20-nproc.conf` pour l'utilisateur racine :
 - `soft nproc 65000`
 - `hard nproc 65000`
 - `soft nofile 65000`
 - `hard nofile 65000`
- Ajoutez les entrées suivantes dans le fichier `/etc/security/limits.d/20-nproc.conf` pour l'utilisateur non-racine :
 - `<non root user name> soft nproc 65000`
 - `<non root user name> hard nproc 65000`
 - `<non root user name> soft nofile 65000`
 - `<non root user name> hard nofile 65000`
- Pour le compte d'utilisateur non-racine disposant des privilèges sudo que vous utilisez pour installer Enterprise Data Catalog, configurez les valeurs ulimit suivantes :
 - f (taille du fichier) : illimitée
 - t (temps CPU) : illimité
 - v (mémoire virtuelle) : illimitée
 - l (taille de la mémoire verrouillée) : illimitée
 - n (fichiers ouverts) : 64 000
 - m (taille de la mémoire) : illimitée

-u (processus/threads) : 64 000

- Désactivez l'invite de mot de passe de l'hôte de domaine vers l'hôte de passerelle de cluster et de ce dernier vers tous les nœuds de l'agent.
- Vérifiez que l'utilisateur de la passerelle dispose des privilèges requis pour exécuter la commande ping.
- Désactivez l'invite de mot de passe pour l'utilisateur de la passerelle.
- Si vous utilisez un compte d'utilisateur sans privilèges racine et que vous voulez supprimer l'accès à la commande sudo, commentez `defaults requiretty` dans le fichier `/etc/sudoers`.
- Désactivez la journalisation des E/S sudoers. Commentez `Defaults log_input, log_output` dans le fichier `/etc/sudoers`.

Prérequis des ports

Vérifiez que les ports suivants sont disponibles :

Service	Port par défaut
HTTP/HTTPS	9075
Serf Nomad	4648
HTTP Nomad	4646
RPC Nomad	4647
ZooKeeper	2181
Homologue ZooKeeper	2888
Leader ZooKeeper	3888
Solr	8983
MongoDB n'est pas configuré comme membre de partition ou serveur de configuration.	27017
MongoDB est configuré comme membre de partition.	27018
MongoDB est configuré comme serveur de configuration.	27019
PostgreSQL	5432

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 :

Système d'exploitation	Prérequis
Red Hat Enterprise Linux	<ul style="list-style-type: none">- Sudo version 1.8.16 ou versions ultérieures.- Installez openssl version v1.0.1 build 16 ou versions ultérieures ou v1.0.2k.- Vérifiez que le répertoire <code>/etc/sysconfig/network</code> existe et configurez l'autorisation de lecture pour celui-ci.- Vérifiez que <code>/etc/sysconfig/network</code> comprend la même entrée que celle configurée pour le nom d'hôte -f.- Pour RHEL 6.x, installez <code>lsb_release</code>.- Pour RHEL 8.x, installez <code>ncurses-c++-libs</code> et <code>ncurses-compat-libs</code>.- Pour RHEL 8.3, installez <code>libidn.so.11</code>.

Pour plus d'informations, reportez-vous à la matrice de disponibilité des produits Informatica 10.5.6.

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	<ul style="list-style-type: none">- Installez <code>netcat-openbsd</code>.- Vérifiez 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> comprend la même entrée que celle configurée pour le nom d'hôte -f.- Installez les RPM Package Manager suivants sur tous les nœuds du cluster :<ul style="list-style-type: none">- <code>openssl-1.0.1c-2.1.3.x86_64.rpm</code>- <code>libopenssl1_0-1.0.1c-2.1.3.x86_64.rpm</code>- <code>libopenssl1_0-32bit-1.0.1c-2.1.3.x86_64.rpm</code>- Installez <code>libncurses5</code>.Remarque: L'utilitaire de pré-validation ne valide pas ce prérequis.- N'installez pas <code>libsnap</code> si vous installez Enterprise Data Catalog sur SUSE Linux Enterprise Server.

Pour plus d'informations, reportez-vous à la matrice de disponibilité des produits Informatica 10.5.6.

Prérequis du nœud

Avant de déployer Enterprise Data Catalog, vérifiez les prérequis pour les nœuds hôtes et les nœuds de cluster.

- Désactivez le pare-feu sur chaque hôte du cluster.
- Activez SSH sans mot de passe entre les nœuds suivants :
 - Nœud qui héberge le domaine Informatica et le nœud qui héberge la passerelle.
 - Nœud de passerelle et tous les nœuds de données et les nœuds de traitement.
 - Nœuds de sauvegarde et nœud de passerelle.
 - Tous les nœuds du cluster et les nœuds de données.
- Vérifiez que les nœuds de cluster répondent à la configuration minimale requise suivante par nœud :

Configuration requise	Valeur
Processeur	4
Mémoire inutilisée	12 Go
Mémoire totale	16 Go
Espace disque	60 Go

CHAPITRE 5

Enregistrer des informations pour les invites du programme d'installation

Ce chapitre comprend les rubriques suivantes :

- [Liste de contrôle pour enregistrer les invites du programme d'installation, 74](#)
- [Enregistrer des informations pour les invites du programme d'installation - Présentation, 75](#)
- [Domaine, 76](#)
- [Nœuds, 77](#)
- [Packages de distribution, 77](#)
- [Services d'application, 77](#)
- [Bases de données , 78](#)
- [Chaîne de connexion à une base de données sécurisée, 80](#)
- [Configuration de cluster, 82](#)
- [Stockage des données sécurisé, 84](#)

Liste de contrôle pour enregistrer les invites du programme d'installation

Ce chapitre présente les informations que vous devez entrer lorsque vous exécutez le programme d'installation. Utilisez cette liste de contrôle pour le suivi des tâches d'enregistrement avant l'exécution du programme d'installation.

- ☐ Enregistrez les noms des nœuds que vous souhaitez créer et les services que vous souhaitez créer sur chaque nœud.
- ☐ Enregistrez les informations de base sur chaque base de données associée à un service que vous créez.
- ☐ Si les bases de données de configuration du domaine et du référentiel modèle sont sécurisées, enregistrez la chaîne de connexion JDBC avec les paramètres de sécurité requis.
- ☐ Enregistrez la clé de site pour le programme d'installation.

- ☐ Si vous souhaitez activer l'authentification Kerberos lors de l'exécution du programme d'installation, enregistrez les informations Kerberos pour chaque nœud du domaine.
- ☐ Consignez les informations du cluster.

Enregistrer des informations pour les invites du programme d'installation - Présentation

Lorsque vous installez les services Informatica, vous devez connaître les informations sur le domaine, les nœuds, les services d'application, les bases de données et les packages de distribution pour l'environnement.

Cette section répertorie les informations que vous devez fournir lors de l'exécution du programme d'installation. Informatica recommande d'enregistrer les invites du programme d'installation avant de démarrer le processus d'installation. Par exemple, il est conseillé de créer un fichier texte regroupant les informations afin de pouvoir les copier dans le programme d'installation.

Conventions de dénomination d'objets de domaine

Vous ne pouvez pas modifier les noms de domaine, de nœud et de service d'application. 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 des noms qui expriment la manière dont l'objet de domaine est utilisé. Les conventions de nommage sont fournies dans les rubriques applicables.

Domaine

Lorsque vous créez un domaine, vous devez fournir un nom de domaine et un nom de nœud de passerelle.

Le tableau suivant décrit les informations de domaine que vous devez entrer pendant le processus d'installation :

Informations de domaine	Description
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 : ` % * + ; " ? , < > \ / Le nom doit respecter l'une des conventions de dénomination suivantes : DMN, DOM, DOMAIN, _<ORG>_<ENV>
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. Respectez la convention de dénomination suivante : Noeud<noeud##>_<ORG>_<signe distinctif facultatif>_<ENV>

Nœuds

Lorsque vous installez les services Informatica, vous ajoutez la machine d'installation dans le domaine en tant que nœud. Vous pouvez ajouter plusieurs nœuds à un domaine.

Le tableau suivant décrit les informations sur les nœuds que vous devez entrer lorsque vous joignez un domaine.

Informations sur les nœuds	Description
Nom d'hôte du nœud	Nom d'hôte complet de la machine sur laquelle créer des nœuds. 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 des nœuds que vous prévoyez de créer sur cette machine. Le nom du nœud n'est pas le nom d'hôte de la machine. Respectez la convention de dénomination suivante : Noeud<noeud##>_<ORG>_<signe distinctif facultatif>_<ENV>

Packages de distribution

Si vous prévoyez d'installer un package de distribution via le programme d'installation, enregistrez le package de distribution que vous avez téléchargé.

Services d'application

Enregistrez les noms des services d'application et les nœuds sur lesquels vous souhaitez les créer.

Le tableau suivant répertorie les services d'application que vous pouvez créer lorsque vous exécutez le programme d'installation :

Service d'application	Convention de dénomination
Service de catalogue	CS_<ORG>_<ENV>
Gestion du contenu	CMS_<ORG>_<ENV>
Service d'intégration de données	DIS_<ORG>_<ENV>
Service Data Privacy Management	DPM_<ORG>_<ENV>
Service de préparation de données interactive	DPS_<ORG>_<ENV>

Service d'application	Convention de dénomination
Service Enterprise Data Preparation	EDLS_<ORG>_<ENV>
Service d'accès aux métadonnées	MAS_<ORG>_<ENV>
Service de cluster Informatica	ICS_<ORG>_<ENV>
Service de référentiel modèle	MRS_<ORG>_<ENV>
Service de référentiel modèle de surveillance	mMRS_<ORG>_<ENV>
Service de référentiel PowerCenter	PCRS, RS _<ORG>_<ENV>
Service d'intégration PowerCenter	PCIS, IS _<ORG>_<ENV>

Pour plus d'informations sur les conventions de dénomination de services, consultez l'article Meilleures pratiques d'Informatica Velocity disponible sur le réseau Informatica : [Velocity Naming Conventions](#)

Bases de données

Lorsque vous planifiez l'installation, vous devez également planifier les bases de données relationnelles requises. Le domaine requiert une base de données pour stocker les informations de configuration ainsi que les privilèges et les autorisations des comptes utilisateur. Certains services d'application requièrent des bases de données pour stocker les informations traitées par le service d'application.

Domaine

Le tableau suivant décrit les informations que vous devez entrer pendant le processus d'installation :

Informations de la base de données	Description
Type de base de données de configuration du domaine	Type de base de données pour le référentiel de configuration du domaine. The domain configuration repository supports IBM DB2 UDB, Microsoft SQL Server, Oracle, PostgreSQL, or Sybase ASE.
Nom d'hôte de la base de données de configuration du domaine	Nom de la machine qui héberge la base de données.

Service de gestion de contenu

Le tableau suivant décrit les informations que vous devez entrer pendant le processus d'installation :

Informations de la base de données	Description
Type de base de données de l'entrepôt de données de référence	Type de base de données pour l'entrepôt de données de référence. The reference data warehouse supports IBM DB2 UDB, Microsoft Azure SQL Database, Microsoft SQL Server, Oracle, or PostgreSQL.
Nom d'hôte de la base de données pour l'entrepôt de données de référence	Nom de la machine qui héberge la base de données.

Service d'intégration de données

Le tableau suivant décrit les informations que vous devez entrer pendant le processus d'installation :

Informations de la base de données	Description
Type de base de données de cache d'objet de données	Type de base de données pour la base de données de cache d'objet de données. The data object cache database supports IBM DB2 UDB, Microsoft SQL Server, or Oracle.
Nom d'hôte de la base de données pour le cache d'objet de données	Nom de la machine qui héberge la base de données.
Type de base de données d'entrepôt de profilage	Type de base de données pour l'entrepôt de profilage. The profiling warehouse supports IBM DB2 UDB, Microsoft SQL Server, Oracle, or PostgreSQL.
Nom d'hôte de la base de données de l'entrepôt de profilage	Nom de la machine qui héberge la base de données.
Type de base de données de flux de travail	Type de la base de données de flux de travail. The workflow database supports IBM DB2 UDB, Microsoft Azure SQL Database, Microsoft SQL Server, Oracle, or PostgreSQL.
Nom d'hôte de base de données de flux de travail	Nom de la machine qui héberge la base de données.

Service de référentiel modèle

Le tableau suivant décrit les informations que vous devez entrer pendant le processus d'installation :

Informations de la base de données	Description
Type de base de données du référentiel modèle	Type de base de données pour le référentiel modèle. The Model repository supports IBM DB2 UDB, Microsoft SQL Server, PostgreSQL, or Oracle.
Nom d'hôte de la base de données du référentiel modèle	Nom de la machine qui héberge la base de données.

Service de catalogue

Si vous prévoyez d'activer l'analyse des actifs de données pour Enterprise Data Catalog, vérifiez que les informations du tableau suivant sont disponibles :

Informations de la base de données	Description
Type de base de données de référentiel	Type de base de données pour le référentiel de l'analyse des actifs de données. Vous pouvez sélectionner une base de données Oracle, SQLServer ou PostgreSQL.
Nom d'utilisateur de la base de données	Nom d'utilisateur pour accéder à la base de données.
Mot de passe de la base de données	Mot de passe pour accéder à la base de données.

MetaDex

Si vous prévoyez d'utiliser MetaDex, vous devez fournir des informations sur le référentiel. Le tableau suivant décrit les informations de la base de données du référentiel MetaDex que vous devez entrer pendant le processus d'installation :

Informations de la base de données	Description
Type de base de données de référentiel	Type de base de données pour le référentiel MetaDex. Vous pouvez sélectionner une base de données Oracle, Microsoft SQL Server ou PostgreSQL.
Nom d'utilisateur de la base de données	Nom d'utilisateur pour accéder à la base de données.
Mot de passe de la base de données	Mot de passe pour accéder à la base de données.
Nom du schéma	Schéma à utiliser.
Chemin d'accès au fichier truststore de la base de données	S'applique si vous avez spécifié que la base de données est activée pour SSL. Fournissez le chemin d'accès complet au fichier truststore.
Mot de passe du truststore	Mot de passe utilisé pour accéder au fichier truststore.

Chaîne de connexion à une base de données sécurisée

Si vous créez un référentiel dans une base de données sécurisée, vous devez fournir les informations de truststore et une chaîne de connexion JDBC qui comprend les paramètres de sécurité de la base de données.

Lors de l'installation, vous pouvez créer le référentiel de configuration du domaine dans une base de données sécurisée. Vous pouvez également créer le référentiel modèle et le référentiel PowerCenter dans une base de données sécurisée.

Vous pouvez configurer une connexion sécurisée aux bases de données suivantes :

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- PostgreSQL
- Azure PostgreSQL
- Oracle

Remarque: Vous ne pouvez pas configurer une connexion sécurisée à une base de données Sybase.

Lorsque vous configurez la connexion à la base de données sécurisée, vous devez indiquer les informations de connexion dans une chaîne de connexion JDBC. Outre le nom d'hôte et le numéro de port du serveur de base de données, la chaîne de connexion doit inclure les paramètres de sécurité.

Le tableau suivant décrit les paramètres de sécurité que vous devez inclure dans la chaîne de connexion JDBC :

Paramètre	Description
EncryptionMethod	Requis. Indique si les données sont chiffrées 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. Si le cryptage et la validation SSL sont activés et que cette propriété n'est pas spécifiée, le pilote utilise le nom de serveur spécifié dans l'URL de connexion ou dans la source de données de la connexion pour valider le certificat.
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.

Vous pouvez utiliser la syntaxe suivante dans la chaîne de connexion JDBC pour la connexion à une base de données sécurisée :

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

Utilisez la chaîne de connexion suivante pour vous connecter à la base de données Oracle via le gestionnaire de connexions Oracle :

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS server name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

Microsoft SQL Server avec les informations d'identification de Windows NT

Si vous avez spécifié les informations d'identification de Windows NT pour la base de données du référentiel modèle sur Microsoft SQL Server, spécifiez la syntaxe de la chaîne de connexion pour inclure la méthode d'authentification NTLM.

Microsoft SQL Server qui utilise l'instance par défaut avec les informations d'identification de Windows NT :

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server qui utilise l'instance nommée avec les informations d'identification de Windows NT :

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

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.

Configuration de cluster

Vous pouvez importer des propriétés de configuration à partir du cluster non natif pour créer une configuration de cluster. La configuration de cluster permet au service d'intégration de données de transmettre les travaux à l'environnement non natif.

Vous pouvez importer les propriétés à partir d'un fichier d'archive créé par l'administrateur Hadoop, ou vous pouvez les importer directement à partir du cluster. Lorsque vous créez la configuration de cluster, vous pouvez également choisir de créer des connexions Hadoop, Hive, HBase, HDFS ou Databricks associées au cluster. Le programme d'installation ajoute le type de connexion au nom de configuration du cluster pour créer chaque nom de connexion.

Le tableau suivant décrit les informations initiales que vous devez entrer lors du processus d'installation :

Informations sur le cluster	Description
Nom de configuration de cluster	Nom de la configuration de cluster à créer.
Type de distribution	Type de distribution de cluster non native.
Méthode d'importation de la configuration du cluster	Méthode d'importation de la configuration de cluster. Vous pouvez choisir d'importer la configuration du cluster à partir d'un fichier d'archive ou du cluster.

Importer la configuration de cluster à partir d'un fichier d'archive

Pour importer les propriétés de la configuration de cluster à partir d'un fichier d'archive, spécifiez le chemin du fichier d'archive de configuration.

Importer la configuration de cluster à partir de ce dernier

Le tableau suivant décrit les propriétés du cluster pour Cloudera, Hortonworks ou Azure HDInsight que vous devez entrer lors de l'importation depuis le cluster pendant le processus d'installation :

Propriété	Description
Hôte	Le nom d'hôte ou l'adresse IP du gestionnaire de cluster.
Port	Port du gestionnaire de cluster.
ID d'utilisateur	Nom d'utilisateur du cluster.
Mot de passe	Mot de passe de l'utilisateur du cluster.
Nom du cluster	Nom du cluster. Utilisez le nom complet si le gestionnaire de cluster gère plusieurs clusters. Si vous ne spécifiez pas de nom de cluster, l'assistant importe des informations en fonction du cluster par défaut.
Type de moteur	Pour un cluster Cloudera, le programme d'installation vous demande le type de moteur. Si vous vous trouvez sur un cluster CDP, acceptez le type de moteur par défaut de Tez. Si vous vous trouvez sur un cluster CDH, définissez le type de moteur sur MRv2.

Le tableau suivant décrit les propriétés du cluster pour Databricks que vous devez entrer lors du processus d'installation :

Propriété	Description
Domaine Databricks	URL du cluster Databricks.
ID de jeton Databricks	ID de jeton du cluster Databricks.
Cluster Databricks ID	ID du cluster Databricks.

Stockage des données sécurisé

Lorsque vous installez les services Informatica, vous devez sauvegarder la clé de site que le programme d'installation génère et vous assurer que vous enregistrez la clé de site. En cas de perte de la clé de site, vous ne pouvez plus la régénérer.

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

Propriété	Description
Répertoire de la clé de chiffrement	Répertoire dans lequel stocker la clé de chiffrement pour le domaine. Par défaut, la clé de chiffrement est créée dans le répertoire suivant : <code><Informatica installation directory>/isp/config/keys</code> .
Spécifiez si vous souhaitez sauvegarder ou non la clé de site générée par le programme d'installation :	<p>Spécifiez si vous souhaitez sauvegarder ou non la clé de site générée par le programme d'installation :</p> <ul style="list-style-type: none"> - Sélectionnez 1 pour Non. Si vous choisissez Non, le programme d'installation ferme. - Sélectionnez 2 pour Oui. Si vous choisissez Oui, vous acceptez de sauvegarder le fichier manuellement. <p>Une clé de site unique est générée. En cas de perte de la clé de site, vous ne pouvez plus la régénérer. Veillez à enregistrer une copie de cette clé et de ne pas partager la clé de site unique avec d'autres.</p>

CHAPITRE 6

Configurer les certificats SSL personnalisés

Ce chapitre comprend les rubriques suivantes :

- [Configurer les certificats SSL personnalisésPrésentation, 85](#)
- [Générer des certificats SSL personnalisés signés par une autorité de certification \(CA\), 86](#)
- [Générer des certificats SSL personnalisés auto-signés, 91](#)

Configurer les certificats SSL personnalisésPrésentation

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

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

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

Exigences d'activation des certificats SSL personnalisés

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

Vérifiez les prérequis suivants pour le domaine Informatica :

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

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

Pour savoir comment convertir un domaine Informatica non-SSL en un domaine Informatica compatible SSL, reportez-vous à l'article de la base de connaissances [Convert a non-SSL Informatica domain to an SSL-enabled Informatica domain](#).

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

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

Utilisez les scripts `generate_csr.sh` et `generate_certs.sh` pour générer la demande de signature de certificat (CSR, Certificate Signing Request) à envoyer à une autorité de certification (CA) et générer les certificats SSL requis. Vous pouvez télécharger les scripts à partir du site de téléchargement de logiciels électroniques Informatica.

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

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

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

Paramètre	Description
CertsOutputDir	Répertoire \$CUSTOM TRUSTSTORE LOC de stockage des fichiers truststore générés. Les répertoires \$ICS SERVICENAME/client_certs et \$ICS SERVICENAME/cluster_certs sont créés sous le répertoire \$CUSTOM TRUSTSTORE LOC. \$CUSTOM TRUSTSTORE LOC est le répertoire dans lequel se trouve le truststore personnalisé pour le domaine Informatica (infa_truststore.jks).
DNSDomainName	Nom de domaine DNS pour les nœuds de cluster.
ClusterCert_OrganizationUnit	Facultatif. Valeur du paramètre OrganizationUnit pour le certificat des nœuds de cluster.
ClusterCert_Organization	Valeur du paramètre Organisation pour le certificat des nœuds de cluster. Remarque: Vérifiez que la combinaison des paramètres Organisation (O) et Unité d'organisation (OU) dans l'objet du certificat est distincte pour les certificats clients et de cluster
ClusterCert_Location	Valeur du paramètre Emplacement pour le certificat des nœuds de cluster.
ClusterCert_State	Valeur du paramètre État pour le certificat des nœuds de cluster.
ClusterCert_CountryCode	Valeur du paramètre Code de pays pour le certificat des nœuds de cluster.
DomainCert_OrganizationUnit	Facultatif. Valeur du paramètre Unité d'organisation pour le certificat des nœuds de domaine.
DomainCert_Organization	Valeur du paramètre Organisation pour le certificat des nœuds de domaine. Remarque: Vérifiez que la combinaison des paramètres Organisation (O) et Unité d'organisation (OU) dans l'objet du certificat est distincte pour les certificats clients et de cluster
DomainCert_Location	Facultatif. Valeur du paramètre Emplacement pour le certificat des nœuds de domaine. La valeur par défaut est le paramètre ClusterCert_Location.
DomainCert_State	Facultatif. Valeur du paramètre État pour le certificat des nœuds de domaine. La valeur par défaut est le paramètre ClusterCert_State.
DomainCert_CountryCode	Facultatif. Valeur du paramètre Code de pays pour le certificat des nœuds de domaine. La valeur par défaut est le paramètre ClusterCert_CountryCode.

Paramètre	Description
Custom_Server_Certificate_CN	Facultatif. Valeur du paramètre Nom commun dans le certificat des nœuds de cluster qui peut être utilisée à la place de l'élément \$InfaDomainName-\$ICSServiceName par défaut. Valeur \$DNSDomainName. Remarque: Vous devez entrer des valeurs conformes à RFC2253. Les caractères spéciaux suivants ne sont pas pris en charge : , + " \ < > ;. Les guillemets (") doivent être utilisés par paires. Les caractères \ et " ne doivent pas être utilisés conjointement. La valeur ne peut contenir aucun espace.
Custom_Client_Certificate_CN	Facultatif. Valeur du paramètre Nom commun dans le certificat des nœuds de domaine qui peut être utilisée à la place de l'élément \$InfaDomainName-\$ICSServiceName par défaut. Valeur \$DNSDomainName. La valeur par défaut est le paramètre Custom_Server_Certificate_CN. Remarque: Vous devez entrer des valeurs conformes à RFC2253. Les caractères spéciaux suivants ne sont pas pris en charge : , + " \ < > ;. Les guillemets (") doivent être utilisés par paires. Les caractères \ et " ne doivent pas être utilisés conjointement. La valeur ne peut contenir aucun espace.

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

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

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

Les fichiers suivants sont générés pour le client :

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

- Validez le contenu des fichiers `.csr`. Exécutez la commande suivante pour afficher le contenu : `keytool -printcertreq -file $PATH TO CSR`
- Envoyez les fichiers `.csr` suivants à une autorité de certification (CA) à des fins de signature :
 - `<CertsOutputDir>/<ICSServiceName>/client_certs/infa_nodecert.csr`
 - `<CertsOutputDir>/<ICSServiceName>/cluster_certs/infa_nodecert.csr`
 - `<CertsOutputDir>/<ICSServiceName>/client_certs/browser_cert.csr`

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

7. Après avoir reçu les certificats ou les chaînes de certificats de l'autorité de certification (CA) au format .pem, ["Valider les certificats signés par une autorité de certification \(CA\)" à la page 90](#) et stockez-les dans un emplacement sous le répertoire \$INFA_HOME sur votre machine.

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

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

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

Paramètre	Description
InfadomainKeystorePassword	Mot de passe du keystore de domaine Informatica en texte brut.
InfadomainTruststorePassword	Mot de passe du truststore de domaine Informatica en texte brut.
ClusterCertificate	Chemin d'accès au certificat de cluster signé par l'autorité de certification (CA) au format .pem. Il s'agit d'un certificat d'utilisateur final.
ClientCertificate	Chemin d'accès au certificat client signé par l'autorité de certification (CA) au format .pem. Il s'agit d'un certificat d'utilisateur final.
BrowserCertificate	Chemin d'accès au certificat de navigateur signé par l'autorité de certification (CA) au format .pem.
ICSServiceName	Nom du service de cluster Informatica.
IsCACertificateChainAvailable	Spécifiez si la chaîne de certificats de l'autorité de certification (CA) est disponible sous forme de fichier .pem unique. Entrez true ou false. Remarque: La chaîne de certificats doit contenir uniquement les certificats racine et intermédiaires.
SingleCACertificateChain	Chemin d'accès à la chaîne de certificats de l'autorité de certification (CA) au format .pem.
IndividualCertificatesFromCACChain	Facultatif. Uniquement nécessaire si le paramètre IsCACertificateChainAvailable est défini sur false. Chemins séparés par des virgules vers les certificats publics dans la chaîne de certificats de l'autorité de certification (CA) au format .pem si la chaîne de certificats CA complète est disponible sous forme de fichiers .pem individuels.

Paramètre	Description
KeysOutputDir	Répertoire \$CUSTOM KEYSTORE LOC de stockage des clés générés. Les répertoires \$ICS SERVICENAME/client_certs et \$ICS SERVICENAME/cluster_certs sont créés sous le répertoire \$CUSTOM KEYSTORE LOC. \$CUSTOM KEYSTORE LOC est le répertoire où se trouve le keystore personnalisé pour le domaine Informatica (infa_keystore.jks). \$ICS SERVICENAME est le nom du service de cluster Informatica
CertsOutputDir	Répertoire \$CUSTOM TRUSTSTORE LOC de stockage des fichiers truststore générés. Les répertoires \$ICS SERVICENAME/client_certs et \$ICS SERVICENAME/cluster_certs sont créés sous le répertoire \$CUSTOM TRUSTSTORE LOC. \$CUSTOM TRUSTSTORE LOC est le répertoire dans lequel se trouve le truststore personnalisé pour le domaine Informatica (infa_truststore.jks).

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

Le truststore truststore.jks truststore et les clés publiques infa_nodecert.pem, infa_nodecertkey.pem et infa_pubcert.pem sont stockés dans les répertoires \$CUSTOM TRUSTSTORE LOC/\$ICSServiceName/client_certs et \$CUSTOM TRUSTSTORE LOC/\$ICSServiceName/cluster_certs.

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

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

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

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

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

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

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

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

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

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

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

Générer des certificats SSL personnalisés auto-signés

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

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

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

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

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

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

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

- infa_privkey.pem

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

- Certificats :

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

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

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

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

CHAPITRE 7

Présentation du programme d'installation des services

Ce chapitre comprend les rubriques suivantes :

- [Tâches du programme d'installation des services, 94](#)
- [Sécuriser les fichiers et les répertoires, 94](#)
- [Utilitaires de pré-installation, 95](#)
- [Exécuter l'outil Pre-Installation System Check \(i10Pi\) en mode console, 95](#)
- [Exécuter l'outil Pre-Installation System Check \(i10Pi\) en mode silencieux, 99](#)

Tâches du programme d'installation des services

Le programme d'installation effectue les tâches d'installation en fonction du produit ou des produits que vous installez.

Il peut effectuer les tâches suivantes :

1. Procéder à la validation et à la vérification système pré-installation.
2. Créer un domaine ou joindre un nœud à un domaine existant.
3. Installer des fichiers binaires pour la prise en charge du service.
4. Créer des services d'application.
5. Configurer la sécurité entre le domaine et les services.
6. Démarrer le domaine et les services d'application que vous avez créés.
7. Écrire un message dans le fichier journal.

Sécuriser les fichiers et les répertoires

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. Le programme d'installation attribue des autorisations différentes pour les répertoires et les fichiers dans les répertoires.

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.

<Informatica installation directory>/services/shared/security

Si vous activez la communication sécurisée pour le domaine, le répertoire /security contient les fichiers truststore et les fichiers entrepôt de clé pour les certificats SSL par défaut.

Pour préserver la sécurité des répertoires et des fichiers, le programme d'installation limite l'accès aux répertoires et aux fichiers des répertoires. Le programme d'installation attribue des autorisations spécifiques au groupe et au compte utilisateur propriétaires des répertoires et des fichiers.

Pour plus d'informations sur les autorisations attribuées aux répertoires et aux fichiers, consultez le Guide de sécurité d'Informatica.

Utilitaires de pré-installation

Informatica fournit des utilitaires qui facilitent le processus d'installation des services Informatica. Vous pouvez utiliser le programme d'installation Informatica pour exécuter les utilitaires.

Avant d'installer les services, exécutez l'outil Pre-Installation System Check (i10Pi), qui vérifie qu'une machine répond à la configuration système requise pour l'installation d'Informatica. Informatica vous recommande de vérifier la configuration système minimale requise avant de démarrer l'installation. Lorsque vous exécutez l'outil de vérification du système avant d'effectuer l'installation, le programme d'installation définit des valeurs de certains champs, tels que la connexion de la base de données et les numéros de port du domaine, sur la base des informations que vous avez entrées lors de la vérification du système.

Exécuter l'outil Pre-Installation System Check (i10Pi) en mode console

Exécutez l'outil Pre-Installation System Check (i10Pi) pour vérifier si la machine correspond à la configuration système requise pour l'installation ou la mise à niveau.

Veillez à vérifier les spécifications système et à préparer la base de données du référentiel de configuration du domaine.

1. Connectez-vous à la machine à l'aide d'un compte d'utilisateur système.
2. Fermez toutes les autres applications.
3. Sur une ligne de commande shell, exécutez le fichier d'installation.

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

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

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

5. Entrez **1** pour installer ou mettre à niveau Informatica.
6. Appuyez sur **1** pour exécuter l'outil Pre-Installation System Check (i10Pi) qui vérifie si la machine correspond à la configuration système requise pour l'installation ou la mise à niveau.
7. Dans la section **Bienvenue** de l'outil Informatica Pre-Installation System Check (i10Pi), appuyez sur **Entrée**.

La section **Informations système** s'affiche.

8. Tapez le chemin d'accès absolu du répertoire d'installation.

Les noms de répertoire dans le chemin ne doivent pas contenir d'espaces ou les caractères spéciaux suivants : @|* \$ # ! % () { } [] , ; ' .

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.

9. Appuyez sur **Entrée**.
10. Entrez le numéro de port initial du nœud que vous allez créer ou mettre à niveau sur la machine. Le numéro de port par défaut pour le nœud est 6005.
11. Appuyez sur **Entrée**.

La section **Informations de base de données et de connexion** s'affiche.

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

Pour vous connecter à une base de données sécurisée, vous devez entrer la connexion JDBC à l'aide d'une chaîne de connexion JDBC personnalisée.

13. Entrez les informations de connexion JDBC.

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

Utilisez la syntaxe suivante dans la chaîne de connexion JDBC :

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Utilisez la chaîne de connexion suivante pour vous connecter à la base de données Oracle via le gestionnaire de connexions Oracle :

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```


Microsoft SQL Server avec les informations d'identification de Windows NT

Si vous avez spécifié les informations d'identification de Windows NT pour la base de données du référentiel modèle sur Microsoft SQL Server, spécifiez la syntaxe de la chaîne de connexion pour inclure la méthode d'authentification NTLM.

Microsoft SQL Server qui utilise l'instance par défaut avec les informations d'identification de Windows NT :

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server qui utilise l'instance nommée avec les informations d'identification de Windows NT :

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Azure SQL Database avec authentification Active Directory

```
jdbc:informatica: sqlserver://  
<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Sybase

```
jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
```

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

- 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 :

Invite	Description
Type de base de données	Type de base de données pour le référentiel de configuration du domaine. Sélectionnez un type de base de données parmi les suivants : - 1 - Oracle - 2 - Microsoft SQL Server - 3 - IBM DB2 - 4 - Sybase ASE - 5 - PostgreSQL
ID d'utilisateur de la base de données	ID d'utilisateur du compte d'utilisateur de la base de données pour le référentiel de configuration du domaine.
Mot de passe de l'utilisateur de la base de données	Mot de passe du compte utilisateur de la base de données.
Nom d'hôte de la base de données	Nom d'hôte du serveur de base de données.
Numéro de port de la base de données	Numéro de port de la base de données.
Nom du service de la base de données	Nom du service pour les bases de données Oracle et IBM DB2 ou nom de la base de données pour PostgreSQL, Microsoft SQL Server et Sybase ASE.

- Pour vous connecter à une base de données sécurisée, sélectionnez **1** pour utiliser une chaîne personnalisée et entrez la chaîne de connexion.
Vous devez inclure les paramètres de sécurité en plus des paramètres de connexion. Pour plus d'informations sur les paramètres de sécurité que vous devez inclure dans la connexion JDBC pour une base de données sécurisée, consultez la rubrique ["Chaîne de connexion à une base de données sécurisée" à la page 80](#).

L'outil vérifie les paramètres du disque dur, la disponibilité des ports et la configuration de la base de données. Une fois la vérification système terminée, la section **Résumé de la vérification système** affiche les résultats.

14. Analysez les résultats de la vérification système.

Chaque condition est répertoriée, accompagnée de l'un des statuts de vérification suivants :

- [Réussite] - La spécification répond aux critères d'installation ou de mise à niveau d'Informatica.
- [Échec] - La configuration requise ne répond pas aux critères d'installation ou de mise à niveau d'Informatica. Résolvez le problème avant de continuer l'installation ou la mise à niveau.
- [Information] - vérifiez les informations et effectuez les tâches supplémentaires présentées dans les détails.

Les résultats de la vérification du système sont enregistrés dans le fichier suivant : ...<Informatica installation directory>/Server/I10PI/I10PI/en/I10PI_summary.txt

15. Appuyez sur **Entrée** pour fermer l'outil Pre-Installation System Check (i10Pi).

Vous pouvez continuer vers l'installation ou la mise à niveau immédiate du service Informatica ou terminer la vérification système et poursuivre l'installation ou la mise à niveau ultérieurement. Si vous continuez l'installation ou la mise à niveau immédiatement, vous n'avez pas besoin de redémarrer le programme d'installation.

16. Pour continuer l'installation ou la mise à niveau du service Informatica immédiatement, appuyez sur **o**.
Pour terminer la vérification système et poursuivre l'installation ou la mise à niveau plus tard, appuyez sur **n**.

Si l'outil Pre-Installation System Check (i10Pi) se termine avec des conditions non remplies, résolvez les problèmes, puis exécutez-le à nouveau.

Remarque: Si l'exécution de l'outil Informatica Pre-Installation System Check (i10Pi) se termine avec des conditions non remplies, vous pouvez tout de même effectuer l'installation ou la mise à niveau d'Informatica. Toutefois, Informatica vous recommande fortement de résoudre les conditions non remplies avant de continuer.

Exécuter l'outil Pre-Installation System Check (i10Pi) en mode silencieux

Exécutez l'outil Pre-Installation System Check (i10Pi) en mode silencieux pour vérifier la configuration système requise pour l'installation sans intervention de l'utilisateur.

1. Extrayez le fichier du programme d'installation des services Informatica.
2. Accédez à l'emplacement suivant :
`<Informatica installation directory>/Server/I10PI`
3. Pour spécifier les propriétés de l'outil de vérification du système I10PI en mode silencieux, mettez à jour le fichier `SilentInput.properties` qui se trouve dans le dossier `I10PI`.
4. Pour exécuter l'outil i10Pi en mode silencieux, exécutez le fichier `silentInstall` qui se trouve dans le dossier `I10PI`.

Pour afficher les résultats de l'outil de vérification du système i10Pi en mode silencieux, consultez le fichier `I10PI_summary.txt` qui se trouve à l'emplacement suivant :

`<Informatica installation directory>/Server/I10PI/I10PI/en`

Si l'outil Pre-Installation System Check (i10Pi) se termine avec des conditions non remplies, résolvez les problèmes, puis exécutez-le à nouveau.

Remarque: Si l'exécution de l'outil Informatica Pre-Installation System Check (i10Pi) se termine avec des conditions non remplies, vous pouvez tout de même effectuer l'installation ou la mise à niveau d'Informatica. Toutefois, Informatica vous recommande fortement de résoudre les conditions non remplies avant de continuer.

Partie III : Exécuter le programme d'installation des services

Cette partie contient les chapitres suivants :

- [Installer Enterprise Data Catalog avec des services Informatica, 101](#)
- [Créer un domaine avec des produits Catalog et Data Engineering, 128](#)
- [Joindre un domaine avec des produits Catalog et Data Engineering, 175](#)
- [Installer les fichiers binaires d'Enterprise Data Catalog, 185](#)
- [Exécuter le programme d'installation silencieuse, 201](#)
- [Dépannage , 205](#)

CHAPITRE 8

Installer Enterprise Data Catalog avec des services Informatica

Ce chapitre comprend les rubriques suivantes :

- [Installer Enterprise Data Catalog avec des services Informatica - Présentation, 101](#)
- [Installer en créant un domaine, 101](#)
- [Installer en joignant un domaine, 116](#)

Installer Enterprise Data Catalog avec des services Informatica - Présentation

La première fois que vous exécutez le programme d'installation, vous devez créer un domaine. Ensuite, vous pouvez exécuter le programme d'installation sur une autre machine pour joindre le domaine.

Installer 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 d'utilisateur système.
2. Utilisez la commande suivante pour effacer la variable DISPLAY sur la machine : `unset DISPLAY`
3. Fermez toutes les autres applications.
4. 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.
5. Appuyez sur **0** pour continuer l'installation.
6. Appuyez sur **1** pour installer des produits Informatica 10.5.6.
7. Appuyez sur **3** pour exécuter le programme d'installation.
8. Appuyez sur **2** pour accepter les conditions générales.

9. Appuyez sur **2** pour installer 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.
10. Appuyez sur **1** si la version actuelle des services d'application Informatica n'est pas installée sur votre ordinateur. Sinon, appuyez sur **2**.
11. Indiquez si vous souhaitez installer les packages de distribution via le programme d'installation d'Informatica.
 - Appuyez sur **1** si vous n'avez pas besoin des packages de distribution ou si vous souhaitez les installer ultérieurement.
 - Appuyez sur **2** si vous souhaitez installer les packages de distribution via le programme d'installation.
 La valeur par défaut est 1.
12. Si vous choisissez d'installer les packages de distribution, sélectionnez un ou plusieurs packages à installer dans la liste. Séparez plusieurs packages par une virgule.
La valeur par défaut est 1.
13. Appuyez sur **Entrée** pour confirmer que vous avez vérifié les prérequis de l'installation.
14. Appuyez sur **1** pour que le programme d'installation règle les services d'application Informatica en fonction de la taille des données à déployer. Si vous ne réglez pas les services lors de l'installation, vous pouvez le faire ultérieurement via les programmes de ligne de commande Informatica.
15. 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 : @|* \$ # ! % () { } [] , ; ' La valeur par défaut est `root/Informatica/10.5.3` ou `<répertoire de base utilisateur>/Informatica/10.5.3`.
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.
16. Tapez le chemin d'accès et le nom de fichier de la clé de licence Informatica, puis appuyez sur **Entrée**.
17. Sélectionnez l'environnement d'installation requis parmi les options suivantes :
 - Appuyez sur **1** afin de définir l'environnement Sandbox pour un environnement de base utilisé comme preuve de concept avec un minimum d'utilisateurs.
 - Appuyez sur **2** afin de définir l'environnement de développement pour l'environnement de conception.
 - Appuyez sur **3** afin de définir l'environnement de test pour un traitement de gros volumes plus proche de celui d'un environnement de production.
 - Appuyez sur **4** afin de définir l'environnement de production pour un traitement de gros volumes avec des niveaux élevés d'accès concurrentiel destinés aux utilisateurs finaux. Les environnements de production avancés sont généralement des configurations à plusieurs nœuds.
18. Appuyez sur **2** pour exécuter l'utilitaire de pré-validation. L'utilitaire vous aide à valider les prérequis de l'installation d'Enterprise Data Catalog.
19. Tapez le nom d'hôte de passerelle du cluster d'Informatica au format suivant : `<hostname>.<FQDN>` et appuyez sur la touche **Entrée**.
20. Tapez le nom d'utilisateur de la passerelle et appuyez sur **Entrée**.
21. Tapez **2** si vous souhaitez valider les paramètres de configuration avancés pour le service de cluster Informatica.
Fournissez les paramètres répertoriés dans la section ["Créer et configurer le service de cluster Informatica" à la page 242](#).

22. Spécifiez les noms de domaine complets des nœuds que vous prévoyez de configurer comme nœuds de données. Vous pouvez spécifier plusieurs nœuds de données sous forme de valeurs séparées par des virgules.
23. Spécifiez les noms de domaine complets des nœuds que vous prévoyez de configurer comme nœuds de traitement. Vous pouvez spécifier plusieurs nœuds de données sous forme de valeurs séparées par des virgules.
24. Tapez le chemin d'accès au répertoire de travail, et appuyez sur **Entrée**. Le chemin indique l'emplacement auquel vous souhaitez stocker les fichiers journaux du service de cluster Informatica. La valeur par défaut est `/opt/informatica/ics`.
- Pour une configuration à plusieurs nœuds, le programme d'installation vous invite à confirmer si vous souhaitez spécifier le chemin d'accès au système de fichiers partagés.
25. Tapez **2** si vous souhaitez configurer le chemin du système de fichiers partagés dans une configuration à plusieurs nœuds.
- Tapez le chemin d'accès au système de fichiers partagés du cluster.
- Le programme d'installation démarre l'utilitaire de pré-validation.
26. Appuyez sur **Entrée** pour continuer après avoir exécuté l'utilitaire de pré-validation.
27. 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.
28. Si vous prévoyez d'activer le domaine Informatica pour SAML, importez le certificat SAML copié dans le truststore du domaine Informatica à l'aide de la commande suivante : `keytool -importcert -alias samlcert -file <path to copied SAML certificate file> -keystore <path to Informatics domain truststore> -storepass <password to access the truststore>`.
29. 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 de domaine.
30. 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.
31. 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	Configurez 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 du 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 : <Informatica installation directory>/tomcat/conf/

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

32. Choisissez d'activer ou non l'authentification SAML pour configurer la prise en charge de l'authentification unique (SSO) basée sur SAML (Security Assertion Markup Language) pour les applications Web Informatica dans un domaine Informatica.

Appuyez sur **1** pour désactiver l'authentification SAML. Appuyez sur **2** pour activer et configurer l'authentification SAML.

33. Entrez l'URL du fournisseur d'identité du domaine.
34. Spécifiez le nom de l'approbation de partie de confiance ou l'identificateur de fournisseur de services pour le domaine, tel que défini dans le fournisseur d'identité. Si vous choisissez Non, l'identificateur de fournisseur de services est défini sur « Informatica ».
35. Spécifiez si l'IdP signera ou non l'assertion SAML.
36. Entrez le nom d'alias du certificat de signature d'assertion du fournisseur d'identité.
37. Indiquez si vous souhaitez utiliser les certificats SSL par défaut d'Informatica ou utiliser vos certificats SSL pour activer la communication sécurisée dans le domaine.

Le tableau suivant décrit les options de certificat SSL pour l'authentification SAML :

Option	Description
Utiliser le fichier de certificat SSL Informatica par défaut.	Sélectionnez cette option pour utiliser le fichier truststore Informatica par défaut pour l'authentification SAML.
Spécifier l'emplacement du fichier de certificat SSL.	Sélectionnez cette option pour utiliser un fichier truststore personnalisé pour l'authentification SAML. Spécifiez le répertoire contenant le fichier truststore personnalisé sur les nœuds de passerelle dans le domaine. Spécifiez uniquement le répertoire et non le chemin complet du fichier.

38. Choisissez d'utiliser les certificats SSL par défaut d'Informatica ou vos propres certificats SSL pour activer l'authentification SAML dans le domaine.

Le tableau suivant décrit les options de certificat SSL pour l'authentification SAML :

Option	Description
Utiliser le fichier de certificat SSL Informatica par défaut.	Sélectionnez cette option pour utiliser le fichier truststore Informatica par défaut pour l'authentification SAML.
Spécifier l'emplacement du fichier de certificat SSL.	Sélectionnez cette option pour utiliser un fichier truststore personnalisé pour l'authentification SAML. Spécifiez le répertoire contenant le fichier truststore personnalisé sur les nœuds de passerelle dans le domaine. Spécifiez uniquement le répertoire et non le chemin complet du fichier.

39. Si vous fournissez les certificats de sécurité, spécifiez l'emplacement et les mots de passe des fichiers keystore et truststore.

Le tableau suivant décrit l'emplacement et le mot de passe des fichiers truststore et keystore :

Propriété	Description
Répertoire truststore	Spécifiez le répertoire contenant le fichier truststore personnalisé sur les nœuds de passerelle dans le domaine. Spécifiez uniquement le répertoire et non le chemin complet du fichier.
Mot de passe du truststore	Mot de passe du fichier truststore personnalisé.
Répertoire de keystore	Spécifiez le répertoire contenant le fichier keystore personnalisé.
Mot de passe du keystore	Mot de passe du fichier keystore personnalisé.

40. Pour spécifier la comparaison de contexte d'authentification, spécifiez la comparaison de niveau de sécurité du mécanisme d'authentification utilisé par l'utilisateur avec le serveur IdP.
Les valeurs prises en charge sont l'option MINIMUM, MAXIMUM, BETTER ou EXACT. La valeur par défaut est MINIMUM.
41. Pour définir la classe de contexte d'authentification, spécifiez le mécanisme attendu de la première authentification de l'utilisateur sur le serveur IdP.
Les valeurs prises en charge sont PASSWORD ou PASSWORDPROTECTEDTRANSPORT. La valeur par défaut est PASSWORD.
42. Indiquez si vous souhaitez activer l'application Web pour signer la demande d'authentification SAML ou non ?
Cette option est désactivée par défaut.
43. Spécifiez le nom d'alias de la clé privée importée dans le keystore SAML de nœud à l'aide duquel la demande SAML doit être signée.
44. Spécifiez le mot de passe permettant d'accéder à la clé privée utilisée pour la signature de la demande SAML.
45. Spécifiez l'algorithme que l'application Web utilise pour signer la demande SAML.
Les valeurs prises en charge sont RSA_SHA256, DSA_SHA1, DSA_SHA256, RSA_SHA1, RSA_SHA224, RSA_SHA384, RSA_SHA512, ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256, ECDSA_SHA384, ECDSA_SHA512, RIPEMD160 ou RSA_MD5.
46. Indiquez si vous souhaitez que l'IdP signe la réponse SAML ou non ?

Choisissez d'activer l'application Web pour recevoir ou non la réponse SAML signée. Cette option est désactivée par défaut.

47. Spécifiez si l'IdP chiffrera ou non l'assertion SAML.

Sélectionnez cette option pour activer l'application Web afin de recevoir une assertion SAML chiffrée. La valeur par défaut est activée.

48. Spécifiez le nom d'alias de la clé privée disponible dans le truststore SAML du ou des nœuds de passerelle qu'Informatica utilise pour déchiffrer l'assertion SAML.

49. Fournissez le mot de passe permettant d'accéder à la clé privée à utiliser pour le déchiffrement de la clé de chiffrement de l'assertion.

50. Cliquez sur **Suivant**. La section **Sécurité du domaine - Communication sécurisée** s'affiche.

51. 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 keystore 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. Le répertoire doit contenir les fichiers nommés infa_keystore.jks et infa_keystore.pem.
Mot de passe du keystore	Mot de passe du fichier keystore infa_keystore.jks.
Répertoire de fichiers truststore	Répertoire contenant les fichiers truststore. Le répertoire doit contenir les fichiers nommés infa_truststore.jks et infa_truststore.pem.
Mot de passe du truststore	Mot de passe du fichier infa_truststore.jks.

La page Référentiel de configuration du domaine s'affiche.

52. 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 5 - PostgreSQL

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.

53. Entrez les propriétés de la base de données et du compte utilisateur.

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

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

54. 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.

55. 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 à la configuration requise 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 non partitionné qui se trouve dans la partition du 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.
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 SQL Server, PostgreSQL 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=
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

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

56. 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 du fichier 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;HostNameInCertificate=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.

57. 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 remplacer les données ou de la configuration d'une autre base de données lorsque vous créez un référentiel de configuration du 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.

58. 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 chiffrement que vous devez spécifier :

Propriété	Description
Mot clé	Mot clé à utiliser pour créer une clé de chiffrement personnalisée afin de sécuriser les données sensibles du domaine. Le mot clé doit respecter les critères suivants : <ul style="list-style-type: none"> - Sa longueur doit être comprise 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 chiffrement 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 : <Informatica installation directory>/isp/config/keys.

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

59. Appuyez sur **Entrée**.

La section **Configuration de domaine et de nœud** s'affiche.

60. 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	Nom du 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 de nœud	Nom d'hôte de la machine sur laquelle le nœud est créé. Le nom d'hôte de 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 de nœud	Nom de nœud à créer sur cette machine. Le nom de 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.

Le tableau suivant décrit la complexité du mot de passe :

Propriété	Description
Complexité du mot de passe	Indiquez si vous souhaitez activer la complexité du mot de passe. 1 - Oui 2 - Non Si vous sélectionnez Oui, le mot de passe doit respecter les critères suivants : Il doit contenir au moins huit caractères, au moins un caractère alphabétique, un caractère numérique et un caractère spécial.
Configurer la stratégie des mots de passe	Indiquez si vous souhaitez configurer une stratégie des mots de passe. 1 - Oui 2 - Non Si vous sélectionnez Oui, vous pouvez configurer des règles de complexité du mot de passe. Si vous sélectionnez Non, les règles de stratégie des mots de passe par défaut d'Informatica s'appliquent.

Propriété	Description
Nombre de caractères spéciaux	Nombre minimal de caractères spéciaux requis dans un mot de passe. Vous pouvez également utiliser les caractères spéciaux suivants : " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~] Vous pouvez entrer une valeur entre 0 et 128. La valeur par défaut est de 1.
Nombre de caractères alphabétiques	Nombre minimal de caractères alphabétiques requis dans un mot de passe. Vous pouvez entrer une valeur entre 0 et 128. La valeur par défaut est de 1.
Nombre de caractères numériques	Nombre minimal de caractères numériques requis dans un mot de passe. Vous pouvez entrer une valeur entre 0 et 128. La valeur par défaut est de 1.
Longueur minimale du mot de passe	Nombre minimal de caractères requis dans un mot de passe. Vous pouvez entrer une valeur entre 1 et 128. La valeur par défaut est de 8.
Nombre de mots de passe précédents à stocker	Nombre de mots de passe précédents consécutifs ne pouvant pas être réutilisés. Vous pouvez entrer une valeur entre 0 et 12. La valeur par défaut est de 0.
Expiration du mot de passe en jours	Durée de validité d'un mot de passe. Pour éviter l'expiration des mots de passe, définissez la valeur sur 0. La valeur par défaut est de 0.
Mot de passe du domaine	Mot de passe de l'administrateur du domaine. <ul style="list-style-type: none"> - Si vous n'activez pas la complexité du mot de passe, ce dernier doit comporter entre 2 et 16 caractères. - Si vous l'activez, le mot de passe doit comporter au minimum huit caractères et contenir au moins un caractère alphabétique, un caractère numérique et un caractère spécial. - Si vous configurez une stratégie des mots de passe, le mot de passe doit respecter les règles de complexité que vous avez définies.
Confirmer le mot de passe	Saisissez une nouvelle fois le mot de passe pour le confirmer.

61. 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.

62. 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. Il s'agit également du port pour 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.

63. Pour créer le service de référentiel modèle, le service d'intégration de données et le service de catalogue dans le cadre de l'installation, appuyez sur **1**. Pour terminer l'installation sans créer les services, appuyez sur **2**.

Vous pouvez créer ces services après l'installation à l'aide d'Informatica Administrator ou les créer ultérieurement à l'aide du programme d'installation.

64. Pour configurer le référentiel MetaDex, appuyez sur **1**. Pour ne pas le configurer, appuyez sur **2**.

Si vous n'aviez pas choisi de configurer le référentiel MetaDex lors de l'installation, vous pouvez le faire à la fin de celle-ci.

65. Si vous avez choisi de configurer le référentiel MetaDex, configurez les propriétés suivantes :

Propriété	Description
Type de base de données	Spécifiez la base de données à configurer comme référentiel MetaDex. Vous pouvez sélectionner l'une des options suivantes : - Oracle - SQLServer
Nom d'utilisateur de la base de données	Nom d'utilisateur configuré pour accéder à la base de données.
Mot de passe de la base de données	Mot de passe configuré pour le nom d'utilisateur.
Nom du schéma	Non applicable si vous avez sélectionné Oracle comme base de données. Spécifiez le schéma à utiliser.
La base de données est-elle sécurisée ?	Spécifiez si la base de données est activée pour SSL.
Chemin d'accès au fichier truststore de la base de données	S'applique si vous avez spécifié que la base de données est activée pour SSL. Fournissez le chemin d'accès complet au fichier truststore de la base de données.
Mot de passe du truststore	S'applique si vous avez spécifié que la base de données est activée pour le mot de passe SSL pour accéder au fichier truststore.
Paramètres JDBC sécurisés	S'applique si vous avez spécifié que la base de données est activée pour SSL. Spécifiez les paramètres de base de données sécurisés, comme indiqué dans l'exemple suivant : EncryptionMethod=SSL; HostNameInCertificate=ORATLS.informatica.com; ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2; Enterprise Data Catalog ajoute les paramètres JDBC sécurisés à la chaîne de connexion JDBC. Si vous incluez les paramètres JDBC sécurisés directement dans la chaîne de connexion, n'entrez aucun paramètre dans le champ Paramètres JDBC sécurisés.
Chaîne de connexion JDBC	Chaîne de connexion JDBC pour la connexion à la base de données. Utilisez les formats suivants pour spécifier les chaînes de connexion : - Oracle. jdbc:Informatica:oracle ://<host name>:<port number>;ServiceName= - SQLServer. jdbc:Informatica: sqlserver://<host name>:<portnumber>;SelectMethod=cursor;DatabaseName=
Port de serveur du référentiel MetaDex	Port unique du serveur de référentiel MetaDex. La valeur par défaut est de 48 090.

Propriété	Description
Activer la communication sécurisée pour le référentiel MetaDex ?	Spécifiez si TLS est activé pour la communication avec le référentiel.
Certificats SSL pour sécuriser le référentiel MetaDex ?	Indiquez si vous souhaitez utiliser les certificats SSL par défaut ou les certificats SSL personnalisés pour sécuriser le référentiel. Spécifiez les propriétés suivantes si vous souhaitez utiliser les certificats SSL personnalisés : <ul style="list-style-type: none"> - Type de keystore. Spécifiez le type de keystore. - Alias du keystore. Alias unique permettant d'accéder à l'entrée du keystore. - Fichier keystore. Spécifiez le fichier keystore qui contient les clés et les certificats requis. - Mot de passe du keystore. Mot de passe pour accéder au fichier keystore.
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 pour le nom d'utilisateur : <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 d'utilisateur du domaine	Mot de passe de l'administrateur du domaine. Le mot de passe peut comprendre de 3 à 128 caractères maximum.
Nom de domaine de sécurité	Nom du domaine de sécurité pour l'administrateur du domaine.
Nom de domaine	Nom du domaine que Metadex utilise pour établir la connexion. Requis si le fichier domains.infra spécifie plusieurs domaines. 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 : ` % * + ; " ? , < > \ /

Le programme d'installation démarre l'installation du produit que vous avez spécifié. Le récapitulatif de post-installation indique si l'installation a réussi. Vous pouvez afficher les fichiers journaux de l'installation pour obtenir plus d'informations sur les tâches effectuées par le programme d'installation et pour afficher les propriétés de configuration pour les composants installés.

Installer en joignant un domaine

Vous pouvez joindre un domaine si vous effectuez l'installation sur plusieurs machines et si vous avez créé un domaine sur une autre machine. Vérifiez que vous utilisez la même version d'Informatica sur tous les nœuds.

1. Connectez-vous à la machine à l'aide d'un compte d'utilisateur système.
2. Utilisez la commande suivante pour effacer la variable DISPLAY sur la machine : `unset DISPLAY`

3. Fermez toutes les autres applications.
4. Exécutez la commande `./install.sh` pour démarrer le programme d'installation.
5. Appuyez sur **0** pour continuer l'installation.
6. Appuyez sur **1** pour installer des produits Informatica 10.5.6.
7. Appuyez sur **3** pour exécuter le programme d'installation.
8. Appuyez sur **2** pour accepter les conditions générales.
9. Appuyez sur **2** pour installer Enterprise Data Catalog.
10. Appuyez sur **1** si la version actuelle des services d'application Informatica n'est pas installée sur votre ordinateur. Sinon, appuyez sur **2**.
11. Indiquez si vous souhaitez installer les packages de distribution via le programme d'installation d'Informatica.
 - Appuyez sur **1** si vous n'avez pas besoin des packages de distribution ou si vous souhaitez les installer ultérieurement.
 - Appuyez sur **2** si vous souhaitez installer les packages de distribution via le programme d'installation.

La valeur par défaut est 1.
12. Si vous choisissez d'installer les packages de distribution, sélectionnez un ou plusieurs packages à installer dans la liste. Séparez plusieurs packages par une virgule.
La valeur par défaut est 1.
13. Appuyez sur **Entrée** pour confirmer que vous avez vérifié les prérequis de l'installation.
14. Appuyez sur **1** pour que le programme d'installation règle les services d'application Informatica en fonction de la taille des données à déployer. Si vous ne réglez pas les services lors de l'installation, vous pouvez le faire ultérieurement via `infacmd`.
15. 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 : `@|* $ # ! % () { } [] , ; ' .` La valeur par défaut est `root/Informatica/10.5.3` ou `<répertoire de base utilisateur>/Informatica/10.5.3`.
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.
16. Tapez le chemin d'accès et le nom de fichier de la clé de licence Informatica, puis appuyez sur **Entrée**.
17. Sélectionnez l'environnement d'installation requis parmi les options suivantes :
 - Appuyez sur **1** afin de définir l'environnement Sandbox pour un environnement de base utilisé comme preuve de concept avec un minimum d'utilisateurs.
 - Appuyez sur **2** afin de définir l'environnement de développement pour l'environnement de conception.
 - Appuyez sur **3** afin de définir l'environnement de test pour un traitement de gros volumes plus proche de celui d'un environnement de production.
 - Appuyez sur **4** afin de définir l'environnement de production pour un traitement de gros volumes avec des niveaux élevés d'accès concurrentiel destinés aux utilisateurs finaux. Les environnements de production avancés sont généralement des configurations à plusieurs nœuds.
18. Appuyez sur **2** pour exécuter l'utilitaire de pré-validation. L'utilitaire vous aide à valider les prérequis de l'installation d'Enterprise Data Catalog.
19. Tapez le nom d'hôte de passerelle du cluster d'Informatica au format suivant : `<hostname>.<FQDN>` et appuyez sur la touche **Entrée**.
20. Tapez le nom d'utilisateur de la passerelle et appuyez sur **Entrée**.

21. Tapez **2** si vous souhaitez valider les paramètres de configuration avancés pour Enterprise Data Catalog. Fournissez les paramètres répertoriés dans la section [“Créer et configurer le service de cluster Informatica” à la page 242](#).
22. Spécifiez les noms de domaine complets des nœuds que vous prévoyez de configurer comme nœuds de données. Vous pouvez spécifier plusieurs nœuds de données sous forme de valeurs séparées par des virgules.
23. Spécifiez les noms de domaine complets des nœuds que vous prévoyez de configurer comme nœuds de traitement. Vous pouvez spécifier plusieurs nœuds de données sous forme de valeurs séparées par des virgules.
24. Tapez le chemin d'accès au répertoire de travail, et appuyez sur **Entrée**. Le chemin indique l'emplacement auquel vous souhaitez stocker les fichiers journaux du service de cluster Informatica. La valeur par défaut est `/opt/informatica/ics`.

Pour une configuration à plusieurs nœuds, le programme d'installation vous invite à confirmer si vous souhaitez spécifier le chemin d'accès au système de fichiers partagés.
25. Tapez **2** si vous souhaitez configurer le chemin du système de fichiers partagés dans une configuration à plusieurs nœuds.

Tapez le chemin d'accès au système de fichiers partagés du cluster.

Le programme d'installation démarre l'utilitaire de pré-validation.
26. Appuyez sur **Entrée** pour continuer après avoir exécuté l'utilitaire de pré-validation.
27. 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.
28. Si le domaine Informatica est activé pour SAML, importez le certificat SAML copié dans le truststore du domaine Informatica à l'aide de la commande suivante :

```
keytool -importcert -alias samlcert -file  
<path to copied SAML certificate file> -keystore <path to Informatics domain truststore>  
-storepass <password to access the truststore>.
```
29. 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.
30. 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.
31. Indiquez si vous souhaitez configurer le nœud comme un nœud de passerelle.

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.
32. 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	Configurez 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 du 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 : <Informatica installation directory>\tomcat\conf\

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

33. Choisissez d'activer ou non l'authentification SAML pour configurer la prise en charge de l'authentification unique (SSO) basée sur SAML (Security Assertion Markup Language) pour les applications Web Informatica dans un domaine Informatica.

Appuyez sur **1** pour désactiver l'authentification SAML et passer à [#unique_142](#). Appuyez sur **2** pour activer et configurer l'authentification SAML.

34. Entrez l'URL du fournisseur d'identité du domaine.
35. Spécifiez le nom de l'approbation de partie de confiance ou l'identificateur de fournisseur de services pour le domaine, tel que défini dans le fournisseur d'identité. Si vous choisissez Non, l'identificateur de fournisseur de services est défini sur « Informatica ».
36. Spécifiez si l'IdP signera ou non l'assertion SAML.
37. Entrez le nom d'alias du certificat de signature d'assertion du fournisseur d'identité.
38. Indiquez si vous souhaitez utiliser les certificats SSL par défaut d'Informatica ou utiliser vos certificats SSL pour activer la communication sécurisée dans le domaine.

Le tableau suivant décrit les options de certificat SSL pour l'authentification SAML :

Option	Description
Utiliser le fichier de certificat SSL Informatica par défaut.	Sélectionnez cette option pour utiliser le fichier truststore Informatica par défaut pour l'authentification SAML.
Spécifier l'emplacement du fichier de certificat SSL.	Sélectionnez cette option pour utiliser un fichier truststore personnalisé pour l'authentification SAML. Spécifiez le répertoire contenant le fichier truststore personnalisé sur les nœuds de passerelle dans le domaine. Spécifiez uniquement le répertoire et non le chemin complet du fichier.

39. Indiquez si vous souhaitez utiliser les certificats SSL par défaut d'Informatica ou vos propres certificats SSL pour activer l'authentification SAML dans le domaine.

Le tableau suivant décrit les options de certificat SSL pour l'authentification SAML :

Option	Description
Utiliser le fichier de certificat SSL Informatica par défaut.	Sélectionnez cette option pour utiliser le fichier truststore Informatica par défaut pour l'authentification SAML.
Spécifier l'emplacement du fichier de certificat SSL.	Sélectionnez cette option pour utiliser un fichier truststore personnalisé pour l'authentification SAML. Spécifiez le répertoire contenant le fichier truststore personnalisé sur les nœuds de passerelle dans le domaine. Spécifiez uniquement le répertoire et non le chemin complet du fichier.

40. Si vous fournissez les certificats de sécurité, spécifiez l'emplacement et les mots de passe des fichiers keystore et truststore.

Le tableau suivant décrit l'emplacement et le mot de passe des fichiers truststore et keystore :

Propriété	Description
Répertoire truststore	Spécifiez le répertoire contenant le fichier truststore personnalisé sur les nœuds de passerelle dans le domaine. Spécifiez uniquement le répertoire et non le chemin complet du fichier.
Mot de passe du truststore	Mot de passe du fichier truststore personnalisé.
Répertoire de keystore	Spécifiez le répertoire contenant le fichier keystore personnalisé.
Mot de passe du keystore	Mot de passe du fichier keystore personnalisé.

41. Pour spécifier la comparaison de contexte d'authentification, spécifiez la comparaison de niveau de sécurité du mécanisme d'authentification utilisé par l'utilisateur avec le serveur IdP.
Les valeurs prises en charge sont l'option MINIMUM, MAXIMUM, BETTER ou EXACT. La valeur par défaut est MINIMUM.
42. Pour définir la classe de contexte d'authentification, spécifiez le mécanisme attendu de la première authentification de l'utilisateur sur le serveur IdP.
Les valeurs prises en charge sont PASSWORD ou PASSWORDPROTECTEDTRANSPORT. La valeur par défaut est PASSWORD.

43. Indiquez si vous souhaitez activer l'application Web pour signer la demande d'authentification SAML ou non ?
Cette option est désactivée par défaut.
44. Spécifiez le nom d'alias de la clé privée importée dans le keystore SAML de nœud à l'aide duquel la demande SAML doit être signée.
45. Spécifiez le mot de passe permettant d'accéder à la clé privée utilisée pour la signature de la demande SAML.
46. Spécifiez l'algorithme que l'application Web utilise pour signer la demande SAML.
Les valeurs prises en charge sont RSA_SHA256, DSA_SHA1, DSA_SHA256, RSA_SHA1, RSA_SHA224, RSA_SHA384, RSA_SHA512, ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256, ECDSA_SHA384, ECDSA_SHA512, RIPEMD160 ou RSA_MD5.
47. Indiquez si vous souhaitez que l'IdP signe ou non la réponse SAML.
Choisissez cette option pour activer l'application Web pour recevoir ou non la réponse SAML signée.
Cette option est désactivée par défaut.
48. Spécifiez si l'IdP chiffrera ou non l'assertion SAML.
Sélectionnez cette option pour activer l'application Web afin de recevoir une assertion SAML chiffrée. La valeur par défaut est activée.
49. Spécifiez le nom d'alias de la clé privée disponible dans le truststore SAML du ou des nœuds de passerelle qu'Informatica utilise pour déchiffrer l'assertion SAML.
50. Fournissez le mot de passe permettant d'accéder à la clé privée à utiliser pour le déchiffrement de la clé de chiffrement de l'assertion.
51. Cliquez sur **Suivant**. La section **Sécurité du domaine - Communication sécurisée** s'affiche.
52. 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 keystore 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. Le répertoire doit contenir les fichiers nommés infa_keystore.jks et infa_keystore.pem.
Mot de passe du keystore	Mot de passe du fichier keystore infa_keystore.jks.
Répertoire de fichiers truststore	Répertoire contenant les fichiers truststore. Le répertoire doit contenir les fichiers nommés infa_truststore.jks et infa_truststore.pem.
Mot de passe du truststore	Mot de passe du fichier infa_truststore.jks.

La page Référentiel de configuration du domaine s'affiche.

53. 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.

Propriété	Description
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.

54. 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 devez 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.

55. 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 de nœud	Nom d'hôte de nœud. Le nom d'hôte de nœud ne peut pas contenir le caractère de soulignement (_). Remarque: N'utilisez pas localhost. Le nom d'hôte doit explicitement identifier la machine.
Nom de nœud	Nom du nœud Informatica à créer sur cette machine. Le nom de nœud n'est pas le nom d'hôte de la machine.
Numéro de port du nœud	Numéro de port du nœud.

Propriété	Description
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 du 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.

56. 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.

57. 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. Il s'agit également du port pour 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	Description
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.

58. Pour créer le service de référentiel modèle, le service d'intégration de données et le service de catalogue dans le cadre de l'installation, appuyez sur **1**. Pour terminer l'installation sans créer les services, appuyez sur **2**.

Vous pouvez créer ces services après l'installation à l'aide d'Informatica Administrator ou les créer ultérieurement à l'aide du programme d'installation.

59. Pour configurer le référentiel MetaDex, appuyez sur **1**. Pour ne pas le configurer, appuyez sur **2**.

Si vous n'aviez pas choisi de configurer le référentiel MetaDex lors de l'installation, vous pouvez le faire à la fin de celle-ci.

60. Si vous avez choisi de configurer le référentiel MetaDex, configurez les propriétés suivantes :

Propriété	Description
Type de base de données	Spécifiez la base de données à configurer comme référentiel MetaDex. Vous pouvez sélectionner l'une des options suivantes : - Oracle - SQLServer
Nom d'utilisateur de la base de données	Nom d'utilisateur configuré pour accéder à la base de données.
Mot de passe de la base de données	Mot de passe configuré pour le nom d'utilisateur.
Nom du schéma	Non applicable si vous avez sélectionné Oracle comme base de données. Spécifiez le schéma à utiliser.
La base de données est-elle sécurisée ?	Spécifiez si la base de données est activée pour SSL.

Propriété	Description
Chemin d'accès au fichier truststore de la base de données	S'applique si vous avez spécifié que la base de données est activée pour SSL. Fournissez le chemin d'accès complet au fichier truststore de la base de données.
Mot de passe du truststore	S'applique si vous avez spécifié que la base de données est activée pour le mot de passe SSL pour accéder au fichier truststore.
Paramètres JDBC sécurisés	<p>S'applique si vous avez spécifié que la base de données est activée pour SSL. Spécifiez les paramètres de base de données sécurisés, comme indiqué dans l'exemple suivant :</p> <pre>EncryptionMethod=SSL; HostNameInCertificate=ORATLS.informatica.com; ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;</pre> <p>Enterprise Data Catalog ajoute les paramètres JDBC sécurisés à la chaîne de connexion JDBC. Si vous incluez les paramètres JDBC sécurisés directement dans la chaîne de connexion, n'entrez aucun paramètre dans le champ Paramètres JDBC sécurisés.</p>
Chaîne de connexion JDBC	<p>Chaîne de connexion JDBC pour la connexion à la base de données.</p> <p>Utilisez les formats suivants pour spécifier les chaînes de connexion :</p> <ul style="list-style-type: none"> - Oracle. jdbc:Informatica:oracle: //<host name>:<port number>;ServiceName= - SQLServer. jdbc:Informatica :sqlserver://<host name>:<portnumber>;SelectMethod=cursor;DatabaseName=
Port de serveur du référentiel MetaDex	Port unique du serveur de référentiel MetaDex. La valeur par défaut est de 48 090.
Activer la communication sécurisée pour le référentiel MetaDex ?	Spécifiez si TLS est activé pour la communication avec le référentiel.
Certificats SSL pour sécuriser le référentiel MetaDex ?	<p>Indiquez si vous souhaitez utiliser les certificats SSL par défaut ou les certificats SSL personnalisés pour sécuriser le référentiel.</p> <p>Spécifiez les propriétés suivantes si vous souhaitez utiliser les certificats SSL personnalisés :</p> <ul style="list-style-type: none"> - Type de keystore. Spécifiez le type de keystore. - Alias du keystore. Alias unique permettant d'accéder à l'entrée du keystore. - Fichier keystore. Spécifiez le fichier keystore qui contient les clés et les certificats requis. - Mot de passe du keystore. Mot de passe pour accéder au fichier keystore.
Nom d'utilisateur de domaine	<p>Nom d'utilisateur de l'administrateur du domaine. Vous pouvez utiliser ce nom d'utilisateur pour vous connecter la première fois à Informatica Administrator.</p> <p>Utilisez les directives suivantes pour le nom d'utilisateur :</p> <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.

Propriété	Description
Mot de passe d'utilisateur du domaine	Mot de passe de l'administrateur du domaine. Le mot de passe peut comprendre de 3 à 128 caractères maximum.
Nom de domaine de sécurité	Nom du domaine de sécurité pour l'administrateur du domaine.
Nom de domaine	Nom du domaine que Metadex utilise pour établir la connexion. Requis si le fichier domains.infra spécifie plusieurs domaines. 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 : ` % * + ; " ? , < > \ /

Le programme d'installation démarre l'installation du produit que vous avez spécifié. Le récapitulatif de post-installation indique si l'installation a réussi. Vous pouvez afficher les fichiers journaux de l'installation pour obtenir plus d'informations sur les tâches effectuées par le programme d'installation et pour afficher les propriétés de configuration pour les composants installés.

CHAPITRE 9

Créer un domaine avec des produits Catalog et Data Engineering

Ce chapitre comprend les rubriques suivantes :

- [Commencer l'installation, 128](#)
- [Configurer le domaine, 134](#)
- [Configurer Enterprise Data Catalog, 163](#)

Commencer l'installation

Cette tâche inclut les invites du programme d'installation pour le lancement de l'installation. Vous serez invité à fournir des informations de base telles que l'acceptation des conditions, l'option d'installation et le répertoire d'installation.

Lorsque vous effectuez les tâches préliminaires, vous suivez les invites du programme d'installation et fournissez les informations requises pour configurer le domaine.

Exécuter le programme d'installation

Effectuez les étapes suivantes pour exécuter le programme d'installation :

1. Connectez-vous à la machine à l'aide d'un compte d'utilisateur système.
2. Utilisez la commande suivante pour effacer la variable DISPLAY sur la machine : `unset DISPLAY`
3. Fermez toutes les autres applications.
4. Sur une ligne de commande shell, exécutez le fichier `install.sh`.

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

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

Si les variables d'environnement sont définies, appuyez sur la touche **o** pour continuer.

Bienvenue - Accepter les conditions générales

- Lisez les termes et conditions d'installation d'Informatica et du kit de ressources d'utilisation du produit, puis sélectionnez **J'accepte les conditions générales**.
 - a. Appuyez sur **1** si vous ne souhaitez pas accepter les conditions générales.
 - b. Appuyez sur **2** pour accepter les conditions générales.

Les sections de **sélection des composants** s'affichent.

Choisissez l'option d'installation

Après avoir accepté les conditions générales, vous pouvez installer les services de domaine Informatica qui prennent en charge les produits Data Engineering et Catalog.

1. Appuyez sur **2** pour installer Informatica Enterprise Data Catalog.
2. Sélectionnez si la version actuelle des services du domaine Informatica est installée sur le nœud.
 - a. Appuyez sur **1** si la version actuelle des services de domaine Informatica n'est pas installée sur le nœud.
 - b. Appuyez sur **2** si la version actuelle des services du domaine Informatica est installée sur le nœud.
3. Indiquez si vous souhaitez installer les packages de distribution via le programme d'installation d'Informatica.
 - Appuyez sur **1** si vous n'avez pas besoin des packages de distribution ou si vous souhaitez les installer ultérieurement.
 - Appuyez sur **2** si vous souhaitez installer les packages de distribution via le programme d'installation.

La valeur par défaut est 1.
4. Si vous choisissez d'installer les packages de distribution, sélectionnez un ou plusieurs packages à installer dans la liste. Séparez plusieurs packages par une virgule.

La valeur par défaut est 1.

La page **Pré-requis d'installation** affiche la configuration requise pour l'installation. Vérifiez que toute la configuration requise est correcte avant de poursuivre l'installation.

Adapter les services d'application

Après avoir examiné les prérequis d'installation, vous pouvez choisir d'adapter les services d'application pour de meilleures performances, en fonction du type de déploiement dans votre environnement. Si vous n'optimisez pas les services maintenant, vous pouvez le faire ultérieurement via infacmd.

1. Indiquez si vous souhaitez que le programme d'installation règle les services d'application :
 - Appuyez sur 1 pour ne pas régler les services. La section **Licence et répertoire d'installation** s'affiche.
 - Appuyez sur 2 pour régler les services.

Si vous joignez le nœud au domaine existant, assurez-vous que le type de déploiement que vous sélectionnez ici est le même type de déploiement que les nœuds de passerelle.

2. Sélectionnez le type de déploiement associé à l'environnement Informatica.

Type de déploiement	Espace disque par nœud	Total des cœurs virtuels	RAM par nœud
Sandbox	140 Go	16	32 Go
De base	140 Go	24	64 Go
Standard	140 Go	48	64 Go
Avancé	140 Go	96	128 Go

3. Indiquez si vous souhaitez modifier le type de déploiement ou continuer avec le type de déploiement actuel.
 - a. Appuyez sur **1** pour modifier le type de déploiement.
 - b. Appuyez sur **2** pour continuer avec le type de déploiement actuel.

La section **Licence et répertoire d'installation** s'affiche.

Spécifier le répertoire d'installation

Après avoir vérifié les prérequis d'installation, vous pouvez spécifier le répertoire d'installation.

1. Saisissez le répertoire d'installation.

Les noms de répertoires du chemin d'accès ne doivent pas contenir d'espaces ni les caractères spéciaux suivants : @|* \$ # ! % () { } [] , ; ' La valeur par défaut est <répertoire de base utilisateur>/Informatica/10.5.6.

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.

2. Entrez le chemin et le nom de fichier de la clé de licence , puis appuyez sur **Entrée**.
3. Choisissez un environnement d'installation et appuyez sur **Entrée**.
 - Appuyez sur **1** afin de définir l'environnement Sandbox pour un environnement de base utilisé comme preuve de concept avec un minimum d'utilisateurs.
 - Appuyez sur **2** afin de définir l'environnement de développement pour l'environnement de conception.
 - Appuyez sur **3** afin de définir l'environnement de test pour un traitement de gros volumes plus proche de celui d'un environnement de production.
 - Appuyez sur **4** afin de définir l'environnement de production pour un traitement de gros volumes avec des niveaux élevés d'accès concurrentiel destinés aux utilisateurs finaux. Les environnements de production avancés sont généralement des configurations à plusieurs nœuds.

La valeur par défaut est de 1 pour Sandbox.

4. Indiquez si vous souhaitez exécuter l'utilitaire de pré-validation.
 - a. Appuyez sur **1** pour ignorer l'utilitaire de pré-validation.
 - b. Appuyez sur **2** pour exécuter l'utilitaire de pré-validation.

L'utilitaire vous aide à valider les prérequis de l'installation d'Enterprise Data Catalog.

Si vous choisissez d'ignorer l'utilitaire de pré-validation, la section **Récapitulatif de pré-installation** s'affiche. Examinez le récapitulatif d'installation.

Si vous choisissez d'exécuter l'utilitaire de pré-validation, la section Pré-validation s'affiche.

Préparer l'utilitaire de pré-validation

Vous pouvez utiliser l'utilitaire de pré-validation pour vérifier les prérequis de la création du service de cluster Informatica.

1. Indiquez si vous souhaitez exécuter l'utilitaire de pré-validation :
 - a. Appuyez sur **1** pour ignorer l'exécution de l'utilitaire de pré-validation.
 - b. Appuyez sur **2** pour exécuter l'utilitaire de pré-validation.
2. Si vous avez choisi d'exécuter l'utilitaire de pré-validation, vous devez fournir les détails répertoriés dans le tableau suivant :

Propriété	Description
Hôte de passerelle du cluster Informatica	Nom de domaine complet du nœud à configurer comme hôte de passerelle.
Utilisateur de passerelle	Nom d'utilisateur de l'hôte de la passerelle.
Activer la configuration avancée	<ul style="list-style-type: none">- Appuyez sur 1 pour ignorer la validation des propriétés de configuration avancée pour les services associés.- Appuyez sur 2 pour valider les propriétés de configuration avancée des services associés. Si vous sélectionnez cette option, vous devez spécifier des valeurs pour toutes les propriétés.
Nœuds de données	Liste de noms de domaine complets de nœuds séparée par des virgules à configurer comme nœuds de données.
Nœuds de traitement	Liste de noms de domaine complets de nœuds séparée par des virgules à configurer comme nœuds de traitement.
Chemin du répertoire de travail	<p>Répertoire du service de cluster Informatica. La valeur par défaut est <code>/opt/informatica/ics</code>. Pour une configuration à plusieurs nœuds, le programme d'installation vous invite à confirmer si vous souhaitez spécifier le chemin d'accès au système de fichiers partagés.</p> <ul style="list-style-type: none">- Tapez 1 si vous souhaitez configurer le chemin d'accès au système de fichiers partagés pour la configuration à plusieurs nœuds.- Tapez 2 si vous souhaitez configurer le chemin d'accès au système de fichiers partagés pour la configuration à plusieurs nœuds. Si vous sélectionnez cette option, vous devez spécifier le chemin d'accès au répertoire personnalisé du cluster. <p>Remarque: L'autorisation d'accès au répertoire doit être <code>u=rwx (0700) or u=rwx,g=rx (0750)</code>. Le service Postgres ne démarre pas si le répertoire ne dispose pas de l'autorisation requise.</p>

3. S'applique si vous avez sélectionné l'option de validation des propriétés de configuration avancée des services associés.

Fournissez les valeurs suivantes pour la validation des paramètres de configuration du serveur Nomad :

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

Fournissez les valeurs suivantes pour la validation des paramètres de configuration du serveur Apache ZooKeeper :

Propriété	Description
Hôtes ZooKeeper	Liste de noms de domaine complets de nœuds séparée par des virgules qui hébergent le serveur Apache ZooKeeper.
Port ZooKeeper	Numéro de port configuré pour le serveur Apache ZooKeeper. La valeur par défaut est de 2181.
Port d'homologue ZooKeeper	Numéro de port configuré pour la communication entre entités homologues d'Apache ZooKeeper. La valeur par défaut est de 2888.
Port leader de ZooKeeper	Numéro de port configuré pour le serveur ZooKeeper identifié comme leader. La valeur par défaut est de 3888.
Répertoire d'installation de ZooKeeper	Spécifiez le chemin d'accès au répertoire dans lequel vous souhaitez installer Apache ZooKeeper. La valeur par défaut est \$clusterCustomDir/zk/install

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

Fournissez les valeurs suivantes pour la validation des paramètres de configuration du serveur Apache Solr :

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

Fournissez les valeurs suivantes pour la validation des paramètres de configuration de la base de données MongoDB :

Propriété	Description
Hôtes MongoDB	Liste de noms de domaine complets de nœuds séparée par des virgules qui hébergent la base de données MongoDB.
Port MongoDB	Numéro de port configuré pour MongoDB. La valeur par défaut est de 27017.
Répertoire de journaux de MongoDB	Spécifiez le chemin d'accès au répertoire de stockage des fichiers journaux. La valeur par défaut est \$clusterCustomDir/mongo/log

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

Fournissez les valeurs suivantes pour la validation des paramètres de configuration de la base de données PostgreSQL :

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

Remarque: Les détails pour les services Data Privacy Management, Elasticsearch et Spark ne sont pas validés par l'utilitaire de pré-validation.

- Appuyez sur **Entrée** pour continuer après avoir exécuté l'utilitaire de pré-validation.

Configurer le domaine

Cette tâche inclut les invites du programme d'installation pour configurer le domaine. Vous serez invité à fournir des informations pour créer un domaine et configurer la sécurité du domaine, le référentiel du domaine et les services d'application.

Configurer les options du domaine

Lorsque vous examinez le récapitulatif de pré-installation et poursuivez l'installation, le programme d'installation copie les fichiers d'installation dans le répertoire d'installation. Vous voyez une invite pour créer ou joindre un domaine. Vous pouvez ensuite entrer les informations de domaine.

1. 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.

2. Indiquez si vous souhaitez activer la communication sécurisée pour les services du domaine.

- a. Appuyez sur **1** pour désactiver la communication sécurisée pour le domaine.
- b. Appuyez sur **2** pour activer la communication sécurisée pour le domaine.

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.

3. Spécifiez 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
Activer HTTPS pour Informatica Administrator	Configurez une connexion sécurisée à Informatica Administrator.
Désactivez 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 : <Informatica installation directory>/tomcat/conf/

- c. Si vous spécifiez le keystore, entrez le mot de passe et l'emplacement du fichier keystore.
 - d. Si vous avez activé la communication sécurisée pour le domaine, la section **Sécurité du domaine - Communication sécurisée** s'affiche.
 - e. Si vous n'avez pas activé la communication sécurisée pour le domaine, la section **Référentiel de configuration du domaine** s'affiche. Passez à l'étape ["Configurer les détails du référentiel du domaine"](#) à la page 139.
4. Choisissez d'activer ou non l'authentification SAML pour configurer la prise en charge de l'authentification unique (SSO) basée sur SAML (Security Assertion Markup Language) pour les applications Web Informatica dans un domaine Informatica.
Appuyez sur **1** pour désactiver l'authentification SAML et passer à [#unique_142](#). Appuyez sur **2** pour activer et configurer l'authentification SAML.
 5. Entrez l'URL du fournisseur d'identité du domaine.
 6. Spécifiez le nom de l'approbation de partie de confiance ou l'identificateur de fournisseur de services pour le domaine, tel que défini dans le fournisseur d'identité. Si vous choisissez Non, l'identificateur de fournisseur de services est défini sur « Informatica ».
 7. Spécifiez si l'IdP signera ou non l'assertion SAML.
 8. Entrez le nom d'alias du certificat de signature d'assertion du fournisseur d'identité.
 9. Indiquez si vous souhaitez utiliser les certificats SSL par défaut d'Informatica ou utiliser vos certificats SSL pour sécuriser la communication du domaine.
 10. Indiquez si vous souhaitez utiliser les certificats SSL par défaut d'Informatica ou vos propres certificats SSL pour activer l'authentification SAML dans le domaine.

Le tableau suivant décrit les options de certificat SSL pour l'authentification SAML :

Option	Description
Utilisez les certificats SSL par défaut d'Informatica.	Permet d'utiliser les certificats SSL par défaut fournis par Informatica.
Utilisez les certificats SSL personnalisés.	Sélectionnez un fichier truststore personnalisé pour l'authentification SAML. Spécifiez le répertoire contenant le fichier truststore personnalisé sur les nœuds de passerelle dans le domaine. Spécifiez uniquement le répertoire et non le chemin complet du fichier.

11. Si vous fournissez les certificats de sécurité, spécifiez l'emplacement et les mots de passe des fichiers keystore et truststore.

Le tableau suivant décrit l'emplacement et le mot de passe des fichiers truststore et keystore :

Propriété	Description
Répertoire truststore	Spécifiez le répertoire contenant le fichier truststore personnalisé sur les nœuds de passerelle dans le domaine. Spécifiez uniquement le répertoire et non le chemin complet du fichier.
Mot de passe du truststore	Mot de passe du fichier truststore personnalisé.
Répertoire de keystore	Spécifiez le répertoire contenant le fichier keystore personnalisé.
Mot de passe du keystore	Mot de passe du fichier keystore personnalisé.

12. Pour spécifier la comparaison de contexte d'authentification, spécifiez la comparaison de niveau de sécurité du mécanisme d'authentification utilisé par l'utilisateur avec le serveur IdP.
Les valeurs prises en charge sont l'option MINIMUM, MAXIMUM, BETTER ou EXACT. La valeur par défaut est MINIMUM.
13. Pour définir la classe de contexte d'authentification, spécifiez le mécanisme attendu de la première authentification de l'utilisateur sur le serveur IdP.
Les valeurs prises en charge sont PASSWORD ou PASSWORDPROTECTEDTRANSPORT. La valeur par défaut est PASSWORD.
14. Indiquez si vous souhaitez activer l'application Web pour signer la demande d'authentification SAML ou non ?
Cette option est désactivée par défaut.
15. Spécifiez le nom d'alias de la clé privée importée dans le keystore SAML de nœud à l'aide duquel la demande SAML doit être signée.
16. Spécifiez le mot de passe permettant d'accéder à la clé privée utilisée pour la signature de la demande SAML.
17. Spécifiez l'algorithme que l'application Web utilise pour signer la demande SAML.
Les valeurs prises en charge sont RSA_SHA256, DSA_SHA1, DSA_SHA256, RSA_SHA1, RSA_SHA224, RSA_SHA384, RSA_SHA512, ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256, ECDSA_SHA384, ECDSA_SHA512, RIPEMD160 ou RSA_MD5.
18. Indiquez si vous souhaitez que l'IdP signe la réponse SAML ou non ?

Choisissez cette option pour activer l'application Web pour recevoir ou non la réponse SAML signée. Cette option est désactivée par défaut.

19. Spécifiez si l'IdP chiffrera ou non l'assertion SAML.

Sélectionnez cette option pour activer l'application Web afin de recevoir une assertion SAML chiffrée. La valeur par défaut est activée.

20. Spécifiez le nom d'alias de la clé privée disponible dans le truststore SAML du ou des nœuds de passerelle qu'Informatica utilise pour déchiffrer l'assertion SAML.
21. Fournissez le mot de passe permettant d'accéder à la clé privée à utiliser pour le déchiffrement de la clé de chiffrement de l'assertion.
22. Cliquez sur **Suivant**.

La section **Sécurité du domaine - Communication sécurisée** s'affiche.

Configurer la sécurité du domaine

Après avoir configuré le domaine, vous pouvez configurer la sécurité de domaine.

- 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
Utiliser les certificats SSL Informatica par défaut	Utilisez les certificats SSL par défaut contenus dans le keystore et le truststore par défaut. 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.
Utiliser les certificats SSL personnalisés	Spécifiez le chemin des fichiers keystore et truststore qui contiennent les certificats SSL. Vous devez également spécifier les mots de passe du 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. Le répertoire doit contenir des fichiers nommés infa_keystore.jks.
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.

Configurer les détails du référentiel du domaine

Après avoir configuré la sécurité du domaine, vous pouvez configurer les détails du référentiel du domaine.

1. Sélectionnez la base de données à utiliser pour les détails du 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 5 - PostgreSQL

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.

2. Entrez les propriétés de la base de données et du compte 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 utilisateur de la base de données de configuration du domaine.
Mot de passe utilisateur	Mot de passe du compte utilisateur de la base de données de configuration du domaine.

3. Indiquez 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 du domaine dans une base de données sécurisée, appuyez sur 1 et passez à l'étape 5.

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

4. Si vous ne créez pas de 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	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. Indiquez si vous souhaitez spécifier un espace de table : 1 - Non 2 - Oui
Espace de table	Nom de l'espace de table dans lequel les tables sont créées. 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, 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 non partitionné qui se trouve dans la partition du 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.
Nom du service de la base de données	Nom du service ou de la base de données : <ul style="list-style-type: none">- Oracle : entrez le nom de service.- Microsoft SQL Server : entrez le nom de la base de données.- IBM DB2 : entrez le nom de service.- Sybase ASE : entrez le nom de la base de données.- PostgreSQL : entrez le nom de la base de données.
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 dans la chaîne de connexion JDBC :

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Utilisez la chaîne de connexion suivante pour vous connecter à la base de données Oracle via le gestionnaire de connexions Oracle :

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server avec les informations d'identification de Windows NT

Si vous avez spécifié les informations d'identification de Windows NT pour la base de données du référentiel modèle sur Microsoft SQL Server, spécifiez la syntaxe de la chaîne de connexion pour inclure la méthode d'authentification NTLM.

Microsoft SQL Server qui utilise l'instance par défaut avec les informations d'identification de Windows NT :

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server qui utilise l'instance nommée avec les informations d'identification de Windows NT :

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Azure SQL Database avec authentification Active Directory

```
jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;Authentication Method=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Sybase

```
jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
```

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

5. 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 du fichier truststore de la base de données	Mot de passe du fichier truststore.
Chaîne de connexion JDBC personnalisée	Chaîne de connexion JDBC pour la connexion à la base de données sécurisée qui contient le nom d'hôte, le numéro de port et les paramètres de sécurité de la base de données.

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 JDBC sécurisées :

- **IBM DB2 :** jdbc:Informatica:db2://<host name:port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- **Oracle:** jdbc:Informatica:oracle://<host name:port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- **Microsoft SQL Server:** jdbc:Informatica:sqlserver://<host name:port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- **PostgreSQL:** jdbc:Informatica:postgresql://<host name:port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database 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.

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

Le tableau suivant décrit les options de remplacer les données ou de la configuration d'une autre base de données lorsque vous créez un référentiel de configuration du 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.

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

Sécurité du domaine - Clé de chiffrement

Après avoir configuré le référentiel de domaine, vous pouvez configurer la clé de chiffrement.

- Sur la page **Sécurité du domaine - Clé de chiffrement**, entrez le répertoire de la clé de chiffrement du domaine Informatica.

Le tableau suivant décrit les paramètres de clé de cryptage à spécifier lors de la création d'un domaine :

Propriété	Description
Répertoire de la clé de chiffrement	Répertoire dans lequel stocker la clé de chiffrement pour le domaine. Par défaut, la clé de chiffrement est créée dans le répertoire suivant : <Informatica installation directory>/isp/config/keys.
Spécifiez si vous souhaitez sauvegarder ou non la clé de site générée par le programme d'installation	<p>Une clé de site unique est générée. En cas de perte de la clé de site, vous ne pouvez plus la régénérer. Veillez à enregistrer une copie de cette clé et de ne pas partager la clé de site unique avec d'autres.</p> <p>Spécifiez si vous souhaitez sauvegarder ou non la clé de site générée par le programme d'installation :</p> <ul style="list-style-type: none"> - Sélectionnez 1 pour Non. Si vous choisissez Non, le programme d'installation génère une erreur. Appuyez sur Entrée pour continuer. - Sélectionnez 2 pour Oui. Si vous choisissez Oui, vous acceptez de sauvegarder le fichier manuellement.

Le programme d'installation définit des autorisations différentes pour le répertoire et les fichiers dans le répertoire. Pour plus d'informations sur les autorisations relatives au fichier de clé de cryptage et au répertoire, voir ["Sécuriser les fichiers et les répertoires" à la page 94](#).

La section **Configuration de domaine et de nœud** s'affiche.

Configurer le domaine et le nœud

Après avoir configuré la clé de chiffrement, vous pouvez configurer le domaine et le nœud.

1. 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	<p>Nom du domaine Informatica à créer. Le nom de domaine par défaut est Domain_<MachineName>.</p> <p>Le nom ne doit pas dépasser 128 caractères et doit être en ASCII 7 bits uniquement. Le nom ne peut pas contenir d'espace, ni les caractères spéciaux suivants : ` % * + ; " ? , < > \ /</p>
Nom de nœud	Nom du nœud à créer.
Nom d'hôte de nœud	<p>Nom d'hôte ou adresse IP de la machine sur laquelle créer le nœud.</p> <p>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.</p> <p>Remarque: Le nom d'hôte de nœud ne peut pas contenir le caractère de soulignement (_). N'utilisez pas localhost. Le nom d'hôte doit explicitement identifier la machine.</p>

Propriété	Description
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.

2. Indiquez si vous souhaitez activer la complexité du mot de passe pour sécuriser les données sensibles dans le domaine.

Le tableau suivant décrit la complexité du mot de passe :

Propriété	Description
Complexité du mot de passe	Indiquez si vous souhaitez activer la complexité du mot de passe. 1 - Oui 2 - Non Si vous sélectionnez Oui, le mot de passe doit respecter les critères suivants : Il doit contenir au moins huit caractères, au moins un caractère alphabétique, un caractère numérique et un caractère spécial.
Configurer la stratégie des mots de passe	Indiquez si vous souhaitez configurer une stratégie des mots de passe. 1 - Oui 2 - Non Si vous sélectionnez Oui, vous pouvez configurer des règles de complexité du mot de passe. Si vous sélectionnez Non, les règles de stratégie des mots de passe par défaut d'Informatica s'appliquent.
Nombre de caractères spéciaux	Nombre minimal de caractères spéciaux requis dans un mot de passe. Vous pouvez également utiliser les caractères spéciaux suivants : " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~] Vous pouvez entrer une valeur entre 0 et 128. La valeur par défaut est de 1.
Nombre de caractères alphabétiques	Nombre minimal de caractères alphabétiques requis dans un mot de passe. Vous pouvez entrer une valeur entre 0 et 128. La valeur par défaut est de 1.
Nombre de caractères numériques	Nombre minimal de caractères numériques requis dans un mot de passe. Vous pouvez entrer une valeur entre 0 et 128. La valeur par défaut est de 1.
Longueur minimale du mot de passe	Nombre minimal de caractères requis dans un mot de passe. Vous pouvez entrer une valeur entre 1 et 128. La valeur par défaut est de 8.

Propriété	Description
Nombre de mots de passe précédents à stocker	Nombre de mots de passe précédents consécutifs ne pouvant pas être réutilisés. Vous pouvez entrer une valeur entre 0 et 12. La valeur par défaut est de 0.
Expiration du mot de passe en jours	Durée de validité d'un mot de passe. Pour éviter l'expiration des mots de passe, définissez la valeur sur 0. La valeur par défaut est de 0.
Mot de passe du domaine	Mot de passe de l'administrateur du domaine. <ul style="list-style-type: none"> - Si vous n'activez pas la complexité du mot de passe, ce dernier doit comporter entre 2 et 16 caractères. - Si vous l'activez, le mot de passe doit comporter au minimum huit caractères et contenir au moins un caractère alphabétique, un caractère numérique et un caractère spécial. - Si vous configurez une stratégie des mots de passe, le mot de passe doit respecter les règles de complexité que vous avez définies. Ce champ n'est pas disponible si vous configurez le domaine Informatica afin qu'il s'exécute sur un réseau avec l'authentification Kerberos.
Confirmer le mot de passe	Saisissez une nouvelle fois le mot de passe pour le confirmer. Ce champ n'est pas disponible si vous configurez le domaine Informatica afin qu'il s'exécute sur un réseau avec l'authentification Kerberos.

3. 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.

4. 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.

Le tableau suivant décrit les ports que vous pouvez définir :

Port	Description
Port de gestionnaire de service	Numéro de port utilisé par le Gestionnaire de service sur le nœud. Le gestionnaire de service écoute les demandes de connexions entrantes sur ce port. Les applications clientes utilisent ce port pour communiquer avec les services du domaine. Les programmes de ligne de commande Informatica utilisent ce port pour communiquer avec le domaine. Il s'agit également du port pour 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.

5. Indiquez si vous souhaitez créer les services d'application Enterprise Data Catalog.
Appuyez sur 1 pour créer les services d'application ou appuyez sur 2 si vous souhaitez créer les services d'application à partir de l'outil Administrator tool.
6. Indiquez si vous souhaitez créer un service de référentiel modèle de surveillance pour surveiller les statistiques de domaine.
Appuyez sur 1 pour créer un service de référentiel modèle de surveillance ou appuyez sur 2 si vous souhaitez créer un service de référentiel modèle de surveillance à partir de l'outil Administrator tool.
7. Indiquez si vous souhaitez créer un service de gestion de contenu pour la découverte de domaines de données.
Appuyez sur 1 pour créer un service de gestion de contenu ou appuyez sur 2 si vous souhaitez créer un service de gestion de contenu à partir de l'outil Administrator tool.
8. Indiquez si vous souhaitez configurer une connexion de l'entrepôt de profilage.
Appuyez sur 1 pour configurer une connexion d'entrepôt de profilage ou appuyez sur 2 si vous souhaitez configurer une connexion d'entrepôt de profilage à partir de l'outil Administrator tool.
9. Indiquez si vous souhaitez créer une configuration de cluster pour permettre au service d'intégration de données de transmettre la logique de mappage au cluster.
Appuyez sur 1 pour créer une configuration de cluster ou appuyez sur 2 si vous souhaitez créer une configuration de cluster à partir de l'outil Administrator tool.

10. Indiquez si vous souhaitez créer un service d'accès aux métadonnées Informatica.

Appuyez sur 1 pour créer un service d'accès aux métadonnées Informatica ou appuyez sur 2 si vous souhaitez créer un service d'accès aux métadonnées Informatica à partir de l'outil Administrator tool.

11. Indiquez si vous souhaitez configurer le référentiel pour MetaDex.

Appuyez sur 1 pour configurer le référentiel MetaDex, ou appuyez sur 2 si vous souhaitez le configurer après l'installation à l'aide des étapes spécifiées dans la section ["Configurer le référentiel MetaDex" à la page 252](#).

Si vous avez sélectionné l'option de configuration du référentiel pour MetaDex, configurez les propriétés suivantes :

Propriété	Description
Type de base de données	Spécifiez la base de données à configurer comme référentiel pour MetaDex. Vous pouvez sélectionner l'une des options suivantes : <ul style="list-style-type: none">- Oracle- SQLServer
Nom d'utilisateur de la base de données	Nom d'utilisateur configuré pour accéder à la base de données avant la mise à niveau.
Mot de passe de la base de données	Mot de passe configuré pour le nom d'utilisateur.
Nom du schéma	Non applicable si vous avez sélectionné Oracle comme base de données. Spécifiez le schéma à utiliser.
La base de données est-elle sécurisée ?	Spécifiez si la base de données est activée pour SSL.
Chemin d'accès au fichier truststore de la base de données	S'applique si vous avez spécifié que la base de données est activée pour SSL. Fournissez le chemin d'accès complet au fichier truststore de la base de données.
Mot de passe du truststore	S'applique si vous avez spécifié que la base de données est activée pour le mot de passe SSL pour accéder au fichier truststore.
Paramètres JDBC sécurisés	S'applique si vous avez spécifié que la base de données est activée pour SSL. Spécifiez les paramètres de base de données sécurisés, comme indiqué dans l'exemple suivant : <code>EncryptionMethod=SSL; HostNameInCertificate=ORATLS.informatica.com; ValidateServerCertificate=true; CryptoProtocolVersion=TLSv1.2;</code> Enterprise Data Catalog ajoute les paramètres JDBC sécurisés à la chaîne de connexion JDBC. Si vous incluez les paramètres JDBC sécurisés directement dans la chaîne de connexion, n'entrez aucun paramètre dans le champ Paramètres JDBC sécurisés.

Propriété	Description
Chaîne de connexion JDBC	<p>Chaîne de connexion JDBC pour la connexion à la base de données. Utilisez les formats suivants pour spécifier les chaînes de connexion :</p> <ul style="list-style-type: none"> - Oracle. jdbc:Informatica:oracle ://<host name>:<port number>;ServiceName= - SQLServer. jdbc:Informatica: sqlserver://<host name>:<portnumber>;SelectMethod=cursor;DatabaseName=
Port de serveur du référentiel MetaDex	Port unique du serveur de référentiel MetaDex. La valeur par défaut est de 48 090.
Activer la communication sécurisée pour le référentiel MetaDex ?	Spécifiez si TLS est activé pour la communication avec le référentiel.
Certificats SSL pour sécuriser le référentiel MetaDex ?	<p>Indiquez si vous souhaitez utiliser les certificats SSL par défaut ou les certificats SSL personnalisés pour sécuriser le référentiel. Spécifiez les propriétés suivantes si vous souhaitez utiliser les certificats SSL personnalisés :</p> <ul style="list-style-type: none"> - Type de keystore. Spécifiez le type de keystore. - Alias du keystore. Alias unique permettant d'accéder à l'entrée du keystore. - Fichier keystore. Spécifiez le fichier keystore qui contient les clés et les certificats requis. - Mot de passe du keystore. Mot de passe pour accéder au fichier keystore.
Nom d'utilisateur de domaine	<p>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 pour le nom d'utilisateur :</p> <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 d'utilisateur du domaine	Mot de passe de l'administrateur du domaine. Le mot de passe peut comprendre de 3 à 128 caractères maximum.
Nom de domaine de sécurité	Nom du domaine de sécurité pour l'administrateur du domaine.
Nom de domaine	<p>Nom du domaine que Metadex utilise pour établir la connexion. Requis si le fichier domains.infra spécifie plusieurs domaines. 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 :</p> <p>` % * + ; " ? , < > \ /</p>

Si vous choisissez de créer des services d'application Enterprise Data Catalog, la section **Base de données du référentiel modèle** s'affiche. Si vous choisissez de ne pas créer de services d'application Enterprise Data Catalog, la section **Récapitulatif de post-installation** indique si l'installation s'est terminée correctement. Le récapitulatif présente également le statut des composants installés et leur configuration. Vous pouvez afficher les fichiers journaux de l'installation pour obtenir plus d'informations sur les tâches effectuées par le programme d'installation et pour afficher les propriétés de configuration pour les composants installés.

Configurer la base de données du référentiel modèle

Après avoir configuré le domaine et le nœud, vous pouvez configurer les propriétés de la base de données du référentiel modèle.

1. Entrez le nom du service de référentiel modèle.

Entrez le 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 :

` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ()] [

Vous ne pouvez pas modifier le nom du service après sa création.

Si vous avez sélectionné le SPN au niveau des processus, spécifiez le fichier keytab du service de référentiel modèle. Fichier keytab du processus de service de référentiel modèle. Le fichier keytab doit être nommé : .keytab

2. Sélectionnez la base de données pour configurer la base de données du référentiel modèle.

Le tableau suivant répertorie les types de base de données pour le référentiel modèle :

Invite	Description
Type de base de données	Type de base de données du référentiel modèle. Sélectionnez parmi les options suivantes : 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - PostgreSQL

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

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

Propriété	Description
ID d'utilisateur de la base de données	Nom du compte d'utilisateur de la base de données du référentiel modèle. Vous pouvez entrer le nom d'utilisateur de Windows NT pour une connexion approuvée sur Microsoft SQL Server.
Mot de passe utilisateur	Mot de passe du compte d'utilisateur du référentiel modèle. Vous pouvez entrer le mot de passe de Windows NT pour une connexion approuvée sur Microsoft SQL Server.

4. Indiquez si vous souhaitez créer une base de données de référentiel modèle sécurisée.

Vous pouvez créer un service de référentiel modèle dans une base de données sécurisée avec le protocole SSL. Pour créer un service de référentiel modèle dans une base de données sécurisée, appuyez sur 1 et passez à l'étape de saisie des informations de connexion JDBC.

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

5. Si vous ne créez pas de référentiel modèle sécurisé, 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	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. Indiquez si vous souhaitez spécifier un espace de table : 1 - Non 2 - Oui
Espace de table	Nom de l'espace de table dans lequel les tables sont créées. 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, 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 non partitionné qui se trouve dans la partition du catalogue de la base de données.

- b. Si vous sélectionnez Microsoft SQL Server ou PostgreSQL, 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 ou PostgreSQL :

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.
Nom du service de la base de données	Nom du service ou de la base de données : - Oracle : entrez le nom de service. - Microsoft SQL Server : entrez le nom de la base de données. - IBM DB2 : entrez le nom de service. - PostgreSQL : entrez le nom de la base de données.
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 dans la chaîne de connexion JDBC :

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Utilisez la chaîne de connexion suivante pour vous connecter à la base de données Oracle via le gestionnaire de connexions Oracle :

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server avec les informations d'identification de Windows NT

Si vous avez spécifié les informations d'identification de Windows NT pour la base de données du référentiel modèle sur Microsoft SQL Server, spécifiez la syntaxe de la chaîne de connexion pour inclure la méthode d'authentification NTLM.

Microsoft SQL Server qui utilise l'instance par défaut avec les informations d'identification de Windows NT :

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server qui utilise l'instance nommée avec les informations d'identification de Windows NT :

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Azure SQL Database avec authentification Active Directory

```
"jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;Authentication Method=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

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

La section **Paramètres de service** s'affiche.

Configurer la base de données du référentiel modèle de surveillance

Si vous avez choisi de créer un service de référentiel modèle de surveillance, vous pouvez fournir des informations de connexion sur la base de données du référentiel.

1. Entrez le nom du service de référentiel modèle de surveillance.

Entrez le 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 :

```
` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( ) ] [
```

Vous ne pouvez pas modifier le nom du service après sa création.

Si vous avez sélectionné le SPN au niveau des processus, spécifiez le fichier keytab du service de référentiel modèle de surveillance. Fichier keytab du processus de service de référentiel modèle de surveillance. Le fichier keytab doit être nommé : .keytab

2. Sélectionnez la base de données du référentiel modèle de surveillance.

Le tableau suivant répertorie les types de base de données pour le référentiel modèle de surveillance :

Invite	Description
Type de base de données	Type de base de données du référentiel modèle de surveillance. Sélectionnez parmi les options suivantes : 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - PostgreSQL

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

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

Propriété	Description
ID d'utilisateur de la base de données	Nom du compte d'utilisateur de la base de données du référentiel modèle de surveillance. Vous pouvez entrer le nom d'utilisateur de Windows NT pour une connexion approuvée sur Microsoft SQL Server.
Mot de passe utilisateur	Mot de passe du compte d'utilisateur de la base de données du référentiel modèle de surveillance. Vous pouvez entrer le mot de passe de Windows NT pour une connexion approuvée sur Microsoft SQL Server.

4. Indiquez si vous souhaitez créer un référentiel modèle de surveillance sécurisé.

Vous pouvez créer un référentiel modèle de surveillance dans une base de données sécurisée à l'aide du protocole SSL. Pour créer un référentiel modèle de surveillance dans une base de données sécurisée, appuyez sur 1 et passez à l'étape de saisie des informations de connexion JDBC.

Pour créer un référentiel modèle de surveillance dans une base de données non sécurisée, appuyez sur 2.

5. Si vous ne créez pas de référentiel modèle de surveillance sécurisé, 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	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. Indiquez si vous souhaitez spécifier un espace de table : 1 - Non 2 - Oui
Espace de table	Nom de l'espace de table dans lequel les tables sont créées. 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, 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 non partitionné qui se trouve dans la partition du catalogue de la base de données.

- b. Si vous sélectionnez Microsoft SQL Server ou PostgreSQL, 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 ou PostgreSQL :

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.
Nom du service de la base de données	Nom du service ou de la base de données : - Oracle : entrez le nom de service. - Microsoft SQL Server : entrez le nom de la base de données. - IBM DB2 : entrez le nom de service. - PostgreSQL : entrez le nom de la base de données.
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 dans la chaîne de connexion JDBC :

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Utilisez la chaîne de connexion suivante pour vous connecter à la base de données Oracle via le gestionnaire de connexions Oracle :

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server avec les informations d'identification de Windows NT

Si vous avez spécifié les informations d'identification de Windows NT pour la base de données du référentiel modèle sur Microsoft SQL Server, spécifiez la syntaxe de la chaîne de connexion pour inclure la méthode d'authentification NTLM.

Microsoft SQL Server qui utilise l'instance par défaut avec les informations d'identification de Windows NT :

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server qui utilise l'instance nommée avec les informations d'identification de Windows NT :

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
```

Azure SQL Database avec authentification Active Directory

```
jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Sybase

```
jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
```

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

La section **Paramètres de service** s'affiche.

Configurer les paramètres du service d'intégration de données

Après avoir configuré la base de données du référentiel modèle, vous pouvez configurer les paramètres du service d'intégration de données.

1. Entrez les informations de paramètre de service suivantes :

Port	Description
Nom du service d'intégration de données	Nom du service d'intégration de données à créer dans le domaine Informatica.
Type de protocole HTTP	Type de connexion au service d'intégration de données. Sélectionnez l'une des options suivantes : <ul style="list-style-type: none">- HTTP. Les demandes effectuées auprès du service utilisent une connexion HTTP.- HTTPS. Les demandes effectuées auprès du service utilisent une connexion HTTP sécurisée.- HTTP & HTTPS. Les demandes effectuées auprès du service peuvent utiliser une connexion HTTP ou HTTPS.
Port HTTP	Numéro de port à utiliser pour le service d'intégration de données. La valeur par défaut est 9085.
Port HTTPS	Numéro de port à utiliser pour le service d'intégration de données. La valeur par défaut est 9085.

2. Sélectionnez les certificats SSL à utiliser pour sécuriser le service d'intégration de données.

Option	Description
Utiliser les fichiers de certificat SSL Informatica par défaut	Utilisez les certificats SSL Informatica par défaut contenus dans le keystore et le truststore par défaut. 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.
Utiliser les certificats SSL personnalisés	Utilisez les certificats SSL personnalisés. 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.

Si vous choisissez d'utiliser des certificats SSL personnalisés, entrez les informations suivantes.

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

3. Voulez-vous activer la récupération de Data Engineering pour le service d'intégration de données ?

- Oui
- Non

Si vous choisissez Oui, vous pouvez récupérer les tâches de mappage que le service d'intégration de données transmet au moteur Spark pour le traitement. La valeur par défaut est Non.

4. Voulez-vous créer une configuration de cluster ?

La configuration du cluster permet au service d'intégration de données de transmettre (en push) la logique de mappage au cluster. En cas d'intégration à un environnement Hadoop ou Databricks, vous pouvez créer une configuration de cluster.

Appuyez sur 1 pour créer une configuration de cluster.

Appuyez sur 2 pour ne pas la créer. La valeur par défaut est 1.

Remarque: Pour créer une configuration de cluster de l'environnement Databricks, utilisez l'outil Administrator tool à la fin de l'installation.

Pour créer les services Enterprise Data Preparation lors de l'installation, vous devez créer une configuration de cluster. Reportez-vous ensuite au *Guide de Data Engineering Integration* pour intégrer pleinement le domaine à l'environnement Hadoop.

5. Indiquez si vous souhaitez configurer la connexion de l'entrepôt de profilage.

- Appuyez sur **1** pour configurer la connexion de l'entrepôt de profilage.
- Appuyez sur **2** pour ignorer la configuration de la connexion de l'entrepôt de profilage.
- Si vous choisissez de configurer la connexion de l'entrepôt de profilage, la section **Base de données de connexion de l'entrepôt de profilage** s'affiche.
- Si vous choisissez d'ignorer la connexion à l'entrepôt de profilage, la section **Récapitulatif de post-installation** indique si l'installation s'est terminée correctement. Le récapitulatif présente également le statut des composants installés et leur configuration.

6. Indiquez si vous souhaitez configurer le service de gestion de contenu pour la découverte de domaines de données.

- Appuyez sur **1** pour configurer le service de gestion de contenu pour la découverte de domaines de données.
- Appuyez sur **2** pour ignorer la configuration du service de gestion de contenu pour la découverte de domaines de données.
- Si vous choisissez de configurer le service de gestion de contenu pour la découverte de domaines de données, la section **Paramètres et base de données du service de gestion de contenu** s'affiche.

- d. Si vous choisissez d'ignorer la configuration du service de gestion de contenu pour la découverte de domaines de données, la section **Récapitulatif de post-installation** indique si l'installation s'est terminée correctement. Le récapitulatif présente également le statut des composants installés et leur configuration.

Créer la configuration du cluster

Créez la configuration de cluster, qui contient les informations de configuration sur l'environnement non natif. La configuration de cluster permet au service d'intégration de données de transmettre les travaux à l'environnement non natif. Créez une configuration de cluster si vous prévoyez d'utiliser Enterprise Data Preparation.

Vous pouvez importer des propriétés de configuration à partir de l'environnement non natif pour créer une configuration du cluster. Vous pouvez importer les propriétés à partir d'un fichier d'archive créé par l'administrateur Hadoop, ou vous pouvez les importer directement à partir du cluster.

Lorsque vous créez la configuration du cluster, vous pouvez également choisir de créer des connexions Hadoop, HDFS, Hive, HBase ou Databricks à l'environnement non natif. Le programme d'installation ajoute le type de connexion au nom de configuration du cluster pour créer chaque nom de connexion.

1. Entrez le nom de la configuration de cluster à créer.
2. Spécifiez la distribution non native du cluster.

Le tableau suivant décrit les propriétés que vous pouvez spécifier :

Invite	Description
1	Cloudera. Vous pouvez créer une configuration de cluster Cloudera sur Cloudera Data Platform (CDP) ou pour Cloudera Distribution Hadoop (CDH).
2	Hortonworks
3	Azure HDInsight
4	MapR. Vous devez importer les propriétés de configuration du cluster MapR à partir d'un fichier d'archive.
5	Amazon EMR. Vous devez importer les propriétés de configuration du cluster Amazon EMR à partir d'un fichier d'archive.
6	Databricks
7	Google Dataproc

Remarque: Avant d'importer les propriétés de configuration du cluster Amazon EMR, vérifiez que les ports suivants associés à Amazon EMR sont disponibles :

Composant Hadoop	Port
Lecture HDFS	50010
Écriture HDFS	50020

Composant Hadoop	Port
Metastore Hive	9083
HiveServer	10000
MySQL	3306
NameNode	8020
ResourceManager	8050
Application Web ResourceManager	8088
ResourceTracker	8031
Adresse du planificateur	8030
Shuffle HTTP	13562
ZooKeeper	2181

3. Importez les propriétés de configuration à partir de l'environnement non natif pour créer la configuration du cluster.
 - Pour importer les propriétés à partir d'un fichier d'archive, appuyez sur **1**. Si vous créez une configuration de cluster pour un cluster Amazon EMR, MapR ou Google Dataproc, vous devez importer les propriétés à partir d'un fichier d'archive.
 - Pour importer les propriétés directement à partir du cluster, appuyez sur **2**.
4. Si vous choisissez d'importer les propriétés à partir d'un fichier d'archive, vous devez choisir le nom de fichier d'archive de configuration et le chemin d'accès au fichier.
5. Si vous choisissez d'importer les propriétés directement à partir du cluster, spécifiez les propriétés de la connexion.

Le tableau suivant décrit les propriétés de cluster Cloudera, Hortonworks ou Azure HDInsight que vous spécifiez :

Propriété	Description
Hôte	Le nom d'hôte ou l'adresse IP du gestionnaire de cluster.
Port	Port du gestionnaire de cluster.
ID d'utilisateur	Nom d'utilisateur du cluster.
Mot de passe	Mot de passe de l'utilisateur du cluster.

Propriété	Description
Nom de cluster	Nom du cluster. Utilisez le nom complet si le gestionnaire de cluster gère plusieurs clusters. Si vous ne spécifiez pas de nom de cluster, l'assistant importe des informations en fonction du cluster par défaut.
Type de moteur	Si vous avez spécifié un cluster Cloudera, le programme d'installation vous demande le type de moteur. Si vous vous trouvez sur un cluster CDP, acceptez le type de moteur par défaut de Tez. Si vous vous trouvez sur un cluster CDH, appuyez sur 2 pour définir le type de moteur sur MRv2. La valeur par défaut est 1 .

- Pour créer les connexions Hadoop, HDFS, Hive, HBase ou Databricks au cluster, appuyez sur **1**.

Le programme d'installation ajoute le type de connexion au nom de configuration du cluster pour créer un nom de connexion.

Configurer Enterprise Data Catalog

Cette tâche inclut les invites du programme d'installation pour la configuration d'Enterprise Data Catalog. Vous fournirez des informations de base pour configurer les services d'application et le cluster Hadoop.

Une fois que vous aurez effectué les tâches préliminaires, vous suivrez les invites du programme d'installation pour configurer Enterprise Data Catalog.

Configurer les détails de la base de données de l'entrepôt de profilage

Si vous avez choisi de configurer les paramètres de service, vous pouvez fournir des informations sur l'entrepôt.

- Sélectionnez le type de base de données pour l'entrepôt de profilage.

Le tableau suivant répertorie le type de base de données pour l'entrepôt de profilage.

Invite	Description
Type de base de données	Type de base de données pour la connexion de l'entrepôt de profilage. Sélectionnez parmi les options suivantes : 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2

- Entrez les propriétés de la base de données et du compte 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 utilisateur de la base de données de l'entrepôt de profilage.
Mot de passe utilisateur	Mot de passe du compte utilisateur de la base de données entrepôt de profilage.

3. En fonction du type de base de données sélectionné, 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	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. Indiquez si vous souhaitez spécifier un espace de table : 1 - Non 2 - Oui
Espace de table	Nom de l'espace de table dans lequel les tables sont créées. 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, 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 non partitionné qui se trouve dans la partition du 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
Adresse de la base de données	Nom d'hôte et numéro de port de la base de données.
Nom du service de la base de données	Nom du service ou de la base de données : <ul style="list-style-type: none">- Oracle : entrez le nom de service.- Microsoft SQL Server : entrez le nom de la base de données.- IBM DB2 : entrez le nom de service.
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 dans la chaîne de connexion JDBC :

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=
```

Microsoft Azure SQL Database

```
jdbc:Informatica:sqlserver://  
host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net  
;ValidateServerCertificate=false
```

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

e. Entrez la chaîne de connexion d'accès aux données.

La section **Paramètres et base de données du service de gestion de contenu** s'affiche.

Configurer les paramètres et la base de données du service de gestion de contenu

Après avoir configuré l'entrepôt de profilage, vous pouvez configurer les paramètres du service de gestion de contenu et les propriétés de la base de données.

1. Entrez le nom du service de gestion de contenu.
2. Entrez les informations de paramètre de service suivantes :

Port	Description
Type de protocole HTTP	Type de connexion au service d'intégration de données. Sélectionnez l'une des options suivantes : <ul style="list-style-type: none">- HTTP. Les demandes effectuées auprès du service utilisent une connexion HTTP.- HTTPS. Les demandes effectuées auprès du service utilisent une connexion HTTP sécurisée.
Port HTTP	Numéro de port utilisé pour le service de gestion de contenu. La valeur par défaut est 8105.
Port HTTPS	Numéro de port à utiliser pour le service de gestion de contenu. La valeur par défaut est 8105.

3. Si vous sélectionnez un keystore pour le service de gestion de contenu, entrez le fichier keystore et le numéro de port pour la connexion HTTPS au service de gestion de contenu.

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.

- Utilisez le keystore par défaut généré par le programme d'installation.
- Spécifiez l'emplacement et le mot de passe d'un fichier keystore personnalisé.

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 : <Informatica installation directory>/tomcat/conf/

Les types de certificats du keystore pour le service de gestion de contenu dépendent des types de certificats utilisés par l'outil Administrator tool :

- Si vous avez utilisé le certificat de keystore par défaut pour l'outil Administrator tool, vous pouvez utiliser le certificat de keystore par défaut ou personnalisé pour le service de gestion de contenu.
- Si vous avez utilisé un certificat de keystore personnalisé pour l'outil Administrator tool, vous devez utiliser un certificat de keystore personnalisé pour le service de gestion de contenu.

4. Entrez les informations de la base de données de l'entrepôt de données de référence.

Le tableau suivant répertorie les informations de la base de données de l'entrepôt de données de référence.

Invite	Description
Type de base de données	Type de base de données pour l'entrepôt de données de référence. Sélectionnez parmi les options suivantes : 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2

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

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

Propriété	Description
ID d'utilisateur de la base de données	Nom du compte d'utilisateur de la base de données de l'entrepôt de données de référence.
Mot de passe utilisateur	Mot de passe du compte d'utilisateur de la base de données de l'entrepôt de profilage.

6. En fonction du type de base de données sélectionné, 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	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. Indiquez si vous souhaitez spécifier un espace de table : 1 - Non 2 - Oui
Espace de table	Nom de l'espace de table dans lequel les tables sont créées. 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, 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 non partitionné qui se trouve dans la partition du 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
Adresse de la base de données	Nom d'hôte et numéro de port de la base de données.
Nom du service de la base de données	Nom du service ou de la base de données : - Oracle : entrez le nom de service. - Microsoft SQL Server : entrez le nom de la base de données. - IBM DB2 : entrez le nom de service.
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 dans la chaîne de connexion JDBC :

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=
```

Microsoft Azure SQL Database

```
jdbc:Informatica:sqlserver://  
host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net  
;ValidateServerCertificate=false
```

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

- Entrez la chaîne de connexion d'accès aux données.

La section **Options de cluster et de service d'application** s'affiche.

Créer et configurer le service de cluster Informatica

- Configurez les propriétés suivantes pour créer le service de cluster Informatica :

Propriété	Description
Nom d'utilisateur de l'hôte de passerelle	Nom d'utilisateur de l'hôte de la passerelle. L'utilisateur de la passerelle doit être un utilisateur non-racine avec un accès sudo. Vous devez activer SSH sans mot de passe pour les nœuds suivants : - Entre le domaine Informatica et l'hôte de passerelle pour l'utilisateur de la passerelle. - Entre l'hôte de passerelle et les nœuds de données, et les nœuds de traitement. - Si vous prévoyez d'activer la configuration avancée pour le service, activez SSH sans mot de passe entre le nœud de passerelle et les nœuds de service.
Entrer le nom du service de cluster Informatica	Nom du service. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Il ne peut pas dépasser 128 caractères ni commencer par @. Il ne peut pas non plus contenir d'espaces. Les caractères inclus dans le nom doivent être compatibles avec la page de codes du référentiel modèle. Le nom ne peut pas contenir les caractères spéciaux suivants : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Hôte de passerelle du cluster Informatica	Nom de domaine complet du nœud à configurer comme hôte de passerelle. Le nœud que vous configurez comme hôte de passerelle doit être un nœud de données ou un nœud de traitement.

Propriété	Description
Activer la configuration avancée	Sélectionnez 2 si vous souhaitez configurer les propriétés des applications et des services associés. Si vous sélectionnez 2, les services associés utilisent les valeurs que vous spécifiez pour eux au lieu d'utiliser les valeurs spécifiées pour les nœuds de données. Fournissez les paramètres répertoriés dans la section "Configuration avancée du service de cluster Informatica" à la page 245 .
Nœuds de données	Liste de noms de domaine complets de nœuds séparée par des virgules à configurer comme nœuds de données.
Nœuds de traitement	Liste de noms de domaine complets de nœuds séparée par des virgules à configurer comme nœuds de traitement.
Activer TLS (Transport Layer Security)	Sélectionnez cette option pour activer TLS du service de cluster Informatica.
Entrer le port HTTPS du service de cluster Informatica	Numéro de port de la connexion HTTPS. Requis si vous avez sélectionné l'option Activer TLS (Transport Layer Security) .
Activer la communication sécurisée pour le service	Sélectionnez 1 pour utiliser les certificats SSL Informatica par défaut ou sélectionnez 2 pour utiliser les certificats SSL personnalisés. Si le domaine Informatica est activé pour SSL, vous devez fournir les détails suivants : <ul style="list-style-type: none"> - Port HTTPS. Port HTTPS pour accéder au nœud de domaine Informatica. - Fichier keystore Informatica. Chemin d'accès complet au fichier keystore de domaine Informatica. - Mot de passe du keystore. Mot de passe du fichier keystore.
Protocole SSL à utiliser	Facultatif. Fournissez le protocole SSL à utiliser pour le service.
Activer la configuration avancée de Data Privacy Management	Non applicable si vous ne configurez pas un Service Data Privacy Management.
Répertoire personnalisé de cluster	Répertoire du service. La valeur par défaut est <code>/opt/informatica/ics</code>

- Appuyez sur **Entrée**.

Créer et configurer le service de catalogue

- Configurez les propriétés suivantes pour créer le service de catalogue :

Propriété	Description Catalogue
Nom du service de catalogue	Nom du service. Le nom n'est pas sensible à la casse et doit être unique dans le domaine. Il ne peut pas dépasser 128 caractères ni commencer par @. Il ne peut pas non plus contenir d'espaces. Les caractères 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 : ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [
Port HTTPS du service de catalogue	S'applique si le domaine Informatica est activé pour SSL. Numéro de port de la connexion HTTPS.
Voulez-vous activer la communication sécurisée pour le service ?	Sélectionnez 1 pour utiliser les certificats SSL par défaut ou sélectionnez 2 pour utiliser les certificats SSL personnalisés. Si le domaine Informatica est activé pour SSL, vous devez fournir les détails suivants : - Port HTTPS. Port HTTPS pour accéder au nœud de domaine Informatica. - Fichier keystore Informatica. Chemin d'accès complet au fichier keystore de domaine Informatica. - Mot de passe du keystore. Mot de passe du fichier keystore.
Voulez-vous activer les notifications par e-mail de modification des actifs ?	Sélectionnez 2 pour recevoir des notifications par e-mail en cas de mises à jour pour les actifs.
Voulez-vous activer l'analyse des actifs de données ?	Sélectionnez 2 pour activer l'analyse des actifs de données.

- Appuyez sur **Entrée**.
- Configurez les propriétés suivantes si vous avez activé l'analyse des actifs de données :

Propriété	Description
Sélectionner une base de données	Sélectionnez la base de données du référentiel à utiliser pour l'analyse des actifs de données parmi les options suivantes : - Oracle - SQLServer - PostgreSQL
Nom d'utilisateur	Nom d'utilisateur de la base de données du référentiel.
Mot de passe	Mot de passe du nom d'utilisateur de la base de données.

Propriété	Description
Chaîne de connexion de la base de données	<p>Entrez la chaîne de connexion JDBC permettant de se connecter à la base de données du référentiel.</p> <p>Utilisez la syntaxe suivante pour la chaîne de connexion selon la base de données sélectionnée :</p> <ul style="list-style-type: none"> - Oracle. <code>jdbc:informatica:oracle://<host name>:<port number>;ServiceName=<database name></code> - SQLServer : <ul style="list-style-type: none"> - SQL Server. <code>jdbc:informatica:sqlserver://<host name>: <port number>;DatabaseName=<database name>;SnapshotSerializable=true</code> - PostgreSQL. <code>jdbc:informatica:postgresql://<host name>: <port number>;DatabaseName=<database name></code>
Paramètres JDBC sécurisés	<p>Si la base de données du référentiel est sécurisée avec le protocole SSL, vous devez entrer les paramètres de base de données sécurisés sous la forme de paires nom=valeur séparées par des points-virgules. Par exemple : <code>param1=value1;param2=value2</code></p>

Configurer le référentiel MetaDex

Configurez les propriétés suivantes pour créer le référentiel pour MetaDex.

- Si vous avez sélectionné l'option de configuration du référentiel pour MetaDex, configurez les propriétés suivantes :

Propriété	Description
Type de base de données	<p>Spécifiez la base de données à configurer comme référentiel pour MetaDex.</p> <p>Vous pouvez sélectionner l'une des options suivantes :</p> <ul style="list-style-type: none"> - Oracle - SQLServer
Nom d'utilisateur de la base de données	Nom d'utilisateur configuré pour accéder à la base de données avant la mise à niveau.
Mot de passe de la base de données	Mot de passe configuré pour le nom d'utilisateur.
Nom du schéma	Non applicable si vous avez sélectionné Oracle comme base de données. Spécifiez le schéma à utiliser.
La base de données est-elle sécurisée ?	Spécifiez si la base de données est activée pour SSL.

Propriété	Description
Chemin d'accès au fichier truststore de la base de données	S'applique si vous avez spécifié que la base de données est activée pour SSL. Fournissez le chemin d'accès complet.
Mot de passe du truststore	S'applique si vous avez spécifié que la base de données est activée pour le mot de passe SSL pour accéder au fichier.
Paramètres JDBC sécurisés	S'applique si vous avez spécifié que la base de données est activée pour SSL. Spécifiez les paramètres de base de données suivants : <code>EncryptionMethod=SSL;HostNameInCertificate=ORATLS.informatica.com;ValidateServerCertificate=true</code> Remarque: Si vous souhaitez utiliser des paramètres sécurisés qui ne sont pas répertoriés par défaut, ajoutez-les à la chaîne de connexion JDBC. Enterprise Data Catalog ajoute les paramètres JDBC sécurisés à la chaîne de connexion JDBC. Si vous incluez les paramètres JDBC sécurisés, n'entrez aucun paramètre dans le champ Paramètres JDBC sécurisés.
Chaîne de connexion JDBC	Chaîne de connexion JDBC pour la connexion à la base de données. Utilisez les formats suivants pour spécifier les chaînes de connexion : <ul style="list-style-type: none"> - Oracle. <code>jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=</code> - SQLServer. <code>jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=</code>
Port de serveur du référentiel MetaDex	Port unique du serveur de référentiel MetaDex. La valeur par défaut est de 48 090.
Activer la communication sécurisée pour le référentiel MetaDex ?	Spécifiez si TLS est activé pour la communication avec le référentiel.
Certificats SSL pour sécuriser le référentiel MetaDex ?	Indiquez si vous souhaitez utiliser les certificats SSL par défaut ou les certificats SSL personnalisés pour sécuriser la communication avec le référentiel. Spécifiez les propriétés suivantes si vous souhaitez utiliser les certificats SSL personnalisés : <ul style="list-style-type: none"> - Type de keystore. Spécifiez le type de keystore. - Alias du keystore. Alias unique permettant d'accéder à l'entrée du keystore. - Fichier keystore. Spécifiez le fichier keystore qui contient les clés et les certificats requis. - Mot de passe du keystore. Mot de passe pour accéder au fichier keystore.
Nom d'utilisateur de domaine	Nom d'utilisateur de l'administrateur du domaine. Vous pouvez utiliser ce nom d'utilisateur pour vous connecter à la base de données. Utilisez les directives suivantes pour le nom d'utilisateur : <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'espace sont interdits.
Mot de passe d'utilisateur du domaine	Mot de passe de l'administrateur du domaine. Le mot de passe peut comprendre de 3 à 128 caractères maximum.

Propriété	Description
Nom de domaine de sécurité	Nom du domaine de sécurité pour l'administrateur du domaine.
Nom de domaine	Nom du domaine que Metadex utilise pour établir la connexion. Requis si le fichier domains.infa spécifie plusieurs doit être en ASCII 7 bits uniquement. Il ne peut pas contenir d'espaces ni les caractères spéciaux suivants : ` % * + ; " ? , < > \ /

CHAPITRE 10

Joindre un domaine avec des produits Catalog et Data Engineering

Ce chapitre comprend les rubriques suivantes :

- [Commencer l'installation, 175](#)
- [Configurer le domaine, 178](#)

Commencer l'installation

Cette tâche inclut les invites du programme d'installation pour le lancement de l'installation. Vous serez invité à fournir des informations de base telles que l'acceptation des conditions, l'option d'installation et le répertoire d'installation.

Lorsque vous effectuez les tâches préliminaires, vous suivez les invites du programme d'installation et fournissez les informations requises pour configurer le domaine.

Exécuter le programme d'installation

Effectuez les étapes suivantes pour exécuter le programme d'installation :

1. Connectez-vous à la machine à l'aide d'un compte d'utilisateur système.
2. Utilisez la commande suivante pour effacer la variable DISPLAY sur la machine : `unset DISPLAY`
3. Fermez toutes les autres applications.
4. Sur une ligne de commande shell, exécutez le fichier `install.sh`.
Le programme d'installation affiche un message vous invitant à vérifier que les variables d'environnement régionales sont définies.
5. Si les variables d'environnement ne sont pas définies, appuyez sur la touche **n** pour quitter le programme d'installation et définissez-les de façon appropriée.
Si les variables d'environnement sont définies, appuyez sur la touche **o** pour continuer.

Bienvenue - Accepter les conditions générales

- Lisez les termes et conditions d'installation d'Informatica et du kit de ressources d'utilisation du produit, puis sélectionnez **J'accepte les conditions générales**.
 - a. Appuyez sur **1** si vous ne souhaitez pas accepter les conditions générales.
 - b. Appuyez sur **2** pour accepter les conditions générales.

Les sections de **sélection des composants** s'affichent.

Choisissez l'option d'installation

Après avoir accepté les conditions générales, vous pouvez installer les services de domaine Informatica qui prennent en charge les produits Data Engineering et Catalog.

1. Appuyez sur **2** pour installer Informatica Enterprise Data Catalog.
2. Sélectionnez si la version actuelle des services du domaine Informatica est installée sur le nœud.
 - a. Appuyez sur **1** si la version actuelle des services de domaine Informatica n'est pas installée sur le nœud.
 - b. Appuyez sur **2** si la version actuelle des services du domaine Informatica est installée sur le nœud.
3. Indiquez si vous souhaitez installer les packages de distribution via le programme d'installation d'Informatica.
 - Appuyez sur **1** si vous n'avez pas besoin des packages de distribution ou si vous souhaitez les installer ultérieurement.
 - Appuyez sur **2** si vous souhaitez installer les packages de distribution via le programme d'installation.La valeur par défaut est 1.
4. Si vous choisissez d'installer les packages de distribution, sélectionnez un ou plusieurs packages à installer dans la liste. Séparez plusieurs packages par une virgule.
La valeur par défaut est 1.

La page **Pré-requis d'installation** affiche la configuration requise pour l'installation. Vérifiez que toute la configuration requise est correcte avant de poursuivre l'installation.

Adapter les services d'application

Après avoir examiné les prérequis d'installation, vous pouvez choisir d'adapter les services d'application pour de meilleures performances, en fonction du type de déploiement dans votre environnement. Si vous n'optimisez pas les services maintenant, vous pouvez le faire ultérieurement via infacmd.

1. Indiquez si vous souhaitez que le programme d'installation règle les services d'application :
 - Appuyez sur 1 pour ne pas régler les services. La section **Licence et répertoire d'installation** s'affiche.
 - Appuyez sur 2 pour régler les services.

Si vous joignez le nœud au domaine existant, assurez-vous que le type de déploiement que vous sélectionnez ici est le même type de déploiement que les nœuds de passerelle.

2. Sélectionnez le type de déploiement associé à l'environnement Informatica.

Type de déploiement	Espace disque par nœud	Total des cœurs virtuels	RAM par nœud
Sandbox	140 Go	16	32 Go
De base	140 Go	24	64 Go
Standard	140 Go	48	64 Go
Avancé	140 Go	96	128 Go

3. Indiquez si vous souhaitez modifier le type de déploiement ou continuer avec le type de déploiement actuel.
- Appuyez sur **1** pour modifier le type de déploiement.
 - Appuyez sur **2** pour continuer avec le type de déploiement actuel.

La section **Licence et répertoire d'installation** s'affiche.

Spécifier le répertoire d'installation

Après avoir vérifié les prérequis d'installation, vous pouvez spécifier le répertoire d'installation.

1. Saisissez le répertoire d'installation.

Les noms de répertoires du chemin d'accès ne doivent pas contenir d'espaces ni les caractères spéciaux suivants : @|* \$ # ! % () { } [] , ; ' La valeur par défaut est <répertoire de base utilisateur>/Informatica/10.5.6.

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.

2. Entrez le chemin et le nom de fichier de la clé de licence , puis appuyez sur **Entrée**.
3. Choisissez un environnement d'installation et appuyez sur **Entrée**.
- Appuyez sur **1** afin de définir l'environnement Sandbox pour un environnement de base utilisé comme preuve de concept avec un minimum d'utilisateurs.
 - Appuyez sur **2** afin de définir l'environnement de développement pour l'environnement de conception.
 - Appuyez sur **3** afin de définir l'environnement de test pour un traitement de gros volumes plus proche de celui d'un environnement de production.
 - Appuyez sur **4** afin de définir l'environnement de production pour un traitement de gros volumes avec des niveaux élevés d'accès concurrentiel destinés aux utilisateurs finaux. Les environnements de production avancés sont généralement des configurations à plusieurs nœuds.

La valeur par défaut est de 1 pour Sandbox.

4. Indiquez si vous souhaitez exécuter l'utilitaire de pré-validation.
- Appuyez sur **1** pour ignorer l'utilitaire de pré-validation.
 - Appuyez sur **2** pour exécuter l'utilitaire de pré-validation.

L'utilitaire vous aide à valider les prérequis de l'installation d'Enterprise Data Catalog.

Si vous choisissez d'ignorer l'utilitaire de pré-validation, la section **Récapitulatif de pré-installation** s'affiche. Examinez le récapitulatif d'installation.

Si vous choisissez d'exécuter l'utilitaire de pré-validation, la section Pré-validation s'affiche.

Configurer le domaine

Cette tâche inclut les invites du programme d'installation pour configurer le domaine. Vous serez invité à fournir des informations pour joindre un domaine et configurer la sécurité, le référentiel et la clé de chiffrement du domaine.

Une fois que vous aurez effectué ces tâches, vous procéderez à l'installation.

Configurer le domaine

Après avoir examiné le récapitulatif de pré-installation, vous pouvez entrer les informations sur le domaine.

1. Appuyez sur **2** pour joindre un domaine.
Le programme d'installation joint un nœud sur la machine sur laquelle vous effectuez l'installation.
2. 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.
3. Sélectionnez le type de nœud à créer.

Le tableau suivant décrit les types de nœud 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.

4. Spécifiez les détails de connexion à Informatica Administrator.
 - a. Indiquez si vous souhaitez définir une connexion HTTPS 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.

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 : <Informatica installation directory>/tomcat/conf/

- c. Si vous spécifiez le keystore, entrez le mot de passe et l'emplacement du fichier keystore.
- d. Si vous avez activé la communication sécurisée pour le domaine, la section **Sécurité du domaine - Communication sécurisée** s'affiche.
- e. Si vous n'avez pas activé la communication sécurisée pour le domaine, la section **Référentiel de configuration du domaine** s'affiche. Passez à l'étape ["Configurer le référentiel du domaine"](#) à la [page 181](#).
5. Choisissez d'activer ou non l'authentification SAML pour configurer la prise en charge de l'authentification unique (SSO) basée sur SAML (Security Assertion Markup Language) pour les applications Web Informatica dans un domaine Informatica.

Le tableau suivant décrit les informations que vous devez entrer pour activer l'authentification SAML :

Invite	Description
Le domaine utilise-t-il l'authentification SAML ?	Indiquez si le domaine utilise l'authentification SAML : 1 - Non Si vous sélectionnez Non, passez à "Sécurité de domaine" à la page 180 2 - Oui Si vous sélectionnez Oui, configurez l'authentification SAML.

6. Entrez l'URL du fournisseur d'identité du domaine.
7. Entrez le nom d'alias du certificat de signature d'assertion du fournisseur d'identité.
8. Indiquez si vous souhaitez utiliser les certificats SSL par défaut d'Informatica ou vos propres certificats SSL pour activer l'authentification SAML dans le domaine.

Le tableau suivant décrit les options de certificat SSL pour l'authentification SAML :

Option	Description
Utiliser le fichier de certificat SSL Informatica par défaut	Sélectionnez cette option pour utiliser le fichier par défaut d'Informatica truststore pour l'authentification SAML.
Spécifier l'emplacement du fichier de certificat SSL	Sélectionnez un fichier truststore personnalisé pour l'authentification SAML. Spécifiez le répertoire contenant le fichier truststore personnalisé sur les nœuds de passerelle dans le domaine. Spécifiez uniquement le répertoire et non le chemin complet du fichier.

9. Si vous fournissez les certificats de sécurité, spécifiez l'emplacement et les mots de passe des fichiers keystore et truststore.

Le tableau suivant décrit l'emplacement et le mot de passe du fichier truststore :

Propriété	Description
Répertoire truststore	Spécifiez le répertoire contenant le fichier truststore personnalisé sur les nœuds de passerelle dans le domaine. Spécifiez uniquement le répertoire et non le chemin complet du fichier.
Mot de passe truststore	Mot de passe du fichier truststore personnalisé.

La section **Sécurité du domaine - Communication sécurisée** s'affiche.

Sécurité de domaine

Après avoir configuré le domaine, vous pouvez configurer la sécurité de domaine.

- 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
Utiliser les certificats SSL Informatica par défaut	Utilisez les certificats SSL par défaut contenus dans le keystore et le truststore par défaut. 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.
Utiliser les certificats SSL personnalisés	Spécifiez le chemin des fichiers keystore et truststore qui contiennent les certificats SSL. Vous devez également spécifier les mots de passe du 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 qui contient les fichiers keystore. Le répertoire doit contenir des fichiers nommés infa_keystore.jks.
Mot de passe keystore	Mot de passe du fichier keystore infa_keystore.jks.
Répertoire de fichiers truststore	Répertoire qui contient 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.

Configurer le référentiel du domaine

Après avoir configuré le domaine, vous pouvez configurer le référentiel du domaine.

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

Sécurité du domaine - Clé de chiffrement

Après avoir configuré le référentiel de domaine, vous pouvez configurer la clé de chiffrement.

- Entrez le répertoire de la clé de chiffrement du domaine Informatica.

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

Invite	Description
Sélectionnez la clé de cryptage	<p>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.</p> <p>Si vous avez copié le fichier de clé de cryptage 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 cryptage dans le répertoire temporaire.</p>
Répertoire de la clé de cryptage	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.

Le programme d'installation définit des autorisations différentes pour le répertoire et les fichiers dans le répertoire. Pour plus d'informations sur les autorisations pour le fichier de clé de cryptage et le répertoire, consultez ["Sécuriser les fichiers et les répertoires" à la page 94](#).

La page **Joindre un domaine - Configuration de nœud** s'affiche.

Configurer le domaine et le nœud

Après avoir configuré la clé de chiffrement, vous pouvez configurer le domaine et le nœud.

1. Entrez les informations relatives au domaine et au nœud à joindre.

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

Propriété	Description
Nom d'hôte du nœud	Nom d'hôte du 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 à joindre.
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.
Fichier truststore de base de données	Chemin 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 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 sécurisée avec le protocole SSL.

- 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 port que vous entrez ne sont pas utilisés par d'autres applications.

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

Le tableau suivant décrit les ports que vous pouvez définir :

Port	Description
Port de gestionnaire de service	Numéro de port utilisé par le Gestionnaire de service sur le nœud. Le gestionnaire de service écoute les demandes de connexions entrantes sur ce port. Les applications clientes utilisent ce port pour communiquer avec les services du domaine. Les programmes de ligne de commande Informatica utilisent ce port pour communiquer avec le domaine. Il s'agit également du port pour 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.

La section **Récapitulatif de post-installation** indique si l'installation s'est correctement effectuée. Le récapitulatif présente également le statut des composants installés et leur configuration.

CHAPITRE 11

Installer les fichiers binaires d'Enterprise Data Catalog

Ce chapitre comprend les rubriques suivantes :

- [Présentation de l'installation des fichiers binaires d'Enterprise Data Catalog, 185](#)
- [Installation des fichiers binaires pour Enterprise Data Catalog , 185](#)
- [Création de services pour Enterprise Data Catalog, 187](#)

Présentation de l'installation des fichiers binaires d'Enterprise Data Catalog

Si les produits Data Engineering sont installés et configurés dans un domaine, vous pouvez installer les fichiers binaires d'Enterprise Data Catalog sur un nœud du domaine et configurer les services associés.

Effectuez les tâches suivantes pour installer et configurer les produits Catalog sur un nœud existant du domaine :

1. Effectuez les tâches prérequis pour les services d'application et les bases de données.
2. Exécutez le programme d'installation pour installer les fichiers binaires d'Enterprise Data Catalog sur le nœud.
3. Exécutez à nouveau le programme d'installation pour configurer les services associés à Enterprise Data Catalog.

Installation des fichiers binaires pour Enterprise Data Catalog

Vous pouvez installer les fichiers binaires d'Enterprise Data Catalog sur un nœud sur lequel les services Informatica sont installés.

1. Sur une ligne de commande shell, exécutez la commande `./install.sh`.
Le programme d'installation affiche le message pour la documentation et les informations de copyright.
2. Appuyez sur **O** pour continuer l'installation.

3. Appuyez sur **1** pour installer les fichiers binaires d'Informatica 10.5.6 Enterprise Data Catalog
4. Appuyez sur **3** pour exécuter le programme d'installation.
5. Appuyez sur **1** pour indiquer que vous ne souhaitez pas reprendre une installation.
6. Appuyez sur **2** pour accepter les conditions générales.
7. Appuyez sur **2** pour installer Enterprise Data Catalog.
8. Indiquez la marche à suivre.
 - Appuyez sur **1** pour indiquer si les services Informatica ne sont pas installés sur le nœud.
Appuyez sur **2** pour adapter les services d'application pour obtenir de meilleures performances en fonction de votre type de déploiement.
 - Appuyez sur **2** pour indiquer si les services Informatica sont installés sur le nœud.
9. Indiquez si vous souhaitez installer les packages de distribution via le programme d'installation d'Informatica.
 - Appuyez sur **1** si vous n'avez pas besoin des packages de distribution ou si vous souhaitez les installer ultérieurement.
 - Appuyez sur **2** si vous souhaitez installer les packages de distribution via le programme d'installation.

La valeur par défaut est 1.
10. Si vous choisissez d'installer les packages de distribution, sélectionnez un ou plusieurs packages à installer dans la liste. Séparez plusieurs packages par une virgule.
La valeur par défaut est 1.
11. Entrez le répertoire dans lequel vous souhaitez installer les fichiers binaires d'Enterprise Data Catalog.
12. Indiquez la marche à suivre si Enterprise Data Catalog est déjà installé dans le répertoire spécifié.
 - Appuyez sur **1** pour modifier le répertoire d'installation.
 - Appuyez sur **2** pour remplacer l'installation existante.
13. Vérifiez le récapitulatif de pré-installation, puis appuyez sur **Entrée**.
Lorsque vous installez les fichiers binaires d'Enterprise Data Catalog, exécutez le programme d'installation pour configurer les services Enterprise Data Catalog.
Pour plus d'informations sur la configuration des services Enterprise Data Catalog, voir [#unique_178](#).

Lorsque vous installez les fichiers binaires d'Enterprise Data Catalog

Une fois l'installation terminée, vous devez effectuer les étapes de post-installation.

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 :
 - Dans l'outil Administrator tool, sélectionnez le service de référentiel modèle, puis dans le menu **Actions**, choisissez **Contenus du référentiel> Mettre à niveau**.

- À partir de la ligne de commande, exécutez la commande `infacmd mrs upgradeContents`. Pour plus d'informations sur la syntaxe, les paramètres et la description de la commande, reportez-vous à la *Référence des commandes d'Informatica*.
4. Activez le service de catalogue.

Création de services pour Enterprise Data Catalog

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

1. Connectez-vous à la machine à l'aide d'un compte d'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 de création des services d'application.
6. Appuyez sur **2** pour accepter les conditions générales.
7. Appuyez sur **1** pour créer les services Enterprise Data Catalog.
8. Saisissez le répertoire où vous avez installé Enterprise Data Catalog et appuyez sur **Entrée**.
9. Entrez le détails de domaine suivants :
 - 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 sur lequel vous avez installé les fichiers binaires d'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**.
10. Appuyez sur **2** pour indiquer que vous ne souhaitez pas créer de configuration de cluster.
11. Appuyez sur **1** pour créer la connexion de l'entrepôt de profilage.
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 souhaitez créer le service de référentiel modèle de surveillance pour surveiller les statistiques du domaine Informatica.
14. Appuyez sur **1** si vous souhaitez créer le service de gestion de contenu afin de découvrir des domaines de données.
15. Appuyez sur **1** pour configurer le service de gestion de contenu.
16. Vous devez créer le service de cluster Informatica pour gérer les services requis afin d'exécuter Enterprise Data Catalog. 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.

- Sélectionnez 2 pour indiquer que vous ne souhaitez pas 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.
17. Appuyez sur **1** pour confirmer la configuration souhaitée du service de catalogue.
 18. Effectuez les étapes des sections suivantes pour créer les services d'application.

Spécification des détails du domaine Informatica

Effectuez les étapes suivantes pour spécifier les informations du domaine Informatica que vous aviez configurées :

1. Saisissez les informations de domaine suivantes que vous aviez 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. Nom d'utilisateur du domaine. Nom d'utilisateur permettant d'accéder à l'administrateur de domaine Informatica.
 - d. 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**.

Création du service de référentiel modèle

Effectuez les étapes suivantes pour créer 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
 - PostgreSQLLa 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 d'accès et nom du fichier truststore contenant le certificat SSL de la base de données. Si vous n'incluez pas le chemin du fichier truststore, Informatica recherche ce fichier dans le répertoire par défaut suivant : <Informatica installation directory>/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>;BatchP erformanceWorkaround=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>;Snap shotSerializable=true</code> - Microsoft SQL Server qui utilise une instance nommée <code>jdbc:informatica:sqlserver://<nom_hôte> \<nom_instance_nommée>;DatabaseName=<nom_basededonnées>;Snapsh otSerializable=true</code>
Oracle	<code>jdbc:informatica:oracle:// <nom_hôte>:<numéro_port>;SID=<nom_basededonnées>;MaxPooledStatem ents=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

Effectuez les étapes suivantes pour créer 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 souhaitez activer la récupération de Data Engineering pour le service d'intégration de données.

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.

Configuration de 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
 - DB2La 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 d'accès et nom du fichier truststore contenant le certificat SSL de la base de données. Si vous n'incluez pas le chemin du fichier truststore, Informatica recherche ce fichier dans le répertoire par défaut suivant : <Informatica installation directory>/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	jdbc:informatica:db2:// <nom_hôte>:<numéro_port>;DatabaseName=<nom_basededonnées>;BatchPerformanceWorkaround=true;DynamicSections=3000
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server qui utilise l'instance par défaut jdbc:informatica:sqlserver:// <nom_hôte>:<numéro_port>;DatabaseName=<nom_basededonnées>;SnapshotSerializable=true - Microsoft SQL Server qui utilise une instance nommée jdbc:informatica:sqlserver://<nom_hôte>\<nom_instance nommée>;DatabaseName=<nom_basededonnées>;SnapshotSerializable=true
Oracle	jdbc:informatica:oracle:// <nom_hôte>:<numéro_port>;SID=<nom_basededonnées>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true

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. Décidez d'utiliser http ou https pour le service.
Si vous sélectionnez **https** comme protocole pour le service, fournissez les informations suivantes :
 - Port HTTPS. La valeur par défaut est 17466.
 - 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. 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.

8. 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**.
9. Saisissez le mot de passe pour le nom d'utilisateur dans le paramètre **User password** et appuyez sur **Entrée**.
10. 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 d'accès et nom du fichier truststore contenant le certificat SSL de la base de données. Si vous n'incluez pas le chemin du fichier truststore, Informatica recherche ce fichier dans le répertoire par défaut suivant : <Informatica installation directory>/tomcat/bin
TrustStorePassword	Mot de passe du fichier truststore de la base de données sécurisée.

11. Appuyez sur **1** pour spécifier l'URL JDBC pour la connexion à la base de données.
12. 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>
13. 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>

14. Appuyez sur **1** pour spécifier que vous désirez configurer les paramètres JDBC.
15. 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 des options du cluster et du service d'application

Effectuez les étapes suivantes pour configurer les options du cluster et 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.

Création du service de cluster Informatica

Fournissez les détails suivants pour configurer le service de cluster Informatica :

1. Nom d'utilisateur de l'hôte de la passerelle. L'utilisateur de la passerelle doit être un utilisateur non-racine avec un accès sudo.
2. Nom du service de cluster Informatica.
3. Nom de domaine complet du nœud à configurer comme hôte de passerelle.
4. Entrez le nom de la licence à associer au service.
5. Entrez le nom de domaine complet du nœud à configurer comme hôte de passerelle.

6. Appuyez sur **2** si vous souhaitez activer la configuration avancée pour le service. Si vous activez cette propriété, vous pouvez configurer les propriétés des services associés au service de cluster Informatica. Configurez les propriétés de Nomad, comme indiqué dans le tableau suivant :

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

Configurez les propriétés d'Apache Solr, comme indiqué dans le tableau suivant :

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

Configurez les propriétés de la base de données MongoDB, comme indiqué dans le tableau suivant :

Propriété	Description
Hôtes MongoDB	Liste de noms de domaine complets de nœuds séparée par des virgules qui hébergent la base de données MongoDB.
Port MongoDB	Numéro de port configuré pour MongoDB. La valeur par défaut est de 27017. Remarque: Vous ne pouvez pas modifier le port MongoDB après avoir activé le service de cluster Informatica.
Répertoire de journaux de MongoDB	Spécifiez le chemin d'accès au répertoire de stockage des fichiers journaux. La valeur par défaut est \$clusterCustomDir/mongo/log
Répertoire de données de MongoDB	Spécifiez le chemin d'accès au répertoire de stockage des données de la base de données MongoDB. La valeur par défaut est \$clusterCustomDir/mongo/data
Options personnalisées de MongoDB	Spécifiez les options personnalisées pour le service au format suivant : [OptionGroupName.OptionName = OptionValue]. Vous pouvez séparer plusieurs options à l'aide d'un espace blanc. Si OptionValue comprend un espace blanc, vous devez placer OptionValue entre doubles guillemets, comme illustré dans l'exemple suivant : « sample value ».

Configurez les propriétés du référentiel de la base de données PostgreSQL, comme indiqué dans le tableau suivant :

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

- Fournissez la liste de noms de domaine complets de nœuds séparée par des virgules à configurer comme nœuds de données.

8. Fournissez la liste de noms de domaine complets de nœuds séparée par des virgules à configurer comme nœuds de traitement.
9. Spécifiez si vous souhaitez configurer des nœuds de sauvegarde.
10. Spécifiez le port HTTP pour le service. La valeur par défaut est de 9075. Si vous activez la communication sécurisée pour le domaine ou si vous activez une connexion HTTPS pour l'outil Administrator tool, entrez le fichier keystore, le mot de passe du keystore et le numéro de port pour la connexion HTTPS à l'outil Administrator tool.
11. Fournissez le répertoire personnalisé de cluster qui représente le répertoire du service. La valeur par défaut est `/opt/informatica/ics`.
12. Appuyez sur **2** si vous souhaitez configurer le chemin du système de fichiers partagés dans une configuration à plusieurs nœuds. Vous pouvez ensuite spécifier le chemin d'accès au système de fichiers partagés du cluster.
13. Le programme d'installation crée le service de cluster Informatica et passe à la création du service de catalogue.

Création du service de catalogue

Fournissez les informations suivantes pour configurer le service de catalogue :

1. Nom du service de catalogue.
 2. Entrez le nom du service de référentiel modèle à associer au service de catalogue.
 3. Entrez le nom du nœud sur lequel le service doit s'exécuter.
 4. Numéro de port HTTP pour le service de catalogue. La valeur par défaut est de 9085.
 5. Appuyez sur **2** pour activer les notifications de modification des actifs par e-mail dans Enterprise Data Catalog en cas de mises à jour pour les actifs.
 6. Appuyez sur **2** pour configurer les propriétés afin d'activer l'analyse des actifs de données pour Enterprise Data Catalog. Vous pouvez utiliser l'analyse des actifs de données avec Enterprise Data Catalog pour obtenir des recommandations analytiques dans les détails des actifs, telles que les valeurs, l'enrichissement et la collaboration à l'aide de rapports et de graphes.
- Configurez les propriétés suivantes si vous avez activé l'analyse des actifs de données :

Propriété	Description
Sélectionner une base de données	Sélectionnez la base de données du référentiel à utiliser pour l'analyse des actifs de données parmi les options suivantes : <ul style="list-style-type: none"> - Oracle - SQLServer - PostgreSQL
Nom d'utilisateur	Nom d'utilisateur de la base de données du référentiel.
Mot de passe	Mot de passe du nom d'utilisateur de la base de données.

Propriété	Description
Chaîne de connexion de la base de données	<p>Entrez la chaîne de connexion JDBC permettant de se connecter à la base de données du référentiel.</p> <p>Utilisez la syntaxe suivante pour la chaîne de connexion selon la base de données sélectionnée :</p> <ul style="list-style-type: none"> - Oracle. <code>jdbc:informatica:oracle://<host name>:<port number>;ServiceName=<database name></code> - SQLServer : <ul style="list-style-type: none"> - SQL Server. <code>jdbc:informatica:sqlserver://<host name>: <port number>;DatabaseName=<database name>;SnapshotSerializable=true</code> - PostgreSQL. <code>jdbc:informatica:postgresql://<host name>: <port number>;DatabaseName=<database name></code>
Paramètres JDBC sécurisés	<p>Si la base de données du référentiel est sécurisée avec le protocole SSL, vous devez entrer les paramètres de base de données sécurisés sous la forme de paires nom=valeur séparées par des points-virgules. Par exemple : <code>param1=value1;param2=value2</code></p>

Configuration du référentiel MetaDex

Si vous avez sélectionné l'option de configuration du référentiel MetaDex, configurez les propriétés du référentiel MetaDex, comme indiqué dans le tableau suivant :

Propriété	Description
Type de base de données	<p>Spécifiez la base de données à configurer comme référentiel pour MetaDex.</p> <p>Vous pouvez sélectionner l'une des options suivantes :</p> <ul style="list-style-type: none"> - Oracle - SQLServer
Nom d'utilisateur de la base de données	Nom d'utilisateur configuré pour accéder à la base de données avant la mise à niveau.
Mot de passe de la base de données	Mot de passe configuré pour le nom d'utilisateur.
Nom du schéma	Non applicable si vous avez sélectionné Oracle comme base de données. Spécifiez le schéma à utiliser.
La base de données est-elle sécurisée ?	Spécifiez si la base de données est activée pour SSL.
Chemin d'accès au fichier truststore de la base de données	S'applique si vous avez spécifié que la base de données est activée pour SSL. Fournissez le chemin d'accès complet au fichier truststore de la base de données.
Mot de passe du truststore	S'applique si vous avez spécifié que la base de données est activée pour le mot de passe SSL pour accéder au fichier truststore.

Propriété	Description
Paramètres JDBC sécurisés	<p>S'applique si vous avez spécifié que la base de données est activée pour SSL. Spécifiez les paramètres de base de données sécurisés, comme indiqué dans l'exemple suivant :</p> <pre>EncryptionMethod=SSL;HostNameInCertificate=ORATLS.informati ca.com;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1 .2;</pre> <p>Remarque: Enterprise Data Catalog ajoute les paramètres JDBC sécurisés à la chaîne de connexion JDBC. Si vous incluez les paramètres JDBC sécurisés directement dans la chaîne de connexion, n'entrez aucun paramètre dans le champ Paramètres JDBC sécurisés.</p>
Chaîne de connexion JDBC	<p>Chaîne de connexion JDBC pour la connexion à la base de données. Utilisez les formats suivants pour spécifier les chaînes de connexion :</p> <ul style="list-style-type: none"> - Oracle. jdbc:Informatica:oracle ://<host name>:<port number>;ServiceName= - SQLServer. jdbc:Informatica: sqlserver://<host name>:<port number> ;SelectMethod=cursor;DatabaseName=
Port de serveur du référentiel MetaDex	Port unique du serveur de référentiel MetaDex. La valeur par défaut est de 48 090.
Activer la communication sécurisée pour le référentiel MetaDex ?	Spécifiez si TLS est activé pour la communication avec le référentiel.
Certificats SSL pour sécuriser le référentiel MetaDex ?	<p>Indiquez si vous souhaitez utiliser les certificats SSL par défaut ou les certificats SSL personnalisés pour sécuriser le référentiel. Spécifiez les propriétés suivantes si vous souhaitez utiliser les certificats SSL personnalisés :</p> <ul style="list-style-type: none"> - Type de keystore. Spécifiez le type de keystore. - Alias du keystore. Alias unique permettant d'accéder à l'entrée du keystore. - Fichier keystore. Spécifiez le fichier keystore qui contient les clés et les certificats requis. - Mot de passe du keystore. Mot de passe pour accéder au fichier keystore.
Nom d'utilisateur de domaine	<p>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 pour le nom d'utilisateur :</p> <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 d'utilisateur du domaine	Mot de passe de l'administrateur du domaine. Le mot de passe peut comprendre de 3 à 128 caractères maximum.

Propriété	Description
Nom de domaine de sécurité	Nom du domaine de sécurité pour l'administrateur du domaine.
Nom de domaine	Nom du domaine que Metadex utilise pour établir la connexion. Requis si le fichier domains.infa spécifie plusieurs domaines. 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 : ` % * + ; " ? , < > \ /

CHAPITRE 12

Exécuter le programme d'installation silencieuse

Ce chapitre comprend les rubriques suivantes :

- [Présentation du programme d'installation silencieuse d'Enterprise Data Catalog, 201](#)
- [Installation en mode silencieux, 201](#)
- [Installer les services d'application Enterprise Data Catalog en mode silencieux, 203](#)
- [Chiffrement des mots de passe dans le fichier des propriétés, 204](#)

Présentation du programme d'installation silencieuse d'Enterprise Data Catalog

Vous pouvez installer Enterprise Data Catalog sans intervention de l'utilisateur en mode silencieux. Vous pouvez également installer ou configurer les services d'application Enterprise Data Catalog en mode silencieux. Spécifiez les paramètres d'entrée à utiliser pour l'installation dans un fichier de propriétés et exécutez le programme d'installation silencieuse.

Installation en mode silencieux

Pour installer sans interaction utilisateur, procédez à une 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 sur plusieurs machines du réseau ou pour standardiser l'installation entre les machines.

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

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

1. Exécutez l'utilitaire de chiffrement des mots de passe pour chiffrer les mots de passe dans le fichier de propriétés de l'installation.
2. Configurer le fichier de propriétés de l'installation et spécifier les options d'installation dans ce fichier.

3. Exécuter le programme d'installation avec le fichier de propriétés de l'installation.

Configurer le fichier de propriétés

Configurez le fichier qui contient les propriétés de configuration nécessaires à l'installation des services Informatica en mode silencieux.

Informatica fournit deux versions du fichier de propriétés. Utilisez l'un des deux fichiers pour spécifier les options de votre installation.

Fichier de propriétés d'entrée silencieuse

Le fichier de propriétés d'entrée silencieuse contient les propriétés de configuration nécessaires à l'installation des services Informatica en mode silencieux. Utilisez ce fichier afin de prendre en compte la valeur appropriée à définir pour chaque propriété du fichier.

Fichier de propriétés d'entrée silencieuse par défaut

Le fichier de propriétés d'entrée silencieuse par défaut contient des valeurs par défaut pour de nombreuses propriétés de configuration. Les propriétés sont répertoriées dans la partie inférieure du fichier. Utilisez ce fichier si vous prévoyez d'installer les services Informatica à l'aide des valeurs de propriétés par défaut.

Le fichier contient des propriétés définies sur la valeur par défaut des options suivantes :

- Noms de services d'application.
- Authentification SSL (Secure Sockets Layer).
- Authentification Kerberos.
- Attribution de numéros de ports pour les composants domaine et nœud.

Pour configurer le fichier qui contient les propriétés de configuration nécessaires à l'installation des services Informatica en mode silencieux, effectuez les étapes suivantes :

1. Accédez à la racine du répertoire qui contient les fichiers d'installation.
2. Le cas échéant, exécutez l'utilitaire de chiffrement de mot de passe pour chiffrer les mots de passe dans le fichier `.properties`.
3. Créez une copie de sauvegarde du fichier `SilentInput.properties`.
4. Ouvrez le fichier `SilentInput.properties` ou le fichier `SilentInput_Default.properties`.
5. Configurez les propriétés dans le fichier.
6. Enregistrez le fichier de propriétés sous le nom `SilentInput.properties`.

Exécuter le programme d'installation

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

1. Ouvrez une invite de commande.
2. Accédez au répertoire racine qui contient les fichiers d'installation.
3. Vérifiez que le répertoire contient le fichier `SilentInput.properties` que vous avez modifié et réenregistré.
4. Exécutez l'installation silencieuse. Sous Linux, exécutez `silentInstall.sh`.

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

Installer les services d'application Enterprise Data Catalog en mode silencieux

Si vous n'aviez pas installé les services d'application d'Enterprise Data Catalog lors de l'installation d'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.

Configurer le fichier de propriétés

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

1. Accédez à la racine du répertoire qui contient les fichiers d'installation.
2. Le cas échéant, exécutez l'utilitaire de chiffrement de mot de passe pour chiffrer les mots de passe dans le fichier `.properties`.
3. Recherchez le fichier `SilentInput_configure.properties`.
4. Créez une copie de sauvegarde du fichier `SilentInput_configure.properties`.
5. Utilisez un éditeur de texte pour ouvrir le fichier et spécifiez les valeurs des paramètres de service d'application.
6. Enregistrez le fichier de propriétés avec le nom `SilentInput.properties`.

Exécuter le programme d'installation 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 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 enregistré.
4. Exécutez la commande suivante pour démarrer l'installation silencieuse : `./silentinstallConfig.sh`.

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.

Chiffrement des mots de passe dans le fichier des propriétés

Le programme d'installation contient un utilitaire qui peut être utilisé pour chiffrer les mots de passe définis dans le fichier des propriétés que vous utilisez pour spécifier les options lors de l'exécution du programme d'installation en mode silencieux. Informatica utilise le chiffrement AES avec plusieurs clés de 256 bits pour chiffrer les mots de passe.

L'utilitaire doit être exécuté pour chaque mot de passe que vous souhaitez chiffrer. Lorsque vous exécutez l'utilitaire, vous indiquez la valeur du mot de passe en texte brut dans l'invite de commande. L'utilitaire renvoie alors le mot de passe dans un format chiffré. La sortie comprend le préfixe suivant :

```
=INSTALLER:CIPHER:AES:256=
```

Copiez l'intégralité de la chaîne de sortie, préfixe compris, puis collez-la dans le fichier de propriétés en tant que valeur pour la propriété de mot de passe. Lorsque vous exécutez le programme d'installation en mode silencieux, le framework d'installation déchiffre le mot de passe.

1. Accédez au répertoire des utilitaires :

```
<Installer directory>/properties/utils/passwd_encryption
```

2. Exécutez l'utilitaire. Indiquez le mot de passe en texte brut que vous souhaitez chiffrer en tant que valeur pour <password>.

- Sur Linux et UNIX, exécutez la commande suivante :

```
sh install.sh <password>
```

- Sur Windows, exécutez la commande suivante :

```
install.bat <password>
```

3. Copiez la sortie (chaîne du mot de passe chiffré), puis collez-la dans le fichier .properties en tant que valeur pour le mot de passe correspondant.

L'exemple ci-dessous illustre le mot de passe chiffré défini en tant que valeur pour la propriété DOMAIN_PSSWD :

```
DOMAIN_PSSWD==INSTALLER:CIPHER:AES:256=mjkjmDR2kzFJiizfRWIOPg==
```

CHAPITRE 13

Dépannage

Ce chapitre comprend les rubriques suivantes :

- [Présentation du dépannage de l'installation, 205](#)
- [Reprise d'un processus d'installation ayant échoué, 205](#)
- [Dépannage à l'aide des fichiers journaux d'installation, 206](#)
- [Dépannage des domaines et des nœuds, 208](#)
- [Dépannage d'Informatica Developer, 210](#)

Présentation du dépannage de l'installation

Les rubriques dans cette section vous fournissent des informations sur le dépannage des problèmes que vous pouvez rencontrer lors de l'installation d'Informatica. Les exemples inclus décrivent les stratégies générales de dépannage et ne constituent pas une liste exhaustive des causes possibles de problèmes d'installation.

Reprise d'un processus d'installation ayant échoué

Lorsque l'installation s'arrête à mi-chemin, vous pouvez la reprendre à partir du point de défaillance ou quitter.

Lorsque le processus d'installation d'un service échoue sur UNIX ou Linux, vous pouvez le reprendre à partir de la configuration de service précédente et récupérer les derniers détails entrés pour cette installation de service. L'installation peut échouer pour des raisons telles qu'une panne réseau, lorsque vous quittez l'installation avant de terminer l'installation complète, ou en raison d'informations incorrectes entrées.

Tenez compte des directives suivantes pour la reprise de l'installation :

Vous pouvez reprendre le programme d'installation

Si un service échoue ou si le processus d'installation échoue pendant la création d'un service, vous pouvez reprendre le processus d'installation avec le programme d'installation du serveur. Pour reprendre le processus d'installation, vérifiez dans le journal d'installation qu'au moins l'un des services a été créé et que le domaine est opérationnel. Par exemple, si vous souhaitez vérifier que le service de référentiel modèle a été créé, assurez-vous qu'un texte indiquant que la création du service a réussi s'affiche dans le journal du serveur au format suivant :

```
SUCCESS: MRS Service [mrs_name] is created. Command ran successfully.
```

Pour reprendre l'installation, exécutez à nouveau le programme d'installation.

Lorsque vous reprenez le programme d'installation pendant la création d'un service, le programme conserve toutes les informations spécifiques au service et à la base de données, notamment le statut de création du service, le nom du service, le statut activé ou désactivé du service. Vous pouvez confirmer et utiliser les valeurs entrées précédemment ou spécifier de nouvelles valeurs pour le service et reprendre l'installation.

Vous ne pouvez pas reprendre le programme d'installation

Vous ne pouvez pas reprendre le programme d'installation dans les situations suivantes :

- Vous exécutez le programme d'installation pour configurer des services après la création de ceux-ci.
- Vous exécutez l'Assistant de configuration des services.
- Vous joignez un domaine.

Avant de reprendre le programme d'installation

Lorsque le processus d'installation s'arrête en cours de route, vous pouvez le reprendre à partir du point de défaillance ou le quitter.

Avant de reprendre le programme d'installation, remplissez les prérequis suivants :

1. Dans le fichier journal d'installation qui se trouve dans le répertoire d'installation, vérifiez qu'au moins le domaine et un service ont été créés. La syntaxe du nom du fichier journal du programme d'installation est la suivante : `Informatica_<Version>_Services_<horodatage>.log`
2. Veillez à ne pas supprimer le fichier objet `installInst.obj` présent dans le dossier des outils du répertoire d'installation utilisateur.
3. Si vous reprenez l'installation en mode silencieux, assurez-vous que la propriété `RESUME_INSTALLATION` est définie sur `true` dans le fichier `SilentInput.properties`.

Reprendre le programme d'installation

Une fois les tâches prérequis effectuées, vous pouvez reprendre le programme d'installation.

1. Ouvrez une invite de commande et naviguez jusqu'à l'emplacement des fichiers d'installation.
2. Exécutez le programme d'installation en mode console ou silencieux.
3. Lorsque l'installation normale s'exécute, il est possible qu'un message confirmant si vous souhaitez reprendre l'installation précédente ou non s'affiche.
 - Pour ne pas reprendre l'installation, entrez 1 pour Non. La valeur par défaut est 1.
 - Pour reprendre l'installation, entrez 2 pour Oui.

Avant de reprendre le programme d'installation, les services sont validés.

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 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.

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_<timestamp>.log- Informatica_<Version>_Client_<timestamp>.log- Informatica_<Version>_Services_Upgrade_<timestamp>.log- Informatica_<Version>_Client_Upgrade_<timestamp>.log
Emplacement	Répertoire d'installation.
Utilisation	Procurez-vous plus d'informations sur les actions effectuées par le programme d'installation et 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.
Table des matières	Résumé détaillé de chaque action effectuée par le programme d'installation, les informations que vous avez entrées dans le programme d'installation, chaque commande de ligne de commande utilisée par le programme d'installation et le code d'erreur renvoyé par la commande.

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.

Propriété	Description
Utilisation	Obtenez les informations sur les fichiers installés et les entrées de registre créées.
Table des matières	Répertoires créés, nom des fichiers installés et des commandes exécutées, et statut de chaque fichier installé.

Fichiers journaux du gestionnaire de service

Le programme d'installation démarre le service Informatica. Le service Informatica démarre le gestionnaire de service du 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 du gestionnaire de service sont créés sur chaque nœud.

Le tableau suivant décrit les fichiers générés par le gestionnaire de service :

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: Le gestionnaire de service 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.

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. Vous n'avez

pas besoin de configurer ODBC ou une connectivité native sur la machine où vous avez installé les services Informatica.

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 jonction d'un domaine

Le programme d'installation effectue différentes tâches selon que vous créez un domaine ou que vous y accédez :

- **Création d'un domaine.** Le programme d'installation exécute la commande `infasetup DefineDomain` pour créer le domaine et le nœud de passerelle pour le domaine sur la machine actuelle selon les informations entrées dans la fenêtre Configurer le domaine.
- **Accès à 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.

Démarrage d'Informatica

Le programme d'installation exécute `infaservice` pour démarrer le service Informatica. Pour résoudre les problèmes en cas d'échec de démarrage de Informatica, 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.

Informatica peut ne pas démarrer pour les raisons suivantes :

- **La mémoire système du gestionnaire de service est insuffisante.** Il se peut 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 Informatica. Sous UNIX, vous pouvez définir la configuration de la mémoire lors du démarrage de Informatica.
- **La base de données de configuration de domaine n'est pas disponible.** Informatica 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 un délai de 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'exécution sur le répertoire d'installation d'Informatica.
- **Échec de résolution de localhost.** Si vous utilisez un cluster intégré 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 de poursuivre l'installation. Le domaine doit être disponible pour que les objets de licence soient ajoutés au domaine. Si la commande Ping échoue, démarrez Informatica sur le nœud 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 d'Informatica Developer

Tenez compte des conseils suivants lorsque vous utilisez Informatica Developer :

Informatica Developer ne se lance pas

Ce problème peut se produire si le fichier *jvm.dll* de Java nécessite *MSVCR100.dll*.

Pour résoudre ce problème, téléchargez le package redistribuable Microsoft Visual C++ Studio 2010 sur le site Web Microsoft.

Partie IV : Après l'installation des services

Cette partie contient les chapitres suivants :

- [Configuration du domaine, 212](#)
- [Préparation de la création des services d'application, 218](#)
- [Créer et configurer des services d'application, 228](#)

CHAPITRE 14

Configuration du domaine

Ce chapitre comprend les rubriques suivantes :

- [Liste de contrôle pour la configuration du domaine, 212](#)
- [Présentation de la configuration du domaine, 213](#)
- [Intégrer le domaine à l'environnement Hadoop ou Databricks, 213](#)
- [Vérification des paramètres régionaux et de la compatibilité des pages de code, 213](#)
- [Configurer les variables d'environnement sur UNIX ou Linux, 215](#)

Liste de contrôle pour la configuration du domaine

Ce chapitre fournit des informations sur les tâches de configuration de domaine que vous devez effectuer après l'installation. Utilisez cette liste de contrôle pour le suivi des tâches de configuration du domaine.

- ☐ Intégrez le domaine à l'environnement Hadoop.
- ☐ Vérifiez la compatibilité des paramètres régionaux et des pages de code :
 - Vérifiez que la base de données de configuration du domaine est compatible avec les pages de code des services d'application que vous créez dans le domaine.
 - Vérifiez que les paramètres régionaux sur les machines qui accèdent à l'outil Administrator et aux outils client Informatica sont compatibles avec les pages de code des référentiels du domaine.
 - Configurez les variables d'environnement régionales.
- ☐ Configurez les variables d'environnement suivantes :
 - Variables d'environnement Informatica devant stocker les paramètres de mémoire, de domaine et d'emplacement.
 - Variables d'environnement de chemin de bibliothèque sur les machines qui exécutent le service d'intégration de données.
 - Variables d'environnement Kerberos si vous configurez le domaine Informatica pour l'exécuter sur un réseau avec l'authentification Kerberos.

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.

Intégrer le domaine à l'environnement Hadoop ou Databricks

Si vous avez importé la configuration du cluster à partir de l'environnement Hadoop ou Databricks pendant l'installation, vous devez terminer l'intégration entre le domaine et l'environnement Hadoop. Les tâches d'intégration sont requises dans l'environnement Hadoop et dans l'environnement de domaine Informatica.

Pour intégrer le domaine à l'environnement Hadoop, vous effectuez les tâches de haut niveau suivantes :

1. Préparation des répertoires, des utilisateurs et des autorisations.
2. Configurez les fichiers *-site.xml sur l'environnement Hadoop ou Databricks. Les fichiers *-site.xml de propriétés doivent être mis à jour avec les valeurs requises pour le traitement Informatica dans l'environnement tiers.
3. Actualisation de la configuration du cluster dans l'outil Administrator tool. Actualisation de la configuration du cluster pour obtenir les propriétés mises à jour à partir des fichiers *-site.xml du cluster.
4. Mise à jour des connexions dans l'outil Administrator tool. Mise à jour des connexions si vous souhaitez utiliser des valeurs de propriété autres que les valeurs par défaut. Vous devrez également configurer des variables d'environnement dans les propriétés de connexion.

Pour plus d'informations sur l'importation d'une configuration de cluster Hadoop, reportez-vous au *Guide de Data Engineering Integration*.

Vérification des paramètres régionaux et de la compatibilité des pages de code

Les pages de code des services d'application 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'application 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 sur les machines qui accèdent à l'outil Administrator tool et aux outils client 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 des variables d'environnement régionales

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 UNIX ou Linux.

Différents systèmes d'exploitation exigent des valeurs différentes pour le même paramètre régional. La valeur de la variable régionale respecte la casse.

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 et les paramètres régionaux existants.

Définissez les variables d'environnement régionales suivantes :

Paramètre régional sous Linux

Tous les systèmes d'exploitation UNIX sauf Linux ont une valeur unique pour chaque paramètre régional. Linux permet à différentes valeurs 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 la 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
```

Pour lire des caractères multioctets à partir de la base de données, définissez la variable à l'aide de la commande suivante :

```
setenv NLS_LANG=american_america.AL32UTF8
```

Vous devez définir la variable correcte sur la machine sur laquelle est installé le service d'intégration de données de façon à ce qu'il puisse lire les données Oracle correctement.

Configurer les variables d'environnement sur UNIX ou Linux

Informatica utilise des variables d'environnement pour stocker les informations de configuration lors de l'exécution des services d'application et de la connexion aux clients. Configurez les variables d'environnement pour satisfaire aux spécifications 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, connectez-vous avec le compte utilisateur système que vous avez utilisé pour installer Informatica.

Configuration des variables d'environnement Informatica

Vous pouvez configurer des variables d'environnement Informatica pour stocker des 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.

Le tableau suivant décrit la configuration minimale requise pour les paramètres de taille maximum du tas, selon le nombre d'utilisateurs et de services dans le domaine :

Nombre d'utilisateurs du domaine	Taille maximum du tas (1-5 Services)	Taille maximum du tas (6-10 Services)
1000 maximum	512 Mo (par défaut)	1024 Mo
5 000	2048 Mo	3072 Mo
10 000	3072 Mo	5120 Mo
20 000	5120 Mo	6144 Mo
30 000	5120 Mo	6144 Mo

Remarque: Les paramètres de taille maximale du tas mémoire dans le tableau sont basés sur le nombre de services d'application dans le domaine.

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 Informatica. Par exemple, pour configurer 1 Go de mémoire système pour le démon Informatica 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 Informatica. 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 sur laquelle vous installez les services Informatica.

INFA_HOME

Utilisez `INFA_HOME` pour désigner le répertoire d'installation Informatica. Si vous modifiez la structure de répertoires Informatica, vous devez définir la variable d'environnement sur l'emplacement du répertoire d'installation Informatica ou le répertoire où les fichiers Informatica installés sont situés.

Par exemple, vous devez utiliser un lien symbolique pour les répertoires Informatica. Pour configurer `INFA_HOME` afin que les applications ou services Informatica puissent localiser les autres composants Informatica qu'ils doivent exécuter, définissez `INFA_HOME` sur l'emplacement du répertoire d'installation Informatica.

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.

Configurer des variables d'environnement de chemin de bibliothèque

Configurez les variables d'environnement de chemin de bibliothèque sur les machines qui exécutent les processus du service d'intégration de données. Le nom de variable et les spécifications 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	<Database path>/lib
IBM DB2	<Database path>/lib

Base de données	Valeur
Sybase ASE	"\${SYBASE_OCS}/lib:\${SYBASE_ASE}/lib:\${LD_LIBRARY_PATH}"
Teradata	<Database path>/lib
ODBC	<CLOSEDODBCHOME>/lib
PostgreSQL	\$PGHOME/lib:\${LD_LIBRARY_PATH}

CHAPITRE 15

Préparation de la création des services d'application

Ce chapitre comprend les rubriques suivantes :

- [Liste de contrôle pour préparer la création de services d'application, 218](#)
- [Créer des répertoires pour le service Analyst, 219](#)
- [Création d'un keystore pour une connexion sécurisée à un service d'application Web, 219](#)
- [Connexion à Informatica Administrator, 220](#)
- [Création de connexions, 221](#)

Liste de contrôle pour préparer la création de services d'application

Ce chapitre présente les tâches que vous devez effectuer avant de créer ou de configurer le service Analyst, le service d'intégration de données et le service de gestion de contenu. Lorsque vous configurez les services, vous configurez des propriétés en fonction des connexions et des répertoires que vous créez. Utilisez cette liste de contrôle pour le suivi des tâches de configuration.

- ☐ Créez les répertoires suivants pour le service Analyst :
 - Caches de fichiers plats
 - Fichiers de glossaire d'entreprise temporaires
 - Ressources de glossaire
- ☐ Créez les connexions suivantes pour le service d'intégration de données :
 - Base de données du cache d'objet de données
 - Base de données de flux de travail
 - Entrepôt de profilage
- ☐ Créez la connexion suivante pour le service de gestion de contenu :
 - Entrepôt de données de référence

Créer des répertoires pour le service Analyst

Avant de créer le service Analyst, vous devez créer les répertoires dans lesquels l'outil Analyst tool stockera les fichiers temporaires.

Créez les répertoires suivants sur le nœud qui exécute le service Analyst :

Répertoire de cache de fichier plat

Créez un répertoire pour le cache de fichier plat dans lequel l'outil Analyst tool stocke les fichiers plats chargés. Le service d'intégration de données doit également pouvoir accéder à ce répertoire. Si le service Analyst et le service d'intégration de données s'exécutent sur différents nœuds, configurez le répertoire de fichier plat de façon à utiliser un répertoire partagé. Si le service d'intégration de données s'exécute sur des nœuds principaux et de sauvegarde ou sur une grille, chaque processus de service d'intégration de données doit pouvoir accéder aux fichiers dans le répertoire partagé.

Par exemple, vous pouvez créer un répertoire nommé « flatfilecache » dans le lecteur mappé suivant auquel tous les processus de service Analyst et de service d'intégration de données peuvent accéder :

```
F:\shared\<Informatica installation directory>\server
```

Lorsque vous importez une source de table de référence ou de fichier plat, l'outil Analyst tool utilise les fichiers de ce répertoire pour créer un objet de données de table de référence ou de fichier plat.

Répertoire de fichiers d'exportation temporaires

Créez un répertoire pour stocker les fichiers temporaires de glossaire d'entreprise créés par le processus d'exportation de glossaire d'entreprise. Créez ce répertoire sur le nœud qui exécute le service Analyst.

Par exemple, vous pouvez créer un répertoire nommé « exportfiledirectory » à l'emplacement suivant :

```
<Répertoire d'installation Informatica>/server
```

Répertoire des pièces jointes aux ressources

Créez un répertoire pour stocker les fichiers que les gestionnaires de contenu ajoutent en tant que pièces jointes à des ressources de glossaire. Créez ce répertoire sur le nœud qui exécute le service Analyst.

Par exemple, vous pouvez créer un répertoire nommé « répertoirepiècesjointes » à l'emplacement suivant : <Répertoire d'installation d'Informatica>/server

Création d'un keystore pour une connexion sécurisée à un service d'application Web

Vous pouvez sécuriser la connexion entre le domaine Informatica et un service d'application Web, par exemple le service Analyst. Informatica utilise le protocole SSL/TLS pour crypter le trafic réseau. Pour sécuriser la connexion, vous devez créer les fichiers requis.

Avant de sécuriser la connexion à un service d'application Web, vérifiez que les conditions suivantes sont remplies :

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

Note that RSA encryption requires more than 512 bits.

You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into a keystore in JKS format.

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

Le keystore se trouve dans un répertoire accessible.

Le keystore doit se trouver dans un répertoire accessible à l'outil Administrator tool.

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 80.0.39x ou une version ultérieure, vous devez également définir les stratégies AuthServerWhitelist et AuthNegotiateDelegateWhitelist.

1. Démarrez le navigateur Microsoft Internet Explorer ou Google Chrome.
2. Dans le champ **Adresse**, entrez l'URL de l'outil Administrator :
 - Si l'outil Administrator n'est pas configuré pour utiliser une connexion sécurisée, entrez l'URL suivante :
`http://<fully qualified host name>:<http port>/administrator/`
 - Si l'outil Administrator est configuré pour utiliser une connexion sécurisée, entrez l'URL suivante :
`https://<fully qualified host name>:<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.

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** apparaît lorsque le domaine Informatica contient un domaine de sécurité LDAP. Si vous ne connaissez pas le domaine de sécurité auquel appartient votre compte d'utilisateur, contactez l'administrateur de domaine Informatica.

Remarque: Si 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, 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 pour que les services d'application puissent accéder aux bases de données associées.

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	<p>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.</p> <p>Utilisez cette instance du service d'intégration de données lorsque vous configurez les propriétés d'exécution du service Analyst.</p> <p>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.</p>
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 : jdbc:informatica:db2://<host>:50000;databaseName=<dbname>
Chaîne de connexion pour l'accès aux données	Chaîne de connexion qui permet de prévisualiser les données et d'exécuter les mappages. Entrez <dbname> depuis l'alias configuré dans le client DB2.
Page de codes	Page de codes de la base de données.

Propriété	Description
SQL d'environnement	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.
SQL de transaction	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.
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.
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 identificateurs à casse mixte.
Prise en charge des identificateurs 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 à la base de données Microsoft Azure SQL

Utilisez une connexion Azure SQL Data Warehouse pour accéder aux tables d'une base de données Microsoft Azure SQL.

Le tableau suivant décrit les propriétés de la connexion Microsoft Azure SQL Database :

Propriété	Description
URL JDBC Azure DW	Chaîne de connexion à la base de données Microsoft Azure SQL.
Nom d'utilisateur JDBC Azure DW	Nom d'utilisateur de la base de données.
Mot de passe JDBC Azure DW	Mot de passe pour le nom d'utilisateur.
Nom de schéma JDBC Azure DW	Nom du schéma dans la base de données.
Type de stockage Azure	
Nom du compte blob Azure	
Clé du compte blob Azure	
Nom de compte de stockage ADLS Gen2	

Propriété	Description
Clé de compte ADLS Gen2	
Point de terminaison Blob	
Règle de réseau virtuel	

Remarque: Lorsque vous utilisez une connexion Microsoft SQL Server pour accéder aux tables d'une base de données Microsoft SQL Server, l'outil Developer tool n'affiche pas les synonymes des tables.

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 : jdbc:informatica:sqlserver:// <host>:<port>;databaseName=<dbname>
Chaîne de connexion pour l'accès aux données	Chaîne de connexion qui permet de prévisualiser les données et d'exécuter les mappages. Entrez <ServerName>@<DBName>
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.

Propriété	Description
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.
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.

Propriété	Description
Chaîne de connexion pour l'accès aux métadonnées	<p>Chaîne de connexion pour importer des objets de données physiques.</p> <p>Utilisez la chaîne de connexion suivante :</p> <pre>jdbc:informatica:oracle://<host>:1521;SID=<sid></pre> <p>Utilisez la chaîne de connexion suivante pour vous connecter à Oracle via le gestionnaire de connexions Oracle :</p> <pre>jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS server name>;</pre>
Chaîne de connexion pour l'accès aux données	Chaîne de connexion qui permet de prévisualiser les données et d'exécuter les mappages. Entrez <code>dbname.world</code> à partir de l'entrée <code>TNSNAMES</code> .
Page de codes	Page de codes de la base de données.
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 l'environnement de connexion SQL 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 l'environnement de transaction SQL 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. La valeur par défaut est désactivée.
Identificateur SQL	Type de caractère servant à identifier les caractères spéciaux et les mots clés SQL réservés, tels que <code>WHERE</code> . 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 identificateurs à casse mixte.
Prise en charge des identificateurs 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 PostgreSQL

Utilisez une connexion JDBC pour accéder aux tables d'une base de données PostgreSQL.

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.

Propriété	Description
Nom de classe du pilote JDBC	
Chaîne de connexion	Chaîne de connexion à utiliser pour lire les données et les métadonnées de la base de données. Définissez la chaîne de connexion au format suivant : <code>jdbc:informatica:postgresql://<host>:<port>;Database=<id></code>
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 l'environnement de connexion SQL 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 l'environnement de transaction SQL au début de chaque transaction.
Prise en charge des identificateurs 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.
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 identificateurs à casse mixte.
Utiliser le connecteur Sqoop	
Arguments Sqoop	

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 16

Créer et configurer des services d'application

Ce chapitre comprend les rubriques suivantes :

- [Liste de contrôle pour créer et configurer des services d'application, 228](#)
- [Créer et configurer les services d'application - Présentation, 229](#)
- [Créer et configurer le service de référentiel modèle, 229](#)
- [Créer et configurer le service d'intégration de données, 234](#)
- [Créer et configurer le service de gestion de contenu, 237](#)
- [Créer et configurer le service Analyst, 239](#)
- [Créer et configurer le service de cluster Informatica, 242](#)
- [Créer et configurer le service de catalogue, 247](#)
- [Créer et configurer le service d'accès aux métadonnées, 251](#)
- [Configurer le référentiel MetaDex, 252](#)
- [Configurer l'accès au service de catalogue, 254](#)

Liste de contrôle pour créer et configurer des services d'application

Ce chapitre contient des instructions pour la création et la configuration de services d'application. Si vous avez créé des services pendant l'installation, vous devrez peut-être tout de même configurer certains services. Utilisez cette liste de contrôle pour le suivi de la configuration des services d'application.

- ☐ Consultez vos notes pour la planification des services d'application.
- ☐ Identifiez les services que vous avez créés lors de l'installation et procédez à une configuration supplémentaire pour le service.
- ☐ Créez et configurez les autres services souhaités dans le domaine.

Créer et configurer les services d'application - Présentation

Si vous n'avez pas créé les services lors de l'exécution du programme d'installation, utilisez l'outil Administrator tool pour créer les services d'application.

Certains services d'application dépendent d'autres services d'application. Lorsque vous créez ces services d'application dépendants, vous devez fournir le nom des autres services d'application en cours d'exécution. Vérifiez les dépendances du service d'application pour déterminer l'ordre dans lequel vous devez créer les services. Par exemple, vous devez créer un service de référentiel modèle avant de créer un service d'intégration de données.

Avant de créer les services d'application, vérifiez que vous avez effectué les tâches prérequis dont le processus d'installation et de configuration a besoin.

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 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 l'outil client Informatica ou du service d'application, 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	Name of the service. Consider the following guidelines when you name the service: <ul style="list-style-type: none">- It is not case-sensitive.- It must be unique in the domain.- It can't exceed 128 characters.- It can't begin with @.- It can't contain the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- You can't change the name of the service after you create it.
Description	Description of the service. It can't exceed 765 characters.

Propriété	Description
Emplacement	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the service after you create it.
Licence	License object that allows use of the service.
Nœud	Node on which the service runs.
Nœuds de sauvegarde	If your license includes high availability, nodes where the service can run if the primary node is unavailable.

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. Vous pouvez entrer le nom d'utilisateur de Windows NT pour une connexion approuvée de Microsoft SQL Server.
Mot de passe	Mot de passe de la base de données du référentiel pour l'utilisateur de la base de données. Vous pouvez entrer le mot de passe de Windows NT pour une connexion approuvée de Microsoft SQL Server.
Schéma de base de données	Disponible pour Microsoft SQL Server et PostgreSQL. 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	"jdbc:informatica:db2://<host name>:<port number>;DatabaseName=<database name>;BatchPerformanceWorkaround=true;DynamicSections=3000"
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server qui utilise l'instance par défaut "jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true" - Microsoft SQL Server qui utilise une instance nommée "jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true" - Microsoft Azure. jdbc:informatica:sqlserver://<host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.<hostnameincertificate>;ValidateServerCertificate=true - Azure SQL Database avec authentification Active Directory. "jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostnameInCertificate=*.database.windows.net;loginTimeout=<seconds>" <p>Remarque: Si vous avez spécifié les informations d'identification de Windows NT pour la base de données du référentiel modèle sur Microsoft SQL Server, spécifiez la syntaxe de la chaîne de connexion pour inclure la méthode d'authentification NTLM.</p> <ul style="list-style-type: none"> - Microsoft SQL Server qui utilise l'instance par défaut avec les informations d'identification de Windows NT : "jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM" - Microsoft SQL Server qui utilise l'instance nommée avec les informations d'identification de Windows NT : "jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
Oracle	"jdbc:informatica:oracle://<host name>:<port number>;SID=<database name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true"
PostgreSQL	"jdbc:informatica:postgresql://<host name>:<port number>;DatabaseName= "

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 de paires `name=value` 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 <code>SSL</code> .
ValidateServerCertificate	Facultatif. Indique si Informatica valide le certificat envoyé par le serveur de base de données. Si ce paramètre est défini sur <code>True</code> , Informatica valide le certificat envoyé par le serveur de base de données. Si vous spécifiez le paramètre <code>HostNameInCertificate</code> , Informatica valide également le nom d'hôte dans le certificat. Si ce paramètre est défini sur <code>False</code> , Informatica ne valide pas le certificat envoyé par le serveur de base de données. Informatica ignore les informations de <code>truststore</code> 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 <code>SSL</code> .
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.
TrustStore	Requis. Chemin et nom du fichier <code>truststore</code> contenant le certificat <code>SSL</code> pour la base de données. Si vous n'incluez pas le chemin du fichier <code>truststore</code> , Informatica recherche ce fichier dans le répertoire par défaut suivant : <code><Informatica installation directory>/tomcat/bin</code>
TrustStorePassword	Requis. Mot de passe du fichier <code>truststore</code> 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.

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 :

- Créez l'utilisateur du référentiel modèle si le domaine n'utilise pas l'authentification Kerberos.
- Créez les autres services d'application.

Créer l'utilisateur du 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 l'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.
3. 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 : < > "

4. Cliquez sur **OK**.
Les propriétés de l'utilisateur s'affichent.
5. Cliquez sur l'onglet **Privileges**.
6. Cliquez sur **Éditer**.
La boîte de dialogue **Modifier les rôles et les privilèges** s'ouvre.
7. Dans l'onglet **Rôles**, développez le service de référentiel modèle.
8. 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 :

1. Service d'intégration de données
2. Service Analyst
3. Service de gestion de contenu

4. Service de recherche

Créer et configurer le service d'intégration de données

Lorsque vous exécutez des analyses sur des ressources et affichez les statistiques de métadonnées et de profilage dans Enterprise Data Catalog, l'outil client envoie au service d'intégration de données des demandes d'exécution des 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, assurez-vous d'avoir créé le service suivant :

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	Name of the service. Consider the following guidelines when you name the service: <ul style="list-style-type: none">- It is not case-sensitive.- It must be unique in the domain.- It can't exceed 128 characters.- It can't begin with @.- It can't contain the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- You can't change the name of the service after you create it.
Description	Description of the service. It can't exceed 765 characters.
Emplacement	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the service after you create it.
Licence	License object that allows use of the service.
Attribuer	Select Node to configure the service to run on a node. If your license includes grid, you can create a grid and assign the service to run on the grid after you create the service.
Nœud	Node on which the service runs.

Propriété	Description
Nœuds de sauvegarde	If your license includes high availability, nodes where the service can run if the primary node is unavailable.
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 :

- Vérifiez la configuration du fichier hôte.
- Créez les autres services d'application.

Vérifier la configuration du fichier hôte

Si vous avez configuré le service d'intégration de données sous UNIX ou Linux pour lancer des tâches en tant que processus distincts, vérifiez que le fichier d'hôte du nœud qui exécute le service contient une entrée localhost. Autrement, la tâche échoue 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 gestion de contenu
2. Service Analyst
3. Service de recherche

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 les services suivants :

Service de référentiel modèle

Service d'intégration de données

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. Dans la page **Nouveau service de gestion de contenu - Étape 1 sur 2**, entrez les propriétés suivantes :

Propriété	Description
Nom	Name of the service. Consider the following guidelines when you name the service: <ul style="list-style-type: none">- It is not case-sensitive.- It must be unique in the domain.- It can't exceed 128 characters.- It can't begin with @.- It can't contain the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- You can't change the name of the service after you create it.
Description	Description of the service. It can't exceed 765 characters.
Emplacement	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the service after you create it.
Licence	License object that allows use of the service.
Nœud	Node on which the service runs.
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.

Propriété	Description
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.
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 page **Nouveau service de gestion de contenu - Étape 2 sur 2** s'affiche.

5. Acceptez les valeurs par défaut pour les propriétés de sécurité.
6. Sélectionnez **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.

Créer et configurer le service Analyst

Le service Analyst est un service d'application qui exécute l'outil Analyst dans le domaine Informatica. Le service Analyst gère les connexions entre les composants de service et les utilisateurs qui ont accès à l'outil Analyst.

Créer le service Analyst

Utilisez l'assistant de création de service dans l'outil Administrator tool pour créer le service.

Avant de créer le service Analyst, vérifiez que vous avez créé et activé les services suivants :

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

1. Dans l'outil Administrator tool, cliquez sur l'onglet **Gérer**.
2. Cliquez sur **Actions > Nouveau > Service Analyst**.
La boîte de dialogue **Nouveau service Analyst** s'affiche.

3. Sur la page **Nouveau service Analyst - Étape 1 sur 6**, entrez les propriétés suivantes :

Propriété	Description
Nom	Name of the service. Consider the following guidelines when you name the service: <ul style="list-style-type: none">- It is not case-sensitive.- It must be unique in the domain.- It can't exceed 128 characters.- It can't begin with @.- It can't contain the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- You can't change the name of the service after you create it.
Description	Description of the service. It can't exceed 765 characters.
Emplacement	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the service after you create it.
Licence	License object that allows use of the service.
Nœud	Node on which the service runs.

4. Cliquez sur **Suivant**.

La page **Nouveau service Analyst - Étape 2 sur 6** s'affiche.

5. Entrez le numéro de port HTTP à utiliser pour la communication de l'outil Analyst tool vers le service Analyst.
6. Pour activer la communication sécurisée de l'outil Analyst tool vers le service Analyst, sélectionnez **Activer la communication sécurisée**.

Entrez les propriétés suivantes pour configurer la communication sécurisée pour le service Analyst :

Propriété	Description
Port HTTPS	Numéro de port sur lequel l'outil Analyst tool s'exécute lorsque vous activez la communication sécurisée. Utilisez un numéro différent de celui du port HTTP.
Fichier keystore	Répertoire dans lequel le fichier entrepôt de clés contenant les certificats numériques est stocké.
Mot de passe keystore	Mot de passe en texte brut du fichier keystore. Si cette propriété n'est pas définie, le service Analyst utilise le mot de passe par défaut <code>changeit</code> .
Protocole SSL	Facultatif. Indique le protocole à utiliser. Définissez cette propriété sur <code>SSL</code> .

7. Sélectionnez **Activer le service**.

Le service de référentiel modèle et le service d'intégration de données doivent être en cours d'exécution pour activer le service Analyst.

8. Cliquez sur **Suivant**.

La page **Nouveau service Analyst - Étape 3 sur 6** s'affiche.

9. Entrez les propriétés suivantes pour associer le service de référentiel modèle au service Analyst :

Description	Propriété
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.

10. Pour permettre aux utilisateurs de l'outil Analyst tool de travailler sur des données de tâche humaine, définissez la propriété **Service d'intégration de données** sur le service d'intégration de données que vous avez configuré pour l'exécution des flux de travail.

Si les utilisateurs de l'outil Analyst tool n'ont pas besoin de travailler sur des enregistrements de tâche humaine, ne configurez pas cette propriété.

11. Cliquez sur **Suivant**.

La page **Nouveau service Analyst - Étape 4 sur 6** s'affiche.

12. Entrez les propriétés d'exécution suivantes du service Analyst :

Propriété	Description
Service d'intégration de données	<p>Service d'intégration de données à associer au service. Le service Analyst gère la connexion à un service d'intégration de données qui permet aux utilisateurs d'effectuer des tâches en rapport avec la prévisualisation des données, la spécification de mappage, les fiches d'évaluation et les profils dans l'outil Analyst tool.</p> <p>Vous pouvez associer le service Analyst au service d'intégration de données que vous avez configuré pour l'exécution des flux de travail. Vous pouvez également associer le service Analyst avec des services d'intégration de données différents pour les différentes opérations.</p>
Répertoire de cache de fichier plat	Répertoire de cache de fichier plat dans lequel l'outil Analyst tool stocke les fichiers plats chargés. Le service d'intégration de données doit également pouvoir accéder à ce répertoire. Si le service Analyst et le service d'intégration de données s'exécutent sur différents nœuds, configurez le répertoire de fichier plat de façon à utiliser un répertoire partagé.

13. Cliquez sur **Suivant**.

La page **Nouveau service Analyst - Étape 5 sur 6** s'affiche.

14. Entrez le répertoire dans lequel seront stockés les fichiers temporaires de glossaire d'entreprise créés par le processus d'exportation de glossaires d'entreprise et le répertoire dans lequel seront stockés les fichiers que les gestionnaires de contenu joignent aux ressources de glossaire. Ces répertoires doivent se trouver sur le nœud qui exécute le service Analyst.

15. Cliquez sur **Terminer**.

Le domaine crée et active le service Analyst.

Après avoir créé le service via l'assistant, vous pouvez modifier les propriétés ou configurer d'autres propriétés.

Après la création du service Analyst

Après avoir créé le service Analyst, créez le service de recherche qui en dépend.

Créer et configurer le service de cluster Informatica

Le service de cluster Informatica est un service d'application qui exécute et gère les nœuds et les services associés à Enterprise Data Catalog.

Vous pouvez choisir de créer 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.

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

1. Dans l'outil Administrator tool, sélectionnez un domaine, et cliquez sur l'onglet **Services et nœuds**.
2. Dans le menu Actions, cliquez sur **Nouveau > Service de cluster Informatica**.

La boîte de dialogue **Nouveau service de cluster Informatica - Étape 1 sur 4** s'affiche.

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

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

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

Le tableau suivant décrit les propriétés :

Propriété	Description
Port HTTP	Numéro de port HTTP unique pour le service. 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. Requis si vous sélectionnez Activer TLS (Transport Layer Security) . Remarque: Vérifiez que vous avez spécifié le fichier keystore correct pour le service de cluster Informatica. Les certificats du keystore doivent être approuvés par le truststore du domaine. Le fichier truststore doit contenir des certificats signés par une autorité de certification (CA) pour une configuration SSL personnalisée.
Mot de passe du keystore	Mot de passe du fichier keystore. Nécessaire si vous sélectionnez Activer TLS (Transport Layer Security) .
Protocole SSL	Protocole Secure Sockets Layer à utiliser.

6. Cliquez sur **Suivant**.

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

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

Le tableau suivant décrit les propriétés :

Propriété	Description
Hôte de passerelle	Nom de domaine complet du nœud à configurer comme hôte de passerelle. Le nœud que vous configurez comme hôte de passerelle doit être un nœud de données ou un nœud de traitement.
Nœuds de données	Liste de noms de domaine complets de nœuds séparée par des virgules à configurer comme nœuds de données.
Nœuds de traitement	Liste de noms de domaine complets de nœuds séparée par des virgules à configurer comme nœuds de traitement.
Utilisateur de passerelle	Nom d'utilisateur de l'hôte de la passerelle. L'utilisateur de la passerelle doit être un utilisateur non-racine avec un accès sudo. Vous devez activer SSH sans mot de passe pour les nœuds suivants : <ul style="list-style-type: none"> - Entre le domaine Informatica et l'hôte de passerelle pour l'utilisateur de la passerelle. - Entre l'hôte de passerelle et les nœuds de données, et les nœuds précédents. - Si vous prévoyez d'activer la configuration avancée pour le service, activez SSH sans mot de passe entre le nœud de passerelle et les nœuds de service.

Propriété	Description
Répertoire personnalisé de cluster	Répertoire du service. La valeur par défaut est <code>/opt/informatica/ics</code> . Remarque: L'autorisation d'accès au répertoire doit être <code>u=rwx (0700)</code> or <code>u=rwx,g=rx (0750)</code> . Le service Postgres ne démarre pas si le répertoire ne dispose pas de l'autorisation requise.
Chemin du système de fichiers partagés du cluster	S'applique si vous déployez le service sur plusieurs nœuds. Répertoire partagé sur tous les nœuds du cluster. Le service utilise ce répertoire sur tous les nœuds du cluster pour sauvegarder les données d'Apache Solr. Configurez les prérequis du répertoire suivants : <ul style="list-style-type: none"> - Le répertoire doit être vide. - Le système de fichiers NFS doit être monté dans le répertoire. - Le nom d'utilisateur pour accéder au répertoire doit être le même dans tous les nœuds de cluster. - L'utilisateur configuré pour accéder au répertoire doit être un utilisateur non-racine.

8. Facultatif. Cliquez sur l'option **Activer la configuration avancée** si vous souhaitez configurer les propriétés des applications et des services associés. Par défaut, les services utilisent les valeurs que vous avez fournies pour les nœuds de données comme noms d'hôte. La base de données PostgreSQL utilise la valeur spécifiée pour l'hôte de passerelle comme nom d'hôte.
9. Sélectionnez **Activer le service** pour activer le service après avoir cliqué sur **Terminer**.
Par défaut, les services associés utilisent les valeurs que vous avez fournies pour les nœuds de données comme noms d'hôte. La base de données PostgreSQL utilise la valeur spécifiée pour l'hôte de passerelle comme nom d'hôte.

Remarque: Si l'activation du service échoue en raison d'une connexion SSH lente, vous devez augmenter la valeur du délai d'expiration pour le thread de service. Pour augmenter la valeur du délai d'expiration à 150 secondes, créez la propriété personnalisée `IcsCustomOptions.ServiceThreadTime` pour le service de cluster Informatica et définissez la valeur sur 150 000.

10. Cliquez sur **Suivant**.
La boîte de dialogue **Nouveau service de cluster Informatica - Étape 4 sur 4** s'affiche.
11. Ignorez cette étape si vous ne configurez pas un Service Data Privacy Management.
12. Cliquez sur **Terminer**.

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

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

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

Après la création du service de cluster Informatica

Après avoir créé le service de cluster Informatica, créez le service de catalogue qui en dépend.

Configuration avancée du service de cluster Informatica

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

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

Propriétés du service Nomad

Configurez les propriétés de Nomad, comme indiqué dans le tableau suivant :

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

Propriétés du service Apache ZooKeeper

Configurez les propriétés d'Apache ZooKeeper, comme indiqué dans le tableau suivant :

Propriété	Description
Hôtes ZooKeeper	Liste de noms de domaine complets de nœuds séparée par des virgules qui hébergent le serveur Apache ZooKeeper.
Port ZooKeeper	Numéro de port configuré pour le serveur Apache ZooKeeper. La valeur par défaut est de 2181.
Port d'homologue ZooKeeper	Numéro de port configuré pour la communication entre entités homologues d'Apache ZooKeeper. La valeur par défaut est de 2888.
Port leader de ZooKeeper	Numéro de port configuré pour le serveur ZooKeeper identifié comme leader. La valeur par défaut est de 3888.
Répertoire d'installation de ZooKeeper	Spécifiez le chemin d'accès au répertoire dans lequel vous souhaitez installer Apache ZooKeeper. La valeur par défaut est <code><Cluster custom directory>/zk/install</code> .

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

Propriétés du service Apache Solr

Configurez les propriétés d'Apache Solr, comme indiqué dans le tableau suivant :

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

Propriétés du service MongoDB

Configurez les propriétés de la base de données MongoDB, comme indiqué dans le tableau suivant :

Propriété	Description
Hôtes MongoDB	Liste de noms de domaine complets de nœuds séparée par des virgules qui hébergent la base de données MongoDB.
Port MongoDB	Numéro de port configuré pour MongoDB. La valeur par défaut est de 27017.
Répertoire de journaux de MongoDB	Spécifiez le chemin d'accès au répertoire de stockage des fichiers journaux. La valeur par défaut est <code><Cluster custom directory>/mongo/log</code> .

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

Propriétés du service PostgreSQL

Configurez les propriétés de la base de données PostgreSQL, comme indiqué dans le tableau suivant :

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

Créer et configurer le service de catalogue

Créez un service de catalogue pour exécuter 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.

Avant de créer le service de catalogue, assurez-vous d'avoir créé et activé les services suivants :

Service de référentiel modèle
Service de gestion de contenu
Service d'intégration de données
Service de cluster Informatica

Remarque: Le service de catalogue dispose des mêmes privilèges que le compte d'utilisateur qui le crée. Vérifiez que le compte 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 5** 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'espaces. 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 s'exécute le service de catalogue. Si vous modifiez le nœud, vous devez redémarrer le service de catalogue.
Nœuds de sauvegarde	If your license includes high availability, nodes where the service can run if the primary node is unavailable.

4. Cliquez sur **Suivant**.
La boîte de dialogue **Nouveau service de catalogue - Étape 2 sur 5** 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 indiquer un autre service de référentiel modèle, redémarrez le service de catalogue.
Nom d'utilisateur	Nom d'utilisateur de la base de données du référentiel modèle.
Mot de passe	Version chiffrée 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 5** 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 de 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. Si le cluster est activé pour SSL, veillez à activer SSL pour le domaine Informatica et les services d'application.
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. Obligatoire si vous sélectionnez l'option 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. Remarque: Vérifiez que vous avez spécifié le fichier keystore correct pour le service de catalogue. Les certificats du keystore doivent être approuvés par le truststore du domaine. Le fichier truststore doit contenir des certificats signés par une autorité de certification (CA) pour une configuration SSL personnalisée.
Mot de passe du keystore	Mot de passe du fichier keystore. Obligatoire si vous sélectionnez l'option 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 5** s'affiche.

9. Configurez les propriétés suivantes dans la boîte de dialogue.

Le tableau suivant décrit les propriétés :

Propriété	Description
Service de cluster Informatica	Nom du service de cluster Informatica que vous devez associer au service de catalogue.
Recevoir des alertes par e-mail	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, reportez-vous à la <i>Référence de l'administrateur pour Enterprise Data Catalog</i> .
Activer le service de catalogue	Sélectionnez cette option pour activer le service de catalogue.
Activer les notifications par e-mail pour les modifications d'actifs	Sélectionnez l'option de réception des notifications par e-mail dans Enterprise Data Catalog en cas de mises à jour pour les actifs.

10. Cliquez sur **Suivant**.

La boîte de dialogue **Nouveau service de catalogue - Étape 5 sur 5** s'affiche.

11. Facultatif. Cliquez sur **Activer le traitement analytique des actifs de données** afin de configurer les propriétés pour activer le traitement analytique des actifs de données pour Enterprise Data Catalog. Vous pouvez utiliser le traitement analytique des actifs de données avec Enterprise Data Catalog pour obtenir des recommandations analytiques dans les détails des actifs, telles que les valeurs, l'enrichissement et la collaboration à l'aide de rapports et de graphes.

Configurez les propriétés suivantes pour activer le traitement analytique des actifs de données :

Propriété	Description
Sélectionner une base de données	Sélectionnez la base de données du référentiel à utiliser pour le traitement analytique des actifs de données parmi les options suivantes : <ul style="list-style-type: none">- Oracle- SQLServer- PostgreSQL
Nom d'utilisateur	Nom d'utilisateur de la base de données du référentiel.
Mot de passe	Mot de passe du nom d'utilisateur de la base de données.

Propriété	Description
Chaîne de connexion de la base de données	<p>Entrez la chaîne de connexion JDBC permettant de se connecter à la base de données du référentiel.</p> <p>Utilisez la syntaxe suivante pour la chaîne de connexion selon la base de données sélectionnée :</p> <ul style="list-style-type: none"> - Oracle. jdbc:informatica:oracle://<host name>:<port number>;ServiceName=<database name> - SQLServer. jdbc:informatica:sqlserver://<host name>: <port number>;DatabaseName=<database name>;SnapshotSerializable=true - PostgreSQL. jdbc:informatica:postgresql://<host name>: <port number>;DatabaseName=<database name>
Paramètres JDBC sécurisés	<p>Si la base de données du référentiel est sécurisée avec le protocole SSL, vous devez entrer les paramètres de base de données sécurisés sous la forme de paires nom=valeur séparées par des points-virgules. Par exemple : param1=value1;param2=value2</p>

Le traitement analytique des actifs de données prend en charge les schémas suivants pour les bases de données répertoriées :

- Schéma dbo pour SQL Server.
- Schéma public pour PostgreSQL.

Facultatif. Cliquez sur **Tester la connexion** pour valider les détails de la configuration.

12. Cliquez sur **Terminer**.

Créer et configurer le service d'accès aux métadonnées

Le service d'accès aux métadonnées est un service d'application qui permet à l'outil Developer tool d'accéder à l'environnement Hadoop pour importer et prévisualiser des métadonnées. Si le domaine utilise une authentification non-Kerberos, vous pouvez créer et configurer le service d'accès aux métadonnées. Si le domaine utilise l'authentification Kerberos, ne choisissez pas de créer le service d'accès aux métadonnées.

Pour créer le service d'accès aux métadonnées, utilisez l'assistant de création des services dans l'outil Administrator tool. Lorsque vous y êtes invité, spécifiez les informations de service requises, telles que la licence, l'emplacement et le nœud sur lequel le service peut s'exécuter.

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'accès aux métadonnées**.

L'assistant **Nouveau service d'accès aux métadonnées** s'affiche.

5. Sur la page **Nouveau service d'accès aux métadonnées - Étape 1 sur 3**, entrez les propriétés suivantes :

Propriété	Description
Nom	Name of the service. Consider the following guidelines when you name the service: <ul style="list-style-type: none">- It is not case-sensitive.- It must be unique in the domain.- It can't exceed 128 characters.- It can't begin with @.- It can't contain the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- You can't change the name of the service after you create it.
Description	Description of the service. It can't exceed 765 characters.
Emplacement	Domain and folder where the service is created. Click Browse to choose a different folder. You can move the service after you create it.
Licence	License object that allows use of the service.
Nœud	Node on which the service runs.
Nœuds de sauvegarde	If your license includes high availability, nodes where the service can run if the primary node is unavailable.

6. Cliquez sur **Suivant**.

La page **Nouveau service d'accès aux métadonnées - Étape 2 sur 3** s'affiche.

7. Sélectionnez le type de protocole HTTP et entrez le numéro de port respectif à utiliser pour le service d'accès aux métadonnées.

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'accès aux métadonnées.

9. Sélectionnez **Activer le service**.

Le service d'accès aux métadonnées n'a pas d'autre dépendance de service.

10. Cliquez sur **Suivant**.

La page **Nouveau service d'accès aux métadonnées - Étape 3 sur 3** s'affiche.

11. Le cas échéant, spécifiez les options d'exécution pour l'utilisateur d'emprunt d'identité, le cluster Kerberos, les options de journalisation et cliquez sur **Suivant**.

12. Cliquez sur **Terminer**.

Le domaine crée et active le service d'accès aux métadonnées.

Configurer le référentiel MetaDex

Si vous n'aviez pas configuré le référentiel MetaDex lors de l'installation, vous pouvez le configurer après avoir installé Enterprise Data Catalog.

Effectuez les étapes suivantes pour configurer le référentiel :

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

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

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

Propriété	Description
MDX_KEYSTORE_FILE	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Spécifiez le fichier keystore qui contient les clés et les certificats requis.
MDX_KEYSTORE_PASSWD	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Mot de passe pour accéder au fichier keystore.
MDX_KEYSTORE_TYPE	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Spécifiez le type de keystore.
MDX_KEYSTORE_ALIAS	S'applique si vous avez défini MDX_CUSTOM_SELECTION sur <code>true</code> . Alias unique permettant d'accéder à l'entrée du keystore.
MDX_AUTH_USERNAME	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 pour le nom d'utilisateur : <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 : <code>% * + / ? ; < ></code> - Le nom peut inclure des espaces ASCII, sauf en première et dernière position. Tous les autres caractères d'espacement sont interdits.
MDX_AUTH_PASSWD	Mot de passe de l'administrateur du domaine. Le mot de passe peut comprendre de 3 à 128 caractères maximum.
MDX_AUTH_SECURITY_DOMAIN	Nom du domaine de sécurité pour l'administrateur du domaine.
MDX_AUTH_DOMAIN	Nom du domaine que Metadex utilise pour établir la connexion. Requis si le fichier <code>domains.infra</code> spécifie plusieurs domaines. 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 : <code>` % * + ; " ? , < > \ /</code>

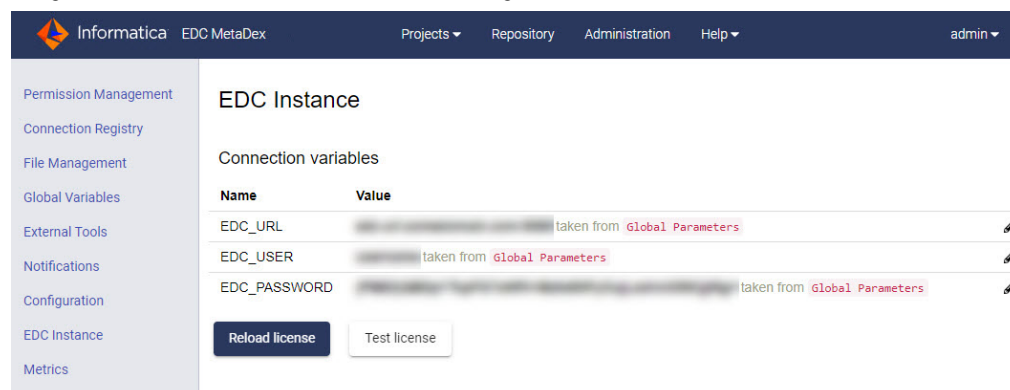
- Entrez la commande suivante : `./configureMetaDex.sh`
- Si le service de catalogue est en cours d'exécution, recyclez le service.

Configurer l'accès au service de catalogue

Configurez le serveur MetaDex pour vous connecter au service de catalogue.

- Connectez-vous à l'outil MetaDex.
Pour plus d'informations, reportez-vous à la section « Connexion à l'outil MetaDex » du *Guide de l'administrateur des scanners MetaDex*.
- Dans l'en-tête de l'outil MetaDex, cliquez sur **Administration > Instance d'EDC**.

La page **Instance d'EDC** s'affiche avec les variables de connexion prédéfinies et les informations sur l'origine de la variable, comme illustré sur l'image suivante :



3. Cliquez sur l'icône **Modifier** à droite de chaque variable.
La boîte de dialogue **Modifier la variable globale** s'affiche.
4. Entrez les valeurs des variables suivantes :

Nom	Description
EDC_URL	Nom d'hôte et numéro de port du service de catalogue au format suivant : <host>:<port>
EDC_USER	Nom d'utilisateur configuré pour l'utilisateur administrateur du catalogue.
EDC_PASSWORD	Mot de passe configuré pour l'utilisateur administrateur du catalogue. Lorsque vous ajoutez le mot de passe, cliquez sur l'icône Masquer le mot de passe .

5. Cliquez sur **Enregistrer**.
La boîte de dialogue **Modifier la variable globale** se ferme.
6. Testez et rechargez la licence.

Partie V : Installation du client Informatica

Cette partie contient les chapitres suivants :

- [Installer Informatica Developer , 257](#)
- [Installer en mode silencieux , 263](#)

CHAPITRE 17

Installer Informatica Developer

Ce chapitre comprend les rubriques suivantes :

- [Avant l'installation Informatica Developer, 257](#)
- [Installer l'outil Developer tool, 258](#)
- [Après l'installation d'Informatica Developer, 259](#)
- [Démarrage de l'outil Developer, 261](#)

Avant l'installation Informatica Developer

Avant d'installer Informatica Developer, vérifiez que la configuration minimale et les logiciels tiers requis sont conformes. Si la machine sur laquelle vous installez Informatica Developer n'est pas correctement configurée, l'installation peut échouer.

Vérifier la somme de contrôle du package d'installation

Avant d'exécuter le programme d'installation du client, vérifiez l'intégrité du package d'installation via la commande cksum. Celle-ci calcule la valeur de la somme de contrôle pour le programme d'installation.

Vérifiez la somme de contrôle des fichiers du programme d'installation spécifiques par rapport à la somme de contrôle des fichiers d'installation téléchargés depuis le site de téléchargement de logiciels électroniques Informatica.

Le tableau suivant répertorie la somme de contrôle et la taille de fichier pour le client Informatica sous Windows :

Fichier	Valeur de la somme de contrôle	Taille du fichier
informatica_1056_client_winem-64t.zip	1702676137	3353746081

Une incompatibilité de somme de contrôle peut se produire lorsqu'il existe des erreurs de données pendant le téléchargement en raison de problèmes réseau ou de corruption des données dans le fichier sur le disque.

Pour plus d'informations sur les erreurs de somme de contrôle, reportez-vous à la section

[HOW TO: Identify file errors after downloading Informatica installation files.](#)

Vérifier les spécifications système

Avant d'installer le client, assurez-vous que les conditions requises ci-dessous sont remplies pour installer et exécuter le client :

Espace disque pour les fichiers temporaires

Le programme d'installation écrit des fichiers temporaires sur le disque dur. Vérifiez que vous disposez de suffisamment d'espace (1 Go) 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.

Autorisations à installer

Assurez-vous que le compte utilisateur que vous utilisez pour installer le client dispose d'une autorisation en écriture sur le répertoire d'installation et le Registre Windows.

Configuration système minimale requise

Le tableau suivant répertorie la configuration système minimale requise pour l'exécution des outils clients :

Processeur	RAM	Espace disque
1 processeur	1 Go	6 Go

Vérifier la configuration requise de tiers pour Informatica Developer

Avant d'installer l'outil Developer tool, vérifiez la configuration requise suivante pour l'installation de tiers :

- Installez .NET Framework 4.0 ou une version ultérieure. Si vous prévoyez d'utiliser les transformations Processeur de données ou Hiérarchique à relationnel, vous devez installer .NET Framework avant d'installer l'outil Developer tool.
- Installez la dernière version du package redistribuable Microsoft Visual C++ (x64) avant d'utiliser ou d'installer l'outil Developer tool. Vous pouvez le télécharger sur le site Web Microsoft.

Installer l'outil Developer tool

Effectuez les étapes suivantes pour installer l'outil Developer tool:

1. Fermez toutes les autres applications.
2. Accédez à la racine du répertoire des fichiers d'installation et exécutez install.bat en tant qu'administrateur.

Pour exécuter le fichier en tant qu'administrateur, cliquez avec le bouton droit de la souris sur le fichier install.bat et sélectionnez **Exécuter en tant qu'administrateur**.

Remarque: Si vous n'exécutez pas le programme d'installation en tant qu'administrateur, l'administrateur système Windows peut rencontrer des problèmes lors de l'accès aux fichiers du répertoire d'installation d'Informatica.

Si vous rencontrez des problèmes lorsque vous exécutez le fichier install.bat depuis le répertoire racine, exécutez le fichier suivant : <Répertoire des fichiers du programme d'installation>\client\install.exe

3. Sélectionnez **Installer des clients Informatica <Version>** et cliquez sur **Suivant**.
4. La page **Configuration requise pour l'installation** affiche les spécifications système requises. Vérifiez toute la configuration requise pour l'installation avant de poursuivre l'installation.
5. Sur la page **Répertoire d'installation**, entrez le chemin d'accès absolu pour le répertoire d'installation.
Le répertoire d'installation doit figurer sur l'ordinateur actuel. La longueur maximale du chemin d'accès doit être inférieure à 260 caractères. Les noms de répertoires dans le chemin ne doivent pas contenir d'espaces ni les caractères spéciaux suivants : @|* \$ # ! % () { } [] , ; '
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.
6. Si vous souhaitez installer les packages de distribution via le programme d'installation d'Informatica, cochez la case.
7. Si vous choisissez d'installer les packages de distribution, sélectionnez un ou plusieurs packages à installer dans la liste.
8. Cliquez sur **Suivant**.
9. Sur la page **Récapitulatif de post-installation**, vérifiez les informations d'installation, et cliquez sur **Installer**.
Le programme d'installation copie les fichiers de l'outil Developer tool dans le répertoire d'installation.
La page **Récapitulatif de post-installation** indique si l'installation a été effectuée.
10. Cliquez sur **Terminé** pour fermer le programme d'installation.
Vous pouvez afficher les fichiers journaux de l'installation pour obtenir plus d'informations sur les tâches effectuées par le programme d'installation.

Après l'installation d'Informatica Developer

Une fois que vous avez installé Informatica Developer, vous pouvez installer d'autres langues, activer la communication sécurisée dans le domaine et démarrer l'outil Developer tool.

Installation des langues

Pour afficher des langues autres que celles des paramètres régionaux du système et pour travailler avec des référentiels utilisant une page de code UTF-8, installez des langues supplémentaires sous Windows à utiliser avec les clients Informatica.

Vous devez aussi installer les langues pour utiliser l'Éditeur de méthode d'entrée Windows (IME).

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration**.
2. Cliquez sur **Options régionales**.
3. Sous les paramètres de langue du système, sélectionnez les langues à installer.
4. Cliquez sur **Appliquer**.

Si vous modifiez les paramètres régionaux du système lorsque vous installez la langue, redémarrez la machine Windows.

Configuration du client pour un domaine sécurisé

Lorsque vous activez la communication sécurisée au sein du domaine, vous sécurisez également les connexions entre le domaine et les applications clientes Informatica. En fonction des fichiers truststore utilisés, il est possible que vous deviez spécifier l'emplacement et le mot de passe de ces fichiers dans les variables d'environnement de chaque hôte client.

Il est possible que vous deviez définir les variables d'environnement suivantes sur chaque hôte client :

INFA_TRUSTSTORE

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

INFA_TRUSTSTORE_PASSWORD

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

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

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

Vous devez définir ces variables sur chaque hôte client dans les cas suivants :

Vous utilisez un certificat SSL personnalisé pour sécuriser le domaine.

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

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

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

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

Configuration du répertoire d'espace de travail de l'outil Developer

Configurez Informatica Developer pour écrire les métadonnées d'espace de travail sur la machine sur laquelle l'utilisateur est connecté.

1. Accédez au répertoire suivant : `<Répertoire d'installation Informatica>\clients\DeveloperClient\configuration\`
2. Recherchez le fichier `config.ini`.
3. Créez une copie de sauvegarde du fichier `config.ini`.
4. Utilisez un éditeur de texte pour ouvrir le fichier `config.in`.

5. Ajoutez la variable `osgi.instance.area.default` à la fin du fichier `config.ini` et définissez-la sur l'emplacement du répertoire dans lequel enregistrer les métadonnées d'espace de travail. Le chemin d'accès au fichier ne peut pas contenir de caractères non-ANSI. Les noms de dossier figurant dans le répertoire d'espace de travail ne peuvent pas contenir le caractère `#`. Si des noms de dossier figurant dans le répertoire d'espace de travail contiennent des espaces, placez le répertoire complet entre guillemets doubles.

- Si vous exécutez Informatica Developer à partir de la machine locale, définissez la variable sur le chemin absolu du répertoire d'espace de travail :

```
osgi.instance.area.default=<Drive>/<WorkspaceDirectory>
```

ou

```
osgi.instance.area.default=<Drive>\\<WorkspaceDirectory>
```

- Si vous exécutez Informatica Developer à partir d'une machine distante, définissez la variable à l'emplacement du répertoire sur la machine locale :

```
osgi.instance.area.default=\\\\<LocalMachine>/<WorkspaceDirectory>
```

ou

```
osgi.instance.area.default=\\\\<LocalMachine>\\<WorkspaceDirectory>
```

L'utilisateur doit avoir l'autorisation d'écriture sur le répertoire d'espace de travail local.

Informatica Developer écrit les métadonnées d'espace de travail dans le répertoire d'espace de travail. Si vous vous connectez à Informatica Developer à partir d'une machine locale, Informatica Developer écrit les métadonnées d'espace de travail dans la machine locale. Si le répertoire d'espace de travail n'existe pas sur la machine à partir de laquelle vous vous êtes connecté, Informatica Developer crée le répertoire lors de l'écriture des fichiers.

Vous pouvez remplacer le répertoire d'espace de travail au démarrage d'Informatica Developer.

Démarrage de l'outil Developer

Lors du démarrage de l'outil Developer, vous devez vous connecter à un référentiel Modèle. Le référentiel Modèle stocke les métadonnées créées dans l'outil Developer. Le service de référentiel modèle gère le référentiel Modèle. Connectez-vous au référentiel avant de créer un projet.

1. Dans le menu Démarrer de Windows, cliquez sur **Programmes > Informatica[Version] > Client > Developer Client > Lancer Informatica Developer**.

Lors de la première exécution de l'outil Developer, la page d'accueil affiche plusieurs icônes. La page de bienvenue ne s'affiche pas lors de l'exécution ultérieure de l'outil Developer.

2. Cliquez sur **Workbench**.

Lors du premier démarrage de l'outil Developer, vous devez sélectionner le référentiel dans lequel enregistrer les objets que vous créez.

3. Cliquez sur **Fichier > Connexion au référentiel**.

La boîte de dialogue **Connexion au référentiel** s'ouvre.

4. Si vous n'avez pas configuré un domaine dans l'outil Developer, cliquez sur **Configurer les domaines** pour configurer un domaine.

Vous devez configurer un domaine pour accéder à un Service de référentiel modèle.

5. Cliquez sur le bouton **Ajouter** pour ajouter un domaine.

La boîte de dialogue **Nouveau domaine** s'affiche.

6. Entrez le nom du domaine, le nom d'hôte et le numéro de port.
7. Cliquez sur **Terminer**.
8. Cliquez sur **OK**.
9. Dans la boîte de dialogue **Connexion au référentiel**, cliquez sur **Parcourir** et sélectionnez le Service de référentiel modèle.
10. Cliquez sur **OK**.
11. Cliquez sur **Suivant**.
12. Entrez un nom d'utilisateur et un mot de passe.
13. Cliquez sur **Terminer**.

L'outil Developer ajoute le référentiel Modèle à la vue Explorateur d'objets. Lors de la prochaine exécution de l'outil Developer, vous pouvez vous connecter au même référentiel.

CHAPITRE 18

Installer en mode silencieux

Ce chapitre comprend les rubriques suivantes :

- [Présentation de l'installation en mode silencieux, 263](#)
- [Configurer le fichier de propriétés, 263](#)
- [Exécuter le programme d'installation silencieuse, 264](#)

Présentation de l'installation en mode silencieux

Pour installer les clients Informatica sans intervention de l'utilisateur, installez 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 le mode d'installation silencieux pour installer les clients Informatica sur plusieurs machines du réseau ou pour standardiser l'installation parmi les machines.

Pour installer en mode silencieux, effectuez les tâches suivantes :

1. Configurez le fichier de propriétés de l'installation et spécifiez les options d'installation dans ce fichier.
2. Exécutez le programme d'installation avec le fichier de propriétés.

Configurer le fichier de propriétés

Informatica fournit un exemple de fichier de propriétés qui comprend les propriétés requises par le programme d'installation. Personnalisez l'exemple de fichier de propriétés pour en créer un et indiquez les options de votre installation. Lancez ensuite l'installation silencieuse.

L'exemple de fichier `SilentInput.properties` est stocké dans l'emplacement de téléchargement du programme d'installation.

1. Accédez à la racine du répertoire 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 et modifier les valeurs des propriétés dans le fichier.

Le tableau suivant décrit les propriétés de l'installation que vous pouvez modifier :

Nom de la propriété	Description
INSTALL_TYPE	Indique s'il faut installer ou mettre à niveau les clients Informatica. Si la valeur est 0, les clients Informatica sont installés dans le répertoire que vous indiquez. Si la valeur est 1, les clients Informatica sont mis à niveau. La valeur par défaut est 0.
USER_INSTALL_DIR	Répertoire d'installation des clients Informatica
DXT_COMP	Indique s'il faut installer Informatica Developer. Si la valeur est 1, l'outil Developer tool est installé. Si la valeur est 0, l'outil Developer tool n'est pas installé. La valeur par défaut est 1.
INSTALL_HADOOP_LIBRARIES	Détermine s'il faut installer les packages de distribution via le programme d'installation. Définissez la valeur sur true si vous souhaitez installer les packages de distribution via le programme d'installation. Définissez la valeur sur false si vous n'avez pas besoin de packages de distribution ou si vous souhaitez les installer ultérieurement.
SELECTED_HADOOP_LIBRARIES	Détermine les packages d'intégration que vous souhaitez installer à partir de la liste des packages pris en charge. Entrez les packages de distribution que vous souhaitez installer, en séparant plusieurs packages par une virgule.

5. Enregistrez le fichier de propriétés.

Exécuter le programme d'installation silencieuse

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

1. Ouvrez une invite de commande.
2. Accédez au répertoire racine qui contient les fichiers d'installation.
3. Vérifiez que le répertoire contient le fichier SilentInput.properties que vous avez modifié et réenregistré.
4. Pour exécuter l'installation silencieuse, exécutez silentInstall.bat.

Le programme d'installation silencieuse s'exécute en arrière-plan. Le processus peut prendre du temps. L'installation silencieuse est terminée lorsque le fichier Informatica_<Version>_Client_InstallLog<horodatage>.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.

Partie VI : Désinstallation

- [Désinstallation, 266](#)

CHAPITRE 19

Désinstallation

Ce chapitre comprend les rubriques suivantes :

- [Désinstallation d'Informatica - Présentation, 266](#)
- [Règles et instructions pour la désinstallation, 266](#)
- [Désinstallation du serveur Informatica en mode console, 267](#)
- [Désinstallation du serveur Informatica en mode silencieux, 268](#)

Désinstallation d'Informatica - Présentation

Désinstallez Informatica pour supprimer le serveur ou les clients Informatica d'une machine.

Le processus de désinstallation d'Informatica supprime tous les fichiers Informatica et toutes les configurations Informatica d'une machine. Le processus de désinstallation ne supprime pas les fichiers qui n'ont pas été installés avec Informatica. 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 pour une désinstallation propre.

Important: Si vous installez les services Informatica et le client PowerCenter dans le même répertoire d'installation, les fichiers binaires des services seront désinstallés lorsque vous désinstallez le client PowerCenter.

Règles et instructions pour la désinstallation

Utilisez les règles et instructions suivantes lors de la désinstallation des composants de Informatica :

- Le mode de désinstallation du serveur Informatica dépend du mode utilisé pour l'installer. Par exemple, imaginez que vous installiez le serveur Informatica en mode console. Lors de l'exécution du programme de désinstallation, celui-ci fonctionnera en mode console. Le mode de désinstallation des clients Informatica ne dépend pas du mode utilisé pour les installer. Par exemple, imaginez que vous installiez les clients Informatica en mode silencieux. Lors de l'exécution du programme de désinstallation, celui-ci pourra fonctionner en mode graphique ou silencieux.
- La désinstallation de Informatica n'affecte pas ses référentiels. Le programme de désinstallation supprime les fichiers de Informatica. 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 de Informatica ne supprime pas les tables de métadonnées de la base de données de configuration du domaine. Si vous installez à nouveau Informatica à l'aide de la base de données de configuration du domaine et de compte d'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'Informatica supprime tous les fichiers d'installation et sous-répertoires du répertoire d'installation d'Informatica. Avant de désinstaller Informatica, arrêtez tous les services et processus Informatica 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 de répertoires ne pouvant être supprimés.
- L'installation du serveur Informatica crée le dossier suivant pour les bibliothèques et les fichiers requis par les adaptateurs tiers généré à l'aide des API d'Informatica Development Platform :
`<Répertoire d'installation Informatica>/services/shared/extensions`
 La désinstallation du serveur Informatica supprime ce dossier et tous les sous-dossiers créés en dessous. Si des fichiers d'adaptateurs sont stockés dans le dossier /extensions, sauvegardez le dossier avant de démarrer la désinstallation.
- Si vous effectuez la désinstallation sur une machine, vous devez sauvegarder le dossier ODBC avant la désinstallation. Restaurez le dossier à la fin de la désinstallation.

Désinstallation du serveur Informatica en mode console

Si vous avez installé le serveur Informatica en mode console, vous devez le désinstaller en mode console.

Avant d'exécuter le programme de désinstallation, arrêtez tous les services et processus Informatica 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 :

```
<Répertoire d'installation Informatica>/Uninstaller_Server
```

2. Tapez la commande suivante pour exécuter le programme de désinstallation :

```
./uninstaller.sh
```

Si vous avez installé le serveur Informatica en mode console, le programme de désinstallation démarre en mode console.

Désinstallation du serveur Informatica en mode silencieux

Si vous avez installé le serveur Informatica en mode silencieux, vous devez le désinstaller en mode silencieux.

Avant d'exécuter le programme de désinstallation, arrêtez tous les services et processus Informatica 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 :

```
<Répertoire d'installation Informatica>/Uninstaller_Server
```

2. Tapez la commande suivante pour exécuter le programme de désinstallation en mode silencieux :

```
./uninstaller.sh
```

Si vous avez installé le serveur Informatica en mode silencieux, le programme de désinstallation démarre 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.

Après avoir désinstallé le serveur Informatica, supprimez tous les dossiers et fichiers qui restent dans le répertoire d'installation Informatica. Par exemple :

- Fichier Informatica _<Version>_Services_InstallLog.log
- Fichier Informatica _<Version>_Services_<horodatage>.log

ANNEXE A

Démarrage et arrêt des services Informatica

Cette annexe comprend les rubriques suivantes :

- [Démarrage et arrêt des services Informatica - Présentation , 269](#)
- [Démarrage et arrêt des services Informatica à partir de la console, 269](#)
- [Arrêt d'Informatica dans Informatica Administrator, 270](#)
- [Règles et instructions pour démarrer ou arrêter Informatica, 270](#)

Démarrage et arrêt des services Informatica - Présentation

Le service Informatica exécute le gestionnaire de service sur le nœud. Le gestionnaire de service gère toutes les fonctions du domaine et démarre les services d'application configurés pour s'exécuter sur le nœud. La méthode que vous utilisez pour démarrer ou arrêter Informatica dépend du système d'exploitation. Vous pouvez utiliser Informatica Administrator pour arrêter un nœud. Lorsque vous arrêtez un nœud, vous arrêtez Informatica dans ce nœud.

Le service Informatica exécute aussi Informatica Administrator. Vous utilisez Informatica Administrator pour administrer les objets de domaine et les comptes d'utilisateur Informatica. Connectez-vous à Informatica Administrator pour créer des comptes pour les utilisateurs d'Informatica et pour créer et configurer les services d'application dans le domaine.

Démarrage et arrêt des services Informatica à partir de la console

Exécutez `infaservice.sh` pour démarrer et arrêter le démon Informatica. Les `infaservice.sh` est installé dans le répertoire suivant :

```
<Informatica 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: Démarrez toujours les nœuds Informatica avec un utilisateur non-racine. Si vous utilisez un softlink pour spécifier l'emplacement de `infaservice.sh`, définissez la variable d'environnement `INFA_HOME` sur l'emplacement du répertoire d'installation Informatica.

Arrêt d'Informatica dans Informatica Administrator

Lorsque vous arrêtez un nœud à l'aide d'Informatica Administrator, vous arrêtez également le service Informatica 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 pouvez perdre les modifications qui n'ont pas encore été écrites dans le référentiel. Si vous abandonnez un nœud exécutant des processus de service d'intégration, les flux de travail sont 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 pour démarrer ou arrêter Informatica

Respectez les règles et instructions suivantes lors du démarrage et de l'arrêt d'Informatica 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 comprend pas d'autres, le domaine n'est plus disponible.
- Lors du démarrage de Informatica, vérifiez que le port utilisé par le service sur le nœud est disponible. Par exemple, si vous arrêtez Informatica sur un nœud, vérifiez que le port n'est pas utilisé par un autre processus sur la machine avant de démarrer Informatica. Si le port n'est pas disponible, Informatica ne peut pas 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 Informatica 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

Gestion des packages de distribution

Cette annexe comprend les rubriques suivantes :

- [Présentation de la gestion des packages de distribution, 271](#)
- [Avant de commencer, 272](#)
- [Installer ou supprimer des packages de distribution en mode console, 272](#)
- [Installer ou supprimer des packages de distribution en mode silencieux, 273](#)
- [Après l'installation, 274](#)

Présentation de la gestion des packages de distribution

Vous pouvez utiliser Integration Package Manager (gestionnaire de packages) pour installer et supprimer des packages de distribution des machines de service et clientes d'Informatica.

Un package de distribution est un ensemble de fichiers binaires de distribution que vous installez dans le domaine pour les exigences de traitement suivantes :

- Pour transférer le traitement vers l'environnement Hadoop ou Databricks.
- Pour traiter des fichiers complexes dans le domaine Informatica.
- Pour vous connecter à l'environnement Hadoop ou Databricks en cas de traitement dans le domaine Informatica.

Vous pouvez installer des packages de distribution si vous ne l'avez pas fait lors du processus de mise à niveau ou d'installation, ou si vous souhaitez ajouter un package de distribution. Vous pouvez supprimer un package de distribution si vous souhaitez utiliser un package différent ou si vous avez installé un package que vous n'utilisez pas.

Lorsque vous installez ou supprimez des packages de distribution, vérifiez que vous effectuez l'opération sur toutes les machines de service et clientes.

Avant de commencer

Avant d'exécuter Integration Package Manager, effectuez les tâches telles que la définition des variables d'environnement et le téléchargement des fichiers.

1. Arrêtez les services Informatica.
2. Définissez l'une des variables d'environnement suivantes :

Variable	Description
INFA_JDK_HOME	Emplacement du dossier qui contient le kit de développement Java (JDK) pris en charge. Définissez la variable d'environnement INFA_JDK_HOME dans les scénarios suivants : <ul style="list-style-type: none">- Le domaine Informatica se trouve sur la plate-forme Windows ou Linux- Client Informatica
INFA_JRE_HOME	Emplacement du dossier contenant le Java Runtime Environment (JRE) pris en charge. Si le domaine Informatica se trouve sur la plate-forme AIX, définissez la variable d'environnement INFA_JRE_HOME.

3. Vérifiez que l'utilisateur qui exécute le gestionnaire de packages dispose des autorisations de lecture et d'écriture sur le répertoire d'installation d'Informatica et des autorisations d'exécution sur le fichier exécutable.
4. Téléchargez les fichiers à partir du site de téléchargement de logiciels électroniques Informatica :
 - [Integration Package Manager](#)
 - [Distribution packages](#)
5. Extrayez le fichier ZIP d'Integration Package Manager sur un lecteur local.
6. Copiez les fichiers ZIP des packages de distribution dont vous avez besoin à l'emplacement suivant :
<Integration Package Manager directory>/source

Remarque: Le gestionnaire de packages échoue si les fichiers ZIP des packages de distribution ne sont pas disponibles dans le répertoire source.

Installer ou supprimer des packages de distribution en mode console

Vous pouvez exécuter Integration Package Manager en mode console pour installer ou supprimer des packages de distribution.

1. Dans le répertoire d'Integration Package Manager, exécutez l'une des commandes suivantes :
 - `./Server.sh console` pour Linux ou UNIX
 - `Server.bat console` pour Windows
 - `Client.bat console` pour le client

Remarque: Pour exécuter la commande sous Windows, utilisez l'invite de commandes de l'administrateur.
2. Entrez le répertoire d'installation des services ou du client et appuyez sur **Entrée**.

3. Choisissez le type d'opération et appuyez sur **Entrée**.

- Sélectionnez 1 pour supprimer les packages de distribution existants.
- Sélectionnez 2 pour installer un ou plusieurs packages de distribution.

La console répertorie les packages de distribution que vous pouvez installer ou supprimer.

4. Entrez les packages de que vous souhaitez installer ou supprimer, en séparant plusieurs packages de distribution par une virgule et appuyez sur **Entrée**.

5. Vérifiez l'état de l'installation ou de la suppression dans le fichier journal d'Integration Package Manager.

Le fichier journal est disponible à l'emplacement suivant : `<Integration Package Manager directory>/ IntegrationPackageManager_<date and timestamp>.log`

Installer ou supprimer des packages de distribution en mode silencieux

Vous pouvez exécuter Integration Package Manager en mode silencieux pour installer ou supprimer des packages de distribution. Le fichier de propriétés d'entrée en mode silencieux contient les propriétés permettant au gestionnaire de packages de s'exécuter en mode silencieux pour le service et les clients. Définissez la valeur appropriée pour chaque propriété dans le fichier.

1. Recherchez le fichier `IntegrationPackageManager.properties` à l'emplacement suivant : `<Integration Package Manager directory>/`

2. Modifiez le fichier de propriétés dans un éditeur de texte.

Le tableau suivant décrit les propriétés que vous pouvez modifier :

Nom de la propriété	Description
USER_INSTALL_DIR	Répertoire d'installation du service ou du client.
OPERATION_TYPE	Opération à effectuer : <ul style="list-style-type: none">- Définissez la propriété sur DELETE pour supprimer les packages de distribution existants.- Définissez la propriété sur EXTRACT pour installer un ou plusieurs packages de distribution.
SELECTED_HADOOP_LIBRARIES	Répertorie les packages de distribution et les versions. Entrez les packages de distribution que vous souhaitez installer ou supprimer. Séparez plusieurs packages par une virgule.

3. Enregistrez le fichier de propriétés.

4. Dans le répertoire d'Integration Package Manager, exécutez l'une des commandes suivantes :

- `./Server.sh silent` pour Linux ou UNIX
- `Server.bat silent` pour Windows
- `Client.bat silent` pour le client

Remarque: Pour exécuter la commande sous Windows, utilisez l'invite de commandes de l'administrateur.

5. Vérifiez l'état de l'installation ou de la suppression dans le fichier journal d'Integration Package Manager.

Le fichier journal se trouve à l'emplacement suivant : <Integration Package Manager directory>/IntegrationPackageManager_<date and timestamp>.log

Après l'installation

Pour utiliser les packages de distribution installés à l'aide du gestionnaire de packages, configurez la propriété ou la variable d'environnement sur les machines de service et clientes.

Configurez l'outil Developer tool.

Après avoir installé les packages de distribution dans l'outil Developer tool, mettez à jour le fichier developerCore.ini avec le package de distribution installé.

1. Recherchez le fichier developerCore.ini à l'emplacement suivant : <Informatica installation directory>\clients\DeveloperClient
2. Modifiez le fichier pour mettre à jour la propriété suivante :

```
-DINFA_HADOOP_DIST_DIR=hadoop\<Hadoop distribution name>_<version>
```

Par exemple :

```
-DINFA_HADOOP_DIST_DIR=hadoop\CDH_7.1
```

3. Redémarrez l'outil Developer tool.

Configuration des variables d'environnement

Certains adaptateurs nécessitent des variables d'environnement pour que le service d'intégration de données et le service d'accès aux métadonnées accèdent aux packages de distribution. Pour plus d'informations, reportez-vous à la section [Configure environment variables to process complex files](#).

ANNEXE C

Connexion à des bases de données sous UNIX ou Linux

Cette annexe comprend les rubriques suivantes :

- [Présentation de la connexion à des bases de données sous UNIX ou Linux, 275](#)
- [Connexion à une base de données universelle IBM DB2, 276](#)
- [Connexion à une base de données Microsoft SQL Server, 278](#)
- [Connexion à une base de données Oracle, 279](#)
- [Connexion à une base de données Sybase ASE, 281](#)
- [Connexion à une base de données Teradata, 283](#)
- [Connexion à une source de données JDBC, 286](#)
- [Connexion à une source de données ODBC, 286](#)
- [Exemple de fichier odbc.ini, 288](#)

Présentation de la connexion à des bases de données sous UNIX ou Linux

Pour utiliser la connectivité native, vous devez installer et configurer le logiciel client de base de données pour la base de données à laquelle vous voulez accéder. Pour assurer la compatibilité entre le service d'application et la base de données, utilisez les bibliothèques clients de la base de données appropriées et installez un logiciel client qui est compatible avec la version de la base de données. Pour augmenter les performances, utilisez la connectivité native.

L'installation d'Informatica inclut les pilotes ODBC DataDirect. Si vous avez des sources de données ODBC existantes créées avec une version antérieure de pilotes, vous devez créer de nouvelles sources de données ODBC utilisant les nouveaux pilotes. Configurez les connexions ODBC à l'aide des pilotes ODBC DataDirect fournis par Informatica ou des pilotes tiers ODBC étant conformes au niveau 2 ou plus.

Vous devez configurer une connexion de base de données pour les services suivants dans le domaine Informatica :

- Service de référentiel PowerCenter
- Service de référentiel modèle
- Service d'intégration de données
- Service Analyst

Lorsque vous vous connectez à des bases de données depuis un système Linux ou UNIX, utilisez les pilotes natifs pour vous connecter aux bases de données IBM DB2, Oracle ou Sybase ASE. Vous pouvez utiliser ODBC pour vous connecter à d'autres sources et cibles.

Connexion à une base de données universelle IBM DB2

Pour la connectivité native, installez la version IBM DB2 Client Application Enabler (CAE) appropriée pour la version de serveur de base de données IBM DB2. Pour assurer la compatibilité entre Informatica et les bases de données, utilisez les bibliothèques de client de base de données appropriées.

Configuration de la connectivité native

Vous pouvez configurer la connectivité native sur une base de données IBM DB2 pour augmenter les performances.

Les étapes suivantes fournissent une directive pour configurer la connectivité native. Pour des instructions spécifiques, consultez la documentation de la base de données.

1. Pour configurer la connectivité sur la machine sur laquelle le processus du service d'intégration de données, du service d'intégration PowerCenter ou du service de référentiel PowerCenter est exécuté, connectez-vous à la machine en tant qu'utilisateur pouvant démarrer un processus de service.
2. Définissez les variables d'environnement DB2INSTANCE, INSTHOME, DB2DIR et PATH.

Le logiciel UNIX IBM DB2 comporte toujours un nom d'utilisateur associé, souvent db2admin, qui sert de détenteur des configurations de la base de données. Cet utilisateur détient l'instance pour DB2.

DB2INSTANCE. Nom du détenteur de l'instance.

Utilisation d'un shell Bourne :

```
$ DB2INSTANCE=db2admin; export DB2INSTANCE
```

Utilisation d'un shell C :

```
$ setenv DB2INSTANCE db2admin
```

INSTHOME. Ceci est un chemin d'accès au répertoire de base db2admin.

Utilisation d'un shell Bourne :

```
$ INSTHOME=~db2admin
```

Utilisation d'un shell C :

```
$ setenv INSTHOME ~db2admin>
```

DB2DIR. Définissez la variable pour qu'elle désigne le répertoire d'installation IBM DB2 CAE. Par exemple, si le client est installé dans le répertoire /opt/IBM/db2/V9.7 :

Utilisation d'un shell Bourne :

```
$ DB2DIR=/opt/IBM/db2/V9.7; export DB2DIR
```

Utilisation d'un shell C :

```
$ setenv DB2DIR /opt/IBM/db2/V9.7
```

PATH. Pour exécuter les programmes de ligne de commande IBM DB2, définissez la variable pour inclure le répertoire bin de DB2.

Utilisation d'un shell Bourne :

```
$ PATH=${PATH}:$DB2DIR/bin; export PATH
```

Utilisation d'un shell C :

```
$ setenv PATH ${PATH}:$DB2DIR/bin
```

3. Définissez la variable de bibliothèque partagée pour inclure le répertoire lib de DB2.

Le logiciel client IBM DB2 contient un certain nombre de composants de bibliothèque partagée que les processus du service d'intégration de données, du service d'intégration PowerCenter et du service de référentiel PowerCenter chargent dynamiquement. Définissez la variable d'environnement de bibliothèque partagée de sorte que les services puissent trouver les bibliothèques partagées lors de l'exécution.

Le chemin d'accès à la bibliothèque partagée doit aussi inclure le répertoire d'installation Informatica (*server_dir*).

Définissez la variable d'environnement de bibliothèque partagée en fonction du système d'exploitation.

Le tableau suivant décrit les variables de bibliothèques partagées pour chaque système d'exploitation :

Système d'exploitation	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

Par exemple, utilisez la syntaxe suivante pour Linux :

- Utilisation d'un shell Bourne :

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib; export LD_LIBRARY_PATH
```

- Utilisation d'un shell C :

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib
```

Pour AIX :

- Utilisation d'un shell Bourne :

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$DB2DIR/lib; export LIBPATH
```

- Utilisation d'un shell C :

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$DB2DIR/lib
```

4. Éditez la valeur .cshrc ou .profile pour inclure l'ensemble complet de commandes shell. Enregistrez le fichier et soit déconnectez-vous et connectez-vous à nouveau, soit exécutez la commande source.

Utilisation d'un shell Bourne :

```
$ source .profile
```

Utilisation d'un shell C :

```
$ source .cshrc
```

5. Si la base de données DB2 réside sur la machine sur laquelle s'exécute le processus du service d'intégration de données, du service d'intégration PowerCenter ou du service de référentiel PowerCenter, configurez l'instance DB2 en tant qu'instance distante.

Exécutez la commande suivante pour vérifier s'il existe une entrée distante pour la base de données :

```
DB2 LIST DATABASE DIRECTORY
```

La commande indique toutes les bases de données auxquelles le client DB2 peut accéder et leurs propriétés de configuration. Si cette commande indique une entrée pour « Type d'entrée de répertoire » de type « Distant », passez à l'[7](#).

6. Si la base de données n'est pas configurée comme distante, exécutez la commande suivante pour vérifier si un nœud TCP/IP est catalogué pour l'hôte.

```
DB2 LIST NODE DIRECTORY
```

Si le nom du nœud est vide, vous pouvez en créer un lors de la configuration de la base de données. Utilisez la commande suivante pour configurer une base de données distante et, si nécessaire, créez un nœud :

```
db2 CATALOG TCP/IP NODE <nodename> REMOTE <hostname_or_address> SERVER <port number>
```

Exécutez la commande suivante pour cataloguer la base de données :

```
db2 CATALOG DATABASE <dbname> as <dbalias> at NODE <nodename>
```

Pour plus d'informations sur ces commandes, consultez la documentation de la base de données.

7. Vérifiez que vous pouvez vous connecter à la base de données DB2. Exécutez le processeur de ligne de commande DB2 et exécutez la commande :

```
CONNECT TO <dbalias> USER <username> USING <password>
```

Si la connexion est réussie, nettoyez à l'aide de la commande `CONNECT RESET` ou `TERMINATE`.

Connexion à une base de données Microsoft SQL Server

Utilisez la connexion Microsoft SQL Server pour vous connecter à une base de données Microsoft SQL Server depuis une machine UNIX ou Linux.

Configuration de l'authentification SSL via ODBC

Vous pouvez configurer l'authentification SSL pour Microsoft SQL Server via ODBC en utilisant le pilote du protocole DataDirect New SQL Server Wire Protocol.

1. Ouvrez le fichier `odbc.ini` et ajoutez une entrée pour la source de données ODBC et le pilote du protocole DataDirect New SQL Server Wire Protocol dans la section [ODBC Data Sources].
2. Ajoutez les attributs suivants dans le fichier `odbc.ini` pour configurer SSL ;

Le tableau suivant présente les attributs que vous devez ajouter au `odbc.ini` lorsque vous configurez l'authentification SSL :

Attribut	Description
EncryptionMethod	Méthode utilisée par le pilote pour crypter les données envoyées entre le pilote et le serveur de base de données. Définissez la valeur sur 1 pour crypter les données en utilisant SSL.
ValidateServerCertificate	Détermine si le pilote valide le certificat envoyé par le serveur de base de données lorsque cryptage SSL est activé. Définissez la valeur à 1 pour que le pilote valide le certificat du serveur.
TrustStore	Emplacement et nom du fichier entrepôt d'approbation Le fichier entrepôt d'approbation contient une liste d'autorités de certification que le pilote utilise pour l'authentification du serveur SSL.

Attribut	Description
TrustStorePassword	Mot de passe pour accéder au contenu du fichier entrepôt d'approbation.
HostNameInCertificate	Facultatif. Nom d'hôte qui est établi par l'administrateur SSL pour permettre au pilote de valider le nom d'hôte contenu dans le certificat.

Connexion à une base de données Oracle

Pour la connectivité native, installez la version de client Oracle appropriée pour votre version de serveur de base de données Oracle. Pour assurer la compatibilité entre Informatica et les bases de données, utilisez les bibliothèques de client de base de données appropriées.

Vous devez installer des versions compatibles du client Oracle et du serveur de base de données Oracle. Vous devez aussi installer la même version du client Oracle sur tous les ordinateurs qui le requièrent. Pour vérifier la compatibilité, contactez Oracle.

Configuration de la connectivité native

Vous pouvez configurer la connectivité native sur une base de données Oracle afin d'en augmenter les performances.

Les étapes suivantes fournissent une directive pour configurer la connectivité native par le biais d'Oracle Net Services ou de Net8. Pour des instructions spécifiques, consultez la documentation de la base de données.

1. Pour configurer la connectivité du processus de service d'intégration de données, du service d'intégration PowerCenter ou du service de référentiel PowerCenter, connectez-vous à la machine en tant qu'un utilisateur pouvant démarrer le processus de serveur.
2. Définissez les variables d'environnement ORACLE_HOME, NLS_LANG, TNS_ADMIN et PATH.

ORACLE_HOME. Définissez la variable sur le répertoire d'installation du client Oracle. Par exemple, si le client est installé dans le répertoire /HOME2/oracle : définissez la variable comme suit :

Utilisation d'un shell Bourne :

```
$ ORACLE_HOME=/HOME2/oracle; export ORACLE_HOME
```

Utilisation d'un shell C :

```
$ setenv ORACLE_HOME /HOME2/oracle
```

NLS_LANG Définissez la variable sur les paramètres régionaux (langue, territoire et jeu de caractères) que vous voulez que le client et le serveur de base de données utilisent avec le nom de connexion. La valeur de cette variable dépend de la configuration. Par exemple, si la valeur est american_america.UTF8, définissez la variable comme suit :

Utilisation d'un shell Bourne :

```
$ NLS_LANG=american_america.UTF8; export NLS_LANG
```

Utilisation d'un shell C :

```
$ NLS_LANG american_america.UTF8
```

Pour déterminer la valeur de cette variable, contactez l'administrateur.

TNS_ADMIN. Si le fichier tnsnames.ora n'est pas dans le même emplacement que l'emplacement d'installation du client Oracle, définissez la variable d'environnement TNS_ADMIN sur le répertoire dans

lequel réside le fichier `tnsnames.ora`. Par exemple, si le fichier est dans le répertoire `/HOME2/oracle/files`, définissez la variable comme suit :

Utilisation d'un shell Bourne :

```
$ TNS_ADMIN=$HOME2/oracle/files; export TNS_ADMIN
```

Utilisation d'un shell C :

```
$ setenv TNS_ADMIN=$HOME2/oracle/files
```

Remarque: Le fichier `tnsnames.ora` est stocké dans le répertoire suivant : `$ORACLE_HOME/network/admin`.

PATH. Pour exécuter les programmes de ligne de commande Oracle, définissez la variable pour inclure le répertoire `bin` d'Oracle.

Utilisation d'un shell Bourne :

```
$ PATH=${PATH}:$ORACLE_HOME/bin; export PATH
```

Utilisation d'un shell C :

```
$ setenv PATH ${PATH}:ORACLE_HOME/bin
```

3. Définissez la variable d'environnement de bibliothèque partagée.

Le logiciel client Oracle contient un certain nombre de composants de bibliothèque partagée que les processus de service d'intégration de données, du service d'intégration PowerCenter et du service de référentiel PowerCenter chargent dynamiquement. Pour rechercher les bibliothèques partagées lors de l'exécution, définissez la variable d'environnement de bibliothèque partagée.

Le chemin d'accès à la bibliothèque partagée doit aussi inclure le répertoire d'installation d'Informatica (`server_dir`).

Définissez la variable d'environnement de bibliothèque partagée sur `LD_LIBRARY_PATH`.

Par exemple, utilisez la syntaxe suivante :

- Utilisation d'un shell Bourne :

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib; export LD_LIBRARY_PATH
```

- Utilisation d'un shell C :

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib
```

4. Éditez la valeur `.cshrc` ou `.profile` pour inclure l'ensemble complet de commandes shell. Enregistrez le fichier et déconnectez-vous et reconnectez-vous ou exécutez la commande `source`.

Utilisation d'un shell Bourne :

```
$ source .profile
```

Utilisation d'un shell C :

```
$ source .cshrc
```

5. Vérifiez que le client Oracle est configuré pour accéder à la base de données.

Utilisez l'utilitaire `SQL*Net Easy Configuration` ou copiez un fichier `tnsnames.ora` existant dans le répertoire de base et modifiez-le.

Le fichier `tnsnames.ora` est stocké dans le répertoire suivant : `$ORACLE_HOME/network/admin`.

Saisissez la syntaxe correcte de la chaîne de connexion Oracle, généralement `databasename.world`.

Voici un exemple de fichier `tnsnames.ora`. Saisissez les informations de la base de données.

```
mydatabase.world =
  (DESCRIPTION
    (ADDRESS_LIST =
      (ADDRESS =
        (COMMUNITY = mycompany.world
```



```

        (PROTOCOL = TCP)
        (Host = mymachine)
        (Port = 1521)
    )
    (CONNECT_DATA =
        (SID = MYORA7)
        (GLOBAL_NAMES = mydatabase.world)
    )
)

```

Voici un exemple de fichier `tnsnames.ora` pour se connecter à Oracle à l'aide du gestionnaire de connexions Oracle :

```

ORCL19C_CMAN =
(description=
(address_list=
(source_route=yes)
(address=(protocol=tcp) (host=lnrh74ocm.mycompany.com) (port=1521))
(address=(protocol=tcp) (host=lnrh74oradb.mycompany.com) (port=1521))
)
(connect_data=
(service_name=ORCL19C.mycompany.com)
)
)

```

6. Vérifiez que vous pouvez vous connecter à la base de données Oracle.

Pour vous connecter à la base de données Oracle, lancez SQL*Plus et entrez les informations de connectivité. Si la connexion à la base de données échoue, vérifiez que vous avez correctement saisi toutes les informations de connectivité.

Saisissez le nom d'utilisateur et la chaîne de connexion définis dans le fichier `tnsnames.ora`.

Connexion à une base de données Sybase ASE

Pour la connectivité native, installez la version OpenClient appropriée pour votre version de base de données. Pour assurer la compatibilité entre Informatica et les bases de données, utilisez les bibliothèques de client de base de données appropriées.

Installez une version Open Client compatible avec le serveur de base de données Sybase ASE. Vous devez aussi installer la même version d'Open Client sur les ordinateurs hébergeant la base de données Sybase ASE et Informatica. Pour vérifier la compatibilité, contactez Sybase.

Si vous voulez créer, restaurer ou mettre à niveau un référentiel Sybase ASE, définissez *permettre nulls par défaut* sur TRUE au niveau de la base de données. La définition de cette option change le type null par défaut de la colonne pour le null conforme au standard SQL.

Configuration de la connectivité native

Vous pouvez configurer la connectivité native à une base de données Sybase ASE pour augmenter les performances.

Les étapes suivantes fournissent une directive pour configurer la connectivité native. Pour des instructions spécifiques, consultez la documentation de la base de données.

1. Pour configurer la connectivité avec le processus du service d'intégration de données, du service d'intégration PowerCenter ou du service de référentiel PowerCenter, connectez-vous à la machine en tant qu'un utilisateur pouvant démarrer le processus de serveur.
2. Définissez les variables d'environnement SYBASE et PATH.

SYBASE. Définissez la variable sur le répertoire d'installation client Sybase Open. Par exemple, si le client est installé dans le répertoire /usr/sybase :

Utilisation d'un shell Bourne :

```
$ SYBASE=/usr/sybase; export SYBASE
```

Utilisation d'un shell C :

```
$ setenv SYBASE /usr/sybase
```

PATH. Pour exécuter les programmes de ligne de commande Sybase, définissez la variable de façon à ce qu'elle inclue le répertoire bin de Sybase OCS.

Utilisation d'un shell Bourne :

```
$ PATH=${PATH}:/usr/sybase/OCS-15_0/bin; export PATH
```

Utilisation d'un shell C :

```
$ setenv PATH ${PATH}:/usr/sybase/OCS-15_0/bin
```

3. Définissez la variable d'environnement de bibliothèque partagée.

Le logiciel Sybase Open Client contient un certain nombre de composants de bibliothèque partagée que les processus du service d'intégration de données, du service d'intégration PowerCenter et du service de référentiel PowerCenter chargent dynamiquement. Définissez la variable d'environnement de bibliothèque partagée de sorte que les services puissent trouver les bibliothèques partagées lors de l'exécution.

Le chemin d'accès à la bibliothèque partagée doit aussi inclure le répertoire d'installation des services Informatica (*server_dir*).

Définissez la variable d'environnement de bibliothèque partagée en fonction du système d'exploitation.

Le tableau suivant décrit les variables de bibliothèques partagées pour chaque système d'exploitation.

Système d'exploitation	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

Par exemple, utilisez la syntaxe suivante pour Linux :

- Utilisation d'un shell Bourne :

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64; export LD_LIBRARY_PATH
```

- Utilisation d'un shell C :

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64;
```

Pour AIX

- Utilisation d'un shell Bourne :

```
$ LIBPATH=${LIBPATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64; export LIBPATH
```

- Utilisation d'un shell C :

```
$ setenv LIBPATH ${LIBPATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64;
```

4. Éditez la valeur .cshrc ou .profile pour inclure l'ensemble complet de commandes shell. Enregistrez le fichier et déconnectez-vous et reconnectez-vous ou exécutez la commande source.

Utilisation d'un shell Bourne :

```
$ source .profile
```

Utilisation d'un shell C :

```
$ source .cshrc
```

5. Vérifiez le nom du serveur Sybase ASE dans le fichier des interfaces Sybase stocké dans le répertoire \$SYBASE.
6. Vérifiez que vous pouvez vous connecter à la base de données Sybase ASE.

Pour vous connecter à la base de données Sybase ASE, lancez ISQL et entrez les informations de connectivité. Si la connexion à la base de données échoue, vérifiez que vous avez correctement saisi toutes les informations de connectivité.

Les noms d'utilisateurs et de base de données sont sensibles à la casse.

Connexion à une base de données Teradata

Installez et configurez le logiciel client natif sur les machines sur lesquelles le processus du service d'intégration de données ou du service d'intégration PowerCenter est exécuté. Pour assurer la compatibilité entre Informatica et les bases de données, utilisez les bibliothèques client de base de données appropriées.

Installez le service d'intégration de données, le pilote Teradata ODBC et tout autre logiciel client Teradata dont vous pouvez avoir besoin sur la machine sur laquelle le service d'intégration de données ou le service d'intégration PowerCenter est exécuté. Vous devez également configurer la connectivité ODBC.

Remarque: Sur la base des recommandations de Teradata, Informatica utilise ODBC pour se connecter à Teradata. ODBC est une interface native pour Teradata.

Configuration de la connectivité ODBC

Vous pouvez configurer la connectivité ODBC vers une base de données Teradata.

Les étapes suivantes fournissent une directive pour configurer la connectivité ODBC. Pour des instructions spécifiques, consultez la documentation de la base de données.

1. Pour configurer la connectivité pour le processus de service d'intégration, connectez-vous à la machine en tant qu'utilisateur pouvant démarrer un processus de service.
2. Définissez les variables d'environnement TERADATA_HOME, ODBC_HOME et PATH.

TERADATA_HOME. Définissez la variable sur le répertoire d'installation du pilote Teradata. Les valeurs par défaut sont les suivantes :

Utilisation d'un shell Bourne :

```
$ TERADATA_HOME=/opt/teradata/client/<version>; export TERADATA_HOME
```

Utilisation d'un shell C :

```
$ setenv TERADATA_HOME /opt/teradata/client/<version>
```

ODBC_HOME. Définissez la variable sur le répertoire d'installation ODBC. Par exemple :

Utilisation d'un shell Bourne :

```
$ ODBC_HOME=$INFA_HOME/ODBC<version>; export ODBC_HOME
```

Utilisation d'un shell C :

```
$ setenv ODBC_HOME $INFA_HOME/ODBC<version>
```

PATH Pour exécuter l'utilitaire *ddtestlib* et pour vérifier que le gestionnaire des pilotes ODBC d'UNIX peut charger les fichiers de pilote, définissez la variable comme suit :

Utilisation d'un shell Bourne :

```
PATH="${PATH}:%ODBCHOME/bin:%TERADATA_HOME/bin"
```

Utilisation d'un shell C :

```
$ setenv PATH ${PATH}:%ODBCHOME/bin:%TERADATA_HOME/bin
```

3. Définissez la variable d'environnement de bibliothèque partagée.

Le logiciel Teradata contient plusieurs composants de bibliothèque partagée que le processus du service d'intégration charge dynamiquement. Définissez la variable d'environnement de bibliothèque partagée de sorte que les services puissent trouver les bibliothèques partagées lors de l'exécution.

Le chemin d'accès à la bibliothèque partagée doit aussi inclure le répertoire d'installation du service Informatica (*server_dir*).

Définissez la variable d'environnement de bibliothèque partagée en fonction du système d'exploitation.

Le tableau suivant décrit les variables de bibliothèques partagées pour chaque système d'exploitation :

Système d'exploitation	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

Par exemple, utilisez la syntaxe suivante pour Linus :

- Utilisation d'un shell Bourne :

```
$ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:%HOME/server_dir:%ODBCHOME/lib:
%TERADATA_HOME/lib64:%TERADATA_HOME/odbc_64/lib";
export LD_LIBRARY_PATH
```

- Utilisation d'un shell C :

```
$ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:%HOME/server_dir:%ODBCHOME/
lib:%TERADATA_HOME/lib64:
%TERADATA_HOME/odbc_64/lib"
```

Pour AIX

- Utilisation d'un shell Bourne :

```
$ LIBPATH=${LIBPATH}:%HOME/server_dir:%ODBCHOME/lib:%TERADATA_HOME/
lib64:%TERADATA_HOME/odbc_64/lib; export LIBPATH
```

- Utilisation d'un shell C :

```
$ setenv LIBPATH ${LIBPATH}:%HOME/server_dir:%ODBCHOME/lib:%TERADATA_HOME/lib64:
%TERADATA_HOME/odbc_64/lib
```

4. Éditez le fichier *odbc.ini* existant ou copiez le fichier *odbc.ini* dans le répertoire de base et éditez-le.

Ce fichier existe dans le répertoire *%ODBCHOME*.

```
$ cp %ODBCHOME/odbc.ini %HOME/.odbc.ini
```

Ajoutez une entrée pour la source de données Teradata dans la section [Sources de données ODBC] et configurez la source de données.

Par exemple, pour les utilitaires Teradata Parallel Transporter, version 15.10 :

```
MY_TERADATA_SOURCE=Teradata Driver
[MY_TERADATA_SOURCE]
Driver=/opt/teradata/client/15.10/lib64/tdata.so
Description=NCR 3600 running Teradata V1R5.2
DBCName=208.199.59.208
DateTimeFormat=AAA
SessionMode=ANSI
DefaultDatabase=
Username=
Password=
```

Par exemple, pour les utilitaires Teradata Parallel Transporter, version 16.20 :

```
MY_TERADATA_SOURCE=Teradata Driver
[dwtera]
Driver=/opt/teradata/client/16.20/lib64/tdataodbc_sb64.so
Description=NCR 3600 running Teradata V1R5.2
DBCName=tdvbe1510
LastUser=
Username=
Password=
Database=
DefaultDatabase=
UseNativeLOBSupport=Yes
CharacterSet=UTF8
SessionMode=ANSI
```

5. Définissez `DateTimeFormat` sur AAA dans la configuration ODBC des données de Teradata.
6. Définissez éventuellement `SessionMode` sur ANSI. Si vous utilisez le mode de session ANSI, Teradata n'annule pas la transaction quand une erreur de ligne se produit.

Si vous choisissez le mode de session Teradata, Teradata annule la transaction quand une erreur de ligne se produit. En mode Teradata, le processus du service d'intégration ne peut pas détecter l'annulation et ne le signale pas dans le journal de session.

7. Pour configurer la connexion à une seule base de données Teradata, entrez le nom `DefaultDatabase`. Pour créer une seule connexion à la base de données par défaut, entrez le nom d'utilisateur et le mot de passe. Pour vous connecter à plusieurs bases de données, à l'aide du même DSN de ODBC, ne remplissez pas le champ `DefaultDatabase`.

Pour plus d'informations sur la connectivité de Teradata, consultez la documentation du pilote ODBC de Teradata.

8. Vérifiez que la dernière entrée dans le fichier `odbc.ini` est `InstallDir` et définissez-le sur le répertoire d'installation `odbc`.

Par exemple :

```
InstallDir=<Informatica installation directory>/ODBC<version>
```

9. Éditez la valeur `.cshrc` ou `.profile` pour inclure l'ensemble complet de commandes shell.
10. Enregistrez le fichier et déconnectez-vous et reconnectez-vous ou exécutez la commande source.

Utilisation d'un shell Bourne :

```
$ source .profile
```

Utilisation d'un shell C :

```
$ source .cshrc
```

11. Pour chaque source de données que vous utilisez, notez le nom de fichier sous `Driver=<parameter>` dans l'entrée de source de données de `odbc.ini`. Utilisez l'utilitaire `ddtestlib` pour vérifier que le gestionnaire de pilote ODBC DataDirect peut charger le fichier de pilote.

Par exemple, si vous avez l'entrée de pilote :

```
Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
```

exécutez la commande suivante :

```
ddtestlib /u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
```

12. Testez la connexion à l'aide de BTEQ ou d'un autre outil de client Teradata.

Connexion à une source de données JDBC

Pour permettre au service d'intégration de données d'écrire dans des cibles relationnelles, téléchargez les fichiers .jar du pilote JDBC dans l'hôte du service d'intégration de données et dans toutes les machines clientes disposant de cibles relationnelles.

Récupérez le fichier .jar du pilote depuis le fournisseur de bases de données. Pour accéder, par exemple, à une base de données Oracle, téléchargez le fichier `ojdbc.jar` sur le site Web Oracle.

1. Placez le fichier .jar du pilote JDBC dans le répertoire suivant sur la machine exécutant le service d'intégration de données `<Informatica installation directory>/externaljdbcjars`. Recyclez ensuite le service d'intégration de données.
2. Placez le fichier .jar du pilote JDBC dans le répertoire suivant sur les machines qui hébergent l'outil Developer tool : `<Informatica installation directory>/clients/externaljdbcjars`. Puis, recyclez l'outil Developer tool.

Connexion à une source de données ODBC

Installez et configurez le logiciel client natif sur la machine sur laquelle le service d'intégration de données, le service d'intégration PowerCenter et le service de référentiel PowerCenter sont exécutés. Installez et configurez également tout logiciel d'accès client sous-jacent requis par le pilote ODBC. Pour garantir la compatibilité entre Informatica et les bases de données, utilisez les bibliothèques client de base de données appropriées.

L'installation d'Informatica inclut les pilotes ODBC DataDirect. Si le fichier `odbc.ini` contient des connexions qui utilisent des versions antérieures du pilote ODBC, mettez à jour les informations de connexion pour utiliser les nouveaux pilotes. Utilisez le système DSN pour indiquer une source de données ODBC sous Windows.

1. Sur la machine sur laquelle le service d'application est exécuté, connectez-vous en tant qu'utilisateur pouvant démarrer un processus de service.
2. Définissez les variables d'environnement `ODBCHOME` et `PATH`.

ODBCHOME. Définissez le répertoire d'installation ODBC de DataDirect. Par exemple, si le répertoire d'installation est `/export/home/Informatica/10.0.0/ODBC7.1`.

Utilisation d'un shell Bourne :

```
$ ODBCHOME=/export/home/Informatica/10.0.0/ODBC7.1; export ODBCHOME
```

Utilisation d'un shell C :

```
$ setenv ODBCHOME /export/home/Informatica/10.0.0/ODBC7.1
```

PATH. Pour exécuter les programmes de ligne de commande ODBC, tels que `ddtestlib`, définissez la variable de façon à ce qu'elle inclue le répertoire bin ODBC.

Utilisation d'un shell Bourne :

```
$ PATH=${PATH}:$ODBCHOME/bin; export PATH
```

Utilisation d'un shell C :

```
$ setenv PATH ${PATH}:$ODBCHOME/bin
```

Exécutez l'utilitaire *ddtestlib* pour vérifier que le gestionnaire de pilote ODBC DataDirect peut charger les fichiers de pilote.

3. Définissez la variable d'environnement de bibliothèque partagée.

Le logiciel ODBC contient un certain nombre de composants de bibliothèque partagée que les processus de service chargent dynamiquement. Définissez la variable d'environnement de bibliothèque partagée de sorte que les services puissent trouver les bibliothèques partagées lors de l'exécution.

Le chemin d'accès à la bibliothèque partagée doit aussi inclure le répertoire d'installation Informatica (*server_dir*).

Définissez la variable d'environnement de bibliothèque partagée en fonction du système d'exploitation.

Le tableau suivant décrit les variables de bibliothèques partagées pour chaque système d'exploitation :

Système d'exploitation	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

Par exemple, utilisez la syntaxe suivante pour Linux :

- Utilisation d'un shell Bourne :

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib; export LD_LIBRARY_PATH
```

- Utilisation d'un shell C :

```
$ setenv LD_LIBRARY_PATH $HOME/server_dir:$ODBCHOME:${LD_LIBRARY_PATH}
```

Pour AIX

- Utilisation d'un shell Bourne :

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib; export LIBPATH
```

- Utilisation d'un shell C :

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib
```

4. Éditez le fichier *odbc.ini* existant ou copiez le fichier *odbc.ini* dans le répertoire de base et éditez-le.

Ce fichier existe dans le répertoire *\$ODBCHOME*.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

Ajoutez une entrée pour la source de données ODBC dans la section [Sources de données ODBC] et configurez la source de données.

Par exemple :

```
MY_MSSQLSERVER_ODBC_SOURCE=<Driver name or data source description>
[MY_MSSQLSERVER_ODBC_SOURCE]
Driver=<path to ODBC drivers>
Description=DataDirect 8.0 SQL Server Wire Protocol
Database=<SQLServer_database_name>
LogonID=<username>
Password=<password>
Address=<TCP/IP address>,<port number>
QuoteId=No
```

```
AnsiNPW=No
ApplicationsUsingThreads=1
```

Il se peut que ce fichier existe déjà si vous avez configuré une ou plusieurs sources de données ODBC.

5. Vérifiez que la dernière entrée dans le fichier `odbc.ini` est `InstallDir` et définissez-le sur le répertoire d'installation `odbc`.

Par exemple :

```
InstallDir=/export/home/Informatica/10.0.0/ODBC7.1
```

6. Si vous utilisez le fichier `odbc.ini` dans le répertoire de base, définissez la variable d'environnement `ODBCINI`.

Utilisation d'un shell Bourne :

```
$ ODBCINI=$HOME/.odbc.ini; export ODBCINI
```

Utilisation d'un shell C :

```
$ setenv ODBCINI $HOME/.odbc.ini
```

7. Éditez la valeur `.cshrc` ou `.profile` pour inclure l'ensemble complet de commandes shell. Enregistrez le fichier et déconnectez-vous et reconnectez-vous ou exécutez la commande `source`.

Utilisation d'un shell Bourne :

```
$ source .profile
```

Utilisation d'un shell C :

```
$ source .cshrc
```

8. Utilisez l'utilitaire `ddtestlib` pour vérifier que le gestionnaire du pilote ODBC DataDirect peut charger le fichier de pilote que vous avez indiqué pour la source de données dans le fichier `odbc.ini`.

Par exemple, si vous avez l'entrée de pilote :

```
Driver = /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
```

exécutez la commande suivante :

```
ddtestlib /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
```

9. Installez et configurez tout logiciel d'accès client sous-jacent requis par le pilote ODBC.

Remarque: Bien que certains pilotes ODBC soient autonomes et ont toutes les informations à l'intérieur du fichier `.odbc.ini`, la plupart ne le sont pas. Par exemple, si vous voulez utiliser un pilote ODBC pour accéder à Sybase IQ, installez le logiciel client réseau Sybase IQ et définissez les variables d'environnement appropriées.

Pour utiliser les pilotes ODBC Informatica (DWxxxxnn.so), définissez manuellement la variable d'environnement `PATH` et celle du chemin d'accès aux bibliothèques partagées. Sinon, exécutez le script `odbc.sh` ou `odbc.csh` dans le dossier `$ODBCHOME`. Ce script permettra de définir le `PATH` requis et les variables d'environnement de chemin de bibliothèque partagée pour les pilotes ODBC fournis par Informatica.

Exemple de fichier `odbc.ini`

L'exemple suivant illustre les entrées pour les pilotes ODBC dans le fichier `ODBC.ini` :

```
[ODBC Data Sources]
SQL Server Legacy Wire Protocol=DataDirect 7.1 SQL Server Legacy Wire Protocol
DB2 Wire Protocol=DataDirect 7.1 DB2 Wire Protocol
Informix Wire Protocol=DataDirect 7.1 Informix Wire Protocol
Oracle Wire Protocol=DataDirect 8.0 Oracle Wire Protocol
Sybase Wire Protocol=DataDirect 7.1 Sybase Wire Protocol
SQL Server Wire Protocol=DataDirect 8.0 SQL Server Wire Protocol
```



```

MySQL Wire Protocol=DataDirect 7.1 MySQL Wire Protocol
PostgreSQL Wire Protocol=DataDirect 7.1 PostgreSQL Wire Protocol
Greenplum Wire Protocol=DataDirect 7.1 Greenplum Wire Protocol

[ODBC]
IANAAppCodePage=4
InstallDir=/<<Informatica installation directory>/ODBC7.1
Trace=0
TraceFile=odbctrace.out
TraceDll=/<<Informatica installation directory>/ODBC7.1/lib/DWtrc27.so

[DB2 Wire Protocol]
Driver=/<<Informatica installation directory>/ODBC7.1/lib/DWdb227.so
Description=DataDirect 7.1 DB2 Wire Protocol
AccountingInfo=
AddStringToCreateTable=
AlternateID=
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CatalogSchema=
CharsetFor65535=0
ClientHostName=
ClientUser=
#Collection applies to z/OS and iSeries only
Collection=
ConcurrentAccessResolution=0
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CurrentFuncPath=
#Database applies to DB2 UDB only
Database=<database_name>
DefaultIsolationLevel=1
DynamicSections=1000
EnableBulkLoad=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GrantAuthid=PUBLIC
GrantExecute=1
GSSClient=native
HostNameInCertificate=
IpAddress=<DB2_server_host>
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
#Location applies to z/OS and iSeries only
Location=<location_name>
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
PackageCollection=NULLID
PackageNamePrefix=DD
PackageOwner=
Pooling=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
TcpPort=50000
TrustStore=

```

```

TrustStorePassword=
UseCurrentSchema=0
ValidateServerCertificate=1
WithHold=1
XMLDescribeType=-10

[Informix Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWifcl27.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ServerName=<Informix_server>
TrimBlankFromIndexName=1
UseDelimitedIdentifiers=0

[Oracle Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWora28.so
Description=DataDirect 8.0 Oracle Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
AccountingInfo=
Action=
ApplicationName=
ArraySize=60000
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CachedCursorLimit=32
CachedDescLimit=0
CatalogIncludesSynonyms=1
CatalogOptions=0
ClientHostName=
ClientID=
ClientUser=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
DataIntegrityLevel=0
DataIntegrityTypes=MD5,SHA1
DefaultLongDataBufLen=1024
DescribeAtPrepare=0
EditionName=
EnableBulkLoad=0
EnableDescribeParam=0
EnableNcharSupport=0
EnableScrollableCursors=1
EnableStaticCursorsForLongData=0
EnableTimestampWithTimeZone=0
EncryptionLevel=0
EncryptionMethod=0
EncryptionTypes=AES128,AES192,AES256,DES,3DES112,3DES168,RC4_40,RC4_56,RC4_128,
RC4_256
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
GSSClient=native
HostName=<Oracle_server>
HostNameInCertificate=

```

```

InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LocalTimeZoneOffset=
LockTimeOut=-1
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Module=
Password=
Pooling=0
PortNumber=<Oracle_server_port>
ProcedureRetResults=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
ReportRecycleBin=0
ServerName=<server_name in tnsnames.ora>
ServerType=0
ServiceName=
SID=<Oracle_System_Identifier>
TimestampEscapeMapping=0
TNSNamesFile=<tnsnames.ora_filename>
TrustStore=
TrustStorePassword=
UseCurrentSchema=1
ValidateServerCertificate=1
WireProtocolMode=2

[Sybase Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWase27.so
Description=DataDirect 7.1 Sybase Wire Protocol
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
ArraySize=50
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
Charset=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CursorCacheSize=1
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableBulkLoad=0
EnableDescribeParam=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GSSClient=native
HostNameInCertificate=
InitializationString=
Language=
LoadBalancing=0
LoadBalanceTimeout=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
NetworkAddress=<Sybase_host,Sybase_server_port>

```

```

OptimizePrepare=1
PacketSize=0
Password=
Pooling=0
QueryTimeout=0
RaiseErrorPositionBehavior=0
ReportCodePageConversionErrors=0
SelectMethod=0
ServicePrincipalName=
TruncateTimeTypeFractions=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=

[SQL Server Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWsqls28.so
Description=DataDirect 8.0 SQL Server Wire Protocol
AlternateServers=
AlwaysReportTriggerResults=0
AnsiNPW=1
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadOptions=2
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
EnableBulkLoad=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTasTimestamp=0
FetchTWFSasTime=1
GSSClient=native
HostName=<SQL_Server_host>
HostNameInCertificate=
InitializationString=
Language=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
PacketSize=-1
Password=
Pooling=0
PortNumber=<SQL_Server_server_port>
QueryTimeout=0
ReportCodePageConversionErrors=0
SnapshotSerializable=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=
XML Describe Type=-10

[MySQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWmysql27.so
Description=DataDirect 7.1 MySQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0

```

```

ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableDescribeParam=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
HostName=<MySQL_host>
HostNameInCertificate=
InteractiveClient=0
LicenseNotice=You must purchase commercially licensed MySQL database software or
a MySQL Enterprise subscription in order to use the DataDirect Connect for ODBC
for MySQL Enterprise driver with MySQL software.
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LogonID=
LoginTimeout=15
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<MySQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TreatBinaryAsChar=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1

[PostgreSQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWpsql27.so
Description=DataDirect 7.1 PostgreSQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=1
EncryptionMethod=1
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
GSSClient=native
HostName=<PostgreSQL_host>
HostNameInCertificate=<Host name in SSL certificate>
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<PostgreSQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
TrustStore=<Path of the truststore certificates>
TrustStorePassword=<Password of the truststore certificates>

```

```

ValidateServerCertificate=1
XMLDescribeType=-10

[Greenplum Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWgplm27.so
Description=DataDirect 7.1 Greenplum Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=0
EnableKeysetCursors=0
EncryptionMethod=0
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
HostName=<Greenplum_host>
InitializationString=
KeyPassword=
KeysetCursorOptions=0
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<Greenplum_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
XMLDescribeType=-10

```

Remarque: Vous devrez peut-être personnaliser les entrées DSN dans le fichier `ODBC.ini`, en fonction du pilote tiers que vous utilisez. Pour plus d'informations sur les entrées DSN, consultez la documentation correspondante du pilote tiers.

INDEX

A

- AddLicense (infacmd)
 - dépannage [210](#)
- avant l'installation des clients
 - vérification des spécifications de l'installation [258](#)
 - vérification des spécifications système minimales [258](#)

B

- base de données de flux de travail
 - Configuration requise de la base de données PostgreSQL [55](#)
 - Configuration requise de Microsoft Azure SQL Database [54](#)
- base de données, préparations
 - référentiels [39](#)
- bases de données
 - connexion à (UNIX) [275](#)
 - connexion à IBM DB2 [276](#)
 - connexion à Oracle [279](#)
 - connexion à Sybase ASE [281](#)
 - connexion à Teradat (UNIX) [283](#)
 - référentiel [39](#)
 - test des connexions [63](#)
- bases de données cible
 - connexion par le biais de ODBC (UNIX) [286](#)
 - connexion via JDBC (UNIX) [286](#)
- bases de données source
 - connexion via JDBC (UNIX) [286](#)

C

- cache d'objet de données
 - Configuration requise de Microsoft Azure SQL Database [51](#)
 - configuration requise pour la base de données Oracle [51](#)
 - spécifications de la base de données [50](#)
 - spécifications de la base de données IBM DB2 [51](#)
 - spécifications de la base de données Microsoft SQL Server [51](#)
- catalina.out
 - dépannage de l'installation [208](#)
- chemins de bibliothèque
 - variables d'environnement [31](#)
- clés de licence
 - vérification [36](#)
- clients
 - configuration pour les domaines sécurisés [260](#)
- clients de bases de données
 - clients natifs Microsoft SQL Server [63](#)
 - clients Oracle [63](#)
 - clients Sybase Open Client [63](#)
 - configuration [63](#)
 - IBM DB2 client application enabler [63](#)
 - variables d'environnement [63](#)
- clients Informatica
 - désinstallation [266](#)

- clients Informatica (*a continué*)
 - installation en mode graphique [258](#)
 - installation en mode silencieux [263](#)
- compatibilité des pages de code
 - paramètre régional [213](#)
 - services d'application [213](#)
- comptes d'utilisateur
 - Référentiel modèle [233](#)
 - UNIX [32](#)
- comptes d'utilisateur de la base de données.
 - directives de configuration [39](#)
- conditions requises pour l'installation
 - variables d'environnement [31](#)
- configuration
 - domaines [213](#)
 - variables d'environnement sous UNIX [216](#)
 - variables d'environnement [215](#)
- configuration requise de la base de données Microsoft SQL Server
 - référentiel de configuration du domaine [60](#)
- Configuration requise de la base de données PostgreSQL
 - base de données de flux de travail [55](#)
- configuration requise de logiciels tiers
 - outil Developer tool [258](#)
- Configuration requise de Microsoft Azure SQL Database
 - base de données de flux de travail [54](#)
 - cache d'objet de données [51](#)
 - entrepôt de données de référence [48](#)
 - référentiel de configuration du domaine [42](#), [59](#)
- configuration requise pour l'installation
 - fichiers keystore [33](#)
 - fichiers truststore [33](#)
 - spécifications de port [28](#)
- configuration requise pour la base de données
 - base de données de flux de travail [53](#)
 - entrepôt de profilage [51](#)
- configuration requise pour la base de données IBM DB2
 - cache d'objet de données [51](#)
 - entrepôt de données de référence [48](#)
 - entrepôt de profilage [52](#)
- configuration requise pour la base de données Microsoft SQL Server
 - cache d'objet de données [51](#)
 - entrepôt de données de référence [48](#)
 - entrepôt de profilage [52](#)
 - référentiel de configuration du domaine [42](#)
- configuration requise pour la base de données Oracle
 - cache d'objet de données [51](#)
 - entrepôt de données de référence [49](#)
 - référentiel de flux de travail [55](#)
- Configuration requise pour la base de données Oracle
 - Référentiel modèle [60](#)
- Configuration requise pour la base de données PostgreSQL
 - Référentiel de configuration du domaine [43](#)
- configuration système requise
 - minimale [25](#)
- connexion
 - bases de données UNIX [275](#)

- connexion (*a continué*)
 - service d'intégration à IBM DB2 (Windows) [276](#)
 - Service d'intégration aux sources de données JDBC (UNIX) [286](#)
 - Service d'intégration aux sources de données ODBC (UNIX) [286](#)
 - service d'intégration vers Oracle (UNIX) [279](#)
 - service d'intégration vers Sybase ASE (UNIX) [281](#)
- connexions
 - création de connexions de bases de données [221](#), [226](#)
 - Oracle propriétés [224](#)
 - Propriétés de Microsoft Azure SQL Database [222](#)
 - Propriétés de PostgreSQL [225](#)
 - propriétés IBM DB2 [221](#)
 - propriétés Microsoft SQL Server [223](#)
- connexions à la base de données
 - création [221](#)

D

- dbs2 connect
 - test des connexions de bases de données [63](#)
- dépannage
 - création de domaines [209](#)
 - jonction de domaines [209](#)
 - licences [210](#)
 - ping sur les domaines [210](#)
 - référentiel de configuration du domaine [208](#)
 - services Informatica [209](#)
- désinstallation
 - règles et instructions [266](#)
- domaines
 - configuration [213](#)
 - ports [28](#)
 - présentation [17](#)
- domaines sécurisés
 - configuration des clients [260](#)

E

- Enterprise Data Catalog
 - installation en mode silencieux [203](#)
- entrepôt de données de référence
 - Configuration requise de Microsoft Azure SQL Database [48](#)
 - configuration requise pour la base de données Oracle [49](#)
 - spécifications de la base de données [47](#)
 - spécifications de la base de données IBM DB2 [48](#)
 - spécifications de la base de données Microsoft SQL Server [48](#)
- entrepôt de profilage
 - configuration requise pour la base de données [51](#)
 - configuration requise pour la base de données IBM DB2 [52](#)
 - spécifications de la base de données Microsoft SQL Server [52](#)
- exemples
 - fichier odbci.ini [288](#)
- Exigences de la base de données PostgreSQL
 - Référentiel modèle [60](#)

F

- fichier host
 - Service d'intégration de données [237](#)
- fichier odbci.ini
 - exemple [288](#)
- fichiers journaux
 - catalina.out [208](#)
 - installation [206](#)
 - journaux d'installation [207](#)

- fichiers journaux (*a continué*)
 - journaux de débogage [207](#)
 - node.log [208](#)
 - types [206](#)
- fichiers keystore
 - configuration requise pour l'installation [33](#)
- fichiers truststore
 - configuration requise pour l'installation [33](#)
- flux de travail
 - configuration requise pour la base de données [53](#)
 - configuration requise pour la base de données Oracle [55](#)
 - spécifications de la base de données IBM DB2 [53](#)
 - spécifications de la base de données Microsoft SQL Server [54](#)

G

- Gestionnaire de service
 - fichiers journaux [208](#)

H

- HTTPS
 - configuration requise pour l'installation [33](#)

I

- i10Pi
 - UNIX [95](#)
- IATMPDIR
 - variables d'environnement [31](#)
- IBM DB2
 - connexion à un service d'intégration (Windows) [276](#)
- infacmd
 - ajout de nœuds aux domaines [209](#)
 - ping sur objets [210](#)
- infasetup
 - définition de domaines [209](#)
 - définition des nœuds de travail [209](#)
- Informatica Administrator
 - connexion [220](#)
- Informatica Developer
 - Configuration du répertoire d'espace de travail local [260](#)
 - installation des langues [259](#)
 - machines distantes [260](#)
 - machines locales [260](#)
- installation
 - sauvegarde préalable des fichiers [31](#)
- isql
 - test des connexions de bases de données [63](#)

J

- journaux d'installation
 - descriptions [207](#)
- journaux de débogage
 - dépannage de l'installation [207](#)
- JRE_HOME
 - variables d'environnement [31](#)

L

- LANG
 - variables d'environnement régionales [31](#)

LANG (a continué)

variables d'environnement [214](#)

langues

outils clients [259](#)

LC_ALL

variables d'environnement régionales [31](#)

variables d'environnement [214](#)

LC_CTYPE

variables d'environnement [214](#)

licences

ajout [210](#)

Linux

variables d'environnement client de base de données [63](#)

localhost

Service d'intégration de données [237](#)

M

Microsoft SQL Server

connexion sous UNIX [278](#)

mises à niveau

sauvegarde préalable des fichiers [31](#)

mode graphique

installation des clients Informatica [258](#)

mode silencieux

Installation d'Enterprise Data Catalog [203](#)

installation des clients Informatica [263](#)

installation des services Informatica [201](#)

N

node.log

dépannage de l'installation [208](#)

nœuds

dépannage [209](#)

O

Oracle

connexion à un service d'intégration (UNIX) [279](#)

Oracle database requirements

profiling warehouse [52](#)

outil Developer tool

configuration requise de logiciels tiers [258](#)

P

PATH

variables d'environnement [31](#)

Ping (infacmd)

dépannage [210](#)

ports

domaines [28](#)

services d'application [28](#)

spécifications [28](#)

pré-installation

i10Pi sous UNIX [95](#)

prérequis de la base de données

Référentiel modèle [58](#)

prérequis de la base de données IBM DB2

base de données du référentiel modèle [41](#)

profiling warehouse

Oracle database requirements [52](#)

R

référentiel de configuration du domaine

configuration requise de la base de données Microsoft SQL Server [60](#)

Configuration requise de Microsoft Azure SQL Database [42](#), [59](#)

configuration requise pour la base de données Microsoft SQL Server [42](#)

Configuration requise pour la base de données Oracle [43](#)

dépannage [208](#)

préparation des bases de données [41](#)

prérequis de la base de données IBM DB2 [41](#)

spécifications de la base de données IBM DB2 [58](#)

spécifications de la base de données Sybase ASE [43](#)

Référentiel de configuration du domaine

Configuration requise pour la base de données PostgreSQL [43](#)

Référentiel modèle

Configuration requise pour la base de données Oracle [60](#)

Exigences de la base de données PostgreSQL [60](#)

prérequis de la base de données [58](#)

prérequis de la base de données IBM DB2 [41](#)

spécifications de la base de données IBM DB2 [58](#)

utilisateurs [233](#)

référentiels

configuration de la connectivité native [62](#)

installation des clients de bases de données [63](#)

préparation des bases de données [39](#)

S

sauvegarde des fichiers

avant l'installation [31](#)

avant la mise à niveau [31](#)

serveur Informatica

désinstallation [266](#)

service Analyst

après la création [242](#)

Service Analyst

configuration [239](#)

création [239](#)

prérequis [219](#)

répertoires temporaires [219](#)

Service d'accès aux métadonnées

création [251](#)

service d'intégration de données

après la création [237](#)

Service d'intégration de données

configuration [234](#)

configuration du fichier host [237](#)

création [234](#)

Service de catalogue

création [170](#), [247](#)

Service de cluster Informatica

création [169](#), [242](#)

Service de gestion de contenu

configuration [237](#)

création [237](#), [238](#)

service de référentiel modèle

après la création [232](#)

Service de référentiel modèle

configuration [229](#)

création [229](#)

services d'application

Service de gestion de contenu [47](#)

ports [28](#)

produits [40](#)

Service Analyst [45](#)

- services d'application (*a continué*)
 - Service d'accès aux métadonnées [57](#)
 - Service d'intégration de données [50](#)
 - Service de catalogue [46](#)
 - Service de cluster Informatica [56](#)
 - Service de recherche [62](#)
 - Service de référentiel modèle [57](#)
 - service de référentiel modèle de surveillance [61](#)
- services Informatica
 - démarrage et arrêt sous UNIX [269](#)
 - dépannage [209](#)
 - installation en mode silencieux [201](#)
- Services Oracle Net
 - utilisation pour connecter le service d'intégration à Oracle (UNIX) [279](#)
- sources de données
 - connexion par le biais de ODBC (UNIX) [286](#)
- sources de données JDBC
 - connexion (UNIX) [286](#)
- sources de données ODBC
 - connexion à (UNIX) [286](#)
- spécifications de correctif
 - installation [27](#)
- spécifications de la base de données
 - cache d'objet de données [50](#)
 - entrepôt de données de référence [47](#)
- spécifications de la base de données IBM DB2
 - base de données du référentiel modèle [58](#)
 - référentiel de flux de travail [53](#)
 - référentiel du domaine [41](#), [58](#)
- spécifications de la base de données Microsoft SQL Server
 - référentiel de flux de travail [54](#)
- spécifications de la base de données Oracle
 - référentiel de configuration du domaine [43](#)
- spécifications de la base de données Sybase ASE
 - référentiel de configuration du domaine [43](#)
- spécifications de port
 - configuration requise pour l'installation [28](#)
- spécifications système
 - Minimal [24](#)
- sqlplus
 - test des connexions de bases de données [63](#)
- Sybase ASE
 - connexion à un service d'intégration (UNIX) [281](#)

T

- Teradata
 - connexion à un service d'intégration (UNIX) [283](#)

- Teradata (*a continué*)
 - connexion aux clients Informatica (UNIX) [283](#)

U

- UNIX
 - chemins d'accès aux bibliothèques [216](#)
 - comptes d'utilisateur [32](#)
 - connexion aux sources de données JDBC [286](#)
 - connexion aux sources de données ODBC [286](#)
 - démarrage et arrêt des services Informatica [269](#)
 - i10Pi [95](#)
 - pré-installation [95](#)
 - variables client de base de données [63](#)
 - variables d'environnement client de base de données [63](#)
 - variables d'environnement [215](#)

V

- variables d'environnement
 - chemins de bibliothèque sous UNIX [216](#)
 - clients de bases de données [63](#)
 - clients de bases de données UNIX [63](#)
 - configuration des clients [260](#)
 - configuration sous UNIX [216](#)
 - INFA_TRUSTSTORE [260](#)
 - INFA_TRUSTSTORE_PASSWORD [260](#)
 - installation [31](#)
 - LANG_C [214](#)
- variables d'environnement
 - configuration [215](#)
 - LANG [214](#)
 - LC_ALL [214](#)
 - LC_CTYPE [214](#)
 - paramètre régional [214](#)
 - UNIX [215](#)
- variables d'environnement régionales
 - configuration [214](#)

W

- Windows
 - installation des clients Informatica en mode graphique [258](#)