NetIQ Identity Manager

Guide d'installation pour Linux

Février 2018

Mentions légales

Pour plus d'informations sur les mentions légales, les exclusions de garantie, les garanties, les limitations en matière d'exportation et d'utilisation de NetIQ, les droits restreints du gouvernement américain, la politique relative aux brevets et la compatibilité avec la norme FIPS, consultez le site http://www.netiq.com/fr-fr/company/legal/.

Table des matières

À propos de ce guide et de la bibliothèque

Le *guide d'installation* fournit des instructions pour l'installation du produit NetIQ Identity Manager (Identity Manager). Ce guide décrit la procédure d'installation de composants individuels dans un environnement distribué.

Public

Ce guide fournit des informations destinées aux architectes et administrateurs responsables des identités pour installer les composants nécessaires à la création d'une solution de gestion des identités pour leur entreprise.

Autres documents dans la bibliothèque

Pour plus d'informations sur la bibliothèque d'Identity Manager, reportez-vous au site Web de documentation d'Identity Manager.

À propos de NetIQ Corporation

Fournisseur international de logiciels d'entreprise, nos efforts sont constamment axés sur trois défis inhérents à votre environnement (le changement, la complexité et les risques) et la façon dont vous pouvez les contrôler.

Notre point de vue

Adaptation au changement et gestion de la complexité et des risques : rien de neuf

Parmi les défis auxquels vous êtes confronté, il s'agit peut-être des principaux aléas qui vous empêchent de disposer du contrôle nécessaire pour mesurer, surveiller et gérer en toute sécurité vos environnements informatiques physiques, virtuels et en nuage (cloud computing).

Services métier critiques plus efficaces et plus rapidement opérationnels

Nous sommes convaincus qu'en proposant aux organisations informatiques un contrôle optimal, nous leur permettons de fournir des services dans les délais et de manière plus rentable. Les pressions liées au changement et à la complexité ne feront que s'accroître à mesure que les organisations évoluent et que les technologies nécessaires à leur gestion deviennent elles aussi plus complexes.

Notre philosophie

Vendre des solutions intelligentes et pas simplement des logiciels

Pour vous fournir un contrôle efficace, nous veillons avant tout à comprendre les scénarios réels qui caractérisent les organisations informatiques telles que la vôtre, et ce jour après jour. De cette manière, nous pouvons développer des solutions informatiques à la fois pratiques et intelligentes qui génèrent assurément des résultats éprouvés et mesurables. En même temps, c'est tellement plus gratifiant que la simple vente de logiciels.

Vous aider à réussir, telle est notre passion

Votre réussite constitue le fondement même de notre manière d'agir. Depuis la conception des produits jusqu'à leur déploiement, nous savons que vous avez besoin de solutions informatiques opérationnelles qui s'intègrent en toute transparence à vos investissements existants. En même temps, après le déploiement, vous avez besoin d'une formation et d'un support continus. En effet, il vous faut un partenaire avec qui la collaboration est aisée... pour changer. En fin de compte, votre réussite est aussi la nôtre.

Nos solutions

- Gouvernance des accès et des identités
- Gestion des accès
- Gestion de la sécurité
- Gestion des systèmes et des applications

- Gestion des workloads
- Gestion des services

Contacter le support

Pour toute question concernant les produits, tarifs et fonctionnalités, contactez votre partenaire local. Si vous ne pouvez pas contacter votre partenaire, contactez notre équipe de support ventes.

Monde :	www.netiq.com/about_netiq/officelocations.asp
États-Unis et Canada :	1-888-323-6768
Courrier électronique :	info@netiq.com
Site Web :	www.netiq.com

Contacter le support technique

Pour tout problème spécifique au produit, contactez notre équipe du support technique.

Monde :	www.netiq.com/support/contactinfo.asp
Amérique du Nord et du Sud :	1-713-418-5555
Europe, Moyen-Orient et Afrique :	+353 (0) 91-782 677
Courrier électronique :	support@netiq.com
Site Web :	www.netiq.com/support

Contacter le support en charge de la documentation

Notre objectif est de vous proposer une documentation qui réponde à vos besoins. La documentation de ce produit est disponible sur le site Web NetIQ aux formats HTML et PDF, sur une page qui ne nécessite pas l'envoi d'informations de connexion. Pour soumettre vos suggestions d'amélioration de la documentation, cliquez sur le bouton **comment on this topic** (Ajouter un commentaire sur cette rubrique) au bas de chaque page de la version HTML de la documentation disponible à l'adresse www.netiq.com/documentation. Vous pouvez également envoyer un message électronique à l'adresse Documentation-Feedback@netiq.com. Nous accordons une grande importance à vos commentaires et sommes impatients de connaître vos impressions.

Contacter la communauté d'utilisateurs en ligne

Les communautés NetIQ et la communauté en ligne de NetIQ sont un réseau collaboratif vous mettant en relation avec vos homologues et des spécialistes de NetIQ. En proposant des informations immédiates, des liens utiles vers des ressources et un accès aux experts NetIQ, les communautés NetIQ vous aident à maîtriser les connaissances nécessaires pour tirer pleinement parti du potentiel de vos investissements informatiques. Pour plus d'informations, consultez le site community.netiq.com.

Introduction

NetIQ Identity Manager vous aide à créer un cadre de gestion des identités intelligent pour votre entreprise, à la fois à l'intérieur du pare-feu et dans le cloud. Identity Manager centralise l'administration de l'accès des utilisateurs et vérifie que chacun possède une identité unique depuis vos réseaux physiques et virtuels jusqu'au cloud.

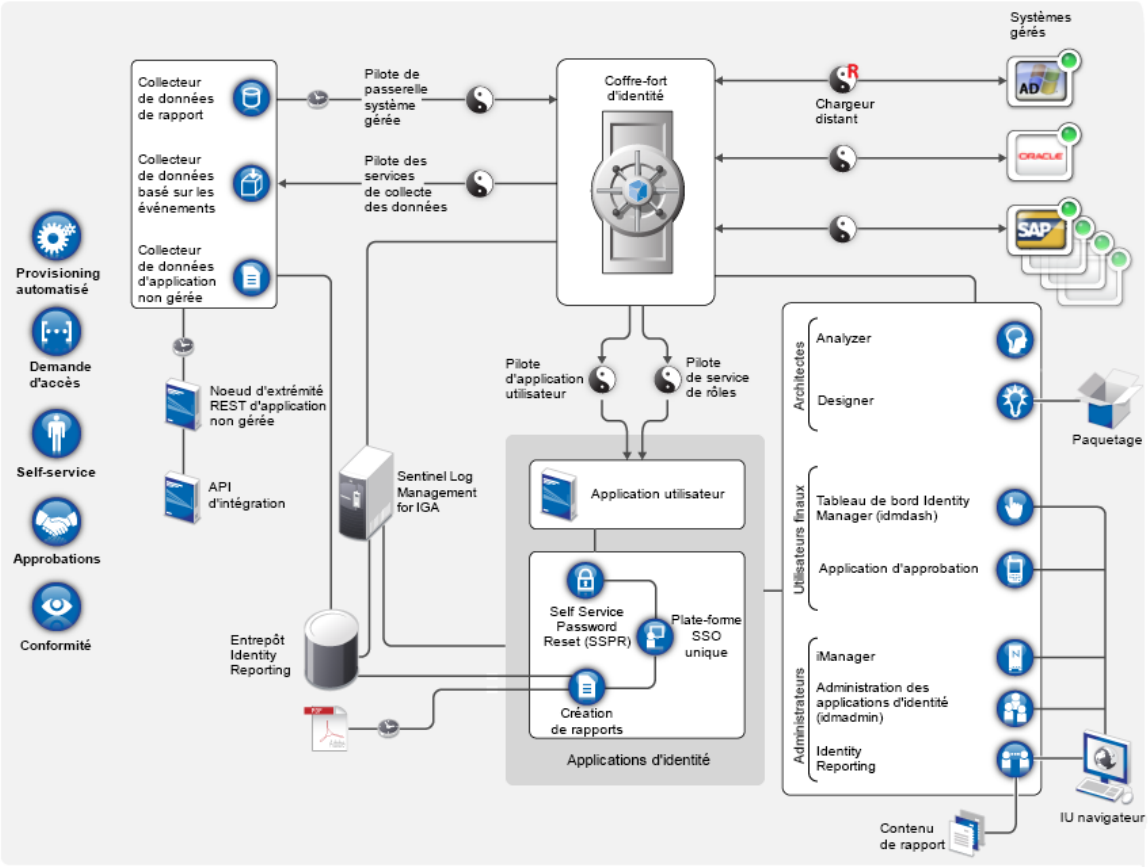
En général, vous pouvez regrouper les composants qui constituent Identity Manager dans les fonctions suivantes :

- Création et gestion de l'environnement Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 2, « Création et gestion de votre environnement Identity Manager », page 19.
- Surveillance de l'environnement Identity Manager, y compris la possibilité de créer des audits et des rapports sur les activités de provisioning des utilisateurs. Vous pouvez ensuite prouver la conformité avec les stratégies métier, IT et de l'entreprise. Pour plus d'informations, reportez-vous au Chapitre 3, « Gestion des données dans l'environnement Identity Manager », page 21.
- Gestion des activités de provisioning des utilisateurs, telles que les rôles, l'attestation et le self-service pour les utilisateurs. Pour plus d'informations, reportez-vous au Chapitre 4, « Provisioning des utilisateurs pour l'accès sécurisé », page 25.

Cette section vous présente les composants Identity Manager qui vous aident à effectuer ces activités. Une fois en possession de ces données, vous pouvez commencer à planifier l'installation du produit. Pour un aperçu des interconnexions existant entre ces composants, reportez-vous au Chapitre 1, « Aperçu des composants Identity Manager », page 17.

1 Aperçu des composants Identity Manager

Identity Manager permet de s'assurer que chaque utilisateur possède une identité unique depuis vos réseaux physiques et virtuels jusqu'au cloud. Le schéma ci-dessous donne un aperçu général des composants qui supportent les fonctionnalités d'Identity Manager. Certains de ces composants peuvent être installés sur le même serveur, en fonction de la taille de votre solution de gestion des identités. Toutefois, d'autres composants, comme les applications d'identité, proposent une interface de type navigateur accessible à partir de postes de travail ou de plates-formes mobiles.



Dans Identity Manager, un **système géré**, également appelé **système connecté** ou **application connectée**, est un système, annuaire, base de données ou système d'exploitation dont vous souhaitez gérer les informations d'identité. Par exemple, les systèmes connectés peuvent être l'application PeopleSoft ou un annuaire LDAP. Un **pilote**, par exemple le pilote des services de collecte de données, établit la connexion entre un système géré et le coffre-fort d'identité. Il permet également de synchroniser et de partager des données entre différents systèmes. Identity Manager stocke les pilotes et les objets de bibliothèque dans un conteneur appelé un **ensemble de pilotes**.

2 Création et gestion de votre environnement Identity Manager

La plupart des entreprises utilisent des environnements distincts pour le développement et le stockage intermédiaire d'Identity Manager, puis le déploient dans leur environnement de production. Pour créer et tenir à jour votre environnement Identity Manager, vous pouvez utiliser les composants Identity Manager suivants :

Ces composants vous aident également à adapter Identity Manager à l'évolution des besoins de votre société pour assurer la continuité des activités et améliorer la productivité des utilisateurs à l'échelle de l'entreprise.

2.1 Designer pour Identity Manager

Designer pour Identity Manager (Designer) vous aide à concevoir, tester, documenter et déployer des solutions Identity Manager dans un environnement réseau ou de test. Vous pouvez configurer votre projet Identity Manager dans un environnement hors ligne, puis le déployer dans votre système en ligne. Du point de vue de la conception, Designer aide à réaliser les opérations suivantes :

- Afficher sous forme graphique les composants de votre solution Identity Manager et observer la façon dont ils interagissent.
- Modifier et tester votre environnement Identity Manager pour vous assurer qu'il fonctionne comme prévu avant de déployer tout ou partie de votre solution dans votre environnement de production.

Designer assure le suivi de vos informations de conception et de présentation. D'un simple clic, vous pouvez imprimer ces informations au format de votre choix. Designer permet également aux équipes de partager le travail sur des projets à l'échelle de l'entreprise.

Pour plus d'informations sur l'utilisation de Designer, reportez-vous au *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).

2.2 Analyzer pour Identity Manager

Analyzer pour Identity Manager (Analyzer) fournit des fonctionnalités d'analyse des données, de nettoyage, d'actualisation et de création de rapports pour vous aider à respecter les stratégies de qualité des données internes. Analyzer permet d'analyser, d'optimiser et de contrôler toutes les zones de stockage de données de l'entreprise. Analyzer propose les fonctionnalités suivantes :

- L'assignation de schéma d'Analyzer associe les attributs de schéma d'une application avec les attributs de schéma correspondant dans le schéma de base d'Analyzer. Ceci vous permet de vous assurer que vos opérations d'analyse et de nettoyage des données associent correctement les valeurs similaires entre les systèmes disparates. Pour ce faire, Analyzer exploite les fonctions d'assignation de schéma de Designer.

- L'éditeur de profil d'analyse permet de configurer un profil pour l'analyse d'une ou de plusieurs instances d'ensemble de données. Chaque profil d'analyse contient une ou plusieurs métriques par rapport auxquelles vous pouvez évaluer les valeurs d'attribut pour vérifier dans quelle mesure les données sont conformes aux normes de format de données définies.
- L'éditeur de profil de concordance vous permet de comparer les valeurs d'un ou de plusieurs ensembles de données. Vous pouvez rechercher les valeurs en double dans un ensemble de données spécifié et les valeurs correspondantes entre deux ensembles de données.

Pour plus d'informations sur l'utilisation d'Analyzer, reportez-vous au *NetIQ Analyzer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Analyzer pour Identity Manager).

2.3 iManager

NetIQ iManager est un outil basé sur un navigateur qui offre un point d'administration unique pour un grand nombre de produits Novell et NetIQ, notamment Identity Manager. Après avoir installé les plug-ins d'Identity Manager pour iManager, vous pouvez gérer Identity Manager et recevoir des informations en temps réel sur la santé et l'état de votre système Identity Manager.

iManager vous permet d'effectuer des tâches similaires à celles réalisées avec Designer, mais aussi de surveiller l'état de santé de votre système. NetIQ vous recommande d'utiliser iManager pour les tâches d'administration. Utilisez Designer pour les tâches de configuration qui nécessitent la modification de paquetages, une modélisation et des tests avant le déploiement.

Pour plus d'informations sur iManager, reportez-vous au *Guide d'administration de NetIQ iManager*.

3 Gestion des données dans l'environnement Identity Manager

Identity Manager applique des contrôles d'accès cohérents sur les réseaux physiques, virtuels et cloud ; il utilise des rapports dynamiques qui vous permettent de prouver votre conformité. Identity Manager synchronise tous les types de données stockées dans une application connectée ou dans le coffre-fort d'identité. Les composants suivants de la solution Identity Manager assure la synchronisation des données, notamment celle des mots de passe :

- Coffre-fort d'identité
- Moteur Identity Manager
- Identity Manager Remote Loader
- Agent Fan-out
- Identity Reporting
- Pilotes Identity Manager
- Systèmes connectés

3.1 Présentation de la synchronisation des données

Identity Manager permet de synchroniser, de transformer et de distribuer des informations parmi une multitude de systèmes connectés, tels que de bases de données, de systèmes d'exploitation et d'annuaires tels que SAP, PeopleSoft, Microsoft SharePoint, Lotus Notes, Microsoft Exchange, Microsoft Active Directory, NetIQ eDirectory et les annuaires LDAP. Identity Manager vous permet de réaliser les activités suivantes :

- Contrôle des flux des données entre les systèmes connectés.
- Détermination des données partagées, du système faisant office de source experte pour certaines données, ainsi que du mode d'interprétation et de transformation des données afin de satisfaire les exigences d'autres systèmes.
- Synchronisation des mots de passe entre les systèmes. Par exemple, si un utilisateur modifie son mot de passe dans Active Directory, Identity Manager peut le synchroniser dans Lotus Notes et Linux.
- Création de nouveaux comptes utilisateur et suppression de comptes existants dans des annuaires tels qu'Active Directory, des systèmes tels que PeopleSoft et Lotus Notes, et des systèmes d'exploitation tels qu'UNIX et Linux. Par exemple, lorsque vous ajoutez un employé à votre système de ressources humaines SAP, Identity Manager peut créer automatiquement un compte utilisateur dans Active Directory, un compte dans Lotus Notes et un compte dans un système de gestion de comptes NIS Linux.

3.2 Présentation des fonctions d'audit, de création de rapports et de conformité

Sans Identity Manager, le provisioning des utilisateurs peut s'avérer fastidieux, long et coûteux. Vous devez alors vérifier que vos activités de provisioning respectent bien les stratégies, les besoins et la réglementation de votre entreprise. Les personnes concernées ont-elles accès aux ressources dont elles ont besoin ? Les personnes non autorisées sont exclues de ces mêmes ressources ? L'employé qui a commencé son activité hier a-t-il accès au réseau, à sa messagerie et aux autres systèmes dont il a besoin pour son travail ? L'accès de l'employé qui a quitté l'entreprise la semaine dernière a-t-il été supprimé ?

Avec Identity Manager, vous pouvez être tranquille car vous savez que toutes vos activités de provisioning des utilisateurs, passées et actuelles, sont suivies et consignées à des fins d'audit. En interrogeant l'entrepôt d'informations d'identité, vous pouvez récupérer toutes les informations requises pour vous assurer que votre entreprise respecte parfaitement toutes les lois et réglementations applicables.

Identity Manager contient des rapports prédéfinis qui vous permettent d'interroger l'entrepôt d'informations d'identité afin de prouver la conformité des stratégies métier, informatiques et d'entreprise. Vous pouvez, par ailleurs, créer des rapports personnalisés si ceux prédéfinis ne répondent pas à vos attentes.

3.3 Présentation des composants pour la synchronisation de vos données d'identité

3.3.1 Coffre-fort d'identité

Le **coffre-fort d'identité** contient toutes les informations dont Identity Manager a besoin. Le coffre-fort d'identité sert de méta-annuaire pour les données que vous souhaitez synchroniser entre les différents systèmes connectés. Par exemple, les données synchronisées d'un système PeopleSoft vers Lotus Notes sont d'abord ajoutées au coffre-fort d'identité, puis envoyées au système Lotus Notes. Il stocke également les informations propres à Identity Manager, telles que les configurations des pilotes, les paramètres et les stratégies.

Le coffre-fort d'identité utilise une base de données eDirectory NetIQ. Pour plus d'informations sur l'utilisation d'eDirectory, reportez-vous au Guide d'administration de NetIQ eDirectory.

3.3.2 Moteur Identity Manager

Le **moteur Identity Manager** traite tous les changements de données qui interviennent au niveau du coffre-fort d'identité ou d'une application connectée. Quant aux événements qui se produisent dans le coffre-fort d'identité, le moteur traite leurs modifications et émet des commandes vers l'application via le pilote. Si des événements se produisent dans l'application, le moteur reçoit les modifications du pilote, les traite et émet des commandes vers le coffre-fort d'identité. Les **pilotes** connectent le moteur Identity Manager aux applications. Un pilote remplit deux fonctions principales : signaler au

moteur Identity Manager les modifications apportées aux données (événements) dans l'application et exécuter les modifications de données (commandes) soumises par ce moteur à l'application. Les pilotes doivent être installés sur le même serveur que l'application connectée.

Le moteur Identity Manager est également désigné sous le terme « moteur méta-annuaire ». Le serveur sur lequel le moteur Identity Manager s'exécute est appelé **serveur Identity Manager**. Vous pouvez disposer de plusieurs serveurs Identity Manager dans votre environnement, en fonction du workload serveur.

3.3.3 Chargeur distant

Le **chargeur distant Identity Manager** charge les pilotes et communique avec le moteur Identity Manager au nom des pilotes installés sur des serveurs distants. Si l'application s'exécute sur le même serveur que le moteur Identity Manager, vous pouvez installer le pilote sur ce serveur. Cependant, si l'application ne s'exécute pas sur le même serveur que le moteur Identity Manager, vous devez installer le pilote sur le serveur de l'application.

Pour plus d'informations sur le chargeur distant, reportez-vous à la Section 8.4.2, « Présentation du chargeur distant », page 69.

3.3.4 Identity Reporting

Identity Manager comprend **l'entrepôt d'informations d'identité**, c'est-à-dire un espace de stockage intelligent pour les informations relatives aux états réels et souhaités du coffre-fort d'identité et des systèmes connectés au sein de votre organisation. Cet entrepôt vous offre une vue globale de vos droits métier, de sorte que vous disposez de toutes les données nécessaires pour connaître l'état passé et présent des autorisations accordées aux identités au sein de votre organisation.

En interrogeant l'entrepôt, vous pouvez récupérer toutes les informations requises pour vous assurer que votre entreprise respecte parfaitement toutes les lois et réglementations applicables. Fort de cette connaissance, vous pouvez répondre aux requêtes GRC (Governance, Risk and Compliance) les plus complexes.

L'infrastructure de l'entrepôt d'informations d'identité nécessite les composants suivants :

- « Identity Reporting pour Identity Manager » page 23
- « Service de collecte de données » page 24
- « Pilote de passerelle système gérée » page 24

Identity Reporting pour Identity Manager

L'entrepôt d'informations d'identité stocke ses informations dans la base de données SIEM de Sentinel Log Management for IGA (Identity Governance and Administration). Le composant de création de rapports, **Identity Reporting**, vous permet d'auditer et de générer des rapports sur votre solution Identity Manager. Vous pouvez utiliser ces rapports pour aider votre entreprise à respecter les normes de conformité qu'elle doit observer. Vous pouvez exécuter des rapports prédéfinis pour démontrer la conformité par rapport aux stratégies métier, IT et de l'entreprise. Vous pouvez, par ailleurs, créer des rapports personnalisés si ceux prédéfinis ne répondent pas à vos attentes. Utilisez Identity Reporting pour générer des rapports sur des informations métier essentielles concernant divers aspects de votre configuration Identity Manager, notamment les données collectées à partir des coffres-forts d'identité et des systèmes connectés. L'interface utilisateur d'Identity Reporting permet de planifier facilement l'exécution des rapports aux heures creuses de manière à optimiser

les performances. Pour plus d'informations sur Identity Reporting, reportez-vous au manuel *Administrator Guide to NetIQ Identity Reporting* (Guide de l'administrateur de NetIQ Identity Reporting).

Service de collecte de données

Le **service de collecte de données** utilise le pilote Services de collecte de données pour capturer les modifications apportées aux objets stockés dans un coffre-fort d'identité, tels que les comptes, rôles, ressources, groupes et adhésions à des équipes. Le pilote s'enregistre lui-même auprès du service et distribue à ce dernier les événements de modification (tels que la synchronisation de données et l'ajout, la modification ou la suppression d'événements).

Le service comprend trois sous-services :

- **Collecteur de données de rapports :** utilise un modèle d'extraction pour récupérer des informations d'une ou de plusieurs sources de données de coffre-fort d'identité. La collecte s'exécute de manière périodique, selon un ensemble de paramètres de configuration. Pour récupérer les données, le collecteur fait appel au pilote de passerelle système gérée.
- **Collecteur de données d'événements :** utilise un modèle de distribution pour rassembler les données d'événements capturées par le pilote du service de collecte de données.
- **Collecteur de données d'applications non gérées :** récupère les données d'une ou de plusieurs applications non gérées en appelant un noeud d'extrémité REST écrit spécifiquement pour chaque application. Les applications non gérées sont des applications de votre entreprise qui ne sont pas connectées au coffre-fort d'identité.

Pilote de passerelle système gérée

Le **pilote de passerelle système gérée** interroge le coffre-fort d'identité pour collecter les types d'informations suivants auprès des systèmes gérés :

- Liste de tous les systèmes gérés
- Liste de tous les comptes des systèmes gérés
- Types de droits, valeurs et assignations, ainsi que profils de compte utilisateur pour les systèmes gérés

4 Provisioning des utilisateurs pour l'accès sécurisé

Identity Manager centralise la gestion des accès et garantit que chaque utilisateur possède une identité unique sur l'ensemble de vos réseaux physiques et virtuels et le cloud. En outre, il est fréquent que les utilisateurs aient besoin d'accéder aux ressources en fonction de leurs rôles dans l'organisation. Par exemple, les avocats d'une société d'avocats peuvent avoir besoin d'accéder à un ensemble de ressources différent de celui utilisé par les adjoints juridiques de la société.

Identity Manager permet de fournir l'accès aux utilisateurs en fonction de leur rôle dans l'organisation. Vous définissez les rôles et effectuez les assignations en fonction des besoins de votre organisation. Lorsqu'un utilisateur est assigné à un rôle, Identity Manager lui donne accès aux ressources associées à ce rôle. Les utilisateurs qui disposent de plusieurs rôles reçoivent un accès aux ressources associées à tous ces rôles.

Les utilisateurs peuvent être ajoutés automatiquement à des rôles selon les événements qui se produisent dans votre organisation. Par exemple, vous pouvez ajouter à votre base de données SAP HR un nouvel utilisateur dont la fonction est Avocat. Si une approbation est requise pour ajouter un utilisateur à un rôle, vous pouvez définir des workflows afin de router les requêtes de rôle vers les approbateurs appropriés. Vous pouvez également assigner manuellement des utilisateurs à des rôles.

Dans certains cas, il peut exister des rôles qui ne doivent pas être assignés à la même personne du fait d'un conflit entre ces rôles. Identity Manager offre une fonction de séparation des tâches qui permet d'éviter que des utilisateurs soient assignés à des rôles en conflit sauf si une personne de votre organisation définit une exception à ce conflit.

La solution Identity Manager fournit les composants suivants pour le provisioning des utilisateurs :

- Tableau de bord Identity Manager
- Administration des applications d'identité
- Application utilisateur

Le tableau de bord offre un point d'accès unique pour tous les utilisateurs et administrateurs d'Identity Manager. Il permet d'accéder à l'ensemble des fonctionnalités existantes de l'administrateur de catalogue et de l'application utilisateur. À partir d'Identity Manager 4.6, le tableau de bord remplace la page d'accueil et le tableau de bord de provisioning d'Identity Manager.

4.1 Présentation du processus d'attestation dans Identity Manager

Identity Manager vous aide à valider la justesse de vos assignations de rôle par l'intermédiaire d'un processus d'attestation. Des assignations de rôle incorrectes peuvent compromettre le respect des réglementations de l'entreprise et des réglementations nationales. Ce processus d'attestation permet aux personnes responsables au sein de votre organisation de certifier les données associées aux rôles :

- **Attestation du profil utilisateur :** les utilisateurs sélectionnés attestent de leurs propres informations de profil (prénom, nom, titre, service, adresse électronique, etc.) et corrigent les éventuelles informations erronées. Des informations de profil exactes sont essentielles pour disposer d'assignations de rôle correctes.
- **Attestation de violation de la séparation des tâches :** les personnes responsables examinent le rapport de violation de la séparation des tâches et attestent son exactitude. Ce rapport indique les exceptions qui permettent l'assignation d'un utilisateur à des rôles en conflit.
- **Attestation d'assignation de rôle :** les personnes responsables examinent le rapport qui répertorie les rôles sélectionnés, ainsi que les utilisateurs, les groupes et les rôles assignés à chaque rôle. Les personnes responsables doivent ensuite attester l'exactitude des informations.
- **Attestation de l'assignation des utilisateurs :** les personnes responsables examinent le rapport qui répertorie les utilisateurs sélectionnés, ainsi que les rôles auxquels ils sont assignés. Elles doivent ensuite attester l'exactitude des informations.

Ces rapports d'attestation sont principalement conçus pour vous aider à vérifier que les assignations de rôle sont exactes et qu'il existe des raisons valables pour autoriser des exceptions concernant les rôles en conflit.

4.2 Présentation du processus de self-service d'Identity Manager

Identity Manager utilise l'identité comme base pour autoriser les utilisateurs à accéder aux systèmes, applications et bases de données. L'identificateur unique et les rôles de chaque utilisateur sont fournis avec des droits d'accès spécifiques aux données d'identité. Par exemple, les utilisateurs qui sont identifiés comme managers peuvent accéder aux informations de salaire de leurs subordonnés directs, mais pas des autres employés de l'entreprise. Avec Identity Manager, vous pouvez déléguer des tâches administratives aux personnes qui doivent en être responsables. Par exemple, vous pouvez autoriser certains utilisateurs à effectuer les tâches suivantes :

- Gérer leurs données personnelles dans l'annuaire de l'entreprise. Vous n'aurez plus à modifier les numéros de téléphone portable de vos employés : ils effectuent la modification eux-mêmes à un emplacement et cette modification se répercute à tous les systèmes que vous avez synchronisés avec Identity Manager.
- Changer leur mot de passe, configurer un indice ou des questions-réponses de vérification d'identité pour les mots de passe oubliés. Ils ne doivent plus vous demander de réinitialiser le mot de passe qu'ils ont oublié, ils peuvent le faire eux-mêmes après avoir reçu un indice ou répondu à une question de vérification d'identité.
- Demander l'accès à des ressources telles que des bases de données, des systèmes ou des annuaires. Plutôt que de vous demander l'accès à une application, ils peuvent la sélectionner dans la liste des ressources disponibles.

Outre le self-service pour les utilisateurs, Identity Manager propose l'administration en self-service des fonctions (gestion, service d'assistance, etc.) régissant l'assistance, la surveillance et l'approbation des demandes des utilisateurs. Par exemple, John utilise la fonction de self-service d'Identity Manager pour demander l'accès aux documents dont il a besoin. Le responsable de John et le directeur financier reçoivent sa demande grâce à la fonction de self-service et peuvent approuver sa requête. Le workflow d'approbation établi permet à John de lancer sa demande et d'en suivre la progression. Il permet également au responsable de John et au directeur financier d'y répondre. L'approbation de la requête par le responsable de John et le directeur financier déclenche le provisioning de droits Active Directory dont John a besoin pour accéder aux documents financiers et les consulter.

Identity Manager offre des fonctionnalités de workflow qui permettent d'impliquer dans vos processus de provisioning les approbateurs de ressources appropriés. Supposons par exemple que John, qui dispose déjà d'un compte Active Directory, ait besoin d'accéder à certains rapports financiers via Active Directory. Cela nécessite l'approbation du responsable immédiat de John et du directeur financier. Heureusement, vous avez configuré un workflow d'approbation qui achemine la requête de John auprès de son responsable et, après approbation de ce dernier, auprès du directeur financier. L'approbation du directeur financier déclenche le provisioning automatique des droits d'Active Directory dont John a besoin pour accéder aux documents financiers et les consulter.

Vous pouvez initier des workflows automatiquement chaque fois qu'un événement déterminé se produit (par exemple, un nouvel utilisateur est ajouté à votre système des ressources humaines) ou manuellement suite à la demande d'un utilisateur. Pour vous assurer que les approbations interviennent au moment opportun, vous pouvez définir des mandataires comme approbateurs et des équipes d'approbation.

4.3 Présentation des composants de gestion du provisioning des utilisateurs

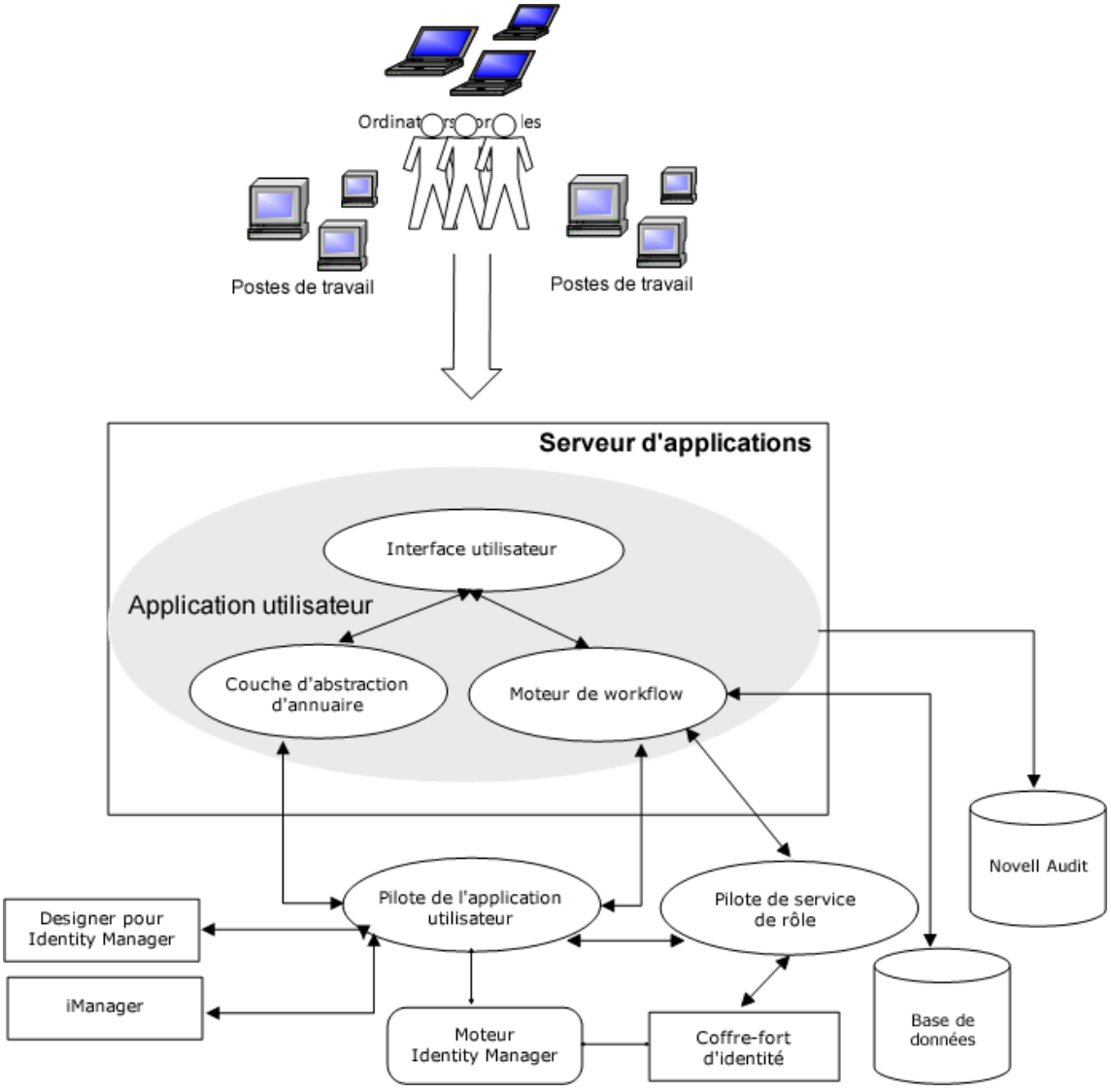
Cette section explique la fonction des composants suivants :

4.3.1 Application utilisateur et module de provisioning basé sur les rôles

L'**application utilisateur** Identity Manager offre à vos utilisateurs et aux administrateurs une vue globale des informations, ressources et fonctionnalités d'Identity Manager. Il s'agit d'une application Web basée sur navigateur qui permet à l'utilisateur d'effectuer diverses tâches de self-service

d'identité et de provisioning de rôles. Les utilisateurs peuvent gérer leurs mots de passe et données d'identité, initier et contrôler les requêtes de provisioning et d'assignation de rôles, gérer le processus d'approbation des requêtes de provisioning et passer en revue les rapports d'attestation.

L'application utilisateur repose sur la combinaison de plusieurs composants indépendants qui peuvent néanmoins fonctionner ensemble.



L'application utilisateur s'exécute sur une structure de **module de provisioning basé sur les rôles** (RBPM). Elle inclut le moteur de workflow qui contrôle que les requêtes sont bien acheminées selon le processus d'approbation approprié. Ces composants nécessitent les pilotes suivants :

Pilote de l'application utilisateur

Stocke les informations de configuration et avertit l'application utilisateur des changements apportés au coffre-fort d'identité. Vous pouvez configurer le pilote pour permettre aux événements du coffre-fort d'identité de déclencher des workflows. Le pilote peut également signaler la réussite ou l'échec d'une activité de provisioning d'un workflow à l'application utilisateur afin que les utilisateurs puissent consulter l'état final de leurs demandes.

Pilote de service de rôle et de ressource

Gère toutes les assignations de rôles et de ressources. Le pilote démarre les workflows pour les requêtes d'assignation de rôles et de ressources nécessitant une approbation et gère les assignations de rôle indirectes en fonction des adhésions au groupe et au conteneur. En outre, le pilote accorde des droits aux utilisateurs ou les révoque sur la base de leur adhésion au rôle. Il effectue des procédures de nettoyage pour les requêtes terminées.

Les utilisateurs peuvent accéder à l'application utilisateur à partir de n'importe quel navigateur Web pris en charge. Pour plus d'informations sur l'application utilisateur et RBPM, reportez-vous au *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur des applications d'identité de NetIQ Identity Manager).

4.3.2 Administration des applications d'identité

L'interface **Administration des applications d'identité** permet de gérer les tâches suivantes avec un rôle d'administrateur approprié :

- Création et gestion des rôles, des ressources et de leurs assignations
- Définition des contraintes de séparation des tâches (SoD) pour éviter les conflits entre les deux rôles différents dans le système
- Configuration de la possibilité pour les utilisateurs d'approuver les demandes d'autorisation par courrier électronique
- Configuration des paramètres par défaut de vos composants d'applications d'identité tels que les rôles, les ressources et la délégation

Les administrateurs peuvent accéder à la page Administration à l'aide de n'importe quel navigateur Web pris en charge, aussi bien à partir d'un ordinateur que d'une tablette. Pour plus d'informations, reportez-vous au manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager - Guide de l'administrateur des applications d'identité).

4.3.3 Tableau de bord Identity Manager

Le **tableau de bord Identity Manager** (le tableau de bord) inclut une vue personnalisée des autorisations, tâches et requêtes de chaque utilisateur. De cette manière, les utilisateurs peuvent se concentrer sur les aspects essentiels suivants :

Je souhaite obtenir quelque chose.

Si vous avez besoin d'un élément, qu'il s'agisse d'un équipement tel qu'un ordinateur portable ou d'un besoin immatériel tel qu'un accès à un serveur ou à une application spécifique, vous pouvez le demander.

Je dois effectuer une opération.

Si vous voulez savoir quelles tâches vous devez gérer, vous pouvez consulter la page **Mes tâches**. Celle-ci reprend en effet l'ensemble de vos tâches en attente d'approbation ou de provisioning dans le système Identity Manager.

Quels sont mes droits d'accès ?

Si vous voulez voir vos autorisations actuelles, vous pouvez consulter la page **Mes autorisations**. Cette dernière reprend la liste des ressources et des rôles auxquels vous avez accès.

Comment l'ai-je obtenu ?

Si vous voulez voir une liste des requêtes déjà effectuées, vous pouvez consulter la page **Historique de requêtes**. Cette dernière indique tout ce que vous avez demandé récemment, ainsi que le statut de vos demandes en attente.

Si vous disposez d'un rôle d'administrateur pour les applications d'identité, vous pouvez personnaliser la page **Applications** dans le tableau de bord de tous les utilisateurs. Vous pouvez configurer la page de manière à afficher les éléments et les liens dont vos utilisateurs ont besoin, et à les classer dans des catégories pertinentes pour votre entreprise. Vous pouvez inclure les types d'éléments suivants :

- Fonctions Identity Manager, telles que la création de groupes ou l'exécution de rapports
- Autorisations requises par la plupart des utilisateurs
- Liens vers les sites ou applications Web couramment utilisés
- Noeuds d'extrémité REST
- Badges, par exemple le nombre d'éléments d'un certain type auxquels un utilisateur peut accéder

Les utilisateurs peuvent accéder au tableau de bord à l'aide de n'importe quel navigateur Web pris en charge sur un ordinateur ou une tablette. Pour plus d'informations, reportez-vous au manuel *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager - Guide de l'administrateur des applications d'identité).

II Planification de l'installation d'Identity Manager

Cette section fournit des informations utiles pour planifier votre environnement Identity Manager. Pour connaître les conditions préalables et la configuration système requise pour les ordinateurs sur lesquels vous souhaitez installer chaque composant Identity Manager, reportez-vous aux sections « Installation » relatives à ces composants.

Vous n'avez pas besoin de code d'activation pour installer ou exécuter Identity Manager pour la première fois. Toutefois, sans code d'activation, Identity Manager arrête de fonctionner 90 jours après l'installation. Vous pouvez activer Identity Manager à tout moment pendant cette période ou ultérieurement.

- Chapitre 5, « Présentation de la planification », page 33

5 Présentation de la planification

Cette section vous aide à planifier la procédure d'installation d'Identity Manager. Certains composants doivent être installés dans un ordre spécifique, car la procédure d'installation requiert un accès à certains composants préalablement installés. Par exemple, vous devez installer et configurer le coffre-fort d'identité avant d'installer le moteur Identity Manager.

5.1 Planification de la liste de contrôle

La liste de contrôle suivante indique les étapes nécessaires pour planifier l'installation d'Identity Manager dans votre environnement. Les sections concernant l'installation des composants Identity Manager présentent des listes de vérifications plus spécifiques.

	Éléments de la liste de contrôle
❑	1. Passez en revue les informations relatives à l'architecture du produit pour en savoir plus sur les composants Identity Manager. Pour plus d'informations, reportez-vous à la Partie I, « Introduction », page 15.
❑	2. (Conditionnel) Si vous installez des composants dans un environnement Red Hat Enterprise Linux 7.*x*, assurez-vous que le serveur comporte les bibliothèques adéquates. Pour plus d'informations, reportez-vous au Section 5.9.4, « Installation d'Identity Manager sur des serveurs RHEL 7.3 ou version ultérieure », page 45.
❑	3. Assurez-vous que vous disposez d'une licence pour exécuter Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.8, « Présentation des licences et de l'activation », page 42.
❑	4. Vérifiez les ports par défaut pour chaque composant Identity Manager afin de déterminer si vous devez personnaliser les paramètres d'installation. Pour plus d'informations, reportez-vous à la Section 5.2, « Présentation de la communication dans Identity Manager », page 34.
❑	5. Déterminez si vous pouvez exécuter les programmes d'installation dans la langue de votre choix. Pour plus d'informations, reportez-vous à la Section 5.10, « Présentation du support linguistique », page 48.

	Éléments de la liste de contrôle
❑	6. Vérifiez que vous disposez des fichiers d'installation d'Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.11, « Téléchargement des fichiers d'installation », page 49.
❑	7. (Conditionnel) Pour installer Identity Manager dans une grappe, vérifiez que votre environnement répond aux conditions requises. Pour plus d'informations, reportez-vous à la Section 5.9.1, « Garantie d'une haute disponibilité pour Identity Manager », page 43.
❑	8. Assurez-vous que vous disposez des références requises pour installer les composants Identity Manager sur vos serveurs et sur les comptes que vous pouvez créer au cours de l'installation.
❑	9. Vérifiez que les ordinateurs sur lesquels vous installez les composants Identity Manager répondent aux conditions requises spécifiées. Pour plus d'informations, reportez-vous à la configuration système requise pour chacun des composants. ◆ Section 8.3.4, « Configuration système requise pour le moteur Identity Manager, le chargeur distant et iManager », page 65 ◆ Section 8.5.3, « Configuration système requise pour les applications d'identité », page 83 ◆ Section 8.6.4, « Configuration système requise pour Identity Reporting », page 88 ◆ Section 12.3, « Configuration système requise pour Designer », page 184 ◆ Section 14.3, « Configuration système requise pour Analyzer », page 190 **REMARQUE :** NetIQ vous recommande de prendre note de chaque compte que vous créez durant la procédure d'installation.
❑	10. Activez vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 24, « Activation d'Identity Manager », page 245.

5.2 Présentation de la communication dans Identity Manager

Pour une bonne communication entre les composants Identity Manager, NetIQ recommande d'ouvrir les ports par défaut répertoriés dans le tableau suivant.

REMARQUE : si un port par défaut est déjà utilisé, assurez-vous de spécifier un autre port pour le composant Identity Manager.

Numéro de port	Composant/ ordinateur	Utilisation du port
389	Coffre-fort d'identité	Utilisé pour les communications LDAP en texte clair avec des composants Identity Manager
465	Identity Reporting	Utilisé pour les communications avec le serveur de messagerie SMTP
524	Coffre-fort d'identité	Utilisé pour la communication NCP (NetWare Core Protocol)
636	Coffre-fort d'identité	Utilisé pour les communications LDAP TLS/SSL avec les composants Identity Manager

Numéro de port	Composant/ ordinateur	Utilisation du port
5432	Applications d'identité	Utilisé pour les communications avec la base de données des applications d'identité
7707	Identity Reporting	Utilisé par le pilote de passerelle système gérée pour communiquer avec le coffre-fort d'identité
8000	Chargeur distant	Utilisé par l'instance du pilote pour la communication TCP/IP **REMARQUE :** chaque instance du chargeur distant doit être assignée à un port spécifique.
8005	Applications d'identité	Utilisé par Tomcat pour écouter les commandes d'arrêt
8009	Applications d'identité	Utilisé par Tomcat pour communiquer avec un connecteur Web qui utilise le protocole AJP au lieu de HTTP
8028	Coffre-fort d'identité	Utilisé pour la communication HTTP en texte clair avec NCP
8030	Coffre-fort d'identité	Utilisé pour la communication HTTPS avec NCP
8080	Applications d'identité iManager	Utilisé par Tomcat pour la communication HTTP en texte clair
8090	Chargeur distant	Utilisé par le chargeur distant pour écouter les connexions TCP/IP à partir du module d'interface (shim) distant **REMARQUE :** chaque instance du chargeur distant ne doit être assignée qu'à un seul port.
8180	Applications d'identité	Utilisé pour les communications HTTP par le serveur d'applications Tomcat sur lequel sont exécutées les applications d'identité
8443	Applications d'identité iManager	Utilisé par Tomcat pour la communication HTTPS (SSL) ou pour le réacheminement des requêtes de communication SSL
8543	Applications d'identité	Utilisé par Tomcat pour rediriger les requêtes qui nécessitent un transport SSL lorsque vous n'utilisez pas le protocole TLS/SSL
9009	iManager	Utilisé par Tomcat pour MOD_JK
15432	Identity Reporting	Utilisé pour la base de données PostgreSQL de
45654	Application utilisateur	Utilisé par le serveur sur lequel la base de données des applications d'identité est installée pour écouter les communications, lors de l'exécution de Tomcat au sein d'un groupe de grappes

5.3 Présentation des fichiers d'installation

Le tableau suivant répertorie les fichiers disponibles pour la version :

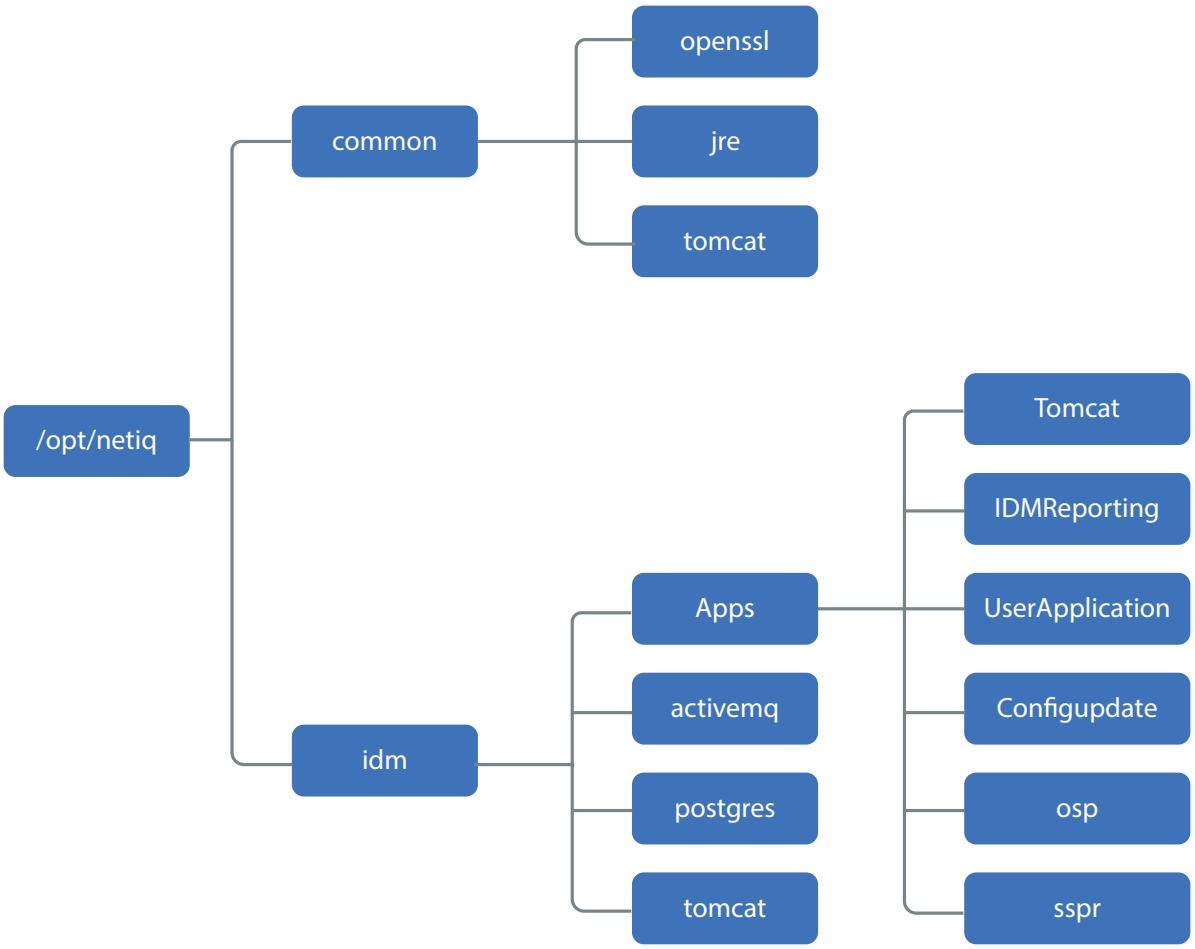
Nom du fichier	Description
`Identity_Manager_4.7_Linux.iso`	Contient les composants Identity Manager suivants : ◆ Moteur Identity Manager ◆ Service de chargeur distant ◆ Agent Fan-out ◆ Designer ◆ Administration Web d'iManager ◆ Identity Reporting ◆ Applications d'identité ◆ Analyzer
`SentinelLogManagementForIGA8.1.1.0.tar.gz`	Contient Sentinel Log Management for IGA.
`Identity_Manager_4.7_Linux_Designer.tar.gz`	Contient Designer pour Identity Manager.
`Identity_Manager_4.7_Linux_Analyzer.tar.gz`	Contient Analyzer pour Identity Manager.

REMARQUE : Le fichier `Identity_Manager_4.7_Linux.iso` fournit également les composants et logiciels de prise en charge requis pour l'exécution d'Identity Manager, tels qu'Oracle JRE, PostgreSQL, ActiveMQ et Apache Tomcat.

5.4 Structure de répertoires

Le processus d'installation crée la structure de répertoires suivante :

- Le répertoire `/opt/netiq` est le point de départ de votre structure de répertoires. Tous les autres fichiers et répertoires se situent sous ce répertoire.
- Le répertoire `common` contient les logiciels de prise en charge, qui sont partagés entre les composants qui les requièrent.
- Le répertoire `idm` contient les sous-répertoires spécifiques de composants qui incluent les fichiers binaires d'installation et de configuration de ces composants.



5.5 Emplacements d'installation par défaut

Le processus d'installation enregistre les composants aux emplacements prédéfinis suivants.

Composants Identity Manager	Chemins d'installation par défaut
Moteur Identity Manager	`/opt/novell/eDirectory/lib/dirxml`
Chargeur distant	`/opt/novell/dirxml/bin/x86_64`
Agent Fan-out	`/opt/novell/dirxml/fanoutagent`
Designer	`/root/designer`
iManager	`/var/opt/novell/iManager`
Application utilisateur	`/opt/netiq/idm/apps/UserApplication`
Applications d'identité	`/opt/netiq/idm/apps`
Utilitaire de mise à jour de la configuration	`/opt/netiq/idm/apps/configupdate`
Identity Reporting	`/opt/netiq/idm/apps/IDMReporting`
SLM for IGA	`/opt/novell/sentinel`
Analyzer	`/root/analyzer`

Composants de prise en charge	Chemins d'installation par défaut
Oracle JRE	`/opt/netiq/common/jre`
Apache Tomcat	`/opt/netiq/idm/tomcat`
PostgreSQL	`/opt/netiq/idm/postgres`
Apache ActiveMQ	`/opt/netiq/idm/activemq`

Les fichiers journaux d'installation sont générés dans le répertoire `/var/opt/netiq/idm/log`.

5.6 Versions installées des composants

Les versions des composants et logiciels de prise en charge disponibles avec cette version sont les suivantes :

Composants Identity Manager	Version
Coffre-fort d'identité	`9.1` **REMARQUE :** Si vous effectuez une mise à niveau vers Identity Manager 4.7, assurez-vous que le coffre-fort d'identité est mis à niveau vers la version 9.1.
Moteur Identity Manager, chargeur distant, agent de dissémination	`4.7`
Designer	`4.7`
iManager	`3.1`
One SSO Provider	`6.2.1`
Self Service Password Reset	`4.2.0.4`
Applications d'identité	`4.7`
Identity Reporting	`6.0`
SLM for IGA	`8.1.1.0`

Composants de prise en charge	Version
Kit de développement Java (JRE) Oracle	`1.8.0_162`
Apache Tomcat	`8.5.27`
PostgreSQL	`9.6.6`
Apache ActiveMQ	`5.15.2`

5.7 Configuration de serveur et scénarios d'installation recommandés

Lorsque vous effectuez une installation autonome, vous devez installer les composants dans un ordre bien défini et sur des serveurs spécifiques. Les programmes d'installation de certains composants ont besoin d'informations au sujet des composants précédemment installés.

Cette section vous permet de déterminer l'ordre d'installation et les types de serveur, en fonction des scénarios spécifiques pour l'audit et la création de rapports.

5.7.1 Envoi d'événements à un service d'audit sans création de rapport dans Identity Manager

Dans ce scénario, vous envisagez d'utiliser Sentinel pour auditer les événements qui se produisent dans Identity Manager. Vous ne prévoyez pas de générer des rapports dans Identity Manager. Installez les composants dans l'ordre suivant :

1. Sentinel Log Management for IGA
2. Moteur Identity Manager, pilotes et plug-ins d'iManager
3. (Facultatif) iManager
4. Designer
5. SSPR
6. Applications d'identité
7. (Facultatif) Analyzer

5.7.2 Envoi d'événements à Identity Manager et génération de rapports

Dans ce scénario, vous prévoyez d'utiliser Sentinel Log Management for IGA fourni avec Identity Manager pour l'audit d'Identity Manager. Vous pouvez également générer des rapports sur ces événements. Installez les composants dans l'ordre suivant :

1. Sentinel Log Management for IGA
2. Moteur Identity Manager, pilotes et plug-ins d'iManager
3. (Facultatif) iManager
4. Designer
5. SSPR
6. Applications d'identité

7. Identity Reporting
8. (Facultatif) Analyzer

5.7.3 Envoi d'événements à un service externe avant de transmettre les événements à Identity Manager

Dans ce scénario, vous envisagez d'utiliser un service tel que Sentinel pour auditer Identity Manager. Installez les composants dans l'ordre suivant :

1. Service d'audit externe, tel que Sentinel
2. Moteur Identity Manager, pilotes et plug-ins d'iManager
3. (Facultatif) iManager
4. Designer
5. SSPR
6. Applications d'identité
7. Identity Reporting
8. (Facultatif) Analyzer

5.7.4 Configuration recommandée pour le serveur

Passez en revue les considérations suivantes pour mieux planifier votre installation :

Adhérence des composants

Composant	Installation indépendante	Remarques
Moteur Identity Manager	Oui	
Applications d'identité	Oui	Ce composant doit disposer de sa propre instance d'OSP. Les applications d'identité et OSP doivent être installés sur le même ordinateur.
Identity Reporting	Oui	Ce composant peut disposer de sa propre instance d'OSP. Le programme d'installation prend en charge une instance d'OSP installée en local ou à distance pour l'installation ou la mise à niveau d'Identity Reporting.
OSP	Non	Le programme d'installation ne prend pas en charge un serveur OSP installé à distance pour les applications d'identité. Vous devez installer OSP et les applications d'identité sur le même ordinateur.
SSPR	Oui	Le programme d'installation prend en charge l'installation et la mise à niveau autonomes de SSPR.
Base de données des applications d'identité	Oui	
Base de données de création de rapports	Oui	
Sentinel Log Management for IGA	Oui	

Dans un environnement de production traditionnel, vous pouvez installer Identity Manager sur sept serveurs ou plus, ainsi que sur des postes de travail clients. Par exemple :

Configuration de l'ordinateur	Installation du composant
Tout-en-un (uniquement recommandé pour une installation de démo/POC)	Installez et configurez tous les composants sur un seul ordinateur (moteur Identity Manager, applications d'identité, Identity Reporting, OSP, SSPR, base de données des applications d'identité et base de données de création de rapports) et Sentinel Log management for IGA sur un ordinateur distinct.
Installation distribuée	
Serveur 1	◆ Coffre-fort d'identité ◆ Moteur Identity Manager
Serveur 2	Applications d'identité et OSP (peuvent être mis en grappe)
Serveur 3	Identity Reporting (OSP)
Serveur 4	SSPR
Serveurs 5 et 6	Bases de données Identity Manager pour : ◆ Applications d'identité ◆ Identity Reporting
Serveur 7	Sentinel Log Management for IGA

5.7.5 Sélection d'une plate-forme de système d'exploitation pour Identity Manager

Vous pouvez installer les composants Identity Manager sur diverses plates-formes de système d'exploitation. Le tableau suivant vous aide à déterminer les serveurs à utiliser pour votre solution de gestion des identités.

Plate-forme	Composant
openSUSE	Analyzer Designer
Serveur Red Hat Linux (RHEL)	Applications d'identité Moteur Identity Manager Identity Reporting iManager Chargeur distant Sentinel Log Management for IGA
SUSE Linux Enterprise Desktop (SLED)	Designer

Plate-forme	Composant
SUSE Linux Enterprise Server (SLES)	Analyzer
	Designer
	Applications d'identité
	Moteur Identity Manager
	Identity Reporting
	iManager
	Chargeur distant
	Sentinel Log Management for IGA

Pour plus d'informations sur la configuration système requise et la configuration préalable, reportez-vous aux sections suivantes :

- « Planification de l'installation de Designer » page 183
- « Planification de l'installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting » page 61

5.8 Présentation des licences et de l'activation

Identity Manager propose un large éventail de fonctionnalités. Pour répondre aux différents besoins des clients, Identity Manager est disponible en version Advanced ou Standard Edition. La version Advanced Edition inclut l'ensemble des fonctionnalités d'Identity Manager. La version Standard Edition n'inclut, quant à elle, qu'un sous-ensemble des fonctionnalités fournies dans la version Advanced Edition. Pour une comparaison des fonctionnalités proposées par les versions Standard et Advanced Edition, reportez-vous à la comparaison des versions d'Identity Manager. NetIQ fournit des modèles de licence différents pour chaque version.

NetIQ fournit les deux éditions Advanced et Standard dans un même fichier ISO pour améliorer son offre de nouvelles fonctionnalités, de correctifs, de documentation et de support, tout en permettant aux clients de sélectionner les fonctionnalités de la solution les mieux adaptées à leurs besoins.

Vous pouvez installer une version d'évaluation d'Identity Manager et l'utiliser gratuitement pendant 90 jours. Toutefois, vous devez activer les composants Identity Manager dans un délai de 90 jours suivant l'installation, sinon ils cessent de fonctionner. Vous pouvez acquérir une licence produit et activer Identity Manager pendant la période d'évaluation de 90 jours ou ultérieurement. Pour plus d'informations, reportez-vous à la Section 24, « Activation d'Identity Manager », page 245.

En fonction de la version achetée, NetIQ fournit les clés de licence appropriées pour activer la fonctionnalité adéquate dans Identity Manager. Pour acheter une licence de produit Identity Manager, visitez le site Web consacré à la procédure d'achat de NetIQ Identity Manager. Une fois la licence produit achetée, NetIQ vous envoie votre ID client. Le message électronique contient également une URL redirigeant vers le site Web de NetIQ où vous pouvez obtenir une référence d'activation pour le produit. Si vous avez oublié votre ID client ou que vous ne l'avez pas reçu, contactez votre représentant commercial.

5.9 Préparation de l'installation

Cette section répertorie les conditions préalables générales pour les ordinateurs sur lesquels vous souhaitez héberger vos composants Identity Manager. En général, il est recommandé d'installer tous les composants afin de bénéficier de l'ensemble des fonctionnalités de gestion des identités dans votre environnement. Toutefois, vous n'avez pas besoin de tous les composants, tels qu'Analyzer ou iManager.

Les recommandations nécessaires à l'implémentation d'Identity Manager dépendent de votre environnement informatique. Vous devez donc contacter les services consulting NetIQ ou un partenaire NetIQ Identity Manager avant de finaliser l'architecture Identity Manager pour votre environnement.

Pour plus d'informations sur la configuration matérielle recommandée, les systèmes d'exploitation pris en charge et les navigateurs, consultez le site Web des informations techniques concernant NetIQ Identity Manager.

5.9.1 Garantie d'une haute disponibilité pour Identity Manager

Une haute disponibilité permet de gérer efficacement les ressources réseau stratégiques, notamment les données, les applications et les services. NetIQ garantit la haute disponibilité de votre solution Identity Manager par le biais de fonctions de mise en grappe ou de mise en grappe d'hyperviseur, telles que VMware VMotion. Lorsque vous planifiez un environnement de haute disponibilité, tenez compte des considérations suivantes :

- Vous pouvez installer les composants ci-dessous dans un environnement de haute disponibilité :
  - Moteur Identity Manager
  - Chargeur distant
  - Applications d'identité, hormis Identity Reporting
- Lorsque vous exécutez le coffre-fort d'identité (eDirectory) dans un environnement de grappe, le moteur Identity Manager est également mis en grappe.

Pour plus d'informations sur...	Voir...
Détermination de la configuration de serveur requise pour les composants Identity Manager	Section 5.7.4, « Configuration recommandée pour le serveur », page 40
Exécution du coffre-fort d'identité dans une grappe	Section 8.3.3, « Conditions préalables à l'installation du coffre-fort d'identité dans un environnement en grappe », page 65 Déploiement de eDirectory sur des grappes haute disponibilité dans le Guide d'installation de NetIQ eDirectory.

Pour plus d'informations sur...	Voir...
Exécution des applications d'identité dans une grappe	« Configuration d'OSP et de SSPR pour la mise en grappe » page 165 « Conditions préalables à l'installation des applications d'identité dans un environnement de grappe » page 81 « Activation de l'index des autorisations pour la mise en grappe » page 77 « Préparation d'une grappe pour les applications d'identité » page 82 « Configuration du pilote d'application utilisateur pour la mise en grappe » page 142 Section 22.3, « Mise à jour des liens SSPR dans le tableau de bord pour un environnement distribué ou de grappe », page 239

5.9.2 Espace minimum requis sur les serveurs Linux

Les composants Identity Manager requièrent un minimum d'espace disponible.

Le Tableau 5-1 page 44 précise l'espace disponible minimum requis pour les différents composants :

Tableau 5-1 *Espace disponible minimum requis*

Chemin	Composant	Espace disponible minimum requis
/opt	IDM	3 Go
/var	IDM	5 Go pour une DIB de 100 000 objets
/etc	IDM	5 Mo
/opt	iManager	700 Mo
/var	iManager	3 Go
/etc	iManager	10 Mo
/opt	Serveur d'applications d'identité	5 Go
/var	Serveur d'applications d'identité	100 Mo

Lors de l'installation, veillez à ce que le dossier `/temp` soit monté en tant qu'exécutable, qu'il possède un espace disponible de 5 Go et qu'il dispose d'autorisations d'écriture.

5.9.3 Installation d'Identity Manager sur des serveurs SLES 12 SP2 ou version ultérieure

- Votre serveur SLES 12 SP2 ou version ultérieure doit déjà être équipé de paquetages spécifiques pour une installation interactive des composants Identity Manager à l'aide de programmes d'installation de composants individuels ou du programme d'installation d'intégration.
  - `libXtst6-32bit-1.2.1-4.4.1.x86_64`
  - `libXrender1-32bit`
  - `libXi6-32bit`
- (Conditionnel) Lorsque vous installez les composants Identity Manager dans un environnement SLES 12 SP3, assurez-vous que le module `glibc-32bit-*x86_64.rpm` est installé, où * indique la dernière version du RPM.

REMARQUE : NetIQ vous recommande d'obtenir les paquetages dépendants auprès du service d'abonnement de votre système d'exploitation pour assurer un support continu de la part de votre fournisseur de système d'exploitation. Si vous ne disposez pas d'un service d'abonnement, vous pouvez vous procurer les paquetages récents à partir d'un site Web tel que http://rpmfind.net/linux.

5.9.4 Installation d'Identity Manager sur des serveurs RHEL 7.3 ou version ultérieure

Pour installer Identity Manager sur un serveur qui exécute des systèmes d'exploitation Red Hat Enterprise Linux 7.3 ou version ultérieure, assurez-vous que le serveur répond à un ensemble spécifique de conditions préalables.

- « Conditions préalables » page 45
- « Exécution d'une vérification préalable » page 46
- « Vérification de la présence de bibliothèques dépendantes sur le serveur » page 46
- « Création d'un dépôt pour le support d'installation » page 46

Conditions préalables

NetIQ vous recommande de vérifier que les conditions suivantes sont remplies :

- Si vous disposez d'un alias d'adresse de bouclage qui pointe vers le nom d'hôte du système dans une entrée `/etc/hosts`, il doit être remplacé par l'adresse IP ou le nom d'hôte. Autrement dit, si le fichier `/etc/hosts` contient une entrée similaire à la suivante, vous devez la modifier comme illustré dans l'exemple d'entrée correcte ci-dessous.

  L'exemple suivant pose problème lorsqu'un utilitaire tente une résolution sur le serveur ndsd :

  ```
  <loopback IP address> test-system localhost.localdomain localhost
  ```

  L'exemple suivant illustre une entrée correcte dans `/etc/hosts` :

  ```
  <loopback IP address> localhost.localdomain localhost
  <loopback IP address> test-system
  ```

Si un utilitaire ou un outil tiers assure la résolution par le biais de l'hôte local, il doit être reconfiguré pour l'effectuer par l'intermédiaire d'un nom d'hôte ou d'une adresse IP et non via l'adresse de l'hôte local.

- Installez les bibliothèques adéquates sur le serveur. Pour plus d'informations, reportez-vous à la « Vérification de la présence de bibliothèques dépendantes sur le serveur » page 46.

Exécution d'une vérification préalable

Vous pouvez générer un rapport sur les conditions requises manquantes pour chaque composant Identity Manager. Exécutez le script `./II-rhel-Prerequisite.sh` situé dans le répertoire `<emplacement extraction version Identity Manager>\install\utilities` du kit d'installation.

Vérification de la présence de bibliothèques dépendantes sur le serveur

Sur une plate-forme 64 bits, les bibliothèques requises pour RHEL varient en fonction de la méthode d'installation choisie. Installez les bibliothèques ou RPM dépendants dans l'ordre indiqué.

REMARQUE : pour ajouter un fichier `ksh`, vous pouvez saisir la commande suivante :

```
yum -y install ksh
```

- `glibc-*.i686.rpm`
- `libstdc++-*.i686.rpm`
- `libgcc-*.i686.rpm`
- `compat-libstdc++-33-*.x86_64.rpm`
- `compat-libstdc++-33-*.i686.rpm`
- `libXtst-*.i686.rpm`
- `libXrender-*.i686.rpm`

Création d'un dépôt pour le support d'installation

Si votre serveur RHEL 7.x a besoin d'un dépôt pour le support d'installation, vous pouvez en créer un manuellement.

REMARQUE

- Votre serveur RHEL doit également disposer des bibliothèques appropriées. Pour plus d'informations, reportez-vous à la « Vérification de la présence de bibliothèques dépendantes sur le serveur » page 46.
- Assurez-vous que le fichier RPM `unzip` est installé avant d'installer Identity Manager. Cette procédure s'applique à toutes les plates-formes Linux.

Pour configurer un dépôt pour l'installation :

1. Créez un point de montage sur votre serveur local.

   Par exemple : `/mnt/rhel (mkdir –p /mnt/rhel)`

2 Si vous utilisez un support d'installation, vous pouvez procéder au montage en exécutant la commande suivante :

```
# mount -o loop /dev/sr0 /mnt/rhel
```

OU

Montez l'image ISO d'installation de RHEL 7 sur un répertoire, par exemple `/mnt/rhel`, en exécutant la commande suivante :

```
# mount -o loop RHEL7.x.iso /mnt/rhel
```

Téléchargez l'image ISO RHEL 7.4 et montez-la.

Par exemple : `mount -o loop <chemin_du_fichier_rhel*.iso_téléchargé> /mnt/rhel`

3 Copiez le fichier `media.repo` situé à la racine du répertoire monté vers l'emplacement `/etc/YUM.repos.d/` et définissez les autorisations requises.

Par exemple :

```
# cp /mnt/rhel/media.repo /etc/yum.repos.d/rhel7dvd.repo
# chmod 644 /etc/yum.repos.d/rhel7dvd.repo
```

4 Modifiez le nouveau fichier .repo en remplaçant le paramètre `gpgcheck=0` par `gpgcheck=1` et ajoutez les lignes suivantes :

```
enabled=1
baseurl=file:///mnt/rhel/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

Au final, le nouveau fichier .repo devrait se présenter comme suit (même si la valeur du paramètre mediaid peut varier en fonction de la version de RHEL) :

```
[InstallMedia]
name=DVD for Red Hat Enterprise Linux 7.1 Server
mediaid=1359576196.686790
metadata_expire=-1
gpgcheck=1
cost=500
enabled=1
baseurl=file:///mnt/rhel
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

5 Pour installer les paquetages 32 bits, remplacez « exactarch=1 » par « exactarch=0 » dans le fichier `/etc/yum.conf`.

6 Pour installer les paquetages requis pour Identity Manager sous RHEL 7.x, créez un fichier install.sh et ajoutez-y les lignes suivantes :

```
#!/bin/bash
yum clean all
yum repolist
yum makecache

PKGS="ksh gettext.x86_64 libXrender.i686 libXau.i686 libxcb.i686 libX11.i686
libXext.i686 libXi.i686 libXtst.i686 glibc.x86_64 libstdc++.i686
libstdc++.x86_64 libgcc.x86_64"

for PKG in $PKGS;
do
yum -y install "$PKG"
done
```

REMARQUE : le support d'installation ne contient pas les fichiers `compat-libstdc++-33-*.i686.rpm` et compat-libstdc++-33-*.x86_64.rpm. Vous devez les télécharger depuis le portail Red Hat.

Exemple : pour installer le fichier `compat-libstdc++-33-*.x86_64.rpm`, exécutez la commande suivante :

```
yum -y install compat-libstdc++-33-*.x86_64.rpm
```

7 Exécutez le fichier install.sh créé à l'étape 8 ou à l'étape 7 selon la version de RHEL.

8 Pour vérifier si les conditions préalables sont remplies, exécutez le script mentionné dans la section 6.3.2.

9 Installez Identity Manager 4.7.

5.10 Présentation du support linguistique

NetIQ traduit (localise) l'interface d'Identity Manager et de ses programmes d'installation pour prendre en charge la langue du système d'exploitation de vos ordinateurs locaux. Toutefois, nous ne pouvons pas prendre en charge toutes les langues. Au cours de l'installation, certains programmes d'installation vérifient les paramètres régionaux de l'ordinateur pour déterminer la langue de la procédure d'installation.

Pour exécuter le programme d'installation dans une langue spécifique, définissez la variable LANG dans le profil ou via la ligne de commande.

5.10.1 Composants et programmes d'installation traduits

Le tableau suivant répertorie les traductions disponibles par installation de composant. Les composants ne figurant pas dans ce tableau ne sont disponibles qu'en anglais. Si le composant n'a pas été traduit dans la langue du système d'exploitation, le programme s'exécute par défaut en anglais. En outre, l'accord de licence utilisateur final du programme d'installation n'est peut-être pas disponible dans toutes les langues prises en charge.

Paramètre régional	Designer	Moteur Identity Manager	iManager	Plug-ins iManager	Applications d'identité
Chinois simplifié	Oui	Oui	Oui	Oui	Oui
Chinois traditionnel	Oui	Oui	Oui	Oui	Oui
Danois	–	–	–	–	Oui
Néerlandais	Oui	–	–	–	Oui
Anglais	Oui	Oui	Oui	Oui	Oui
Français	Oui	Oui	Oui	Oui	Oui
Allemand	Oui	Oui	Oui	Oui	Oui
Italien	Oui	–	Oui	–	Oui
Japonais	Oui	Oui	Oui	Oui	Oui
Portugais (Brésil)	Oui	–	Oui	–	Oui

Paramètre régional	Designer	Moteur Identity Manager	iManager	Plug-ins iManager	Applications d'identité
Russe	–	–	Oui	–	Oui
Espagnol	Oui	–	Oui	–	Oui
Suédois	–	–	–	–	Oui

Les applications d'identité incluent le tableau de bord, l'administration des applications d'identité, Identity Reporting, Approbations d'identité et l'application utilisateur.

5.10.2 Considérations spéciales pour la prise en charge des langues

NetIQ recommande de passer en revue les considérations suivantes pour décider si vous devez utiliser une version traduite d'Identity Manager.

- En général, si un composant Identity Manager ne prend pas en charge la langue du système d'exploitation, l'interface du composant s'exécute par défaut en anglais. Par exemple, les pilotes Identity Manager sont disponibles dans les mêmes langues que le moteur Identity Manager. Lorsqu'Identity Manager ne prend pas en charge la langue du pilote, la configuration du pilote s'exécute par défaut en anglais.
- Les plug-ins iManager suivants sont disponibles en espagnol, russe, italien et portugais, ainsi que dans les langues répertoriées dans le tableau précédent.
- Lorsque vous installez Designer, vous devez installer les utilitaires gettext. Les utilitaires GNU gettext offrent une infrastructure pour les messages internationalisés et multilingues.
- Lorsque vous lancez le programme d'installation pour un composant Identity Manager, les conditions suivantes s'appliquent :
  - Si le système d'exploitation est dans une langue prise en charge par le programme d'installation, le programme s'installe par défaut dans cette langue. Toutefois, vous pouvez spécifier une autre langue pour la procédure d'installation.
  - Si le programme d'installation ne prend pas en charge la langue du système d'exploitation, le programme d'installation s'exécute par défaut en anglais.
  - Si le système d'exploitation est défini sur une langue utilisant l'alphabet latin, le programme d'installation vous permet de spécifier une langue parmi celles qui utilisent l'alphabet latin.
  - Si le système d'exploitation utilise une langue asiatique ou le russe, le programme d'installation vous donne le choix entre la langue correspondant au système d'exploitation et l'anglais.

5.11 Téléchargement des fichiers d'installation

Pour installer les composants Identity Manager, téléchargez les fichiers d'installation suivants à partir du site Web des téléchargement NetIQ :

- **Moteur Identity Manager, Applications d'identité et Identity Reporting :**

  `Identity_Manager_4.7_Linux.iso`

- **Sentinel Log Management for Identity Governance and Administration :**

  `SentinelLogManagementForIGA8.1.1.0.tar.gz`

- **Designer :** `Identity_Manager_4.7_Linux_Designer.tar.gz`
- **Analyzer :** `Identity_Manager_4.7_Linux_Analyzer.tar.gz`

Pour télécharger les fichiers d'installation :

1. Accédez au site Web des téléchargements NetIQ.
2. Cliquez sur le bouton **Download** (Télécharger) en regard du fichier que vous voulez télécharger.
3. Suivez les invites à l'écran pour télécharger le fichier dans un répertoire sur votre ordinateur.

II Installation de Sentinel Log Management for Identity Governance and Administration

Cette section vous guide tout au long du processus d'installation de SLM for IGA, qui est le service d'audit par défaut d'Identity Manager.

Le programme d'installation de SLM for IGA effectue les opérations suivantes :

- Installation et, si vous le souhaitez, configuration du service
- Création du compte utilisateur permettant d'effectuer les tâches d'administration relatives au service (**admin**)
- Création du compte d'administration de la base de données que le service utilise pour interagir avec la base de données (**dbauser**)

6 Planification de l'installation de SLM for IGA

Cette section vous guide pour la préparation de l'installation de SLM for IGA, qui est le service d'audit par défaut d'Identity Manager.

6.1 Liste de contrôle pour l'installation de SLM for IGA

NetIQ vous recommande de suivre les étapes de la liste de contrôle suivante :

	Éléments de la liste de contrôle
❑	1. Avant l'installation, passez en revue la configuration système requise pour vous assurer que les ordinateurs la respectent. Pour plus d'informations, reportez-vous au Section 6.2, « Configuration système requise », page 53.
❑	2. (Conditionnel) Pour les ordinateurs exécutant un système d'exploitation RHEL 7.4, assurez-vous d'avoir installé l'ensemble de bibliothèques approprié.
❑	3. Décidez si vous voulez effectuer une installation standard ou personnalisée de SLM for IGA. Pour plus d'informations, reportez-vous à la section Section 7, « Installation de SLM for IGA », page 55.

6.2 Configuration système requise

Cette section décrit la configuration minimale requise pour le(s) serveur(s) sur le(s)quel(s) vous souhaitez installer. Pour plus d'informations, rendez-vous sur le site Web d'informations techniques sur NetIQ Sentinel.

Veuillez également passer en revue les conditions préalables requises et les considérations relatives à l'installation, en particulier celles liées au système d'exploitation.

Catégorie	Configuration requise
Processeur	4 à 8 coeurs de processeurs
Espace disque	200 Go
Mémoire	24 Go

Catégorie	Configuration requise
Système d'exploitation (certifié)	Un des systèmes d'exploitation 64 bits suivants (minimum requis) : ◆ SLES 12 SP2 ◆ RHEL 7.3 **REMARQUE :** *Certifié* signifie que le système d'exploitation a été entièrement testé et est pris en charge.
Systèmes d'exploitation (pris en charge)	Dernières versions des Service Packs pour les systèmes d'exploitation certifiés **REMARQUE :** *Pris en charge* signifie que le système d'exploitation n'a pas encore été testé, mais qu'il devrait fonctionner

7 Installation de SLM for IGA

Vous pouvez installer Sentinel Log Management for Identity Governance and Administration (IGA) à l'aide d'une installation standard ou personnalisée.

7.1 Installation standard

1. Téléchargez le fichier `SentinelLogManagementForIGA8.1.1.0.tar.gz` à partir du site Web des téléchargements NetIQ.
2. Accédez au répertoire dans lequel vous souhaitez extraire le fichier.
3. Exécutez la commande suivante pour extraire le fichier :

   ```
   tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
   ```
4. Accédez au répertoire `SentinelLogManagementforIGA`.
5. Pour installer SLM for IGA, exécutez la commande suivante :

   ```
   ./install.sh
   ```
6. Spécifiez la langue à utiliser dans le cadre de l'installation, puis appuyez sur la touche `Entrée`.
7. Entrez `o` pour accepter l'accord de licence.

   L'installation peut prendre quelques secondes à charger les paquetages d'installation.
8. Lorsque le système vous y invite, tapez `1` pour effectuer l'installation standard.

   L'installation utilise la clé de licence d'évaluation par défaut incluse avec le programme d'installation. À tout moment, que ce soit pendant ou après la période d'évaluation, vous pouvez remplacer la clé de la licence d'évaluation par celle que vous avez achetée.
9. Spécifiez le mot de passe de l'administrateur `admin`.
10. Confirmez le mot de passe.

    Ce mot de passe est utilisé par les utilisateurs `admin`, `dbauser` et `appuser`.

L'installation de se termine et le serveur démarre. Après l'installation, le démarrage de tous les services peut prendre quelques minutes, car le système effectue une initialisation unique. Patientez jusqu'à la fin de l'installation avant de vous connecter au serveur Sentinel.

Pour accéder à l'interface principale de SLM for IGA, spécifiez l'URL suivante dans votre navigateur Web :

`https://<IP_Address/DNS_SLM for IGA_server>:8443/SLM for IGA/views/main.html`

Où `<IP_Address/DNS_SLM for IGA_server>` correspond à l'adresse IP ou au nom DNS du serveur SLM for IGA et *8443* est le port par défaut du serveur SLM for IGA.

7.2 Installation personnalisée

1. Téléchargez le fichier `SentinelLogManagementForIGA8.1.1.0.tar.gz` à partir du site Web des téléchargements NetIQ.
2. Accédez au répertoire dans lequel vous souhaitez extraire le fichier.
3. Exécutez la commande suivante pour extraire le fichier :

   ```
   tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
   ```
4. Accédez au répertoire `SentinelLogManagementforIGA`.
5. Exécutez la commande suivante :

   ```
   ./install.sh
   ```
6. Tapez `y` pour accepter l'accord de licence et poursuivre l'installation.

   L'installation peut prendre quelques secondes à charger les paquetages d'installation.
7. Spécifiez `2` pour effectuer une configuration personnalisée de SLM for IGA.
8. Indiquez `1` pour utiliser la clé de licence d'évaluation par défaut.

   ou

   Indiquez `2` pour entrer une clé de licence achetée pour SLM for IGA.
9. Indiquez le mot de passe de l'utilisateur administrateur `admin` et confirmez-le en le ressaisissant.
10. Indiquez le mot de passe de l'utilisateur de base de données `dbauser` et confirmez-le en le ressaisissant.

    Le compte `dbauser` correspond à l'identité utilisée par SLM for IGA pour interagir avec la base de données. Le mot de passe que vous saisissez ici peut être utilisé pour les tâches de maintenance de base de données, y compris la réinitialisation du mot de passe admin en cas de perte ou d'oubli.
11. Indiquez le mot de passe de l'utilisateur d'application `appuser` et confirmez-le en le ressaisissant.
12. Modifiez les assignations de port en spécifiant le numéro requis.

    Par exemple, le port par défaut pour le serveur Web est 8443. Pour modifier le numéro de port du serveur Web, indiquez `4`. Entrez la nouvelle valeur de port pour le serveur Web, par exemple, 8643.
13. Après avoir modifié les ports, tapez 8 lorsque vous avez terminé.
14. Saisissez `1` pour authentifier les utilisateurs qui utilisent uniquement la base de données interne.

    ou

    Si vous avez configuré un annuaire LDAP dans votre domaine, saisissez `2` pour authentifier les utilisateurs à l'aide de l'authentification d'annuaires LDAP.

    La valeur par défaut est `1`.
15. Entrez `n` lorsque vous êtes invité à activer le mode FIPS 140-2.
16. Entrez `n` lorsque vous êtes invité à activer le stockage évolutif.

L'installation de se termine et le serveur démarre. Après l'installation, le démarrage de tous les services peut prendre quelques minutes, car le système effectue une initialisation unique. Patientez jusqu'à la fin de l'installation avant de vous connecter au serveur Sentinel.

Pour accéder à l'interface principale de SLM for IGA, spécifiez l'URL suivante dans votre navigateur Web :

`https://<IP_Address/DNS_SLM for IGA_server>:<port>/SLM for IGA/views/main.html`

Où <*IP_Address/DNS_SLM for IGA_server*> correspond à l'adresse IP ou au nom DNS du serveur SLM for IGA et <*port*> est le port par défaut du serveur SLM for IGA.

IV Installation et configuration du moteur Identity Manager, des applications d'identité et d'Identity Reporting

Cette section vous guide tout au long du processus d'installation des composants Moteur Identity Manager, Applications d'identité et Identity Reporting. Avant de commencer l'installation, réfléchissez à la façon dont vous souhaitez implémenter Identity Manager. Vous pouvez installer les composants Identity Manager sur un seul serveur ou sur des serveurs distincts. Pour plus d'informations, reportez-vous à la Section 5.7.4, « Configuration recommandée pour le serveur », page 40.

Vous pouvez installer et configurer les composants en mode interactif ou silencieux. Le programme d'installation prévoit des phases différentes pour l'installation et la configuration des composants. Pour plus d'informations, reportez-vous au Section 8.2, « Présentation du programme d'installation », page 62. Les scripts d'installation et de configuration, `install.sh` et `configure.sh`, se trouvent à la racine du fichier image `.iso` du paquetage d'installation d'Identity Manager. Par défaut, le programme d'installation enregistre les composants aux emplacements par défaut. Pour plus d'informations, reportez-vous à la Section 5.5, « Emplacements d'installation par défaut », page 37.

REMARQUE : vous devez exécuter `install.sh` à partir de l'emplacement où vous avez monté le fichier `.iso`. L'exécution du script `install.sh` à partir d'un emplacement personnalisé entraîne des échecs.

NetIQ recommande de consulter les conditions préalables et la configuration système requise avant de commencer l'installation. Pour plus d'informations, reportez-vous à la Chapitre 8, « Planification de l'installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting », page 61.

8 Planification de l'installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting

Cette section indique les conditions préalables, les considérations et la configuration système requise pour installer les composants Moteur Identity Manager, Applications d'identité et Identity Reporting. Tout d'abord, consultez la liste de contrôle pour comprendre la procédure d'installation.

8.1 Liste de contrôle pour l'installation des composants Identity Manager

Avant d'entamer la procédure d'installation, NetIQ recommande de passer en revue les étapes suivantes.

	Éléments de la liste de contrôle
❑	1. Renseignez-vous sur les interactions entre les différents composants Identity Manager. Pour plus d'informations, reportez-vous au Partie I, « Introduction », page 15.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.7, « Configuration de serveur et scénarios d'installation recommandés », page 39.
❑	3. Vérifiez les considérations relatives à l'installation du moteur Identity Manager pour vous assurer que les ordinateurs remplissent les conditions préalables. Pour plus d'informations, reportez-vous à la Section 8.3, « Planification de l'installation du moteur Identity Manager », page 64.
❑	4. Vérifiez la configuration matérielle et logicielle requise pour les ordinateurs qui hébergeront le moteur Identity Manager. Pour plus d'informations, reportez-vous au « Configuration système requise pour le moteur Identity Manager, le chargeur distant et iManager » page 65.
❑	5. Découvrez quels pilotes sont automatiquement activés après l'installation du moteur Identity Manager. Pour plus d'informations, reportez-vous à la Section 8.3.2, « Considérations relatives à l'installation des pilotes avec le moteur Identity Manager », page 64.
❑	6. (Conditionnel) Pour les ordinateurs exécutant RHEL 7.3 ou version ultérieure, assurez-vous d'avoir installé l'ensemble de bibliothèques approprié.

	Éléments de la liste de contrôle
❑	7. Pour installer le moteur Identity Manager, reportez-vous à l'une des sections suivantes : ◆ Section 9.1.1, « Exécution d'une installation interactive », page 91 ◆ Section 9.1.2, « Exécution d'une installation silencieuse du moteur Identity Manager », page 92
❑	8. (Conditionnel) Pour installer le chargeur distant, reportez-vous à la Section 8.4, « Planification de l'installation du chargeur distant », page 68.
❑	9. (Conditionnel) Si vous effectuez une installation non-root, mettez à jour l'ensemble de pilotes pour prendre en charge les graphiques dans les notifications par message électronique. Pour plus d'informations, reportez-vous au Section 11.1.2, « Ajout de la prise en charge des graphiques dans les notifications par message électronique », page 109.
❑	10. Démarrez l'instance de pilote dans le chargeur distant. Pour plus d'informations, reportez-vous à la Chapitre 11.3, « Configuration des pilotes et du chargeur distant », page 118.

8.2 Présentation du programme d'installation

Le programme d'installation d'Identity Manager prend en charge l'installation et la configuration des composants Identity Manager au cours de phases différentes. Selon l'édition sélectionnée pendant l'installation d'Identity Manager (Advanced Edition ou Standard Edition), différents composants sont installés. Par exemple, les options affichées en cas de sélection d'Identity Manager Advanced Edition sont les suivantes :

- Moteur Identity Manager
- Service du chargeur distant Identity Manager
- Agent de dissémination Identity Manager
- Administration Web d'iManager
- Identity Reporting
- Applications d'identité

Vous pouvez configurer les composants Identity Manager immédiatement après l'installation ou ultérieurement. Identity Manager fournit deux options de configuration : standard et personnalisée.

Une configuration standard utilise les paramètres par défaut pour la plupart des options de configuration. Dans une configuration personnalisée, vous pouvez spécifier des valeurs personnalisées en fonction de vos besoins. Vous pouvez configurer la plupart des paramètres à l'aide de cette option.

Pour plus d'informations sur la configuration selon les composants, reportez-vous à la section Section 10.1, « Présentation des paramètres de configuration », page 101.

Les sections suivantes expliquent les composants qui peuvent être installés avec chaque option d'installation fournie par le programme d'installation :

8.2.1 Moteur Identity Manager

Installe le coffre-fort d'identité, le moteur Identity Manager et les pilotes Identity Manager.

8.2.2 Serveur du chargeur distant Identity Manager

Installe le service du chargeur distant et les instances de pilote dans le chargeur distant. Le chargeur distant permet d'exécuter des pilotes Identity Manager sur les systèmes connectés qui n'hébergent pas le coffre-fort d'identité ni le moteur Identity Manager.

8.2.3 Agent de dissémination Identity Manager

Installe l'agent de dissémination (fan-out) pour le pilote de dissémination JDBC. Ce dernier utilise l'agent de dissémination pour créer plusieurs instances de pilote de dissémination JDBC. L'agent de dissémination charge les instances de pilote JDBC en fonction de la configuration des objets de connexion dans le pilote de dissémination. Pour plus d'informations, reportez-vous au manuel NetIQ Identity Manager Driver for JDBC Fan-Out Implementation Guide (Guide d'implémentation du pilote JDBC Fan-out de NetIQ Identity Manager).

8.2.4 Administration Web d'iManager

Installe la console d'administration Web d'iManager et les plug-ins iManager.

8.2.5 Applications d'identité

Cette option d'installation installe plusieurs composants qui fournissent la structure sous-jacente pour les applications d'identité.

- Tableau de bord Identity Manager
- Console d'administration d'Identity Manager
- Application utilisateur
- Pilote de l'application utilisateur (UAD)
- Pilote du service de rôles et de ressources (RRSD)

Le programme d'installation installe en interne un service d'authentification pour prendre en charge un accès Single Sign-on aux applications d'identité et à Identity Reporting. Le programme d'installation installe également un service de gestion des mots de passe qui vous aide à configurer Identity Manager pour permettre aux utilisateurs de réinitialiser leur mot de passe.

Le processus d'installation déploie le pilote d'application utilisateur ainsi que le pilote du service Rôles et ressource.

8.2.6 Identity Reporting

Cette option d'installation installe plusieurs composants qui fournissent la structure sous-jacente pour Identity Reporting.

- Identity Reporting
- Pilote de passerelle système gérée (MSGW, Managed System Gateway)
- Pilote du service de collecte de données (DCS, Data Collection Service)

Identity Reporting communique avec SLM for IGA à des fins d'audit. Pour consigner des événements, Identity Reporting doit pouvoir accéder à la base de données SIEM installée en même temps que SLM for IGA.

Le processus d'installation permet de déployer les pilotes MSGW et DCS.

8.3 Planification de l'installation du moteur Identity Manager

Cette section fournit des informations pour l'installation du moteur et des pilotes Identity Manager.

- Section 8.3.1, « Considérations relatives à l'installation du moteur Identity Manager », page 64
- Section 8.3.2, « Considérations relatives à l'installation des pilotes avec le moteur Identity Manager », page 64
- Section 8.3.3, « Conditions préalables à l'installation du coffre-fort d'identité dans un environnement en grappe », page 65
- Section 8.3.4, « Configuration système requise pour le moteur Identity Manager, le chargeur distant et iManager », page 65

8.3.1 Considérations relatives à l'installation du moteur Identity Manager

Avant d'installer le moteur Identity Manager, passez en revue les considérations suivantes :

- Le programme d'installation installe une version 64 bits d'Identity Manager sur la base de la version du coffre-fort d'identité.
- (Conditionnel) Pour installer le chargeur distant sur le même ordinateur que le moteur Identity Manager, assurez-vous de sélectionner un système d'exploitation qui prend en charge les deux composants. Pour plus d'informations sur la configuration système requise pour le chargeur distant, reportez-vous à la Section 8.4.5, « Conditions préalables et considérations relatives à l'installation du chargeur distant », page 71.
- (Conditionnel) Si vous installez le moteur Identity Manager en tant qu'utilisateur non-`root`, le processus d'installation n'installe pas l'agent de plate-forme NetIQ Sentinel, ni le pilote de compte Linux, ni le chargeur distant. Vous devez installer ces composants séparément.

  REMARQUE : pour prendre en charge l'audit avec une installation non-root du moteur, installez le dernier correctif pour l'agent de plateforme Novell Audit. Pour plus d'informations, contactez l'équipe de support technique.

8.3.2 Considérations relatives à l'installation des pilotes avec le moteur Identity Manager

De nombreuses variables agissent sur les performances du serveur sur lequel vous installez le moteur Identity Manager, y compris le nombre de pilotes exécutés sur le serveur. Dans le cadre de la planification de l'emplacement d'installation des pilotes, NetIQ formule les recommandations suivantes :

- En général, le nombre de pilotes exécutés sur le serveur dépend de la charge exercée par les pilotes sur le serveur. Certains pilotes traitent un grand nombre d'objets, d'autres pas.
- Si vous envisagez de synchroniser des millions d'objets sur chaque pilote, limitez le nombre de pilotes sur le serveur. Par exemple, déployez moins de 10 pilotes pour ces pilotes.

- Si vous envisagez de synchroniser moins de 100 objets par pilote, vous pourrez probablement exécuter plus de 10 pilotes sur le serveur.
- Pour créer une ligne de base sur les performances du serveur afin de déterminer le nombre optimal de pilotes, utilisez les outils de surveillance de l'état de santé dans iManager. Pour plus d'informations sur les outils de contrôle de l'état de santé, reportez-vous à la section « Monitoring Driver Health » (Contrôle de l'état de santé des pilotes) du manuel NetIQ Identity Manager Driver Administration Guide (Guide d'administration des pilotes de NetIQ Identity Manager).

Pour plus d'informations sur l'activation des pilotes Identity Manager après l'installation, reportez-vous à la Chapitre 24, « Activation d'Identity Manager », page 245.

8.3.3 Conditions préalables à l'installation du coffre-fort d'identité dans un environnement en grappe

Avant d'installer le coffre-fort d'identité dans un environnement en grappe, NetIQ recommande de passer en revue les considérations suivantes :

- Vous devez disposer d'un système de stockage partagé externe pris en charge par le logiciel de grappe, avec suffisamment d'espace disque pour pouvoir stocker toutes les données NICI et du coffre-fort d'identité :
  - La DIB du coffre-fort d'identité doit se trouver sur le stockage partagé de la grappe. Les données d'état du coffre-fort d'identité doivent être situées sur le stockage partagé de sorte qu'elles soient disponibles sur le noeud de grappe qui exécute actuellement les services.
  - L'instance root du coffre-fort d'identité sur chaque noeud de grappe doit être configurée pour utiliser la DIB sur le stockage partagé.
  - Vous devez également partager les données NICI (NetIQ International Cryptographic Infrastructure) de manière à ce que les clés propres aux serveurs soient répliquées sur les noeuds de grappe. Les données NICI utilisées par tous les noeuds de grappe doivent être situées sur le stockage partagé de grappe.
  - NetIQ recommande de stocker toutes les autres données de configuration et de journal d'eDirectory sur le stockage partagé.
- Vous devez disposer d'une adresse IP virtuelle.
- (Conditionnel) Si vous utilisez eDirectory comme structure de support pour le coffre-fort d'identité, l'utilitaire `nds-cluster-config` prend en charge la configuration de l'instance eDirectory root uniquement. eDirectory ne prend pas en charge la configuration de plusieurs instances et les installations non-root d'eDirectory dans un environnement en grappe.

Pour plus d'informations sur l'installation du coffre-fort d'identité dans un environnement de grappe, reportez-vous à la section Déploiement d'eDirectory sur des clusters haute disponibilité du *Guide d'installation de NetIQ eDirectory*.

8.3.4 Configuration système requise pour le moteur Identity Manager, le chargeur distant et iManager

Le tableau suivant répertorie la configuration système requise pour l'installation selon les composants :

REMARQUE : le système de fichiers BTRFS n'est pas pris en charge pour le coffre-fort d’identité.

Catégorie	Coffre-fort d'identité	Moteur Identity Manager	Chargeur distant (64 bits)	iManager
Processeur	1 GHz	1 GHz	1 GHz	1 GHz
Espace disque	◆ 300 Mo pour le coffre-fort d'identité ◆ 150 Mo d'espace disque supplémentaire par tranche de 50 000 utilisateurs	◆ 1 Go ◆ 150 Mo d'espace disque supplémentaire par tranche de 50 000 utilisateurs		200 Mo
Mémoire	2 Go	◆ 2 Go pour le moteur Identity Manager ◆ 2 Go pour les pilotes Identity Manager	512 Mo	512 Mo
Système d'exploitation (certifié) **REMARQUE :** *Certifié* signifie que le système d'exploitation a été entièrement testé et est pris en charge. Avant d'installer Identity Manager, NetIQ recommande d'appliquer les derniers correctifs du système d'exploitation en fonction de la fonctionnalité de mise à jour automatisée du fabricant.	L'un des systèmes d'exploitation 64 bits suivants : ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3	L'un des systèmes d'exploitation 64 bits suivants : ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3	L'un des systèmes d'exploitation 64 bits suivants : ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3	L'un des systèmes d'exploitation 64 bits suivants : ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3
Système d'exploitation (pris en charge) **REMARQUE :** *Pris en charge* signifie que le système d'exploitation n'a pas encore été testé, mais qu'il devrait fonctionner.	Dernières versions des Service Packs pour les systèmes d'exploitation certifiés	Dernières versions des Service Packs pour les systèmes d'exploitation certifiés	Dernières versions des Service Packs pour les systèmes d'exploitation certifiés	Dernières versions des Service Packs pour les systèmes d'exploitation certifiés

Catégorie	Coffre-fort d'identité	Moteur Identity Manager	Chargeur distant (64 bits)	iManager
Système de virtualisation NetIQ prend en charge Identity Manager sur les systèmes de virtualisation d'entreprise qui sont officiellement compatibles avec les systèmes d'exploitation sur lesquels les produits NetIQ s'exécutent. NetIQ prend en charge l'intégralité de la pile Identity Manager sur les systèmes de virtualisation dont les éditeurs prennent officiellement en charge ces systèmes d'exploitation.	◆ Hyper-V Server 2012 R2 ◆ VMware ESX 5.0 et versions ultérieures ◆ Virtualisation de Windows Server 2012 R2 avec Hyper-V (prise en charge)	◆ Hyper-V Server 2012 R 2 ◆ VMware ESX 5.0 et versions ultérieures ◆ Virtualisation de Windows Server 2012 R 2 avec Hyper-V (prise en charge)	◆ Hyper-V Server 2012 R 2 ◆ VMware ESX 5.0 et versions ultérieures ◆ Virtualisation de Windows Server 2012 R 2 avec Hyper-V (prise en charge)	
Logiciel	eDirectory 9.1	Identity Manager Engine 4.7	Remote Loader 4.7	iManager 3.1
Java (Java Runtime Environment [JRE] d'Oracle)	JRE 1.8.0_162	JRE 1.8.0_162	JRE 1.8.0_162	JRE 1.8.0_162
Navigateur Web				Un des navigateurs suivants (versions minimales) : ◆ Google Chrome 61 ◆ Mozilla Firefox 51
Serveur d'applications				Apache Tomcat 8.5.27 fourni avec iManager
Ports par défaut				8080, 8443 et 9009

8.4 Planification de l'installation du chargeur distant

Cette section présente des informations qui vous permettent de préparer l'installation du chargeur distant et du chargeur distant Java.

- Section 8.4.1, « Liste de contrôle pour l'installation du chargeur distant », page 68
- Section 8.4.2, « Présentation du chargeur distant », page 69
- Section 8.4.3, « Présentation du programme d'installation », page 71
- Section 8.4.4, « Utilisation d'un chargeur distant 32 ou 64 bits sur le même ordinateur », page 71
- Section 8.4.5, « Conditions préalables et considérations relatives à l'installation du chargeur distant », page 71

8.4.1 Liste de contrôle pour l'installation du chargeur distant

NetIQ vous recommande de suivre les étapes de la liste de contrôle suivante :

	Éléments de la liste de contrôle
❑	1. Renseignez-vous sur les interactions entre les différents composants Identity Manager. Pour plus d'informations, reportez-vous au Section 3.3.3, « Chargeur distant », page 23.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.7, « Configuration de serveur et scénarios d'installation recommandés », page 39.
❑	3. Vérifiez que le moteur Identity Manager a été installé.
❑	4. Passez en revue les considérations relatives à l'installation du chargeur distant pour vous assurer que les ordinateurs satisfont aux conditions préalables. Pour plus d'informations, reportez-vous à la Section 8.4.5, « Conditions préalables et considérations relatives à l'installation du chargeur distant », page 71.
❑	5. Vérifiez la configuration matérielle et logicielle requise pour les ordinateurs qui hébergeront le chargeur distant. Pour plus d'informations, reportez-vous à la Section 8.3.4, « Configuration système requise pour le moteur Identity Manager, le chargeur distant et iManager », page 65.
❑	6. (Conditionnel) Pour les ordinateurs s'exécutant sous un système d'exploitation RHEL 7.3. ou version ultérieure, assurez-vous d'avoir installé l'ensemble de bibliothèques approprié. Pour plus d'informations, reportez-vous au Section 5.9.4, « Installation d'Identity Manager sur des serveurs RHEL 7.3 ou version ultérieure », page 45.
❑	7. (Conditionnel) Pour installer le chargeur distant sur un serveur qui n'héberge pas le moteur Identity Manager, vérifiez que vous pouvez établir une connexion sécurisée avec le moteur. Pour plus d'informations, reportez-vous au Section 11.3.1, « Création d'une connexion sécurisée au moteur Identity Manager », page 119.
❑	8. Déterminez si vous souhaitez installer une version 32 ou 64 bits du chargeur distant. Pour plus d'informations, reportez-vous à la Section 8.4.4, « Utilisation d'un chargeur distant 32 ou 64 bits sur le même ordinateur », page 71.
❑	9. Déterminez si vous devez utiliser le chargeur distant ou le chargeur distant Java. Pour plus d'informations, reportez-vous à la « Présentation du chargeur distant Java » page 71.
❑	10. Installez le chargeur distant. Pour plus d'informations, reportez-vous au Chapitre 9, « Installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting », page 91.

	Éléments de la liste de contrôle
❑	11. (Conditionnel) Pour installer le chargeur distant Java, reportez-vous à la Section 9.2, « Installation du chargeur distant Java », page 95.
❑	12. Passez en revue les paramètres de configuration d'une instance de pilote. Pour plus d'informations, reportez-vous à la Section 11.3.2, « Présentation des paramètres de configuration du chargeur distant », page 121.
❑	13. Pour configurer une instance de pilote sur le chargeur distant, reportez-vous à l'une des sections suivantes : ◆ Section 11.3.3, « Configuration du chargeur distant pour les instances de pilote », page 130 ◆ Section 11.3.4, « Configuration du chargeur distant Java pour les instances de pilote », page 132
❑	14. Préparez vos pilotes pour le chargeur distant. Pour plus d'informations, reportez-vous à la Section 11.3.5, « Configuration des pilotes Identity Manager pour fonctionner avec le chargeur distant », page 133.
❑	15. Démarrez l'instance de pilote dans le chargeur distant. Pour plus d'informations, reportez-vous à la Section 11.3.8, « Démarrage d'une instance de pilote dans le chargeur distant », page 140.
❑	16. (Conditionnel) Pour configurer l'authentification mutuelle entre le chargeur distant et le moteur Identity Manager, reportez-vous à la Section 11.3.6, « Configuration de l'authentification mutuelle avec le moteur Identity Manager », page 134.
❑	17. Vérifiez que le chargeur distant et le pilote communiquent avec le moteur Identity Manager et le système connecté. Pour plus d'informations, reportez-vous au Section 11.3.7, « Vérification de la configuration », page 140.
❑	18. Installez le reste des composants Identity Manager, y compris Designer et Analyzer.

8.4.2 Présentation du chargeur distant

Le chargeur distant permet d'exécuter des pilotes Identity Manager sur les systèmes connectés qui n'hébergent pas le coffre-fort d'identité et le moteur Identity Manager.

Le chargeur distant peut aussi bien héberger des modules d'interface d'application Identity Manager contenus dans des fichiers spécifiques à la plate-forme par le biais de JNI, que des modules d'interface d'application Identity Manager plus courants contenus dans des fichiers JAR qui ne sont associés à aucune plate-forme spécifique. Le chargeur distant peut être exécuté quelle que soit la plate-forme. Toutefois, les modules d'interface spécifiques à une plate-forme doivent être exécutés sur une plate-forme native (par exemple, fichiers `.iso` sous Linux).

Présentation des modules d'interface

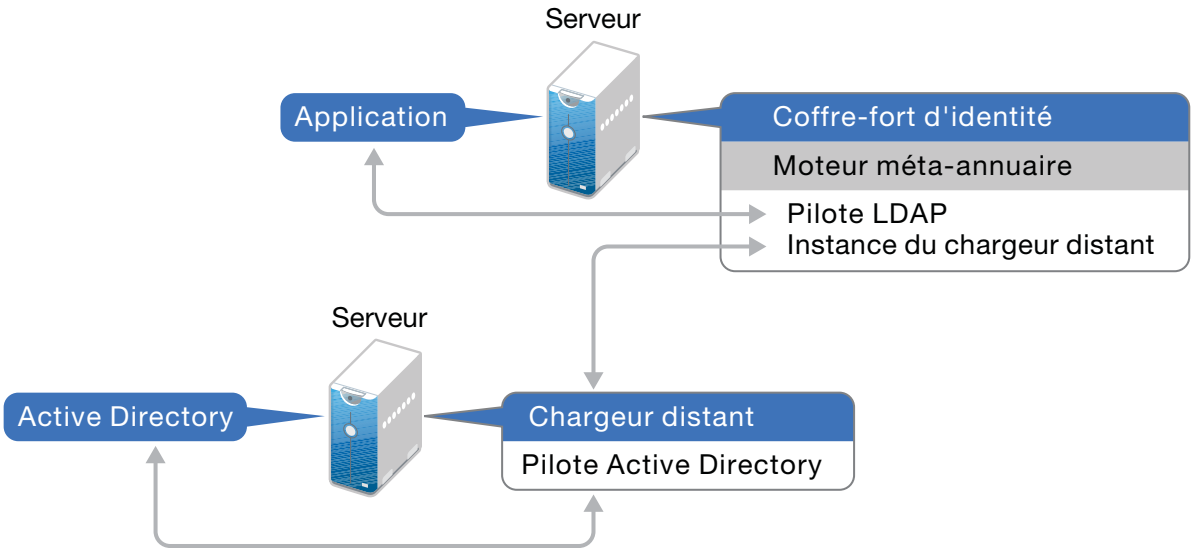
Le chargeur distant utilise des modules d'interface pour communiquer avec l'application sur un système géré. Un *module d'interface* rassemble un ou plusieurs fichiers qui contiennent du code pour traiter les événements qui se synchronisent entre le coffre-fort d'identité et l'application. Avant d'utiliser le chargeur distant, vous devez configurer le module d'interface d'application pour vous connecter au moteur Identity Manager en toute sécurité. Vous devez également configurer le chargeur distant ainsi que les pilotes Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 11.3, « Configuration des pilotes et du chargeur distant », page 118.

Cas d'utilisation du chargeur distant

Vous pouvez installer le moteur Identity Manager, le coffre-fort d'identité et le module d'interface pilote sur le même serveur. Le moteur Identity Manager s'exécute dans le cadre d'un processus eDirectory. Les pilotes Identity Manager peuvent s'exécuter sur le même serveur qu'Identity Manager. Ils peuvent aussi faire partie du même processus que le moteur Identity Manager. Toutefois, dans les cas suivants, vous souhaiterez peut-être que le pilote Identity Manager s'exécute en tant que processus distinct sur le serveur qui héberge le moteur Identity Manager :

- Pour préserver le coffre-fort d'identité des éventuelles exceptions rencontrées par le module d'interface du pilote.
- Pour améliorer les performances du serveur qui exécute le moteur Identity Manager, en déchargeant les commandes du pilote sur l'application ou la base de données distante.
- Pour exécuter d'autres pilotes sur les serveurs n'hébergeant pas le moteur Identity Manager.

Dans ces scénarios, le chargeur distant fournit un canal de communication entre le pilote et le moteur Identity Manager. Par exemple, vous installez un pilote LDAP sur le même serveur que le coffre-fort d'identité et le moteur Identity Manager. Ensuite, vous installez le pilote Active Directory (AD) sur un autre serveur avec le chargeur distant. Pour autoriser les pilotes à accéder à l'application et à communiquer avec le coffre-fort d'identité, installez le chargeur distant sur les deux serveurs, comme l'illustr la figure suivante:



NetIQ vous recommande, dans la mesure du possible, d'utiliser la configuration du chargeur distant avec vos pilotes. Utilisez le chargeur distant même lorsque l'application se trouve sur le même serveur que le moteur Identity Manager.

Présentation du chargeur distant Java

Le chargeur distant Java offre la flexibilité nécessaire pour charger un module d'interface pilote sur des ordinateurs dotés de serveurs Linux qui ne sont pas pris en charge par le chargeur distant natif. Le chargeur distant Java est une application Java compatible avec toute version de Java officiellement prise en charge.

Pour ouvrir l'application, exécutez le script de shell appelé `dirxml_jremote`. Pour plus d'informations, reportez-vous à la Section 11.3.4, « Configuration du chargeur distant Java pour les instances de pilote », page 132.

8.4.3 Présentation du programme d'installation

Le programme d'installation du moteur Identity Manager peut installer une version 32 ou 64 bits, ou les deux versions d'un chargeur distant. Outre le chargeur distant, vous pouvez sélectionner les pilotes à installer sur le système connecté.

8.4.4 Utilisation d'un chargeur distant 32 ou 64 bits sur le même ordinateur

Par défaut, le programme d'installation détecte la version du système d'exploitation, puis installe la version correspondante du chargeur distant. Vous pouvez installer le chargeur distant 32 et 64 bits sur un système d'exploitation 64 bits :

- Si vous mettez à niveau un chargeur distant 32 bits installé sur un système d'exploitation 64 bits, le processus met à niveau le chargeur distant 32 bits vers la dernière version et installe également le chargeur distant 64 bits.
- Si vous choisissez d'héberger les chargeurs distants 32 et 64 bits sur le même ordinateur, les événements d'audit sont générés uniquement avec le chargeur distant 64 bits. Si un chargeur distant 64 bits est installé avant un chargeur distant 32 bits, les événements sont consignés dans le fichier cache 32 bits.

8.4.5 Conditions préalables et considérations relatives à l'installation du chargeur distant

Avant d'installer le chargeur distant, NetIQ vous recommande de passer en revue les considérations suivantes :

- Vérifiez que le moteur Identity Manager est installé avant d'installer le chargeur distant.

  Si vous avez installé le chargeur distant sans installer le moteur Identity Manager, vous devez installer le module `novell-openssl-9.1.0-0.x86_64.rpm` avant de commencer la configuration du moteur Identity Manager.

  1. Accédez à l'emplacement suivant :

     `<emplacement_montage_Identity_Manager_4.7_Linux.iso>/IDM/packages/OpenSSL/x86_64/`

  2. Installez le module `novell-openssl-9.1.0-0.x86_64.rpm` à l'aide de la commande suivante :

     ```
     rpm -ivh novell-openssl-9.1.0-0.x86_64.rpm
     ```

- Installez le chargeur distant sur un serveur pouvant communiquer avec les systèmes gérés. Le pilote pour chaque système géré doit être disponible avec les API pertinentes.

- Vous pouvez installer le chargeur distant sur l'ordinateur sur lequel vous avez installé le moteur Identity Manager.
- Vous pouvez installer le chargeur distant versions 32 et 64 bits sur le même ordinateur.
- Vous pouvez installer le chargeur distant Java sur des plates-formes ne prenant pas en charge le chargeur distant natif. Pour plus d'informations sur les plates-formes prises en charge, reportez-vous à la Section 8.3.4, « Configuration système requise pour le moteur Identity Manager, le chargeur distant et iManager », page 65.
- NetIQ vous recommande, dans la mesure du possible, d'utiliser la configuration du chargeur distant avec vos pilotes. Utilisez le chargeur distant même dans les cas où le système connecté se trouve sur le même serveur que le moteur du serveur Identity Manager.

  Lorsque vous exécutez le module d'interface pilote dans la configuration du chargeur distant, vous bénéficiez des avantages suivants :

  - L'isolation de la mémoire et du traitement entre les modules d'interface pilote améliore les performances et la surveillance de la solution Identity Manager.
  - L'application de correctifs et la mise à niveau du module d'interface pilote n'affectent pas le coffre-fort d'identité ni les autres pilotes.
  - Le coffre-fort d'identité bénéficie d'une protection contre les erreurs fatales susceptibles de se produire dans le module d'interface pilote.
  - La charge des modules d'interface pilote est répartie sur d'autres serveurs.
- Les pilotes suivants prennent en charge les fonctionnalités du chargeur distant :
  - Access Review
  - ACF2
  - Azure Active Directory
  - Bannière
  - Blackboard
  - Service de collecte de données
  - Texte délimité
  - GoogleApps
  - REST
  - GroupWise 2014 (pour le chargeur distant 32 bits)
  - JDBC
  - JMS
  - LDAP
  - Paramètres Linux
  - Lotus Notes
  - Passerelle système gérée
  - Services de tâches manuelles
  - nuls et en boucle
  - Office 365
  - Oracle EBS HRMS
  - Oracle EBS TCA
  - Oracle EBS User Management
  - PeopleSoft 5.2

- Privileged User Management
- Remedy
- Salesforce.com
- SAP Business Logic
- Portail SAP
- SAP HR (non pris en charge avec le chargeur distant Java)
- SAP User Management (non pris en charge avec le chargeur distant Java)
- ServiceNow
- Module d'intégration 2.0 pour Sentinel
- SharePoint
- SOAP
- Top Secret
- WorkOrder

- Les pilotes suivants ne prennent pas en charge le chargeur distant :
  - Bidirectional eDirectory
  - eDirectory
  - Services de droits
  - Service de rôle
  - Application utilisateur

8.5 Planification de l'installation des applications d'identité

L'installation des applications d'identité comprend les composants suivants :

- Tableau de bord Identity Manager
- Interface d'administration d'Identity Manager
- Application utilisateur
- Pilote de service de rôle et de ressource
- Pilote d'application utilisateur

La section contient les informations suivantes :

8.5.1 Liste de contrôle de l'installation des applications d'identité

Avant d'entamer la procédure d'installation, NetIQ recommande de passer en revue les étapes suivantes :

	Éléments de la liste de contrôle
❑	1. Renseignez-vous sur les interactions entre les différents composants Identity Manager. Pour plus d'informations, reportez-vous au Section 4.3.1, « Application utilisateur et module de provisioning basé sur les rôles », page 27.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.7.4, « Configuration recommandée pour le serveur », page 40.
❑	3. Déterminez si vous devez installer Sentinel avant d'installer les applications d'identité. Pour plus d'informations, reportez-vous au Section 5.7, « Configuration de serveur et scénarios d'installation recommandés », page 39.
❑	4. Vérifiez que le moteur Identity Manager est installé. Pour plus d'informations sur l'installation du moteur, reportez-vous au Section 8.3.4, « Configuration système requise pour le moteur Identity Manager, le chargeur distant et iManager », page 65.
❑	5. Passez en revue les considérations concernant l'installation des applications d'identité et leur infrastructure sous-jacente, afin de garantir que vos serveurs répondent aux conditions requises. Pour plus d'informations, reportez-vous à la Section 8.5.2, « Conditions requises et considérations relatives à l'installation des applications d'identité », page 75.
❑	6. (Conditionnel) Pour les ordinateurs s'exécutant sous un système d'exploitation SLES 12 SP2 ou version ultérieure, assurez-vous d'avoir installé l'ensemble approprié de bibliothèques pour une installation interactive. Pour plus d'informations, reportez-vous au Section 5.9.3, « Installation d'Identity Manager sur des serveurs SLES 12 SP2 ou version ultérieure », page 45.
❑	7. (Conditionnel) Pour les ordinateurs s'exécutant sous un système d'exploitation RHEL 7.3. ou version ultérieure, assurez-vous d'avoir installé l'ensemble de bibliothèques approprié. Pour plus d'informations, reportez-vous au Section 5.9.4, « Installation d'Identity Manager sur des serveurs RHEL 7.3 ou version ultérieure », page 45.
❑	8. Vérifiez les conditions matérielles et logicielles requises pour les ordinateurs qui hébergent les applications d'identité et leur infrastructure. Pour plus d'informations, reportez-vous à la Section 8.5.3, « Configuration système requise pour les applications d'identité », page 83.
❑	9. Installez et configurez une base de données pour les applications d'identité sur l'ordinateur local ou un serveur connecté. ◆ Pour en savoir plus sur la base de données, reportez-vous à la « Conditions préalables à l'installation de la base de données pour les applications d'identité » page 78. ◆ Pour installer la base de données, reportez-vous au Chapitre , « Configuration de la base de données des applications d'identité », page 79.
❑	10. Installez les applications d'identité. Pour plus d'informations, reportez-vous à l'une des sections suivantes : ◆ Section 9.1.1, « Exécution d'une installation interactive », page 91 ◆ Section 9.1.2, « Exécution d'une installation silencieuse du moteur Identity Manager », page 92
❑	11. Pour effectuer les tâches finales de la procédure d'installation, reportez-vous au Chapitre 11, « Étapes finales pour terminer l'installation », page 109.

	Éléments de la liste de contrôle
❑	12. Assurez-vous d'avoir configuré correctement les applications d'identité et les paramètres d'authentification unique. Pour plus d'informations, reportez-vous au Chapitre 19, « Vérification de l'accès Single Sign-on pour les applications d'identité », page 211.
❑	13. (Facultatif) Pour commencer à utiliser les applications d'identité, reportez-vous au *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur des applications d'identité de NetIQ Identity Manager).

8.5.2 Conditions requises et considérations relatives à l'installation des applications d'identité

NetIQ vous recommande de consulter les conditions préalables et la configuration système requise pour les applications d'identité avant de lancer la procédure d'installation. Pour plus d'informations sur la configuration de l'environnement de l'application utilisateur, reportez-vous au NetIQ Identity Manager - User's Guide to the Identity Applications (Guide de l'utilisateur des applications d'identité de NetIQ Identity Manager).

Considérations relatives à l'installation des applications d'identité

Les considérations suivantes s'appliquent à l'installation des applications d'identité.

- Veillez à utiliser une version prise en charge des composants Identity Manager suivants :
  - Moteur Identity Manager
  - Chargeur distant
- (Facultatif) NetIQ vous recommande d'activer le protocole SSL (Secure Sockets Layer) pour la communication entre les composants Identity Manager. Pour utiliser le protocole SSL, vous devez activer SSL dans votre environnement et spécifier **https** lors de l'installation. Pour plus d'informations sur l'activation de SSL, reportez-vous à la section Configuring Security in the Identity Applications (Configuration de la sécurité des applications d'identité) du *NetIQ Analyzer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Analyzer pour Identity Manager).
- Vous ne pouvez pas utiliser le pilote du service de rôles et de ressources avec le chargeur distant étant donné que le pilote utilise jClient.

- Par défaut, le processus d'installation place les fichiers du programme dans le répertoire `/opt/netiq/idm`. Si vous envisagez d'installer l'application utilisateur à un emplacement autre que celui par défaut, le répertoire doit répondre aux conditions suivantes avant de lancer le processus d'installation :
  - Le répertoire existe et est accessible en écriture.
  - Le répertoire est accessible en écriture par les utilisateurs non-`root`.
- Chaque instance de l'application utilisateur ne peut traiter qu'un seul conteneur utilisateur. Par exemple, vous pouvez ajouter des utilisateurs qui ne peuvent effectuer des recherches et introduire des requêtes que pour le conteneur associé à l'instance. En outre, l'association d'un conteneur d'utilisateurs à une application est censée être permanente.
- (Facultatif) Pour récupérer des autorisations des systèmes gérés, installez un ou plusieurs pilotes Identity Manager.
  - Vous devez utiliser des pilotes pris en charge par Identity Manager 4.6 ou version ultérieure. Pour plus d'informations sur l'installation des pilotes, reportez-vous aux guides des pilotes appropriés sur le site Web de documentation des pilotes NetIQ Identity Manager.
  - Pour gérer les pilotes, vous devez avoir installé Designer ou les plug-ins appropriés d'iManager. Les plug-ins iManager sont fournis dans l'installation du moteur Identity Manager.

Considérations relatives à la configuration et à l'utilisation des applications d'identité

Les considérations suivantes s'appliquent à la configuration et à l'utilisation initiale des applications d'identité.

- Pour que les utilisateurs puissent accéder aux applications d'identité, vous devez effectuer les opérations suivantes :
  - Assurez-vous que tous les pilotes Identity Manager nécessaires sont installés.
  - Vérifiez que les index pour le coffre-fort d'identité sont en mode en ligne. Pour plus d'informations sur la configuration d'un index lors de l'installation, reportez-vous à la « Divers » page 152.
  - Activez les cookies dans tous les navigateurs. Les applications ne fonctionnent pas si les cookies sont désactivés.
- Au cours de l'installation, le programme d'installation écrit des fichiers journaux dans le répertoire d'installation. Ces fichiers contiennent des informations relatives à votre configuration. Une fois que vous avez configuré votre environnement d'applications d'identité, envisagez de supprimer ces fichiers journaux ou de les stocker à un emplacement sécurisé. Au cours de l'installation, vous avez la possibilité d'écrire le schéma de base de données dans un fichier. Étant donné que ce fichier contient des informations descriptives sur votre base de données, il est conseillé de le déplacer vers un emplacement sécurisé une fois la procédure d'installation terminée.
- (Conditionnel) Pour auditer les applications d'identité, Identity Reporting et un service d'audit doivent être installés dans votre environnement et configurés pour capturer les événements. Vous devez également configurer les applications d'identité à des fins d'audit.

Spécification de l'emplacement de l'index des autorisations

Lorsque vous installez les applications d'identité, le processus crée un index des autorisations pour Tomcat. Si vous ne spécifiez pas d'emplacement pour l'index, le programme d'installation crée un dossier dans un répertoire temporaire. Par exemple : `/opt/netiq/idm/apps/tomcat/temp/permindex` sous Tomcat.

Dans un environnement de test, l'emplacement n'est généralement pas important. Toutefois, dans un environnement de production ou de stockage, vous ne souhaitez peut-être pas placer l'index dans un répertoire temporaire.

Pour spécifier un emplacement pour l'index :

1. Arrêtez Tomcat.
2. Dans un éditeur de texte, ouvrez le fichier `ism-configuration.properties`.
3. À la fin du fichier, ajoutez le texte suivant :

   `com.netiq.idm.cis.indexdir = path/permindex`

   Exemple :

   `com.netiq.idm.cis.indexdir = /opt/netiq/idm/apps/tomcat/temp/permindex`
4. Enregistrez et fermez le fichier.
5. Supprimez le dossier `permindex` existant dans le répertoire temporaire.
6. Démarrez Tomcat.

Activation de l'index des autorisations pour la mise en grappe

Cette section explique comment activer l'index des autorisations pour la mise en grappe.

1. Connectez-vous à iManager sur le premier noeud de la grappe et sélectionnez **Afficher les objets**.
2. Sous **Système**, accédez à l'ensemble de pilotes contenant le **pilote d'application utilisateur**.
3. Sélectionnez **AppConfig** > **AppDefs** > **Configuration**.
4. Sélectionnez l'attribut XMLData et définissez la propriété `com.netiq.idm.cis.clustered` sur **true**.

   Par exemple :

   ```
   <property>
   <key>com.netiq.idm.cis.clustered</key>
   <value>true</value>
   </property>
   ```
5. Cliquez sur **OK**.

Conditions préalables à l'installation de la base de données pour les applications d'identité

La base de données stocke les informations de configuration et les données de l'application d'identité.

Avant d'installer l'instance de base de données, vérifiez que les conditions préalables suivantes sont remplies :

- Pour configurer une base de données à utiliser avec Tomcat, vous devez créer un pilote JDBC. Les applications d'identité utilisent des appels JDBC standard pour accéder à la base de données et la mettre à jour. Les applications d'identité utilisent un fichier de source de données JDBC liée à l'arborescence JNDI pour ouvrir une connexion à la base de données.
- Vous devez disposer d'un fichier de source de données qui pointe vers la base de données. Le programme d'installation de l'application utilisateur crée une entrée de source de données pour Tomcat dans les fichiers `server.xml` et `context.xml` qui pointe vers la base de données.
- Vérifiez que vous disposez des informations suivantes :
  - Hôte et port du serveur de base de données.
  - Nom de la base de données à créer. La base de données par défaut pour les applications d'identité est `idmuserappdb`.
  - Nom d'utilisateur et mot de passe de la base de données. Le nom d'utilisateur de la base de données doit représenter un compte d'administrateur ou disposer des autorisations suffisantes pour créer des tables sur le serveur de base de données. Par défaut, l'administrateur de l'application utilisateur est `idmadmin`.
  - Fichier de pilote `.jar` livré par le fournisseur de base de données pour la base utilisée. NetIQ ne prend pas en charge les fichiers JAR de pilote fournis par d'autres fournisseurs.
- L'instance de base de données peut être sur l'ordinateur local ou un serveur connecté.
- Le jeu de caractères de la base de données doit utiliser le codage Unicode. Ainsi, UTF-8 est un exemple de jeu de caractères employant ce codage, alors que Latin1 ne l'utilise pas. Pour plus d'informations sur la spécification du jeu de caractères, reportez-vous à la « Configuration du jeu de caractères » page 81 ou à la « Configuration d'une base de données Oracle » page 79.
- Pour éviter les erreurs de clés en double au cours de la migration, utilisez un classement sensible à la casse. Si le problème se pose, vérifiez le classement et corrigez-le, puis réinstallez les applications d'identité.
- (Conditionnel) Pour utiliser la même instance de base de données à des fins d'audit et pour les applications d'identité, NetIQ recommande d'installer la base de données sur un serveur dédié distinct du serveur qui héberge l'instance Tomcat qui exécute les applications.
- (Conditionnel) Si vous effectuez une migration vers une nouvelle version des applications d'identité, vous devez utiliser la même base de données que celle utilisée pour l'installation précédente.
- La mise en grappe de bases de données est une caractéristique propre à chaque serveur de base de données. NetIQ n'effectue officiellement pas de test avec les configurations de base de données en grappe, car la mise en grappe est indépendante de la fonctionnalité du produit. Par conséquent, nous prenons en charge les serveurs de base de données en grappe avec les mises en garde suivantes :
  - Par défaut, le nombre maximal de connexions est défini sur 100. Toutefois, cette valeur peut être insuffisante pour gérer la charge de requêtes de workflow dans une grappe. Le cas échéant, le message d'exception suivant peut s'afficher :

    ```
    (java.sql.SQLException: Data source rejected establishment of connection,
    message from server: "Too many connections."
    ```

Pour augmenter le nombre maximal de connexions, augmentez la valeur de la variable `max_connections` dans le fichier `my.cnf`.

- Certains aspects ou fonctionnalités de votre serveur de base de données en grappe devront peut-être être désactivés. Par exemple, la réplication transactionnelle doit être désactivée dans certaines tables en raison de violations de contraintes en cas de tentative d'insertion d'une clé dupliquée.
- Nous ne fournissons pas d'aide pour l'installation, la configuration ou l'optimisation de la base de données mise en grappe, y compris l'installation de nos produits dans un serveur de base de données en grappe.
- Nous mettons tout en oeuvre pour résoudre les éventuels problèmes qui pourraient survenir lors de l'utilisation de nos produits dans un environnement de base de données en grappe. Les méthodes de dépannage dans un environnement complexe nécessitent souvent un travail coopératif pour résoudre les problèmes. NetIQ fournit son savoir-faire en matière d'analyse, de planification et de dépannage pour les produits NetIQ. Le client doit quant à lui fournir une expertise d'analyse, de planification et de dépannage pour les produits tiers. Nous demandons aux clients de reproduire ou d'analyser le comportement des composants dans un environnement non mis en grappe pour mieux distinguer les éventuels problèmes liés à la configuration des grappes des problèmes liés aux produits NetIQ.

Configuration de la base de données des applications d'identité

La base de données des applications d'identité traite des tâches telles que le stockage des données de configuration et des données relatives aux activités de workflow. Avant de pouvoir installer les applications, la base de données doit être installée et configurée. Pour plus d'informations sur les bases de données compatibles, reportez-vous à la « Configuration système requise pour les applications d'identité » page 83. Pour plus d'informations sur les considérations concernant la base de données de l'application utilisateur, reportez-vous à la « Conditions préalables à l'installation de la base de données pour les applications d'identité » page 78.

Configuration d'une base de données Oracle

Cette section fournit des options de configuration afin d'utiliser une base de données Oracle pour l'application utilisateur. Pour plus d'informations sur les versions d'Oracle prises en charge, reportez-vous à la « Configuration système requise pour les applications d'identité » page 83.

Vérification du niveau de compatibilité des bases de données

Différentes versions de bases de données Oracle sont compatibles si elles prennent en charge les mêmes fonctionnalités et que ces fonctionnalités s'exécutent de la même façon. Si elles ne sont pas compatibles, certaines fonctionnalités ou opérations risquent de ne pas fonctionner comme prévu. Par exemple, la création du schéma peut échouer, empêchant le déploiement des applications d'identité.

Pour vérifier le niveau de compatibilité de votre base de données, procédez comme suit :

1. Connectez-vous au moteur de base de données.
2. Une fois connecté à l'instance appropriée du moteur de base de données SQL Server, cliquez sur le nom de serveur dans l'**explorateur d'objets**.
3. Développez **Bases de données** et, en fonction de la base de données, sélectionnez une base de données utilisateur ou développez **Bases de données système** et sélectionnez une base de données système.

4. Cliquez avec le bouton droit de la souris sur la base de données, puis cliquez sur **Propriétés**.

   La boîte de dialogue **Propriétés de base de données** s'affiche.

5. Dans le volet **Sélectionner une page**, cliquez sur **Options**.

   Le niveau de compatibilité actuel s'affiche dans la zone de liste **Niveau de compatibilité**.

6. Pour vérifier le **niveau de compatibilité**, entrez les informations ci-après dans la fenêtre de requête, puis cliquez sur **Exécuter**.

   ```
   SQL> SELECT name, value FROM v$parameter
   WHERE name = 'compatible';
   ```

Le résultat attendu est 12.1.0.2.

Configuration du jeu de caractères

La base de données de votre application utilisateur doit utiliser un jeu de caractères basé sur le codage Unicode. Lors de la création de la base de données, utilisez AL32UTF8 pour le spécifier.

Pour confirmer que la base de données Oracle 12c est configurée pour UTF-8 12c, exécutez la commande suivante :

```
select * from nls_database_parameters;
```

Si la base de données n'est pas configurée pour UTF-8, le système répond par les informations suivantes :

```
NLS_CHARACTERSET
WE8MSWIN1252
```

Sinon, le système répond par les informations suivantes, qui confirment que la base de données est configurée pour UTF-8 :

```
NLS_CHARACTERSET
AL32UTF8
```

Pour plus d'informations sur la configuration d'un jeu de caractères, reportez-vous à la documentation « Choosing an Oracle Database Character Set » (Choix d'un jeu de caractères pour une base de données Oracle).

Configuration du compte administrateur

L'application utilisateur requiert que le compte utilisateur de la base de données Oracle dispose de privilèges spécifiques. Dans l'utilitaire SQL Plus, entrez les commandes suivantes :

```
CREATE USER idmuser IDENTIFIED BY password
GRANT CONNECT, RESOURCE to idmuser
ALTER USER idmuser quota 100M on USERS;
```

où *idmuser* représente le compte utilisateur.

Configuration d'une base de données SQL Server

Cette section fournit des options de configuration afin d'utiliser une base de données SQL Server pour l'application utilisateur. Pour plus d'informations sur les versions de SQL Server prises en charge, reportez-vous à la « Configuration système requise pour les applications d'identité » page 83.

Configuration du jeu de caractères

SQL Server ne permet pas de sélectionner le jeu de caractères des bases de données. L'application utilisateur stocke les données de caractères SQL Server dans un type de colonne NCHAR, qui prend en charge le codage UTF-8.

Configuration du compte administrateur

Après l'installation de Microsoft SQL Server, créez une base de données et son utilisateur à l'aide d'une application telle que SQL Server Management Studio. Le compte utilisateur de la base de données doit disposer des privilèges suivants :

- `CREATE TABLE`
- `DELETE`
- `INSERT`
- `SELECT`
- `UPDATE`

REMARQUE : il est recommandé d'utiliser la version JAR de JDBC`sqljdbc42.jar`.

Conditions préalables à l'installation des applications d'identité dans un environnement de grappe

Vous pouvez installer la base de données des applications d'identité dans un environnement pris en charge par les grappes Tomcat, en tenant compte des considérations suivantes :

- La grappe doit porter un nom de partition de grappe, une adresse de multidiffusion et un port de multidiffusion uniques. L'utilisation d'identifiants uniques permet de séparer plusieurs grappes pour éviter les problèmes de performances et les comportements anormaux.
  - Pour chaque membre de la grappe, vous devez indiquer le même numéro de port d'écoute pour la base de données des applications d'identité.
  - Pour chaque membre de la grappe, vous devez indiquer le même nom d'hôte ou l'adresse IP du serveur qui héberge la base de données des applications d'identité.
- Vous devez synchroniser les horloges des serveurs de la grappe. Si les horloges des serveurs ne sont pas synchronisées, les sessions peuvent expirer prématurément et entraver le basculement correct de session HTTP.
- NetIQ recommande de ne pas utiliser d'identifiants multiples dans les onglets ou les sessions de navigateur sur le même hôte. Certains navigateurs partagent des cookies dans les onglets et les processus ; dès lors, l'utilisation de plusieurs identifiants risque de causer des problèmes de basculement de session HTTP (outre le risque d'erreur d'authentification inattendue si plusieurs utilisateurs partagent le même ordinateur).
- Les noeuds de la grappe résident sur le même sous-réseau.
- Un proxy de basculement ou une solution d'équilibrage de charge est installé sur un ordinateur distinct.

Préparation d'une grappe pour les applications d'identité

Les applications d'identité prennent en charge la réplication de session HTTP et le basculement de session. Si une session est en cours sur un noeud et qu'une défaillance survient au niveau de ce noeud, un autre serveur de la grappe peut reprendre la session sans intervention. Avant d'installer les applications d'identité dans une grappe, vous devez préparer l'environnement.

- « Présentation des groupes de grappes dans les environnements Tomcat » page 82
- « Configuration des propriétés système pour les ID de moteur de workflow » page 82
- « Utilisation de la même clé principale pour chaque application utilisateur dans la grappe » page 83

Présentation des groupes de grappes dans les environnements Tomcat

Le groupe de grappes de l'application utilisateur emploie un nom UUID pour réduire le risque de conflit avec d'autres groupes de grappes que les utilisateurs peuvent ajouter à leurs serveurs. Vous pouvez modifier les paramètres de configuration du groupe de grappes de l'application utilisateur à l'aide des fonctions d'administration de l'application utilisateur. Les modifications apportées à la configuration de la grappe ne prennent effet pour un noeud de serveur qu'après redémarrage de ce noeud.

Pour plus d'informations sur les conditions requises pour l'installation dans un environnement de grappe, reportez-vous à la Section 8.5.2, « Conditions requises et considérations relatives à l'installation des applications d'identité », page 75.

Configuration des propriétés système pour les ID de moteur de workflow

Chaque serveur qui héberge les applications d'identité dans la grappe peut exécuter un moteur de workflow. Pour garantir les performances de la grappe et du moteur de workflow, chaque serveur de la grappe doit utiliser les mêmes nom de partition et groupe de partition UDP. Par ailleurs, chaque serveur de la grappe doit être démarré avec un ID unique pour le moteur de workflow, car la mise en grappe pour le moteur de workflow fonctionne indépendamment de l'infrastructure de cache des applications d'identité.

Pour vous assurer que les moteurs de workflow s'exécutent correctement, vous devez définir des propriétés système pour Tomcat.

1. Créez une nouvelle propriété système JVM pour chaque serveur d'applications d'identité de la grappe.
2. Nom de la propriété système `com.novell.afw.wf.`*`engine-id`* où l'ID de moteur est une valeur unique.

Utilisation de la même clé principale pour chaque application utilisateur dans la grappe

Les applications d'identité codent les données sensibles à l'aide d'une clé principale. Toutes les applications d'identité d'une grappe doivent utiliser la même clé principale. Cette section vous permet de vérifier que toutes les applications d'identité d'une grappe utilisent la même clé principale.

Pour plus d'informations sur le chiffrement des données sensibles dans les applications d'identité, reportez-vous à la section Encrypting Sensitive Identity Applications Data (Chiffrement des données sensibles des applications d'identité) du *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager - Guide de l'administrateur des applications d'identité).

1. Installez l'application utilisateur sur le premier noeud de la grappe.
2. Dans la fenêtre Sécurité - Clé principale du programme d'installation, notez l'emplacement du fichier `master-key.txt` qui contient la nouvelle clé principale pour les applications d'identité. Par défaut, le fichier se trouve dans le répertoire d'installation.
3. Installez les applications d'identité sur les autres noeuds de la grappe.
4. Dans la fenêtre Sécurité - Clé principale, cliquez sur **Oui**, puis sur **Suivant**.
5. Dans la fenêtre Importer la clé principale, copiez la clé principale du fichier texte créée à l'Étape 2.

8.5.3 Configuration système requise pour les applications d'identité

Cette section fournit la configuration minimale requise pour le ou les serveurs sur lesquels vous souhaitez installer les applications d'identité et leur structure sous-jacente qui comprend PostgreSQL, Tomcat, OSP et SSPR.

Catégorie	Configuration requise
Processeur	1 GHz
Espace disque	1 Go **REMARQUE :** suffisamment d'espace pour le contenu des applications sous-jacentes, telles que la base de données et les journaux du serveur d'applications.
Mémoire	512 Mo (4 Go recommandé)
Système d'exploitation (certifié)	L'un des systèmes d'exploitation 64 bits suivants : ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3 Avant d'installer Identity Manager, NetIQ recommande d'appliquer les derniers correctifs du système d'exploitation en fonction de la fonctionnalité de mise à jour automatisée du fabricant. **REMARQUE :** *Certifié* signifie que le système d'exploitation a été entièrement testé et est pris en charge.

Catégorie	Configuration requise
Systèmes d'exploitation (pris en charge)	Dernières versions des Service Packs pour les systèmes d'exploitation certifiés **REMARQUE :** *Pris en charge* signifie que le système d'exploitation n'a pas encore été testé, mais qu'il devrait fonctionner.
Système de virtualisation	◆ Hyper-V Server 2012 R2 ◆ VMware ESX 5.5 et versions ultérieures NetIQ prend en charge Identity Manager sur les systèmes de virtualisation d'entreprise qui sont officiellement compatibles avec les systèmes d'exploitation sur lesquels les produits NetIQ s'exécutent. Aussi longtemps que les fournisseurs de systèmes de virtualisation prennent officiellement en charge ces systèmes d'exploitation, NetIQ prend en charge l'intégralité des composants Identity Manager qui y sont installés.
Base de données	◆ PostgreSQL 9.6.6 ◆ Oracle 12c ◆ MsSQL 2016 **REMARQUE :** n'incluez pas de versions PostgreSQL (par exemple 9.6.6) dans le chemin de classe de Tomcat. Les images de la page d'accueil peuvent ne pas se charger si ces versions sont spécifiées.
Serveur d'applications	Apache Tomcat 8.5.27
Java	Kit de développement Java (JDK) ou Version 1.8.0_162 ou ultérieure de JRE (Java Runtime Environment) de Sun (Oracle)
Port	8180
Navigateur Web	Un des navigateurs suivants (versions minimales) : ◆ Apple Safari 9 ◆ Google Chrome 61 ou version ultérieure ◆ Microsoft Edge 20.10240.17146.0 ◆ Microsoft Internet Explorer 11.0.10240.17443 **REMARQUE :** l'option d'affichage de la compatibilité n'est pas prise en charge dans le navigateur Internet Explorer. ◆ Mozilla FireFox 51 ou version ultérieure **REMARQUE :** les cookies du navigateur doivent être activés. Si les cookies sont désactivés, le produit ne peut pas fonctionner.
Audit	Agent de plate-forme 2011.1r6 (au minimum)
Services Annuaire	NetIQ eDirectory 9.1

8.6 Planification de l'installation du module Identity Reporting

Cette section fournit des recommandations concernant la préparation à effectuer en vue d'installer les composants du module Identity Reporting. Vous pouvez utiliser Sentinel pour auditer des événements.

- Section 8.6.1, « Liste de contrôle pour l'installation du module Identity Reporting », page 85
- Section 8.6.2, « Conditions préalables à l'installation des composants du module Identity Reporting », page 86
- Section 8.6.3, « Présentation de la procédure d'installation des composants du module Identity Reporting », page 87
- Section 8.6.4, « Configuration système requise pour Identity Reporting », page 88

8.6.1 Liste de contrôle pour l'installation du module Identity Reporting

NetIQ vous recommande de suivre les étapes de la liste de contrôle suivante :

	Éléments de la liste de contrôle
❑	1. Renseignez-vous sur les interactions entre les différents composants Identity Manager. Pour plus d'informations, reportez-vous au Section 3.3.4, « Identity Reporting », page 23.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.7, « Configuration de serveur et scénarios d'installation recommandés », page 39.
❑	3. Prenez en compte les considérations relatives à l'installation d'Identity Reporting. Pour plus d'informations, reportez-vous à la Section 8.6.2, « Conditions préalables à l'installation des composants du module Identity Reporting », page 86.
❑	4. Vérifiez les configurations matérielle et logicielle requises pour les ordinateurs qui hébergeront Identity Reporting. Pour plus d'informations, reportez-vous à la Section 8.6.4, « Configuration système requise pour Identity Reporting », page 88.
❑	5. (Conditionnel) Pour les ordinateurs s'exécutant sous un système d'exploitation RHEL 7.3. ou version ultérieure, assurez-vous d'avoir installé l'ensemble de bibliothèques approprié.
❑	6. (Conditionnel) Vérifiez l'installation des applications d'identité. Cette étape est nécessaire si vous avez installé la version Advanced Edition. Pour plus d'informations, reportez-vous au Chapitre 8, « Planification de l'installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting », page 61.
❑	7. Installez Sentinel. Pour plus d'informations, reportez-vous à la Section 7, « Installation de SLM for IGA », page 55
❑	8. Installez Identity Reporting. Pour plus d'informations, reportez-vous à l'une des sections suivantes : ◆ Section 9.1.1, « Exécution d'une installation interactive », page 91 ◆ Section 9.1.2, « Exécution d'une installation silencieuse du moteur Identity Manager », page 92
❑	9. Terminez la configuration d'Identity Reporting. Pour plus d'informations, reportez-vous au Chapitre 11.10, « Configuration d'Identity Reporting », page 176.

	Éléments de la liste de contrôle
❑	10. Configurez l'environnement pour les pilotes. Pour plus d'informations, reportez-vous à la Section 11.9, « Configuration de l'environnement d'exécution », page 167.

8.6.2 Conditions préalables à l'installation des composants du module Identity Reporting

Avant d'entamer la procédure d'installation, NetIQ vous invite à passer en revue les informations suivantes.

- « Conditions préalables requises pour Identity Reporting » page 86
- « Identification des événements d'audit pour Identity Reporting » page 86

Conditions préalables requises pour Identity Reporting

Lors de l'installation d'Identity Reporting, tenez compte des conditions préalables requises et considérations suivantes :

- Vérifiez la version prise en charge et configurée des composants Identity Manager suivants :
  - Applications d'identité, y compris le pilote d'application utilisateur (applicable uniquement pour la version Advanced Edition)
  - Sentinel installé sur un ordinateur Linux distinct.
- N'installez pas Identity Reporting sur un serveur appartenant à un environnement de grappes.
- Pour exécuter des rapports à partir d'une base de données Oracle, vous devez vous assurer que vous avez copié le fichier `ojdbc8.jar`. Pour plus d'informations, reportez-vous à la Section 11.10.2, « Génération de rapports à partir d'une base de données Oracle », page 176.
- Assignez le rôle Administrateur de rapports à tous les utilisateurs auxquels vous voulez accorder l'accès à la fonctionnalité de création de rapports.
- Vérifiez que l'heure de tous les serveurs de votre environnement Identity Manager est synchronisée. Si vous ne synchronisez pas l'heure sur vos serveurs, il est possible que, parmi les rapports que vous créez, certains soient vides. Par exemple, ce problème peut affecter les données relatives aux nouveaux utilisateurs lorsque les serveurs hébergeant le moteur d'Identity Manager et l'entrepôt indiquent un tampon horaire différent. Si vous créez un utilisateur puis que vous le modifiez, les données correspondantes figurent sur les rapports.
- La procédure d'installation modifie les entrées `JAVA_OPTs` ou `CATALINA_OPTS` du mappage JRE dans le fichier `setenv.sh` pour Tomcat.

Identification des événements d'audit pour Identity Reporting

Cette section fournit des informations sur la façon d'identifier les différents événements d'audit requis pour les rapports personnalisés et les rapports Identity Manager. Vous pouvez décompresser toutes les sources de rapport et exécuter le script suivant pour identifier les événements d'audit :

```
find . -name *.jrxml -print0 |xargs -0 grep -H "'000[B3]" | perl -ne '($file) = /
^\.\/(.*?)\//;@a = /000[3B]..../g; foreach $a (@a) { print "$file;$a\n"}' |sort -u
```

La section suivante fournit des informations sur la façon d'identifier et de sélectionner divers événements d'audit pour les rapports Identity Manager et les rapports s :

Nom de l'événement	Drapeau d'audit
Authentification et changement de mot de passe	**Sélection d'un drapeau d'audit à l'aide de SSPR :** lancez **SSPR Configuration Editor** (Éditeur de configuration SSPR) **Audit Configuration** (Configuration de l'audit) > Sélectionnez l'un des drapeaux d'audit suivants : ◆ Authenticate (Authentification) ◆ Change Password (Changer le mot de passe) ◆ Unlock Password (Déverrouiller le mot de passe) ◆ Recover Password (Récupérer le mot de passe) ◆ Intruder Attempt (Tentative d'intrusion) ◆ Intruder Lock (Verrouillage en cas d'intrusion) ◆ Intruder Lock User (Utilisateur du verrouillage en cas d'intrusion) **Sélection d'un drapeau d'Audit à l'aide d'iManager :** accédez à **Rôles et tâches dans iManager** > **Audit eDirectory** > **Configuration de l'audit** > **Novell Audit** > Sélectionnez l'un des drapeaux d'audit suivants : ◆ Change Password (Changer le mot de passe) ◆ Vérifier le mot de passe ◆ Connexion ◆ Logout
Tous les autres événements de création de rapports	Accédez à l'**application utilisateur NetIQ Identity Manager** > **Administration** > **Consignation** > **Activer le service d'audit**

8.6.3 Présentation de la procédure d'installation des composants du module Identity Reporting

NetIQ recommande d'installer Sentinel et Identity Reporting sur des serveurs distincts.

S'il s'agit d'une nouvelle installation, le programme d'installation crée des tables dans la base de données et vérifie la connectivité. Le programme installe également un fichier JAR pour le pilote JDBC PostgreSQL et utilise automatiquement ce fichier pour établir la connectivité à la base de données.

Si vous avez migré vos données, par exemple, SIEM, d'une base de données EAS vers une base de données PostgreSQL, le programme d'installation se connecte à la base de données existante.

Le programme d'installation d'Identity Reporting effectue les opérations suivantes :

- Configuration des services d'authentification pour Identity Reporting
- Configuration du système de messagerie électronique pour Identity Reporting
- Configuration des principaux services de création de rapports pour Identity Reporting
- Déploiement des pilotes, de la passerelle système gérée et des services de collecte de données requis pour qu'Identity Reporting puisse fonctionner
- Configuration de la base de données PostgreSQL pour Identity Reporting

8.6.4 Configuration système requise pour Identity Reporting

Cette section décrit la configuration minimale requise pour le ou les serveurs sur lesquels vous souhaitez installer Identity Reporting.

Veuillez également passer en revue les conditions préalables requises et les considérations relatives à l'installation, en particulier celles liées au système d'exploitation.

Catégorie	Configuration requise
Processeur	1 GHz
Espace disque	1 Go **REMARQUE :** suffisamment d'espace pour le contenu des applications sous-jacentes, telles que la base de données et les journaux du serveur d'applications.
Mémoire	512 Mo (4 Go recommandé)
Système d'exploitation (certifié)	L'un des systèmes d'exploitation 64 bits suivants : ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3 Avant d'installer Identity Manager, NetIQ recommande d'appliquer les derniers correctifs du système d'exploitation en fonction de la fonctionnalité de mise à jour automatisée du fabricant. **REMARQUE :** *Certifié* signifie que le système d'exploitation a été entièrement testé et est pris en charge.
Systèmes d'exploitation (pris en charge)	Dernières versions des Service Packs pour les systèmes d'exploitation certifiés **REMARQUE :** *Pris en charge* signifie que le système d'exploitation n'a pas encore été testé, mais qu'il devrait fonctionner.
Système de virtualisation	◆ Hyper-V Server 2012 R2 ◆ VMware ESX 5.5 et versions ultérieures NetIQ prend en charge Identity Manager sur les systèmes de virtualisation d'entreprise qui sont officiellement compatibles avec les systèmes d'exploitation sur lesquels les produits NetIQ s'exécutent. Aussi longtemps que les fournisseurs de systèmes de virtualisation prennent officiellement en charge ces systèmes d'exploitation, NetIQ prend en charge l'intégralité des composants Identity Manager qui y sont installés.
Base de données	◆ PostgreSQL 9.6.6 ◆ Oracle12.2.01
Serveur d'applications	Apache Tomcat 8.5.27

Catégorie	Configuration requise
Java	Kit de développement Java (JDK) ou Version 1.8.0_162 ou ultérieure de JRE (Java Runtime Environment) de Sun (Oracle)
Navigateur Web	Un des navigateurs suivants (versions minimales) : **Desktop** ◆ Apple Safari 9 ◆ Google Chrome 61 ou version ultérieure ◆ Microsoft Internet Explorer 11 ◆ Mozilla FireFox 51 ou version ultérieure **iPad** ◆ Apple Safari 9 ◆ Google Chrome 61 ou version ultérieure **REMARQUE :** les cookies du navigateur doivent être activés. Si les cookies sont désactivés, le produit ne peut pas fonctionner.
Audit	Sentinel Log Management for IGA

9 Installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting

Cette section vous guide tout au long du processus d'installation des composants requis pour les composants Moteur Identity Manager, Applications d'identité et Identity Reporting.

Vous pouvez les installer selon un mode interactif ou silencieux. Le programme d'installation fournit une option permettant de créer un fichier de propriétés silencieux. Vous pouvez enregistrer les options d'installation de plusieurs composants dans le fichier de propriétés et ensuite utiliser celui-ci pour exécuter l'installation silencieuse sur différents serveurs de votre environnement. Le programme d'installation en mode silencieux lit les valeurs du fichier pour effectuer l'installation.

Vous pouvez configurer les composants Identity Manager immédiatement après l'installation ou ultérieurement.

Le programme d'installation installe les composants aux emplacements prédéfinis décrits à la Section 5.5, « Emplacements d'installation par défaut », page 37.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous au Chapitre 8, « Planification de l'installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting », page 61.

9.1 Installation du moteur Identity Manager

Le moteur Identity Manager peut être installé à l'aide des méthodes suivantes :

- Section 9.1.1, « Exécution d'une installation interactive », page 91
- Section 9.1.2, « Exécution d'une installation silencieuse du moteur Identity Manager », page 92
- Section 9.1.3, « Installation du moteur Identity Manager en tant qu'utilisateur non-root », page 92

9.1.1 Exécution d'une installation interactive

1. Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.
2. Montez le fichier `.iso` téléchargé.
3. À partir du répertoire racine du fichier `.iso`, exécutez la commande suivante :

   ```
   ./install.sh
   ```
4. Lisez le contrat de licence.
5. Entrez o pour accepter l'accord de licence.
6. Indiquez l'édition de serveur Identity Manager que vous souhaitez installer. Entrez y pour Advanced Edition et n pour Standard Edition.

7 Sélectionnez le moteur Identity Manager et poursuivez l'installation.

8 Configurez les composants installés. Pour plus d'informations, reportez-vous au Chapitre 10, « Configuration des composants installés », page 101.

9.1.2 Exécution d'une installation silencieuse du moteur Identity Manager

1 Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.

2 Montez le fichier `.iso` téléchargé.

3 À partir du répertoire racine du fichier `.iso`, exécutez la commande suivante :

```
./create_silent_props.sh
```

4 Entrez `y` pour confirmer la création du fichier.

5 Pour installer JRE, entrez `y`.

6 Pour mettre à niveau les composants Identity Manager existants, entrez `y`.

7 Indiquez l'édition de serveur Identity Manager que vous souhaitez installer. Entrez `y` pour Advanced Edition et `n` pour Standard Edition.

8 Sélectionnez un mode de configuration des composants. Pour plus d'informations, reportez-vous à la Chapitre 10, « Configuration des composants installés », page 101.

9 Spécifiez les composants à installer.

10 Exécutez la commande suivante pour effectuer une installation silencieuse :

```
./install.sh -s -f <emplacement_fichier_propriétés_silencieux>
```

Exemples :

`./install.sh -s -f /mnt/silent.properties`, où `/mnt/silent.properties` correspond à l'emplacement où vous avez enregistré le fichier de propriétés silencieux.

9.1.3 Installation du moteur Identity Manager en tant qu'utilisateur non-root

Vous pouvez installer le moteur Identity Manager en tant qu'utilisateur non-`root` afin d'améliorer la sécurité de votre serveur Linux. Vous ne pouvez pas installer le moteur Identity Manager en tant qu'utilisateur non-`root` si vous avez installé le coffre-fort d'identité en tant que `root`. Vous devez effectuer les étapes suivantes si vous souhaitez installer le moteur en tant qu'utilisateur non-root :

1. Vérifiez que NICI est installé. Pour plus d'informations, reportez-vous à la « Installation de l’infrastructure NICI » page 93.
2. Effectuez une installation non-root du coffre-fort d'identité. Pour plus d'informations, reportez-vous à la « Exécution d'une installation non-root du coffre-fort d'identité » page 93.
3. Effectuez une installation non-root du moteur Identity Manager. Pour plus d'informations, reportez-vous à la « Exécution d'une installation non-root du moteur » page 94.

Installation de l’infrastructure NICI

Vous devez installer NICI avant de procéder à l'installation du coffre-fort d'identité. Étant donné que les paquetages NICI requis sont utilisés sur l'ensemble du système, il est recommandé d'installer les paquetages nécessaires en tant qu'utilisateur root. Si nécessaire, vous pouvez toutefois déléguer l'accès à un autre compte à l'aide de `sudo` et utiliser ce compte pour installer les paquetages NICI.

1. À partir de l'image `iso` que vous avez montée, accédez au répertoire `/IDVault/setup/`.
2. Exécutez la commande suivante :

   ```
   rpm -ivh nici64-3.1.0-0.00.x86_64.rpm
   ```
3. Vérifiez que NICI est défini en mode serveur. Saisissez la commande suivante :

   ```
   /var/opt/novell/nici/set_server_mode
   ```

   Il s'agit d'une étape obligatoire pour s'assurer que la configuration du coffre-fort d'identité n'échoue pas.

Exécution d'une installation non-root du coffre-fort d'identité

Cette section décrit comment utiliser le fichier Tarball pour installer le coffre-fort d'identité. Lorsque vous extrayez le fichier, le système crée les répertoires `etc`, `opt` et `var`.

1. Connectez-vous sous l'identité d'un utilisateur `sudo` disposant des droits nécessaires sur l'ordinateur sur lequel vous souhaitez installer le coffre-fort d'identité.

   REMARQUE : vous pouvez aussi vous connecter en tant qu'utilisateur `root` si vous souhaitez spécifier un chemin d'installation personnalisé.

   ---
2. À partir de l'image `iso` que vous avez montée, accédez au répertoire `/IDVault/`.
3. Créez un répertoire et copiez-y le fichier `eDir_NonRoot.tar.gz`. Par exemple, /home/user/install/eDirectory.
4. Utilisez la commande suivante pour extraire le fichier :

   ```
   tar -zxvf eDir_NonRoot.tar.gz
   ```
5. (Conditionnel) Pour exporter manuellement les chemins des variables d'environnement, entrez la commande suivante :

   ```
   export LD_LIBRARY_PATH=custom_location/eDirectory/opt/novell/eDirectory/
   lib64:custom_location/eDirectory/opt/novell/eDirectory/lib64/ndsmodules:
   custom_location/eDirectory/opt/novell/lib64:$LD_LIBRARY_PATH

   export PATH=custom_location/eDirectory/opt/novell/eDirectory/
   bin:custom_location/eDirectory/opt/novell/eDirectory/sbin:/opt/novell/
   eDirectory/bin:$PATH

   export MANPATH=custom_location/eDirectory/opt/novell/man:custom_location/
   eDirectory/opt/novell/eDirectory/man:$MANPATH

   export TEXTDOMAINDIR=custom_location/eDirectory/opt/novell/eDirectory/
   share/locale:$TEXTDOMAINDIR
   ```
6. (Conditionnel) Pour utiliser le script ndspath afin d'exporter les chemins des variables d'environnement, vous devez ajouter le script ndspath devant l'utilitaire. Procédez comme suit :

   6a À partir du répertoire `emplacement_personnalisé/eDirectory/opt`, exécutez l'utilitaire à l'aide de la commande suivante :

custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath *utility_name_with_parameters*

6b Exportez les chemins dans le shell actuel à l'aide de la commande suivante :

```
. custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath
```

6c Exécutez les utilitaires normalement.

6d Ajoutez les instructions d'exportation du chemin à la fin du script `/etc/profile`, `~/bashrc` ou autre script similaire.

Cette étape vous permet de démarrer les utilitaires directement lorsque vous vous connectez ou ouvrez un nouveau shell.

7 Pour configurer le coffre-fort d'identité, effectuez l'une des opérations suivantes :

7a Pour exécuter l'utilitaire ndsconfig, saisissez le texte suivant dans la ligne de commande :

```
ndsconfig new [-t treename] [-n server_context] [-a admin_FDN] [-w
admin password] [-i] [-S server_name] [-d path_for_dib] [-m module] [e] [-L
ldap_port] [-l SSL_port] [-o http_port] -O https_port] [-p IP
address:[port]] [-c] [-b port_to_bind] [-B interface1@port1,
interface2@port2,..] [-D custom_location] [--config-file
configuration_file]
```

Par exemple :

```
ndsconfig new -t mary-tree -n novell -a admin.novell -S linux1 -d /home/
mary/inst1/data -b 1025 -L 1026 -l 1027 -o 1028 -O 1029 -D /home/mary/
inst1/var --config-file /home/mary/inst1/nds.conf
```

REMARQUE

- Vous devez spécifier des numéros de port compris entre 1024 et 65535. Par conséquent, le port par défaut 524 ne peut pas être utilisé pour des applications eDirectory.

  Cette restriction relative à la spécification des numéros de port peut avoir une incidence négative sur les types d'applications suivants :

  - applications ne permettant pas de spécifier le port du serveur cible ;
  - anciennes applications qui utilisent NCP et s'exécutent en tant que root pour le port 524.
- Vous pouvez spécifier des adresses IPv6 dans les options `-B` et `-P`. Pour spécifier une adresse IPv6, vous devez mettre l'adresse entre crochets `[ ]`, par exemple, `-B [2015::4]@636`.

7b Utilisez l'utilitaire ndsmanage pour configurer une nouvelle instance. Pour plus d'informations, reportez-vous à la « Création d'une instance dans le coffre-fort d'identité » page 117.

Exécution d'une installation non-root du moteur

Lorsque vous utilisez cette méthode, vous ne pouvez pas installer les composants suivants :

- **Chargeur distant :** pour installer le chargeur distant en tant qu'utilisateur non-root, utilisez le chargeur distant Java. Pour plus d'informations, reportez-vous à la « Installation du chargeur distant Java » page 95.
- **Pilote de compte Linux :** nécessite des privilèges `root` pour fonctionner.

REMARQUE : lorsque vous installez le moteur Identity Manager en tant qu'utilisateur non-root, les fichiers d'installation sont situés sous le répertoire des utilisateurs non-root. Par exemple : `/home/utilisateur`, où utilisateur est non-root). Les fichiers d'installation ne sont pas nécessaires pour exécuter Identity Manager. Vous pouvez les supprimer une fois l'installation terminée.

Pour installer le moteur Identity Manager en tant qu'utilisateur non-root :

1. Connectez-vous à l'aide du compte utilisateur non-root employé pour installer le coffre-fort d'identité.

   Le compte utilisateur doit disposer d'un accès en écriture aux répertoires et aux fichiers d'installation non-root du coffre-fort d'identité.
2. Accédez à l'emplacement où vous avez monté le fichier `Identity_Manager_4.7_Linux.iso`.
3. À partir de l'emplacement de montage, accédez au répertoire `/IDM`.
4. Exécutez la commande suivante :

   ```
   ./idm-nonroot-install.sh
   ```
5. Les informations suivantes permettent de terminer l'installation :

   Répertoire de base de l'installation non-root d'eDirectory

   Indiquez le répertoire dans lequel se trouve l'installation non-`root` d'eDirectory. Par exemple, `/home/user/install/eDirectory`.

   Extension du schéma eDirectory

   S'il s'agit du premier serveur Identity Manager installé dans cette instance d'eDirectory, entrez `Y` pour étendre le schéma. Si le schéma n'est pas étendu, Identity Manager ne fonctionne pas.

   Vous êtes invité à étendre le schéma de chaque instance d'eDirectory appartenant à l'utilisateur non-`root` hébergée par l'installation non-`root` d'eDirectory.

   Si vous choisissez d'étendre le schéma, indiquez le nom distinctif (DN) complet de l'utilisateur eDirectory qui dispose des droits nécessaires pour étendre le schéma. Pour pouvoir étendre le schéma, l'utilisateur doit disposer du droit Superviseur sur l'ensemble de l'arborescence. Pour plus d'informations sur l'extension du schéma en tant qu'utilisateur non-`root`, reportez-vous au fichier `schema.log` situé dans le répertoire `data` de chaque instance d'eDirectory.

   Exécutez le programme `/opt/novell/eDirectory/bin/idm-install-schema` pour étendre le schéma sur d'autres instances d'eDirectory une fois l'installation terminée.
6. Pour terminer le processus d'installation, passez à la Section 11.1, « Exécution d'une installation en tant qu'utilisateur non-root », page 109.
7. Activez Identity Manager. Pour plus d'informations, reportez-vous à la Chapitre 24, « Activation d'Identity Manager », page 245.
8. Pour créer et configurer vos objets Pilote, consultez le guide spécifique à celui-ci. Pour plus d'informations, reportez-vous au site Web de documentation des pilotes Identity Manager.

9.2 Installation du chargeur distant Java

Le chargeur distant Java, `dirxml_jremote`, est généralement installé sur des ordinateurs dont le système d'exploitation n'est pas compatible avec le chargeur distant natif. Toutefois, le chargeur distant Java peut également s'exécuter sur des serveurs sur lesquels le chargeur distant natif est installé. Identity Manager utilise le chargeur distant Java pour permettre l'échange de données entre

le moteur Identity Manager exécuté sur un serveur et les pilotes Identity Manager situés à un autre emplacement, où `rdxml` ne s'exécute pas. Vous pouvez installer `dirxml_jremote` sur n'importe quel ordinateur Linux compatible disposant d'une version de Java officiellement prise en charge.

1. Sur le serveur qui héberge le moteur Identity Manager, copiez les fichiers `.iso` ou `.jar` du module d'interface d'application situés par défaut dans le répertoire `/opt/novell/eDirectory/lib/dirxml/classes`.
2. Connectez-vous à l'ordinateur sur lequel vous voulez installer le chargeur distant Java (l'ordinateur cible).
3. Vérifiez que l'ordinateur cible dispose d'une version prise en charge de JRE.
4. Pour accéder au programme d'installation, effectuez l'une des opérations suivantes :
   - **4a** (Conditionnel) Si vous disposez du fichier image `.iso` pour le paquetage d'installation d'Identity Manager, accédez au répertoire contenant les fichiers d'installation du chargeur distant Java, situé par défaut sous `products/IDM/java_remoteloader`.
   - **4b** (Conditionnel) Si vous avez téléchargé les fichiers d'installation du chargeur distant Java à partir du site Web de téléchargement NetIQ, procédez comme suit :
     - **4b1** Accédez au fichier `.tgz` pour localiser l'image téléchargée.
     - **4b2** Décompressez le contenu du fichier dans un dossier sur l'ordinateur local.
5. Copiez le fichier `dirxml_jremote_dev.tar.gz` à l'emplacement souhaité sur l'ordinateur cible. Par exemple, copiez le fichier à l'emplacement `/usr/idm`.
6. Copiez l'un des fichiers suivants à l'emplacement souhaité sur l'ordinateur cible :
   - `dirxml_jremote.tar.gz`
   - `dirxml_jremote_mvs.tar`

     Pour plus d'informations sur mvs, décompressez le fichier `dirxml_jremote_mvs.tar`, puis reportez-vous au document `usage.html`.
7. Sur l'ordinateur cible, dézippez et décompressez les fichiers `.tar.gz`.

   Par exemple, entrez `gunzip dirxml_jremote.tar.gz` ou `tar -xvf dirxml_jremote_dev.tar`.
8. Déplacez les fichiers `.iso` ou `.jar` du module d'interface d'application que vous avez copiés à l'Étape 1 dans le répertoire `dirxml/classes` vers le répertoire `lib`.
9. Pour personnaliser le script `dirxml_jremote` afin de rendre accessible l'exécutable Java par le biais de la variable d'environnement `RDXML_PATH`, procédez de l'une des manières suivantes :
   - **9a** Entrez l'une des commandes suivantes pour définir la variable d'environnement `RDXML_PATH` :
     - `set RDXML_PATH=path`
     - `export RDXML_PATH`
   - **9b** Modifiez le script `dirxml_jremote` et préfixez la ligne de script exécutant Java avec le chemin vers l'exécutable Java.
10. Vous devez spécifier l'emplacement des fichiers JAR du script `dirxml_jremote` à partir du sous-répertoire lib du répertoire désarchivé `dirxml_jremote.tar.gz`, par exemple, `/lib/*.jar`.
11. Configurez le fichier de configuration d'exemple `config8000.txt` à utiliser avec votre module d'interface d'application.

    Le fichier exemple se trouve par défaut dans le répertoire `/opt/novell/dirxml/doc`. Pour plus d'informations, reportez-vous au Chapitre 11.3, « Configuration des pilotes et du chargeur distant », page 118.

9.3 Installation des applications d'identité

Les applications d'identité peuvent être installées à l'aide des méthodes suivantes :

- Section 9.3.1, « Exécution d'une installation interactive », page 97
- Section 9.3.2, « Installation silencieuse », page 97
- Section 9.3.3, « Exécution d'une installation interactive de SSPR », page 98
- Section 9.3.4, « Exécution d'une installation silencieuse de SSPR », page 98

9.3.1 Exécution d'une installation interactive

1. Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.
2. Montez le fichier `.iso` téléchargé.
3. À partir du répertoire racine du fichier `.iso`, exécutez la commande suivante :

   ```
   ./install.sh
   ```
4. Lisez le contrat de licence.
5. Entrez `o` pour accepter l'accord de licence.
6. Indiquez l'édition de serveur Identity Manager que vous souhaitez installer. Entrez `y` pour Advanced Edition et `n` pour Standard Edition.
7. Sélectionnez les applications d'identité et poursuivez l'installation.
8. Configurez les composants installés. Pour plus d'informations, reportez-vous à la Chapitre 10, « Configuration des composants installés », page 101.

9.3.2 Installation silencieuse

1. Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargements NetIQ.
2. Montez le fichier `.iso` téléchargé.
3. À partir du répertoire racine du fichier `.iso`, exécutez la commande suivante :

   ```
   ./create_silent_props.sh
   ```
4. Entrez `y` pour confirmer la création du fichier.
5. Pour installer JRE, entrez `y`.
6. Indiquez l'édition de serveur Identity Manager que vous souhaitez installer. Entrez `y` pour Advanced Edition et `n` pour Standard Edition.
7. Sélectionnez un mode de configuration des composants. Pour plus d'informations, reportez-vous au Chapitre 10, « Configuration des composants installés », page 101.
8. Sélectionnez les applications d'identité et poursuivez l'installation.
9. Exécutez la commande suivante pour effectuer une installation silencieuse :

   ```
   ./install.sh -s -f <emplacement_fichier_propriétés_silencieux>
   ```

   Exemples :

   `./install.sh -s -f /mnt/silent.properties`, où `/mnt/silent.properties` correspond à l'emplacement où vous avez enregistré le fichier de propriétés silencieux.

9.3.3 Exécution d'une installation interactive de SSPR

Si vous souhaitez installer les applications d'identité et SSPR dans un environnement distribué, le programme d'installation vous propose une option permettant d'installer SSPR séparément.

1. Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.
2. Montez le fichier `.iso` téléchargé.
3. À partir du répertoire racine du fichier `.iso`, accédez au répertoire `SSPR`.
4. Exécutez la commande suivante :

   ```
   ./install.sh
   ```

5. Lisez le contrat de licence.
6. Entrez `o` pour accepter l'accord de licence.
7. Configurez les composants installés. Pour plus d'informations, reportez-vous à la Chapitre 10, « Configuration des composants installés », page 101.

9.3.4 Exécution d'une installation silencieuse de SSPR

1. Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.
2. Montez le fichier `.iso` téléchargé.
3. À partir du répertoire racine du fichier `.iso`, accédez au répertoire `SSPR`.
4. Exécutez la commande suivante :

   ```
   ./install.sh -s sspr_silentinstall.properties
   ```

9.4 Installation d'Identity Reporting

Identity Reporting peut être installé à l'aide des méthodes suivantes :

- Section 9.4.1, « Exécution d'une installation interactive », page 98
- Section 9.4.2, « Installation silencieuse », page 99

9.4.1 Exécution d'une installation interactive

1. Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.
2. Montez le fichier `.iso` téléchargé.
3. À partir du répertoire racine du fichier `.iso`, exécutez la commande suivante :

   ```
   ./install.sh
   ```

4. Lisez le contrat de licence.
5. Entrez `o` pour accepter l'accord de licence.
6. Indiquez l'édition de serveur Identity Manager que vous souhaitez installer. Entrez `y` pour Advanced Edition et `n` pour Standard Edition.

7 Spécifiez Identity Reporting et poursuivez l'installation.

8 Configurez les composants installés. Pour plus d'informations, reportez-vous à la Chapitre 10, « Configuration des composants installés », page 101.

9.4.2 Installation silencieuse

1 Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.

2 Montez le fichier `.iso` téléchargé.

3 À partir du répertoire racine du fichier `.iso`, exécutez la commande suivante :

```
./create_silent_props.sh
```

4 Entrez `y` pour confirmer la création du fichier.

5 Pour installer le JRE, entrez `y`.

6 Indiquez l'édition de serveur Identity Manager que vous souhaitez installer. Entrez `y` pour Advanced Edition et `n` pour Standard Edition.

7 Sélectionnez un mode de configuration des composants. Pour plus d'informations, reportez-vous à la Chapitre 10, « Configuration des composants installés », page 101.

8 Spécifiez Identity Reporting et poursuivez l'installation.

9 Exécutez la commande suivante pour effectuer une installation silencieuse :

```
./install.sh -s -f <emplacement_fichier_propriétés_silencieux>
```

Exemples :

`./install.sh -s -f /mnt/silent.properties`, où `/mnt/silent.properties` correspond à l'emplacement où vous avez enregistré le fichier de propriétés silencieux.

10 Configuration des composants installés

Cette section vous guide dans le processus de configuration des composants Identity Manager que vous avez installés au Chapitre 9, « Installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting », page 91. Vous pouvez effectuer la configuration en mode interactif (console) ou silencieux.

Vous devez passer en revue les options de configuration de chaque composant avant de commencer le processus de configuration. Pour plus d'informations, reportez-vous à la Section 10.1, « Présentation des paramètres de configuration », page 101.

10.1 Présentation des paramètres de configuration

Cette section définit les paramètres que vous devez spécifier pour configurer l'installation d'Identity Manager. Vous pouvez utiliser le programme d'installation pour configurer les composants immédiatement après leur installation ou ultérieurement.

REMARQUE

- Si vous configurez les applications d'identité et Identity Reporting en mode de configuration standard, vous ne pouvez pas vous connecter à une base de données installée sur une machine différente.
- Le processus d'installation ne permet pas d'activer la fonction d'audit. Vous devez l'activer séparément pour les composants Identity Manager. Pour plus d'informations, reportez-vous au manuel NetIQ Identity Manager - Configuring Auditing in Identity Manager (NetIQ Identity Manager - Configuration de l'audit dans Identity Manager).

Configuration standard des paramètres	
Moteur Identity Manager	
Mot de passe commun	Indique si vous souhaitez définir un mot de passe commun.
Nom de l'administrateur du coffre-fort d'identité	Permet de spécifier le nom distinctif relatif (RDN) de l'objet Administrateur de l'arborescence qui possède les droits complets, au moins sur le contexte auquel ce serveur est ajouté.
Applications d'identité	
Mot de passe commun	Indique si vous souhaitez définir un mot de passe commun.
Nom de l'administrateur du coffre-fort d'identité	Permet de spécifier le nom distinctif relatif (RDN) de l'objet Administrateur de l'arborescence qui possède les droits complets, au moins sur le contexte auquel ce serveur est ajouté.
Nom d'hôte (nom de domaine complet en minuscules)	Indique le nom distinctif complet ou l'adresse IP par défaut du serveur.
Adresse DNS/IP du serveur d'applications	Indique l'adresse IP du serveur Tomcat.

Configuration standard des paramètres	
Nom de l'administrateur des applications d'identité	Permet de spécifier le nom du compte administrateur pour les applications d'identité.
Identity Reporting	
Mot de passe commun	Indique si vous souhaitez définir un mot de passe commun.
Nom de l'administrateur du coffre-fort d'identité	Permet de spécifier le nom distinctif relatif (RDN) de l'objet Administrateur de l'arborescence qui possède les droits complets, au moins sur le contexte auquel ce serveur est ajouté.
Nom d'hôte (nom de domaine complet en minuscules)	Indique le nom distinctif complet ou l'adresse IP par défaut du serveur.
Connecter à un serveur SSO One externe	Indique si vous souhaitez une connexion vers un autre serveur One SSO.
Adresse DNS/IP du serveur d'applications	Indique l'adresse IP du serveur Tomcat.
Adresse DNS/IP du serveur SSO One	Spécifie l'adresse IP du serveur sur lequel le service Single Sign-on est installé.
Nom de l'administrateur d'Identity Reporting	Spécifie le nom de l'administrateur d'Identity Reporting. La valeur par défaut est `cn=uaadmin,ou=sa,o=data`.

Configuration personnalisée des paramètres	
Moteur Identity Manager	
Nom de l'arborescence du coffre-fort d'identité	Spécifie une nouvelle arborescence pour votre coffre-fort d'identité. Ce nom doit satisfaire aux conditions suivantes : ◆ Le nom de l'arborescence doit être unique sur votre réseau. ◆ Le nom de l'arborescence doit se composer de 2 à 32 caractères. ◆ Le nom de l'arborescence doit uniquement contenir des caractères de type lettres (A-Z), chiffres (0-9), tirets (-) et traits de soulignement (_).
Nom de l'administrateur du coffre-fort d'identité	Permet de spécifier le nom distinctif relatif (RDN) de l'objet Administrateur de l'arborescence qui possède les droits complets, au moins sur le contexte auquel ce serveur est ajouté.
Mot de passe de l'administrateur du coffre-fort d'identité	Indique le mot de passe de l'objet Administrateur, Par exemple : *password*.
Emplacement du dossier var NDS	Indique le chemin de cette instance du coffre-fort d'identité sur ce serveur. Le chemin d'accès par défaut est `/var/opt/novell/eDirectory`.
Emplacement des données NDS	Spécifie le chemin sur le système local où vous souhaitez installer les fichiers de base de données des informations de l'Annuaire (DIB). Les fichiers DIB sont vos fichiers de base de données du coffre-fort d'identité. L'emplacement par défaut est `/var/opt/novell/eDirectory/data/dib`.

Configuration personnalisée des paramètres	
Port NCP	Permet de spécifier le port NCP (NetWare Core Protocol) que le coffre-fort d'identité utilise pour communiquer avec les composants Identity Manager. La valeur par défaut est `524`.
Port non-SSL LDAP	Permet de spécifier le port sur lequel le coffre-fort d'identité doit être à l'écoute des requêtes LDAP en texte clair. La valeur par défaut est `389`.
Port SSL LDAP	Permet de spécifier le port sur lequel le coffre-fort d'identité doit être à l'écoute des requêtes LDAP à l'aide du protocole SSL (Secure Sockets Layer). La valeur par défaut est `636`.
Port HTTP du coffre-fort d'identité	Permet de spécifier le port sur lequel la pile HTTP fonctionne en texte clair. La valeur par défaut est `8028`.
Port HTTPS du coffre-fort d'identité	Permet de spécifier le port sur lequel la pile HTTP fonctionne à l'aide du protocole TLS/SSL. La valeur par défaut est `8030`.
Fichier de configuration NDS avec chemin d'accès	Spécifie l'emplacement du fichier de configuration du coffre-fort d'identité. La valeur par défaut est `/etc/opt/novell/eDirectory/conf/nds.conf`.
Nom de l'ensemble de pilotes du coffre-fort d'identité	Spécifie le nom d'un nouvel objet Ensemble de pilotes d'Identity Manager.
Contexte de déploiement de l'ensemble de pilotes du coffre-fort d'identité	Spécifie le DN LDAP du conteneur dans lequel vous souhaitez créer l'objet Ensemble de pilotes.
Applications d'identité	
Nom d'hôte (nom de domaine complet en minuscules)	Indique le nom distinctif complet ou l'adresse IP par défaut du serveur. **REMARQUE :** assurez-vous que le nom de domaine complet est indiqué en minuscules. Le serveur qui héberge votre composant doit également être configuré pour utiliser le nom de domaine complet en minuscules.
Nom d'hôte/adresse IP du coffre-fort d'identité	Spécifie l'adresse IP du serveur sur lequel le coffre-fort d'identité est installé.
Nom de l'administrateur du coffre-fort d'identité	Permet de spécifier le nom distinctif relatif (RDN) de l'objet Administrateur de l'arborescence qui possède les droits complets, au moins sur le contexte auquel ce serveur est ajouté.
Mot de passe de l'administrateur du coffre-fort d'identité	Indique le mot de passe de l'objet Administrateur, Par exemple : *password*.
Adresse DNS/IP du serveur d'applications	Indique l'adresse IP du serveur Tomcat.
Nom de l'écran de connexion personnalisé OSP	Indique le nom qui s'affichera sur l'écran de connexion OSP.
Mot de passe de configuration de SSPR	*S'applique uniquement si vous avez défini le mot de passe commun sur* **Non**. Spécifie le mot de passe de gestion des mots de passe utilisé par les applications d'identité.

Configuration personnalisée des paramètres	
Mot de passe du Keystore OAuth	*S'applique uniquement si vous avez défini le mot de passe commun sur* **Non**. Permet de spécifier le mot de passe que vous souhaitez créer pour le chargement du nouveau keystore sur le serveur OAuth.
DN du conteneur de recherche Utilisateur	Spécifie le conteneur par défaut pour tous les objets Utilisateur dans le coffre-fort d'identité.
DN du conteneur de recherche Admin	Spécifie tous les objets Données des emplacements Identity Manager dans l'organisation Données. Les administrateurs doivent veiller à ce que tous les utilisateurs aient accès à ce conteneur et à l'ensemble de ses sous-conteneurs.
Port HTTPS du serveur d'applications	Indique le port HTTPS que le serveur Tomcat doit utiliser pour la communication avec les ordinateurs client. La valeur par défaut est 8543.
Port SSL du serveur SSO One	Spécifie le port que le service Single Sign-on doit utiliser. La valeur par défaut est 8543.
Mot de passe du service SSO One des applications d'identité	*S'applique uniquement si vous avez défini le mot de passe commun sur* **Non**. Spécifie le mot de passe du client Single Sign-on utilisé par les applications d'identité.
Nom de l'administrateur des applications d'identité	Permet de spécifier le nom du compte administrateur pour les applications d'identité.
Port non-SSL LDAP	Permet de spécifier le port sur lequel le coffre-fort d'identité doit être à l'écoute des requêtes LDAP en texte clair. La valeur par défaut est 389.
Nom de l'ensemble de pilotes du coffre-fort d'identité	Indique le nom de l'ensemble de pilotes pour le coffre-fort d'identité.
Contexte de déploiement de l'ensemble de pilotes du coffre-fort d'identité	Spécifie le DN LDAP du conteneur dans lequel vous souhaitez créer l'objet Ensemble de pilotes.
Plate-forme de la base de données	Spécifie les bases de données requises pour les applications d'identité.
Configurer PostgreSQL sur le serveur actuel	Indique si vous souhaitez configurer la base de données PostgreSQL sur le même serveur.
Port de la base de données des applications d'identité	Spécifie le port de la base de données pour les applications d'identité.
Nom de la base de données des applications d'identité	Indique le nom de la base de données. La valeur par défaut est `idmuserappdb`.
Nom de l'utilisateur de la base de données des applications d'identité	Spécifie le nom d'utilisateur de l'administrateur de la base de données des applications d'identité.
Fichier JAR JDBC de la base de données des applications d'identité	Spécifie le fichier JAR pour la plate-forme de base de données.
Créer un schéma	Indique si vous souhaitez créer le schéma de base de données dans le cadre du processus d'installation. Les options disponibles sont **Maintenant**, **Démarrage** et **Fichier**.

Configuration personnalisée des paramètres	
Créer une base de données ou mettre à jour/migrer une base de données existante	Indique si vous souhaitez créer une base de données ou effectuer une mise à niveau à partir d'une base de données existante.
Utiliser le conteneur personnalisé comme conteneur racine	Indique si vous souhaitez utiliser le conteneur personnalisé comme conteneur root. Par défaut, le programme d'installation crée `o=data` et le choisit comme conteneur des utilisateurs ; il lui assigne les stratégies de mot de passe et les droits d'ayant droit requis. Pour créer un conteneur personnalisé, choisissez **Oui**.
Chemin du fichier LDIF du conteneur personnalisé	*S'applique uniquement si vous avez défini le conteneur personnalisé sur* **Oui**. Indique le chemin du fichier LDIF pour le conteneur personnalisé.
Conteneur racine	Indique le conteneur root. La valeur par défaut est `o=data`.
DN du conteneur racine de la recherche de groupe	Indique le DN du conteneur racine de la recherche de groupe.
Identity Reporting	
Nom d'hôte (nom de domaine complet en minuscules)	Indique le nom distinctif complet ou l'adresse IP par défaut du serveur. **REMARQUE :** assurez-vous que le nom de domaine complet est indiqué en minuscules. Le serveur qui héberge votre composant doit également être configuré pour utiliser le nom de domaine complet en minuscules.
Nom d'hôte/adresse IP du coffre-fort d'identité	Spécifie l'adresse IP du serveur sur lequel le coffre-fort d'identité est installé.
Port SSL LDAP	Permet de spécifier le port sur lequel le coffre-fort d'identité doit être à l'écoute des requêtes LDAP à l'aide du protocole SSL (Secure Sockets Layer). La valeur par défaut est 636.
Nom de l'administrateur du coffre-fort d'identité	Permet de spécifier le nom distinctif relatif (RDN) de l'objet Administrateur de l'arborescence qui possède les droits complets, au moins sur le contexte auquel ce serveur est ajouté.
Mot de passe de l'administrateur du coffre-fort d'identité	Indique le mot de passe de l'objet Administrateur, Par exemple : *password*.
Adresse DNS/IP du serveur d'applications	Indique l'adresse IP du serveur Tomcat.
Nom de l'écran de connexion personnalisé OSP	Indique le nom qui s'affichera sur l'écran de connexion OSP.
DN du conteneur de recherche Utilisateur	Spécifie le conteneur par défaut pour tous les objets Utilisateur dans le coffre-fort d'identité.
DN du conteneur de recherche Admin	Spécifie tous les objets Données des emplacements Identity Manager dans l'organisation Données. Les administrateurs doivent veiller à ce que tous les utilisateurs aient accès à ce conteneur et à l'ensemble de ses sous-conteneurs.

Configuration personnalisée des paramètres	
Port HTTPS du serveur d'applications	Indique le port HTTPS que le serveur Tomcat doit utiliser pour la communication avec les ordinateurs client. La valeur par défaut est 8543.
Adresse DNS/IP du serveur SSO One	Spécifie l'adresse IP du serveur sur lequel le service Single Sign-on est installé.
Port SSL du serveur SSO One	Spécifie le port que le service Single Sign-on doit utiliser. La valeur par défaut est 8543.
Nom de la base de données d'Identity Reporting	Indique le nom de la base de données d'Identity Reporting. La valeur par défaut est `idmrptdb`.
Utilisateur de la base de données d'Identity Reporting	Spécifie le compte d'administration qui permet à Identity Reporting d'accéder et de modifier les données dans les bases de données. La valeur par défaut est `rptadmin`.
Hôte de base de données d'Identity Reporting	Spécifie le nom DNS ou l'adresse IP du serveur sur lequel la base de données doit être créée.
Port de la base de données d'Identity Reporting	Permet de spécifier le port de connexion à la base de données. Le port par défaut est 5432.
Fichier JAR JDBC de la base de données des applications d'identité	Spécifie le fichier JAR pour la plate-forme de base de données.
Mot de passe du compte de la base de données d'Identity Reporting	Spécifie le mot de passe du compte de base de données d'Identity Reporting.
Créer un schéma	Indique si vous souhaitez créer le schéma de base de données dans le cadre du processus d'installation. Les options disponibles sont **Maintenant**, **Démarrage** et **Fichier**. Si vous sélectionnez l'option de création du schéma de base de données **Démarrage** ou **Fichier**, vous devez ajouter manuellement la source des données à la page des services de collecte des données d'identité. Pour plus d'informations, reportez-vous à la Section 11.10.1, « Ajout manuel de la source de données dans la page des services de collecte de données d'identité », page 176. Si votre base de données est en cours d'exécution sur un serveur distinct, vous devez vous connecter à cette base de données. Pour une base de données PostgreSQL installée à distance, vérifiez que celle-ci est en cours d'exécution. Pour vous connecter à une base de données PostgreSQL à distance, reportez-vous à la Section 11.10.6, « Connexion à une base de données PostgreSQL distante », page 178. Si vous vous connectez à une base de données Oracle, vérifiez que vous avez créé une instance de base de données Oracle. Pour plus d'informations, reportez-vous à la documentation Oracle. Si vous sélectionnez l'option de création du schéma de base de données **Démarrage** ou **Fichier**, vous devez manuellement créer les tables et vous connecter à la base de données après la configuration. Pour plus d'informations, reportez-vous à la Section 11.10.3, « Génération manuelle du schéma de base de données », page 176.

Configuration personnalisée des paramètres	
Adresse électronique par défaut	Permet de spécifier l'adresse électronique que vous souhaitez que le module Identity Reporting utilise pour émettre des notifications par message électronique.
Serveur SMTP	Permet d'indiquer le nom DNS ou l'adresse IP de l'hôte de messagerie électronique SMTP utilisé par Identity Reporting pour les notifications.
Port du serveur SMTP	Permet d'indiquer le numéro de port du serveur SMTP. Le numéro de port par défaut est 465.
Créer les pilotes MSGW et DCS pour Identity Reporting	Indique si vous souhaitez créer les pilotes MSGW et DCS.

10.2 Exécution de la configuration

Les sections suivantes fournissent des informations sur la configuration des composants Identity Manager.

10.2.1 Exécution d'une configuration interactive

1. Accédez à l'emplacement où vous avez monté le fichier Identity_Manager_4.7_Linux.iso.
2. Exécutez la commande suivante :

   ```
   ./configure.sh
   ```

3. Indiquez si vous souhaitez effectuer une configuration standard ou personnalisée. Les options de configuration varient selon les composants que vous sélectionnez pour la configuration.
4. Pour configurer les composants, utilisez les informations de la Section 10.1, « Présentation des paramètres de configuration », page 101.

10.2.2 Configuration en mode silencieux

1. Accédez à l'emplacement où vous avez monté le fichier `Identity_Manager_4.7_Linux.iso`.
2. Exécutez la commande suivante :

   ```
   ./configure.sh -s -f <emplacement_fichier_propriétés_silencieux>
   ```

   Exemples :

   `./configure.sh -s -f /mnt/silent.properties`, où `/mnt/silent.properties` correspond à l'emplacement où vous avez enregistré le fichier de propriétés silencieux.
3. Pour configurer les composants, utilisez les informations de la Section 10.1, « Présentation des paramètres de configuration », page 101.

11 Étapes finales pour terminer l'installation

Après l'installation d'Identity Manager, vous devez configurer les pilotes installés conformément aux stratégies et exigences définies par vos processus métiers. Vous devez également configurer Sentinel Log Management for IGA pour collecter les événements d'audit. Les tâches post-installation comprennent généralement les éléments suivants :

11.1 Exécution d'une installation en tant qu'utilisateur non-root

Lorsque vous installez le moteur et les plug-ins Identity Manager en tant qu'utilisateur non-`root`, le processus exécute toutes les opérations d'installation prévues. Cette section vous guide à travers la procédure manuelle requise pour terminer l'installation.

11.1.1 Création d'un conteneur de stratégies de mot de passe

Identity Manager requiert la définition d'objets Stratégie de mot de passe dans le coffre-fort d'identité. Toutefois, le processus d'installation non-`root` ne crée aucun conteneur pour les stratégies de mot de passe.

1. Connectez-vous à l'arborescence Identity Manager dans iManager.
2. Accédez au conteneur de sécurité dans eDirectory.

11.1.2 Ajout de la prise en charge des graphiques dans les notifications par message électronique

Si vous installez le coffre-fort d'identité et le moteur Identity Manager en tant qu'utilisateur non-`root`, il se peut que les notifications par message électronique n'incluent pas les graphiques ou les images dans le modèle de message électronique. Par exemple, lorsque vous exécutez l'opération `do-send-`

`email-from-template`, Identity Manager envoie le message électronique, mais les images incluses sont vides. Le cas échéant, vous devez mettre à jour l'ensemble de pilotes pour garantir la prise en charge des graphiques.

1. Connectez-vous à votre projet dans Designer.
2. Dans le volet Mode plan, développez le **coffre-fort d'identité**.
3. Cliquez avec le bouton droit de la souris sur **Ensemble de pilotes**.
4. Sélectionnez **Propriétés > Java**.
5. Pour les options JVM, entrez le contenu suivant :

   ```
   -Dcom.novell.nds.dirxml.util.mail.templatepath=path_to_graphics_files
   ```

   Par exemple :

   ```
   -Dcom.novell.nds.dirxml.util.mail.templatepath=/prod/eDirectory/opt/novell/
   eDirectory/lib/dirxml/rules/manualtask/mt_files
   ```

6. Cliquez sur **OK**.
7. Déployez les modifications apportées à l'ensemble de pilotes :
   - **7a** Cliquez avec le bouton droit de la souris sur **Ensemble de pilotes**.
   - **7b** Sélectionnez **En direct > Déploiement**.
   - **7c** Sélectionnez **Déployer**.
8. Redémarrez le coffre-fort d'identité.

11.2 Configuration du coffre-fort d'identité après l'installation

Après avoir installé le coffre-fort d'identité, vous pouvez utiliser l'utilitaire ndsconfig pour configurer l'annuaire, et l'utilitaire ndsmanage pour créer, démarrer et arrêter les instances du serveur. Vous pouvez également configurer le coffre-fort d'identité pour qu'il fonctionne avec des adresses IPv6, si votre serveur prend déjà en charge l'adressage IPv6.

11.2.1 Modification de l'arborescence eDirectory et du serveur de répliques à l'aide de l'utilitaire ndsconfig

Une fois le coffre-fort d'identité installé, vous pouvez le configurer à l'aide de l'utilitaire ndsconfig. Pour pouvoir exécuter cet utilitaire, vous devez disposer de droits d'administrateur. Lorsque vous l'utilisez avec des arguments, cet utilitaire valide tous les arguments et vous invite à saisir le mot de passe de l'utilisateur disposant de droits d'administrateur. Si vous l'utilisez sans arguments, ndsconfig affiche une description de l'utilitaire et des options disponibles.

Vous pouvez également exécuter cet utilitaire pour supprimer le serveur de répliques eDirectory et modifier la configuration actuelle du serveur eDirectory. Pour plus d'informations, reportez-vous au Chapitre 11.2, « Configuration du coffre-fort d'identité après l'installation », page 110.

Lorsque vous utilisez l'utilitaire ndsconfig, les conditions suivantes s'appliquent :

- Les nombres maximum de caractères autorisés pour les variables *`nom_arborescence`*, *`FDN_admin`* et *`FDN_serveur`* sont les suivants :
  - *`nom_arborescence`* : 32 caractères

- *FDN_admin* : 255 caractères
- *FDN_serveur* : 255 caractères

- Lorsque vous ajoutez un serveur à une arborescence existante et que le contexte que vous spécifiez n'existe pas dans l'objet Serveur, l'utilitaire ndsconfig le crée lors de l'ajout du serveur.
- Après avoir installé le coffre-fort d'identité, vous pouvez ajouter des services LDAP et de sécurité à l'arborescence existante.
- Pour activer la réplication chiffrée sur le serveur, incluez l'option `-E` dans les commandes permettant d'ajouter un serveur à une arborescence existante. Pour plus d'informations sur la réplication chiffrée, reportez-vous à la section Réplication codée du Guide d'administration de NetIQ eDirectory.

Pour plus d'informations sur l'utilisation de l'utilitaire ndsconfig pour modifier eDirectory, reportez-vous au *Guide d'administration de NetIQ eDirectory* .

Description des paramètres de l'utilitaire ndsconfig

L'utilitaire ndsconfig prend en charge les paramètres suivants :

new

Crée une arborescence. Si vous ne spécifiez pas les paramètres dans la ligne de commande, l'utilitaire vous invite à saisir les valeurs de chaque paramètre manquant.

def

Crée une arborescence. Si vous ne spécifiez pas les paramètres dans la ligne de commande, ndsconfig applique la valeur par défaut de chaque paramètre manquant.

add

Ajoute un serveur à une arborescence existante. Cette option ajoute également des services LDAP et SAS une fois le coffre-fort d'identité configuré dans l'arborescence existante.

rm

Supprime l'objet Serveur et les services Annuaire d'une arborescence.

REMARQUE : cette option ne supprime pas les objets Matériels clé. Ces objets doivent être supprimés manuellement.

---

upgrade

Met à niveau eDirectory vers une version ultérieure.

-i

Indique à l'utilitaire de ne pas vérifier l'existence éventuelle d'une arborescence portant le même nom si vous configurez une nouvelle arborescence. Plusieurs arborescences portant le même nom peuvent coexister.

-t *nom_arborescence*

Indique le nom de l'arborescence à laquelle vous souhaitez ajouter le serveur. Il peut contenir un maximum de 32 caractères. S'il n'est pas spécifié, l'utilitaire ndsconfig utilise le nom d'arborescence du paramètre `n4u.nds.nom_arborescence` défini dans le fichier `/etc/opt/novell/eDirectory/conf/nds.conf`. Le nom d'arborescence par défaut est `$LOGNAME-$HOSTNAME-NDStree`.

-n *contexte_serveur*

Contexte du serveur auquel l'objet Serveur est ajouté. Il peut contenir un maximum de 64 caractères. Si le contexte n'est pas spécifié, ndsconfig utilise le contexte du paramètre de configuration `n4u.nds.server-context` défini dans le fichier `/etc/opt/novell/eDirectory/conf/nds.conf`. Le contexte de serveur doit être spécifié sous la forme d'un nom avec type. Le contexte par défaut est `org`.

-d *chemin_DIB*

Indique le chemin du répertoire dans lequel les fichiers de base de données seront stockés.

-r

Ajoute de force la réplique du serveur, quel que soit le nombre de serveurs déjà ajoutés au serveur.

-L *port_ldap*

Indique le numéro du port TCP sur le serveur LDAP. Si le port par défaut 389 est déjà utilisé, l'utilitaire vous demande de spécifier un autre port.

-l *port_ssl*

Indique le numéro du port SSL sur le serveur LDAP. Si le port par défaut 636 est déjà utilisé, l'utilitaire vous demande de spécifier un autre port.

-a *FDN_admin*

Nom distinctif complet de l'objet Utilisateur disposant des droits Superviseur sur le contexte dans lequel l'objet Serveur et les services Annuaire doivent être créés. Le nom admin doit être spécifié sous la forme d'un nom avec type. Il peut contenir un maximum de 64 caractères. La valeur par défaut est admin.org.

-e

Active les mots de passe en texte clair pour les objets LDAP.

-m *nom_module*

Indique le nom du module à installer ou configurer. Si vous configurez une nouvelle arborescence, vous ne pouvez spécifier que le module ds. Une fois le module ds configuré, vous pouvez ajouter les services NMAS, LDAP, SAS, SNMP et HTTP ainsi que NetIQ SecretStore (ss) à l'aide de la commande add. Si vous n'indiquez pas le nom du module, tous les modules sont installés.

REMARQUE : si vous ne voulez pas configurer le SecretStore pendant une mise à niveau d'eDirectory effectuée à l'aide de la commande `nds-install`, définissez la valeur `no_ss` sur cette option. Par exemple, entrez `ndsinstall '-m no_ss'`.

-o

Indique le numéro de port en texte clair HTTP.

-O

Indique le numéro de port sécurisé HTTP.

-p *adresse_IP:[port]*

Indique l'adresse IP de l'hôte distant qui contient une réplique de la partition à laquelle ce serveur est ajouté. Utilisez cette option lorsque vous ajoutez un serveur secondaire (commande add) à une arborescence. Le numéro de port par défaut est 524. Cela permet de faire des recherches plus rapides de l'arborescence en évitant la recherche SLP.

-R

Réplique sur le serveur local la partition à laquelle le serveur est ajouté. Cette option empêche l'ajout de répliques au serveur local.

-c

Cette option permet de ne pas recevoir d'invites pendant l'exécution de ndsconfig, notamment des invites vous demandant de sélectionner oui/non pour poursuivre le processus ou de ressaisir les numéros de port en cas de conflit. L'utilitaire continue à vous demander de spécifier les paramètres obligatoires s'ils ne sont pas indiqués dans la ligne de commande.

-w *mot_de_passe_admin*

Cette option permet de transmettre le mot de passe de l'administrateur en texte clair.

REMARQUE : NetIQ déconseille d'utiliser cette option dans un environnement où la sécurité des mots de passe est primordiale.

-E

Active la réplication chiffrée pour le serveur que vous tentez d'ajouter.

-j

Indique à l'utilitaire d'ignorer l'option de vérification d'état avant d'installer le coffre-fort d'identité.

-b *port_à_connecter*

Indique le numéro de port par défaut sur lequel une instance spécifique doit écouter. Cette option définit le numéro de port par défaut sur `n4u.server.tcp-port` et `n4u.server.udp-port`. Si vous utilisez l'option -b pour spécifier un port NCP, l'utilitaire considère ce port comme le port par défaut et met à jour les paramètres TCP et UDP en conséquence.

REMARQUE : Les options `-b` et `-B` sont des paramètres qui s'excluent mutuellement.

-B *interface1@port1, interface2@port2,...*

Indique le numéro de port ainsi que l'adresse IP ou l'interface. Par exemple, `-B eth0@524`, `-B 100.1.1.2@524`, `-B[2015::3]@524`.

REMARQUE

- les options `-b` et `-B` sont des paramètres qui s'excluent mutuellement.
- Pour spécifier une adresse IPv6, vous devez mettre l'adresse entre crochets (`[ ]`).

--config-file *fichier_configuration*

Indique le chemin absolu et le nom du fichier de configuration `nds.conf`. Par exemple, pour enregistrer le fichier de configuration dans le répertoire `/etc/opt/novell/eDirectory/`, entrez la commande suivante :

```
--config-file /etc/opt/novell/eDirectory/nds.conf
```

-P URL_LDAP

Permet aux URL LDAP de configurer l'interface LDAP sur l'objet Serveur LDAP. Utilisez des virgules pour séparer les différentes URL, par exemple :

```
-P ldap://1.2.3.4:389,ldaps://1.2.3.4:636,ldap://[2015::3]:389
```

REMARQUE

- Pour spécifier une adresse IPv6, vous devez mettre l'adresse entre crochets (`[ ]`). Par exemple, ldap://[2015::3]:389.
- Si vous ne spécifiez pas les URL LDAP lors de la configuration initiale, vous pouvez les ajouter par la suite dans l'attribut `ldapInterfaces` à l'aide de la commande `ldapconfig` ou dans iManager.

-D chemin_données

Crée les répertoires `data`, `dib` et `log` à l'emplacement spécifié.

set liste_valeurs

Définit la valeur des paramètres configurables spécifiés pour le coffre-fort d'identité. Cette option permet de définir les paramètres d'amorçage avant de configurer une arborescence.

Lorsque vous modifiez les paramètres de configuration, vous devez redémarrer ndsd pour appliquer les nouvelles valeurs. Il n'est pas nécessaire de redémarrer ndsd pour les paramètres de configuration suivants :

- `n4u.nds.inactivity-synchronization-interval`
- `n4u.nds.synchronization-restrictions`
- `n4u.nds.janitor-interval`
- `n4u.nds.backlink-interval`
- `n4u.nds.drl-interval`
- `n4u.nds.flatcleaning-interval`
- `n4u.nds.server-state-up-threshold`
- `n4u.nds.heartbeat-schema`
- `n4u.nds.heartbeat-data`

get help liste_paramètres

Affiche les chaînes d'aide pour les paramètres configurables spécifiés pour le coffre-fort d'identité. Si vous ne spécifiez pas une liste de paramètres, l'utilitaire liste les chaînes d'aide pour tous les paramètres configurables.

Configuration du coffre-fort d'identité en utilisant des paramètres régionaux spécifiques

Pour configurer le coffre-fort d'identité en utilisant des paramètres régionaux spécifiques, vous devez exporter LC_ALL et LANG vers ces paramètres régionaux avant de procéder à la configuration. Par exemple, entrez les commandes suivantes dans l'utilitaire ndsconfig :

```
export LC_ALL=ja
```

```
export LANG=ja
```

Ajout d'une nouvelle arborescence au coffre-fort d'identité

Lorsque vous créez une nouvelle arborescence dans le coffre-fort d'identité, l'utilitaire ndsconfig peut vous guider pendant la configuration ou vous pouvez entrer une commande unique pour spécifier toutes les valeurs des paramètres. Si le serveur de votre coffre-fort d'identité prend déjà en charge les adresses IPv6, vous pouvez spécifier une adresse IPv6 pour la nouvelle arborescence.

1. (Conditionnel) Pour que l'utilitaire ndsconfig vous invite à spécifier les paramètres d'une nouvelle arborescence dans le coffre-fort d'identité, entrez la commande suivante :

   ```
   ndsconfig new [-t tree_name] [-n server_context] [-a admin_FDN]
   ```

   Par exemple :

   ```
   ndsconfig new -t corp-tree -n o=company -a cn=admin.o=company
   ```

2. (Conditionnel) Pour créer une nouvelle arborescence dans le coffre-fort d'identité en spécifiant tous les paramètres dans la ligne de commande, entrez le texte suivant :

   ```
   ndsconfig new [-t nom_arborescence] [-n contexte_serveur] [-a FDN_admin] [-i]
   [-S nom_serveur] [-d chemin_dib] [-m module] [e] [-L port_ldap] [-l port_SSL]
   [-o port_http] [-O port_https] [-p adresse_IP:[port]] [-R] [-c] [-w
   mot_de_passe_admin] [-b port_à_connecter] [-B
   interface1@port1,interface2@port2,..] [-D emplacement_personnalisé] [--config-
   file fichier_configuration]
   ```

   ou

   ```
   ndsconfig def [-t nom_arborescence] [-n contexte_serveur] [-a FDN_admin] [-w
   mot_de_passe_admin] [-c] [-i] [-S nom_serveur] [-d chemin_dib] [-m module] [-e]
   [-L port_ldap] [-l port_SSL] [-o port_http] [-O port_https] [-D
   emplacement_personnalisé] [--config-file fichier_configuration]
   ```

Ajout d'un serveur à une arborescence existante

Pour ajouter un serveur à une arborescence existante, entrez la commande suivante :

```
ndsconfig add [-t treename] [-n server context] [-a admin_FDN] [-i] [-S
server_name] [-d path_for_dib] [-m module] [e] [-L ldap_port] [-l SSL_port] [-o
http_port] [-O https_port] [-p IP_address:[port]] [-R] [-c] [-w admin_password] [-
b port_to_bind] [-B interface1@port1,interface2@port2,..] [-D custom_location] [--
config-file configuration_file]
```

Par exemple :

```
ndsconfig add -t corp-tree -n o=company -a cn=admin.o=company -S srv1
```

Suppression du coffre-fort d'identité et de sa base de données du serveur

1. Accédez au répertoire `dsreports`, situé par défaut dans le répertoire `/var/opt/novell/edirectory/data/`.
2. Supprimez les fichiers HTML que vous avez précédemment créé à l'aide d'iMonitor.
3. À l'aide de l'utilitaire ndsconfig, entrez la commande suivante :

   ```
   ndsconfig rm [-a admin_FDN] [-w admin_password] [-p IP_address:[port]] [-c]
   ```

Suppression d'un objet Serveur eDirectory et des services Annuaire d'une arborescence

Pour supprimer l'objet Serveur et les services Annuaire d'une arborescence, entrez la commande suivante :

```
ndsconfig rm -a Admin_FDN
```

Configuration de plusieurs instances du coffre-fort d'identité

Vous pouvez configurer plusieurs instances du coffre-fort d'identité sur un même hôte. La méthode de configuration de plusieurs instances à l'aide de l'utilitaire ndsconfig est similaire à celle utilisée pour configurer plusieurs fois une seule instance. Chaque instance doit disposer d'identificateurs d'instance qui lui sont propres tels que :

- Des données et un emplacement de fichier journal différents. Utilisez les options `--config-file`, `-d` et `-D`.
- Un numéro de port unique sur lequel l'instance écoute. Utilisez les options `-b` et `-B`.
- Un nom de serveur unique pour l'instance. Utilisez l'option `-S nom_serveur`.

Pour plus d'informations, reportez-vous à la section Utilisation de ndsconfig pour configurer plusieurs instances d'eDirectory du *Guide d'installation de NetIQ eDirectory*.

REMARQUE :

- Lors de la configuration du coffre-fort d'identité, le nom de serveur NCP par défaut est défini sur le nom du serveur hôte. Lorsque vous configurez plusieurs instances, vous devez modifier le nom du serveur NCP. Utilisez l'option de ligne de commande de ndsconfig `-S nom_serveur` pour spécifier un nom de serveur différent. Lorsque vous configurez plusieurs instances, sur la même arborescence ou sur des arborescences différentes, le nom du serveur NCP doit être unique.
- Toutes les instances partagent la même clé de serveur (NICI).

11.2.2 Gestion d'instances à l'aide de l'utilitaire ndsmanage

L'utilitaire ndsmanage permet de créer, de démarrer et d'arrêter des instances de serveur dans le coffre-fort d'identité. Il permet également d'afficher une liste des instances configurées.

Liste des instances du coffre-fort d'identité

Vous pouvez utiliser l'utilitaire ndsmanage pour afficher le chemin d'accès au fichier de configuration, le nom distinctif complet et le port de l'instance de serveur, ainsi que l'état de l'instance (actif ou inactif) des utilisateurs spécifiés. L'utilitaire prend en charge les paramètres suivants :

ndsmanage

Liste toutes les instances que vous avez configurées.

ndsmanage -a|--all

Liste les instances de tous les utilisateurs d'une installation spécifique du coffre-fort d'identité.

ndsmanage *nom_utilisateur*

Liste les instances configurées par l'utilisateur spécifié.

Création d'une instance dans le coffre-fort d'identité

1. Dans la ligne de commande, entrez `ndsmanage`.
2. Entrez `c`.
3. À l'invite de commande, suivez les instructions pour créer la nouvelle instance.

Configuration et annulation de la configuration d'une instance dans le coffre-fort d'identité

Pour configurer une instance, entrez la commande suivante :

```
ndsconfig new -t treename -n server_context -a admin_FDN -b port_to_bind -D
path_for_data
```

Par exemple :

```
ndsconfig new -t mytree -n o=netiq -a cn=admin.o=company -b 1524 -D
/home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

REMARQUE : le système d'exploitation Linux limite la création de sockets sur le système de fichiers monté. Avec eDirectory, NetIQ recommande d'installer le répertoire `var` sur le système de fichiers local (option `-D` avec `ndsconfig`). Le répertoire DIB peut, quant à lui, être installé sur n'importe quel système de fichiers (option `-d` avec `ndsconfig`).

Pour annuler la configuration d'une instance :

1. Dans la ligne de commande, entrez `ndsmanage`.
2. Sélectionnez l'instance dont vous souhaitez annuler la configuration.
3. Entrez `d`.

Appel d'un utilitaire pour une instance du coffre-fort d'identité

Vous pouvez exécuter des utilitaires, tels que DSTrace, pour une instance. Supposons par exemple que vous souhaitez exécuter l'utilitaire DSTrace pour une instance 1 qui écoute sur le port 1524 et dont les fichiers de configuration et `DIB` se trouvent respectivement dans les répertoires `/home/mary/inst1/nds.conf` et `/home/mary/inst1/var`. Dans ce cas, vous pouvez entrer l'une des commandes suivantes :

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

ou

```
ndstrace -h 192.168.0.1:1524
```

Si vous ne spécifiez pas les identificateurs d'instance, l'utilitaire affiche toutes vos instances. Vous pouvez alors sélectionner une instance.

Démarrage et arrêt d'instances dans le coffre-fort d'identité

Vous pouvez démarrer ou arrêter une ou plusieurs instances que vous avez configurées.

1. (Conditionnel) Pour un processus guidé de démarrage ou d'arrêt d'une seule instance, procédez comme suit :
   - **1a** Dans la ligne de commande, entrez `ndsmanage`.
   - **1b** Sélectionnez l'instance que vous voulez démarrer ou arrêter.
   - **1c** Entrez `s` ou `k`, respectivement pour démarrer ou arrêter l'instance.
2. (Conditionnel) Pour démarrer ou arrêter une seule instance, entrez :

   ```
   ndsmanage start --config-file configuration_file_of_the_instance
   ```

   ou

   ```
   ndsmanage stop --config-file configuration_file_of_the_instance
   ```
3. (Conditionnel) Pour démarrer ou arrêter toutes les instances, entrez :

   ```
   ndsmanage startall
   ```

   ou

   ```
   ndsmanage stopall
   ```

11.3 Configuration des pilotes et du chargeur distant

Le chargeur distant peut héberger les modules d'interface d'application Identity Manager contenus dans les fichiers `.so` ou `.jar`. Le chargeur distant Java héberge les modules d'interface pilote Java. Il ne charge ou n'héberge aucun module d'interface pilote (C++) natif.

Avant d'utiliser le chargeur distant, vous devez configurer le module d'interface d'application pour vous connecter au moteur Identity Manager en toute sécurité. Vous devez également configurer le chargeur distant et les pilotes Identity Manager. Pour plus d'informations sur les modules d'interface, reportez-vous à la « Présentation des modules d'interface » page 69.

11.3.1 Création d'une connexion sécurisée au moteur Identity Manager

Vous devez veiller à ce que les transferts de données entre le chargeur distant et le moteur Identity Manager s'effectuent en toute sécurité. NetIQ recommande l'utilisation des protocoles TLS/SSL (Transport Layer Security/Secure Socket Layer) pour les communications. Les connexions TLS/SSL nécessitent un certificat auto-signé dans un fichier Keystore ou KMO. Cette section explique comment créer, exporter et stocker ce certificat.

REMARQUE : utilisez la même version de SSL sur les serveurs hébergeant le moteur Identity Manager et le chargeur distant. Si les versions de SSL sur le serveur et le chargeur distant ne correspondent pas, le serveur renvoie un message d'erreur `SSL3_GET_RECORD:wrong version number`. Ce message est un simple avertissement ; la communication entre le serveur et le chargeur distant n'est pas interrompue. Toutefois, l'erreur peut prêter à confusion.

Présentation du processus de communication

Le chargeur distant ouvre un socket client et écoute les connexions à partir du module d'interface distant. Le module d'interface et le chargeur distants effectuent une reconnaissance mutuelle SSL afin d'établir un canal sécurisé. Le module d'interface distant s'authentifie ensuite auprès du chargeur distant. Si la procédure d'authentification du module d'interface distant aboutit, le chargeur distant s'authentifie auprès du module d'interface distant. Une fois que les deux bords communiquent avec une entité autorisée, le trafic de synchronisation commence.

La procédure d'établissement des connexions SSL entre un pilote et le moteur Identity Manager dépend du type de pilote :

- **Pour un pilote natif**, tel que le pilote Active Directory, pointez vers un certificat codé en base64. Pour plus d'informations, reportez-vous à la « Gestion des certificats de serveur auto-signés » page 119.
- **Pour un pilote Java**, vous devez créer un fichier Keystore. Pour plus d'informations, reportez-vous à la « Création d'un fichier Keystore à l'aide de connexions SSL » page 121.

REMARQUE : le chargeur distant autorise des méthodes de connexion personnalisées entre le chargeur distant et le module d'interface distant hébergé sur le serveur Identity Manager. Pour configurer un module de connexion personnalisé, reportez-vous à la documentation qui accompagne le module pour plus d'informations sur le contenu d'une chaîne de connexion et ce qui est autorisé dans ce cadre.

Gestion des certificats de serveur auto-signés

Vous pouvez créer et exporter un certificat de serveur auto-signé afin d'assurer une communication sécurisée entre le chargeur distant et le moteur Identity Manager. Pour plus de sécurité, vous pouvez configurer des chiffrements plus forts pour la communication SSL comme spécifié par Suite B. Cette communication requiert l'utilisation de certificats ECDSA (Elliptic Curve Digital Signature Algorithm)

pour le chiffrement des données. Lorsque Suite B est activé, le chargeur distant utilise TLS 1.2 comme protocole de communication. Pour plus d'informations sur SuiteB, reportez-vous à la section relative à la technologie de chiffrement SuiteB sur le site Web de la NSA.

Vous pouvez exporter un certificat récemment créé ou utiliser un certificat existant.

REMARQUE : lorsqu'un serveur est intégré à une arborescence, eDirectory crée les certificats par défaut suivants :

- SSL CertificateIP
- SSL CertificateDNS
- Certificats conformes à Suite B

---

1. Connectez-vous à NetIQ iManager.
2. Pour créer un nouveau certificat, procédez comme suit :
   - **2a** Cliquez sur **Serveur de certificats NetIQ > Créer un certificat de serveur**.
   - **2b** Sélectionnez le serveur devant héberger le certificat.
   - **2c** Spécifiez un surnom pour le certificat. Par exemple, `remotecert`.

     REMARQUE : NetIQ vous recommande de ne pas utiliser d'espaces dans le surnom du certificat. Par exemple, utilisez `remotecert` plutôt que `remote cert`.

     N'oubliez pas de noter le surnom. Ce surnom est utilisé pour le nom KMO dans les paramètres de connexion à distance du pilote.

   - **2d** Sélectionnez la méthode de création du certificat, puis cliquez sur **Suivant**.

     Vous avez les options suivantes :

     - **Standard :** cette option crée un objet Certificat de serveur à l'aide de la plus grande taille de clé possible et signe le certificat de clé publique avec votre autorité de certification organisationnelle.
     - **Personnalisé:** cette option crée un objet Certificat de serveur à l'aide des paramètres que vous spécifiez. Elle vous permet de définir un certain nombre de paramètres personnalisés pour l'objet Certificat de serveur. Sélectionnez cette option pour créer des certificats ECDSA pour la communication Suite B.
     - **Importer :** cette option crée un objet Certificat de serveur à l'aide des clés et des certificats d'un fichier PKCS12 (PFX). Vous pouvez utiliser cette option en combinaison avec l'option Exporter pour sauvegarder et restaurer un certificat de serveur, ou pour déplacer un objet Certificat de serveur entre des serveurs.

   - **2e** Spécifiez les paramètres du certificat.
   - **2f** Acceptez les autres paramètres par défaut du certificat.
   - **2g** Passez en revue le résumé, cliquez sur **Terminer**, puis sur **Fermer**.
3. Pour exporter un certificat, procédez comme suit :
   - **3a** Dans iManager, accédez à **Rôles et tâches** > **Accès aux certificats NetIQ > Certificats de serveur**.
   - **3b** Recherchez et sélectionnez le certificat créé ou le certificat de serveur créé (par exemple, SSL CertificateDNS).
   - **3c** Cliquez sur **Exporter**.
   - **3d** Pour **Certificat d'autorité de certification**, sélectionnez **OU=organization CA.O=TREEANAME** dans le menu déroulant.

3e Pour **Format d'exportation**, sélectionnez **BASE64** dans le menu déroulant.

3f Cliquez sur **Suivant**.

3g Cliquez sur **Enregistrer**, puis sur **Fermer**.

Création d'un fichier Keystore à l'aide de connexions SSL

Pour utiliser des connexions SSL entre un pilote Java et le moteur Identity Manager, vous devez créer un fichier Keystore. Un keystore est un fichier Java qui contient des clés de codage et, le cas échéant, des certificats. Si vous voulez utiliser SSL entre le chargeur distant et le moteur Identity Manager et si vous utilisez un module d'interface Java, vous devez créer un fichier Keystore. Les sections suivantes expliquent comment créer un fichier Keystore :

- « Création d'un fichier Keystore sur une plate-forme quelconque » page 121
- « Création d'un fichier Keystore sous Linux » page 121

Création d'un fichier Keystore sur une plate-forme quelconque

Pour créer un keystore sur n'importe quelle plate-forme, vous pouvez entrer ce qui suit à l'invite de la ligne de commande :

```
keytool -import -alias trustedroot -file self-signed_certificate_name -keystore
filename -storepass keystorepass
```

Donnez au fichier le nom de votre choix. Par exemple, `rdev_keystore`.

Création d'un fichier Keystore sous Linux

Dans les environnements Linux, utilisez le fichier `create_keystore` qui est un script shell qui appelle l'utilitaire Keytool. Le fichier est installé avec rdxml situé par défaut dans le répertoire répertoire_installation`/dirxml/bin`. Le fichier create_keystore est également inclus dans le fichier `dirxml_jremote.tar.gz`, situé dans le répertoire `\dirxml\java_remoteloader`.

Entrez la commande suivante sur la ligne de commande :

```
create_keystore self-signed_certificate_name keystorename
```

Par exemple, saisissez une des commandes suivantes :

```
create_keystore tree-root.b64 mystore
create_keystore tree-root.der mystore
```

Le script `create_keystore` spécifie un mot de passe codé en dur de « dirxml », pour le mot de passe Keystore. Cela ne pose pas de risque de sécurité ; en effet, seuls un certificat public et une clé publique sont mémorisés dans le keystore.

11.3.2 Présentation des paramètres de configuration du chargeur distant

Pour que le chargeur distant fonctionne avec une instance de pilote qui héberge un module d'interface d'application Identity Manager, vous devez configurer l'instance de pilote. Par exemple, vous devez spécifier les paramètres de connexion et du port de l'instance. Vous pouvez spécifier les paramètres à partir de la ligne de commande dans un fichier de configuration. Une fois l'instance en

cours d'exécution, vous pouvez utiliser la ligne de commande pour modifier les paramètres de configuration ou demander au chargeur distant d'exécuter une fonction. Par exemple, vous pouvez choisir d'ouvrir la fenêtre de trace ou de décharger le chargeur distant.

Cette section fournit des informations sur les paramètres de configuration. L'explication indique si un paramètre peut être envoyé à partir de la ligne de commande pour mettre à jour le chargeur distant pendant que l'instance est en cours d'exécution.

Pour plus d'informations sur la configuration d'une nouvelle instance de pilote, reportez-vous à la Section 11.3.3, « Configuration du chargeur distant pour les instances de pilote », page 130.

Paramètres de configuration des instances de pilote dans le chargeur distant

Vous pouvez configurer une instance de pilote à partir de la ligne de commande ou dans un fichier de configuration. NetIQ fournit un exemple de fichier `config8000.txt` pour vous aider à configurer le chargeur distant et les pilotes à utiliser avec votre module d'interface d'application. Le fichier exemple se trouve par défaut dans le répertoire `/opt/novell/dirxml/doc`. Par exemple, le fichier de configuration peut contenir les lignes suivantes :

```
-commandport 8000
-connection "port=8090 rootfile=/dirxmlremote/root.pem"
-module $DXML_HOME/dirxmlremote/libcskeldrv.so.0.0.0
-trace 3
```

Utilisez les paramètres suivants :

-description *valeur* (-desc *valeur*)

(Facultatif) Indique une brève description au format de chaîne, par exemple, SAP, que l'application utilise pour le titre de la fenêtre de trace et pour la consignation de l'audit. Par exemple :

```
-description SAP
```

```
-desc SAP
```

-class *nom* (-cl *nom*)

(Conditionnel) Lorsque vous utilisez un pilote Java, spécifie le nom de la classe Java du module d'interface d'application Identity Manager à héberger. Cette option indique à l'application d'utiliser un fichier Keystore Java pour lire les certificats. Par exemple :

```
-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim
```

REMARQUE

- Vous ne pouvez pas utiliser cette option si vous spécifiez une option `-module`.
- Si vous utilisez une `tabulation` comme séparateur dans l'option `-class`, le chargeur distant ne démarre pas automatiquement. À la place, vous devez le démarrer manuellement. Pour que le chargeur distant démarre correctement, vous pouvez utiliser un espace au lieu d'une `tabulation`.
- Pour plus d'informations sur les noms que vous pouvez spécifier pour cette option, reportez-vous à la section « Présentation des noms du paramètre -class Java » page 129.

-commandport *numéro_port* (-cp *numéro_port*)

Spécifie le port TCP/IP utilisé par l'instance de pilote à des fins de contrôle. Par exemple, `-commandport 8001` ou `-cp 8001`. La valeur par défaut est 8000.

Pour utiliser plusieurs instances de pilote avec le chargeur distant sur le même serveur, spécifiez des ports de connexion et de commande différents pour chaque instance.

Si l'instance de pilote héberge un module d'interface d'application, le port utilisé par la commande est celui sur lequel une autre instance communique avec l'instance qui héberge le module d'interface. Si l'instance de pilote envoie une commande à une instance qui héberge un module d'interface d'application, le port utilisé par la commande est celui sur lequel écoute l'instance d'hébergement.

Lorsque vous envoyez ce paramètre à partir de la ligne de commande à une instance qui héberge un module d'interface d'application, le port utilisé par la commande est celui sur lequel écoute l'instance d'hébergement. Vous pouvez envoyer cette commande lorsque le chargeur distant est en cours d'exécution.

-config *nom_fichier*

Spécifie un fichier de configuration pour l'instance de pilote. Par exemple :

```
-config config.txt
```

Le fichier de configuration peut contenir toutes les options de ligne de commande à l'exception de `-config`. Les options spécifiées sur la ligne de commande remplacent celles spécifiées dans le fichier de configuration.

Vous pouvez envoyer cette commande lorsque le chargeur distant est en cours d'exécution.

-connection *"paramètres"* (-conn *"paramètres"*)

Indique les paramètres de connexion au serveur qui héberge le moteur Identity Manager qui exécute le module d'interface distant Identity Manager. La méthode de connexion par défaut est TCP/IP avec SSL.

Pour utiliser plusieurs instances de pilote avec le chargeur distant sur le même serveur, spécifiez des ports de connexion et de commande différents pour chaque instance.

Entrez les paramètres de connexion en utilisant la syntaxe suivante :

```
-connection "parameter parameter parameter"
```

Par exemple :

```
-connection "port=8091 fromaddress=198.51.100.0 rootfile=server1.pem
keystore=ca.pem localaddress=198.51.100.0 hostname=198.51.100.0 kmo=remote
driver cert"
```

Utilisez les paramètres suivants pour spécifier les paramètres d'une connexion TCP/IP :

address=*adresse_IP*

(Facutlatif) Spécifie si le chargeur distant écoute sur une adresse IP locale spécifique. Cette information est utile si le serveur qui héberge le chargeur distant possède plusieurs adresses IP et si ce dernier doit utiliser une seule adresse. Les valeurs suivantes peuvent être utilisées :

- `address=address number`
- `address='localhost'`

Par exemple :

```
address=198.51.100.0
```

Si vous ne spécifiez aucune valeur, le chargeur distant écoute sur toutes les adresses IP locales.

fromaddress=*adresse_IP*

Indique le serveur à partir duquel le chargeur distant accepte les connexions. L'application ignore les connexions si elles proviennent d'autres adresses. Indiquez une adresse IP ou le nom DNS du serveur. Par exemple :

```
fromaddress=198.51.100.0
```

```
fromaddress=testserver1.company.com
```

handshaketimeout=*millisecondes*

(Conditionnel) Se produit lors d'un timeout de la reconnaissance mutuelle pour les connexions généralement valides de la part du moteur Identity Manager. Spécifie le délai d'attente (en millisecondes) pour la reconnaissance mutuelle entre le chargeur distant et le moteur Identity Manager. Par exemple :

```
handshaketimeout=1000
```

Vous pouvez indiquer un nombre entier supérieur ou égal à zéro. La valeur zéro signifie que la connexion n'expire jamais. La valeur par défaut est de 1000 millisecondes.

hostname=*serveur*

Spécifie l'adresse IP ou le nom du serveur sur lequel le chargeur distant s'exécute. Par exemple :

```
hostname=198.51.100.0
```

secureprotocol=*version de TLS*

Indique la version du protocole TLS utilisée par le chargeur distant pour se connecter au moteur Identity Manager. Par exemple :

```
secureprotocol=TLSv1_2
```

Identity Manager prend en charge TLSv1 et TLSv1_2. Par défaut, le chargeur distant utilise TLSv1_2. Pour utiliser TLSv1, spécifiez cette version dans le paramètre.

enforceSuiteB=*true/false*

(Conditionnel) S'applique uniquement lorsque vous voulez que le chargeur distant communique avec le moteur Identity Manager à l'aide d'algorithmes de chiffrement Suite B.

Pour utiliser Suite B pour la communication, spécifiez `true`. Cette communication est prise en charge uniquement avec le protocole TLS 1.2.

Si vous essayez de connecter un moteur pour lequel Suite B est activé à un chargeur distant qui ne prend pas en charge TLS 1.2, la reconnaissance mutuelle échoue et la communication n'est pas établie. Par exemple, un chargeur distant 4.5.3, qui ne prend pas en charge TLS 1.2.

useMutualAuth=*true/false*

(Conditionnel) S'applique uniquement lorsque vous voulez que le chargeur distant et le moteur Identity Manager s'authentifient mutuellement en vérifiant le certificat de clé publique ou le certificat numérique émis par les autorités de certification approuvées ou les certificats auto-signés. Par exemple :

```
useMutualAuth=true
```

keystore=*nom_fichier*

Spécifie le nom du fichier Keystore Java qui contient le certificat de racine approuvée de l'émetteur du certificat utilisé par le module d'interface distant. Par exemple :

```
keystore=keystore filename
```

Il s'agit en général de l'autorité de certification de l'arborescence qui héberge le module d'interface distant.

kmo=*nom*

Indique le nom clé de l'objet Matériel clé qui contient les clés et le certificat utilisés pour les connexions SSL. Par exemple :

```
kmo=remote driver cert
```

localaddress=*adresse_IP*

Indique l'adresse IP à laquelle vous souhaitez lier le socket pour une connexion client. Par exemple :

```
localaddress=198.51.100.0
```

port=*numéro_port*

Spécifie le port TCP/IP sur lequel le chargeur distant écoute des connexions à partir du module d'interface distant. Pour spécifier le numéro de port par défaut, entrez `port=8090`.

rootfile=*nom_cert_approuvé*

Spécifie le nom du fichier qui contient le certificat de racine approuvée de l'émetteur du certificat utilisé par le module d'interface distant. Le fichier de certificat doit être au format Base 64 (PEM). Par exemple :

```
rootfile=trustedcert
```

Il s'agit en général de l'autorité de certification de l'arborescence qui héberge le module d'interface distant.

storepass=*mot_de_passe*

Spécifie le mot de passe du fichier Keystore Java que vous avez indiqué pour le paramètre `keystore`. Par exemple :

```
storepass=mypassword
```

Pour que le chargeur distant communique avec un pilote Java, spécifiez une paire clé-valeur en utilisant la syntaxe suivante :

```
keystore=keystorename storepass=password
```

-datadir *répertoire* (-dd *répertoire*)

Indique le répertoire qui contient les fichiers de données utilisés par le chargeur distant. Par exemple :

```
-datadir /var/opt/novell/dirxml/rdxml/data
```

Lorsque vous utilisez cette commande, le processus `rdxml` change de répertoire pour utiliser le répertoire spécifié. Les fichiers de trace et les autres fichiers pour lesquels aucun chemin n'est explicitement spécifié sont créés dans le répertoire des données.

-help (- h)

Indique à l'application d'afficher l'aide.

-java (- j)

(Conditionnel) Indique que vous souhaitez définir des mots de passe pour une instance de module d'interface pilote Java.

REMARQUE : utilisez cette option conjointement avec l'option `-setpasswords` lorsque vous n'indiquez pas non plus de valeur`-class`.

-javadebugport *numéro_port* (-jdp *numéro_port*)

Indique à l'instance d'activer le débogage Java sur le port spécifié. Par exemple :

```
-javadebugport 8080
```

Utilisez cette commande lorsque vous développez des modules d'interface d'application Identity Manager. Vous pouvez envoyer cette commande lorsque le chargeur distant est en cours d'exécution.

-javaparam *paramètres* (-jp *paramètres*)

Indique les paramètres de l'environnement Java. Entrez les paramètres d'environnement Java en utilisant la syntaxe suivante :

```
-javaparam parameter
-jp parameter
-jp parameter
```

REMARQUE : n'utilisez pas ce paramètre avec le chargeur distant Java.

Pour spécifier plusieurs valeurs pour un seul paramètre, placez le paramètre entre guillemets. Par exemple :

```
-javaparam DHOST_JVM_MAX_HEAP=512M
-jp DHOST_JVM_MAX_HEAP=512M
-jp "DHOST_JVM_OPTIONS=-Dfile.encoding=utf-8 -Duser.language=en"
```

Utilisez les paramètres suivants pour configurer l'environnement Java :

DHOST_JVM_ADD_CLASSPATH

Spécifie d'autres chemins dans lesquels la machine virtuelle Java peut rechercher des fichiers de paquetage (`.jar`) et de classe (`.class`). Pour spécifier plusieurs chemins de classe pour une machine virtuelle Java Linux, insérez le caractère deux-points entre chaque chemin.

DHOST_JVM_INITIAL_HEAP

Indique la taille initiale (minimale) des segments de mémoire de la machine virtuelle Java en nombres d'octets au format décimal. Utilisez une valeur numérique suivie de G, M ou K pour représenter le type d'octet. Par exemple :

```
100M
```

Si vous ne précisez pas le type d'octet, la taille par défaut utilise les octets. Ce paramètre équivaut à la commande Java `-Xms`.

Il est prioritaire par rapport à l'option d'attribut Ensemble de pilotes. L'augmentation de la taille initiale des segments de mémoire peut réduire le temps de démarrage et améliorer le débit.

DHOST_JVM_MAX_HEAP

Indique la taille maximale des segments de mémoire de la machine virtuelle Java en nombres d'octets au format décimal. Utilisez une valeur numérique suivie de G, M ou K pour représenter le type d'octet. Par exemple :

```
100M
```

Si vous ne précisez pas le type d'octet, la taille par défaut utilise les octets.

Il est prioritaire par rapport à l'option d'attribut Ensemble de pilotes.

DHOST_JVM_OPTIONS

Indique les arguments que vous souhaitez utiliser lors du démarrage de l'instance JVM du pilote. Utilisez un espace pour séparer chaque chaîne d'option. Par exemple :

```
-Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
```

L'option d'attribut Ensemble de pilotes est prioritaire par rapport à ce paramètre. Cette variable d'environnement est ajoutée au bas de la liste des pilotes. Pour plus d'informations sur les options valides, reportez-vous à la documentation de JVM.

-password *valeur* (-p *valeur*)

Spécifie le mot de passe de l'instance de pilote lorsque vous émettez des commandes qui affectent le fonctionnement de l'instance ou modifient les paramètres. Vous devez indiquer le même mot de passe que celui spécifié dans setpasswords pour l'instance que vous souhaitez commander. Par exemple :

```
-password netiq4
```

Si vous n'envoyez pas le mot de passe avec vos commandes, l'instance de pilote vous invite à le saisir.

Vous pouvez envoyer cette commande lorsque le chargeur distant est en cours d'exécution.

-piddir *répertoire* (-pd *répertoire*)

Indique le chemin d'accès au répertoire du fichier d'ID de processus (pidfile) utilisé par le processus du chargeur distant. Par exemple :

```
-piddir /var/opt/novell/dirxml/rdxml/data
```

Le fichier pidfile est initialement destiné à être utilisé par les scripts d'initialisation SysV-style. La valeur par défaut est `/var/run`. Sinon, la valeur par défaut peut également être le répertoire actuel, si le chargeur distant est exécuté par un utilisateur ne disposant pas des droits suffisants pour ouvrir le fichier pidfile pour lecture et écriture à l'emplacement `/var/run`.

Ce paramètre est similaire à `-datadir`.

-setpasswords *mot_de_passe_chargeur_distant mot_de_passe_facultatif* (-sp *mot_de_passe_chargeur_distant mot_de_passe_facultatif*)

Spécifie le mot de passe de l'instance de pilote et celui de l'objet Pilote Identity Manager du module d'interface distant avec lequel le chargeur distant communique.

Il n'est pas nécessaire de spécifier de mot de passe. En revanche, le chargeur distant vous invite à fournir les mots de passe. Toutefois, si vous spécifiez le mot de passe du chargeur distant, vous devez également indiquer le mot de passe de l'objet Pilote Identity Manager associé au module d'interface distant sur le serveur du moteur Identity Manager. Pour spécifier les mots de passe, utilisez la syntaxe suivante :

```
-setpasswords Remote_Loader_password driver_object_password
```

Par exemple :

```
-setpasswords netiq4 idmobject6
```

REMARQUE : cette option permet de configurer l'instance de pilote à l'aide des mots de passe spécifiés, mais ne permet pas de charger un module d'interface d'application ni de communiquer avec une autre instance.

Paramètres des fichiers de trace

(Conditionnel) Lors de l'hébergement d'un module d'interface d'application Identity Manager, vous devez définir les paramètres d'un fichier de trace contenant les messages d'information envoyés par le chargeur distant et le pilote pour cette instance.

Ajoutez les paramètres suivants au fichier de configuration :

-trace *entier* (-t *entier*)

Spécifie le niveau des messages que vous voulez afficher dans une fenêtre de trace. Par exemple :

```
-trace 3
```

Les niveaux de trace du chargeur distant correspondent à ceux utilisés sur le serveur qui héberge le moteur Identity Manager.

-tracefile *chemin_fichier* (-tf *chemin_fichier*)

Indique le chemin d'accès au fichier dans lequel les messages de trace sont consignés. Vous devez spécifier un fichier de trace par instance de pilote s'exécutant sur un ordinateur spécifique. Par exemple :

```
-tracefile /home/trace.txt
```

L'application consigne des messages dans le fichier si le paramètre `-trace` est supérieur à zéro. La fenêtre de trace ne doit pas nécessairement être ouverte pour que les messages soient consignés dans le fichier.

-tracefilemax *taille* (-tf *taille*)

Indique une limite à la taille pour le fichier de trace de cette instance. Spécifiez la valeur en kilo-octets, méga-octets, giga-octets ou, à l'aide de l'abréviation correspondant au type d'octet. Par exemple :

- `-tracefilemax 1000K`
- `-tf 100M`
- `-tf 10G`

REMARQUE

- Si la taille des données du fichier de trace est supérieure au maximum spécifié lorsque le chargeur distant est démarré, les données du fichier de trace restent supérieures au maximum spécifié jusqu'à ce que la purge soit terminée sur les 10 fichiers.
- Lorsque vous ajoutez cette option dans le fichier de configuration, l'application utilise le nom spécifié pour le fichier de trace et jusqu'à 9 fichiers « roll-over ». Ces fichiers sont nommés en utilisant la base du nom de fichier de trace principal plus “_n, où n peut être un chiffre de 1 à 9.

-tracechange *entier* (-tc *entier*)

(Conditionnel) Lorsqu'une instance de pilote existante héberge un module d'interface d'application, cette commande permet de définir un nouveau niveau de messages d'information. Les niveaux de trace correspondent à ceux utilisés sur le serveur Identity Manager. Par exemple :

```
-trace 3
```

Vous pouvez envoyer cette commande lorsque le chargeur distant est en cours d'exécution.

-tracefilechange *chemin_fichier* (-tfc *chemin_fichier*)

(Conditionnel) Lorsqu'une instance de pilote existante héberge un module d'interface d'application, cette commande indique à l'instance d'utiliser un fichier de trace ou de fermer un fichier en cours d'utilisation et d'utiliser ce nouveau fichier à la place. Par exemple :

```
-tracefilechange \temp\newtrace.txt
```

Vous pouvez envoyer cette commande lorsque le chargeur distant est en cours d'exécution.

Paramètres de mot de passe de certificat

(Conditionnel) Uniquement lorsque `useMutualAuth` est défini sur true (vrai) dans le fichier de configuration.

-keystorepassword (-ksp)

Spécifie le mot de passe Keystore afin d'activer l'authentification mutuelle pour les pilotes du chargeur distant Java uniquement.

-keypassword (-kp)

Spécifie le mot de passe de la clé afin d'activer l'authentification mutuelle pour les pilotes de chargeur distant natif et Java.

-unload (-u)

Donne une instruction de déchargement à l'instance de pilote. Si le chargeur distant s'exécute comme un service Win32, cette commande arrête le service.

Vous pouvez envoyer cette commande lorsque le chargeur distant est en cours d'exécution.

Présentation des noms du paramètre -class Java

Lorsque vous utilisez le paramètre `-class` pour configurer une instance de pilote pour le chargeur distant et le chargeur distant Java, vous devez spécifier le nom de la classe Java du module d'interface d'application Identity Manager à héberger.

Nom de la classe Java	Pilote
com.novell.nds.dirxml.driver.dcsshim.DCSShim	Pilote du service de collecte de données
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Pilote pour fichier texte délimité
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	Pilote pour Remedy ARS
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	Pilote du service de droits
com.novell.gw.dirxml.driver.rest.shim.GWdriverShim	Pilote GroupWise 2014
com.novell.idm.drivers.idprovider.IDProviderShim	Pilote du fournisseur d'ID
com.novell.nds.dirxml.driver.jdbc.JDBCDriverShim	Pilote JDBC

Nom de la classe Java	Pilote
com.novell.nds.dirxml.driver.jms.JMSDriverShim	Pilote JMS
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	Pilote LDAP
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	Pilote de service de boucle
com.novell.nds.dirxml.driver.ebs.user.EBSUserDriver	Pilote Oracle User Management
com.novell.nds.dirxml.driver.ebs.hr.EBSHRDriver	Pilote Oracle HR
com.novell.nds.dirxml.driver.ebs.tca.EBSTCADriver	Pilote Oracle TCA
com.novell.nds.dirxml.driver.msgateway.MSGatewayDriverShim	Pilote de passerelle système gérée
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	Pilote de tâches manuelles
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	Pilote NIS
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Pilote Notes
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	Pilote PeopleSoft
com.netiq.nds.dirxml.driver.pum.PUMDriverShim	Pilote de gestion des utilisateurs privilégiés
com.novell.nds.dirxml.driver.salesforce.SFDriverShim	Pilote SalesForce
com.novell.nds.dirxml.driver.SAPHRShim.SAPDriverShim	Pilote SAP HR
com.novell.nds.dirxml.driver.sap.portal.SAPPortalShim	Pilote SAP Portal
com.novell.nds.dirxml.driver.sapumshim.SAPDriverShim	Pilote de gestion des utilisateurs SAP
com.novell.nds.dirxml.driver.soap.SOAPDriver	Pilote SOAP
com.novell.idm.driver.ComposerDriverShim	Application utilisateur
com.novell.nds.dirxml.driver.workorder.WorkOrderDriverShim	Pilote WorkOrder

11.3.3 Configuration du chargeur distant pour les instances de pilote

Le chargeur distant peut héberger les modules d'interface d'application Identity Manager contenus dans les fichiers `.dll`, `.so` ou `.jar`. Pour que le chargeur distant s'exécute sur un ordinateur Linux, l'application a besoin d'un fichier de configuration comme `LDAPShim.txt` pour chaque instance de pilote. Vous pouvez également créer ou modifier un fichier de configuration à l'aide des options de ligne de commande.

Par défaut, le chargeur distant se connecte au moteur Identity Manager via TCP/IP en utilisant les protocoles TLS/SSL. Le port 8090 est utilisé comme port TCP/IP par défaut pour cette connexion. Vous pouvez exécuter plusieurs instances de pilote avec le chargeur distant sur le même serveur. Chaque instance héberge une instance du module d'interface d'application Identity Manager. Pour utiliser plusieurs instances du chargeur distant sur le même serveur, spécifiez des ports de connexion et des ports de commande différents pour chaque instance.

REMARQUE

- Le fichier de configuration peut contenir toutes les options de ligne de commande à l'exception de `-config`.

- Lorsque vous ajoutez des paramètres au fichier de configuration, vous pouvez utiliser la forme longue ou abrégée de ce paramètre. Par exemple, `-description` ou `-desc`.
- La procédure suivante décrit d'abord la forme longue suivie par la courte entre parenthèses. Par exemple `-description` *`valeur`* (`-desc` *`valeur`*).
- Pour plus d'informations sur les paramètres mentionnés dans cette section, reportez-vous à la « Présentation des paramètres de configuration du chargeur distant » page 121.

Pour créer un fichier de configuration :

1. Dans un éditeur de texte, créez un fichier.

   NetIQ fournit un exemple de fichier `config8000.txt` pour vous aider à configurer le chargeur distant et les pilotes à utiliser avec votre module d'interface d'application. Le fichier exemple se trouve par défaut dans le répertoire `/opt/novell/dirxml/doc`.

2. Ajoutez les paramètres de configuration suivants au fichier :
   - -description (facultative)
   - -commandport
   - Paramètres de connexion :
     - port (obligatoire)
     - address
     - fromaddress
     - handshaketimeout
     - rootfile
     - keystore
     - localaddress
     - hostname
     - kmo
     - secureprotocol
     - enforceSuiteB
     - useMutualAuth
   - Paramètres des fichiers de trace (facultatifs) :
     - -trace
     - -tracefile
     - -tracefilemax
   - -javaparam
   - -class ou -module

   Pour plus d'informations sur la spécification des valeurs de ces paramètres, reportez-vous à la Section 11.3.2, « Présentation des paramètres de configuration du chargeur distant », page 121.

3. Enregistrez le fichier.

   Pour que le chargeur distant démarre automatiquement au démarrage de l'ordinateur, enregistrez le fichier dans le répertoire `/etc/opt/novell/dirxml/rdxml`.

11.3.4 Configuration du chargeur distant Java pour les instances de pilote

Le chargeur distant Java héberge les modules d'interface pilote Java. Il ne charge ou n'héberge aucun module d'interface pilote (C++) natif.

Pour configurer une nouvelle instance du chargeur distant Java sur des plates-formes Linux, procédez comme suit. Pour plus d'informations sur les paramètres mentionnés dans cette section, reportez-vous à la « Présentation des paramètres de configuration du chargeur distant » page 121.

1. Dans un éditeur de texte, créez un fichier.

   NetIQ fournit un exemple de fichier `config8000.txt` pour vous aider à configurer le chargeur distant et les pilotes à utiliser avec votre module d'interface d'application. Le fichier exemple se trouve par défaut dans le répertoire `/opt/novell/dirxml/doc`.
2. Ajoutez les paramètres suivants au nouveau fichier de configuration :
   - -description (facultative)
   - -class ou -module

     Par exemple, `-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim`
   - -commandport
   - Paramètres de connexion :
     - port (obligatoire)
     - address
     - fromaddress
     - handshaketimeout
     - rootfile
     - keystore
     - localaddress
     - hostname
     - kmo
     - secureprotocol
     - enforceSuiteB
     - useMutualAuth
   - -java (conditionnel)
   - -javadebugport
   - -password
   - -service
   - -keypassword
   - -keystorepassword (uniquement pour les pilotes Java)
   - Paramètres des fichiers de trace (facultatifs) :
     - -trace
     - -tracefile
     - -tracefilemax
3. Enregistrez le nouveau fichier de configuration.

Pour que le chargeur distant s'exécute automatiquement au démarrage de l'ordinateur, enregistrez le fichier dans le répertoire `/etc/opt/novell/dirxml/jremote`.

4 Ouvrez une invite de commande.

5 À l'invite, entrez `-config` *`nom_fichier`*, où *nom_fichier* est le nom du nouveau fichier de configuration. Par exemple :

```
dirxml_jremote -config filename
```

11.3.5 Configuration des pilotes Identity Manager pour fonctionner avec le chargeur distant

Vous pouvez configurer un nouveau pilote ou activer un pilote existant pour qu'il communique avec le chargeur distant. Vous devez configurer un module d'interface d'application Identity Manager à utiliser avec le chargeur distant.

REMARQUE : vous trouverez dans cette section des informations générales sur la configuration des pilotes pour qu'ils communiquent avec le chargeur distant. Pour des informations spécifiques au pilote, reportez-vous au guide d'implémentation du pilote correspondant sur le site Web de la documentation des pilotes Identity Manager.

Pour ajouter ou modifier un objet Pilote dans Designer ou iManager, vous devez configurer des paramètres qui activent l'instance de pilote pour le chargeur distant. Pour plus d'informations sur les paramètres mentionnés dans cette section, reportez-vous à la « Présentation des paramètres de configuration du chargeur distant » page 121.

1 Dans **Présentation**, sélectionnez l'objet Pilote Identity Manager.

2 Dans les propriétés de l'objet Pilote, procédez comme suit :

2a Dans le champ **Module pilote**, sélectionnez **Se connecter au chargeur distant**.

2b Dans le champ **Mot de passe de l'objet Pilote**, spécifiez le mot de passe que le chargeur distant utilise pour s'authentifier auprès du serveur du moteur Identity Manager.

Ce mot de passe doit correspondre à celui de l'objet Pilote défini dans le chargeur distant.

2c Dans le champ **Paramètres de connexion au chargeur distant**, spécifiez les informations requises pour la connexion au chargeur distant. Utilisez la syntaxe suivante.

```
hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename
localaddress=xxx.xxx.xxx.xxx
```

où

hostname

Indique l'adresse IP du serveur qui héberge le chargeur distant. Par exemple, `hostname=192.168.0.1`.

port

Indique le port sur lequel le chargeur distant écoute. La valeur par défaut est 8090.

kmo

Indique le nom clé de l'objet Matériel clé qui contient les clés et le certificat utilisés pour les connexions SSL. Par exemple, `kmo=remotecert`.

localaddress

Spécifie l'adresse IP source si plusieurs adresses IP sont configurées sur le serveur qui héberge le moteur Identity Manager.

2d Dans le champ **Mot de passe du chargeur distant**, spécifiez le mot de passe que le moteur Identity Manager (ou le module d'interface du chargeur distant) utilise pour s'authentifier auprès du chargeur distant.

3 Définissez un utilisateur dont le niveau de sécurité est équivalent.

4 Cliquez sur **Suivant**, puis sur **Terminer**.

11.3.6 Configuration de l'authentification mutuelle avec le moteur Identity Manager

Vous pouvez configurer l'authentification mutuelle pour sécuriser la communication entre le chargeur distant et le moteur Identity Manager. L'authentification mutuelle utilise des certificats pour la reconnaissance mutuelle, au lieu de mots de passe. Le chargeur distant et le moteur Identity Manager s'authentifient mutuellement en échangeant et en validant le certificat de clé publique ou le certificat numérique émis par les autorités de certification approuvées ou les certificats auto-signés. Si l'authentification mutuelle réussit, le chargeur distant s'authentifie auprès du moteur. Le trafic de synchronisation s'effectue une fois que le chargeur distant et le moteur Identity Manager ont établi avec certitude qu'ils communiquent avec une entité autorisée.

Pour configurer l'authentification mutuelle, effectuez les opérations suivantes :

- « Exportation de certificats pour le moteur Identity Manager et le chargeur distant » page 134
- « Activation d'un pilote pour l'authentification mutuelle » page 137

Exportation de certificats pour le moteur Identity Manager et le chargeur distant

Pour que l'authentification mutuelle fonctionne correctement, vous avez besoin d'un certificat de serveur pour le moteur et d'un certificat client pour le chargeur distant. Vous pouvez exporter les certificats à partir d'eDirectory ou les importer depuis un fournisseur tiers. Dans la plupart des cas, vous exporterez simplement un certificat de serveur à partir d'eDirectory. Cela dit, dans certains cas, vous voudrez peut-être exporter un certificat client tiers pour le chargeur distant.

- « Exportation d'un certificat à partir d'eDirectory » page 134
- « Exportation d'un certificat tiers pour le chargeur distant » page 136

Exportation d'un certificat à partir d'eDirectory

Un objet Certificat présent dans le coffre-fort d'identité est appelé KMO (Key Material Object - objet Matériel clé). Cet objet stocke, de façon sécurisée, les données de certificat, notamment la clé publique et la clé privée associées au certificat utilisé pour les connexions SSL. Pour l'authentification mutuelle, vous avez besoin de deux KMO : un pour le moteur et un pour le chargeur distant.

Vous pouvez exporter un KMO existant ou en créer un nouveau, puis l'exporter. La procédure de création d'un KMO côté client et côté serveur est différente.

Création de KMO

Pour créer un KMO côté serveur :

1. Connectez-vous à NetIQ iManager.
2. Dans le volet gauche, cliquez sur **Serveur de certificats NetIQ**, puis sélectionnez certificat de serveur.
3. Sélectionnez le serveur qui doit posséder le certificat que vous avez créé.
4. Spécifiez un surnom pour le certificat. Par exemple, `serverkmo`.
5. Sélectionnez **Standard** comme méthode de création du certificat, puis cliquez sur **Suivant**.
6. Passez en revue le résumé, cliquez sur **Terminer**, puis sur **Fermer**.

Pour créer un KMO côté client :

1. Connectez-vous à NetIQ iManager.
2. Dans le volet gauche, cliquez sur **Serveur de certificats NetIQ**, puis sélectionnez certificat de serveur.
3. Sélectionnez le serveur qui doit posséder le certificat que vous avez créé.
4. Spécifiez un surnom pour le certificat. Par exemple : `clientkmo`
5. Sélectionnez **Personnalisée** comme méthode de création du certificat, puis cliquez sur **Suivant**.
6. Laissez la valeur par défaut pour l'**autorité de certification organisationnelle**, puis cliquez sur **Suivant**.
7. Désélectionnez **Activer l'utilisation de clé étendue**, puis cliquez sur **Suivant**.
8. Acceptez les autres paramètres par défaut du certificat.
9. Passez en revue le résumé, cliquez sur **Terminer**, puis sur **Fermer**.

Exportation de KMO

À partir d'eDirectory, exportez les KMO que le moteur et le chargeur distant vont utiliser pour s'authentifier mutuellement.

Pour exporter le KMO pour le moteur Identity Manager, exécutez l'utilitaire de ligne de commande DirXML (dxcmd) :

```
dxcmd -user <admin DN> -password <password of admin> -exportcerts <kmoname>
<server|client> <java|native|dotnet> <output dir>
```

où

- `user` correspond au nom d'un utilisateur possédant des droits d'administration sur le pilote.
- `password` correspond au mot de passe de l'utilisateur possédant des droits d'administration sur le pilote.
- `exportcerts` exporte les certificats et les clés privées/publiques à partir d'eDirectory. Vous devez indiquer si vous exportez un certificat de serveur ou client, et spécifier le type de pilote qui utilisera le certificat ainsi qu'un dossier de destination dans lequel la commande stockera ces informations.

Par exemple : `dxcmd -user admin.sa.system -password novell -exportcerts serverkmo server java '/home/certs'`

Cette commande génère le fichier `serverkmo_server.ks` dans le répertoire `/home/certs/`. Le mot de passe par défaut du fichier Keystore est `dirxml`.

Lorsque vous exécutez la commande dxcmd afin d'exporter le KMO pour le chargeur distant, tenez compte des aspects suivants :

- L'utilitaire dxcmd s'exécute en mode LDAP. Lorsque vous l'utilisez pour la première fois, il vous demande d'indiquer si vous approuvez le certificat provenant d'eDirectory. En fonction de votre environnement, vous pouvez choisir d'approuver le certificat pour la session en cours uniquement ou pour les sessions en cours et à venir, d'approuver tous les certificats ou de ne pas approuver le certificat.
- Si le chargeur distant s'exécute sur le serveur Identity Manager, exécutez la commande au format LDAP ou à points. Si le chargeur distant est installé sur un serveur distinct, exécutez la commande uniquement au format LDAP.
- Spécifiez le paramètre `-host` dans la commande pour résoudre l'adresse IP ou le nom d'hôte du serveur, afin de pouvoir s'authentifier auprès du serveur Identity Manager.

Exécutez la commande à l'aide de la syntaxe suivante :

```
dxcmd -dnform ldap -host <adresse_IP_hôte> -user <DN_admin> -password
<mot_de_passe_admin> -exportcerts <nom_kmo> <client> <java|native|dotnet>
<rép_sortie>
```

Tableau 11-1 *Exemples de différents types de pilotes*

Types de pilotes	Commande	Sortie
Pilote Java	`dxcmd -dnform ldap -host 192.168.0.1 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client java '/home/certs'`	Fichier `clientkmo_client.ks` dans le répertoire `/home/certs/` Le mot de passe par défaut du fichier Keystore est `dirxml`.

Exportation d'un certificat tiers pour le chargeur distant

Pour utiliser des certificats tiers avec le chargeur distant, vous devez exporter un certificat dans le fichier `.pfx` et un fichier de racine approuvée au format Base64, puis convertir le certificat `.pfx` au format utilisé par le pilote. Par exemple, un pilote natif requiert la clé privée et la clé de certificat au format `.pem`, tandis qu'un pilote Java nécessite que le fichier Keystore soit au format `.jks`.

Pilote Java

Créez un fichier Keystore Java à partir du fichier `.pfx`. Entrez une commande du type `keytool -importkeystore -srckeystore servercert.pfx -srcstoretype pkcs12 -destkeystore servercert.jks -deststoretype JKS`.

Pour terminer, spécifiez les informations correspondant au type de pilote dans le fichier de configuration du chargeur distant. Pour plus d'informations, reportez-vous à la section Activation d'un pilote pour l'authentification mutuelle.

Activation d'un pilote pour l'authentification mutuelle

Pour activer une communication de pilote pour l'authentification mutuelle, vous devez effectuer les opérations suivantes :

- « Configuration d'un pilote à l'aide d'un KMO ou d'un fichier Keystore » page 137
- « Configuration du chargeur distant pour les instances de pilote » page 139

Configuration d'un pilote à l'aide d'un KMO ou d'un fichier Keystore

Vous pouvez configurer le pilote à l'aide d'un KMO ou d'un fichier Keystore dans Designer ou iManager.

Dans Designer, vous pouvez configurer le pilote lors de sa création initiale ou après l'avoir créé.

Pour configurer un pilote dans Designer :

1. Ouvrez votre projet dans Designer.
2. Dans la palette de la vue Modélisateur, sélectionnez le pilote que vous souhaitez créer.
3. Faites glisser l'icône du pilote dans la vue Modélisateur.
4. Suivez les étapes de l'assistant d'installation.
5. Dans la fenêtre relative au chargeur distant, sélectionnez **oui**.
   - 5a **Nom d'hôte :** spécifiez le nom d'hôte ou l'adresse IP du serveur sur lequel s'exécute le service de chargeur distant du pilote. Par exemple, entrez hostname=192.168.0.1. Si vous ne spécifiez aucune valeur pour ce paramètre, il est défini par défaut sur localhost.
   - 5b **Port :** spécifiez le numéro du port sur lequel le chargeur distant est installé et s'exécute pour ce pilote. Le numéro de port par défaut est 8090.
   - 5c **KMO :** spécifiez le nom de clé ou le KMO contenant les clés et le certificat utilisés par le chargeur distant pour une connexion SSL. Par exemple, entrez kmo=`serverkmo`. Si vous configurez l'authentification mutuelle à l'aide du KMO, vous devez spécifier une valeur pour ce paramètre. Vous devez également spécifier une valeur pour le paramètre **Root File** (fichier racine) dans la section Autres paramètres.
   - 5d **Autres paramètres :** définissez les paramètres du chargeur distant que vous souhaitez utiliser. Ces paramètres incluent les informations relatives à la communication d'authentification mutuelle. Tous les paramètres définis doivent être spécifiés au format de paire clé-valeur suivant : `paraName1=paraValue1 paraName2=paraValue2`

     Par exemple, pour keystore, utilisez la syntaxe suivante :

     ```
     UseMutualAuth=true keystore='/home/certs/serverkmo_server.ks'
     storepass='dirxml' keypass='dirxml' key='serverkmo'
     ```

     Par exemple, pour kmo, utilisez la syntaxe suivante :

     ```
     useMutualAuth=true rootFile='/home/cacert.b64'
     ```

   - 5e **Mot de passe distant :** Spécifiez le mot de passe du chargeur distant.
   - 5f **Mot de passe du pilote :** spécifiez le mot de passe du pilote.
6. Cliquez sur **Suivant**.
7. Suivez les autres instructions de l'assistant jusqu'à ce que l'installation du pilote soit terminée.
8. Passez en revue le résumé des opérations qui seront effectuées pour créer le pilote, puis cliquez sur **Terminer**.

Vous pouvez également configurer le pilote après sa création, en procédant comme suit :

1. Dans la vue Mode plan de Designer, cliquez avec le bouton droit sur le pilote.
2. Sélectionnez **Propriétés**.
3. Dans le volet de navigation, sélectionnez **Configuration du pilote**.
4. Sélectionnez **Authentification**.
5. Dans la section **Authentification du chargeur distant**, spécifiez les informations requises pour configurer l'authentification mutuelle entre le chargeur distant et le moteur Identity Manager.

   Utilisez la syntaxe suivante pour kmo :

   ```
   hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true kmo=certificatename
   rootFile=<absolute path to the file>
   ```

   Par exemple :

   ```
   hostname=192.168.0.1 port=8090 useMutualAuth=true kmo=serverkmo rootFile='/
   home/cacert.b64'
   ```

   Utilisez la syntaxe suivante pour keystore :

   ```
   hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true keystore=<absolute path
   to the keystore file> storepass=<keystore password> key=<alias name> keypass=
   <password for the key>
   ```

   Par exemple :

   ```
   hostname=192.168.0.1 port=8097 useMutualAuth=true keystore='/home/certs/
   serverkmo_server.ks' storepass='dirxml' key='serverkmo' keypass='dirxml'
   ```

Pour modifier la configuration dans iManager :

1. Lancez iManager.
2. Dans Présentation, sélectionnez l'objet Pilote Identity Manager.
3. Dans les propriétés de l'objet Pilote, procédez comme suit :
   - **3a** Dans le champ **Module pilote**, sélectionnez **Se connecter au chargeur distant**.
   - **3b** Dans le champ **Mot de passe de l'objet Pilote**, spécifiez le mot de passe utilisé par le chargeur distant pour s'authentifier auprès du moteur.

     Ce mot de passe doit correspondre à celui de l'objet Pilote défini dans le chargeur distant.
   - **3c** Dans le champ **Paramètres de connexion au chargeur distant**, spécifiez les informations requises pour la connexion au chargeur distant.

     Utilisez la syntaxe suivante pour kmo :

     ```
     hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true kmo=certificatename
     rootFile=<absolute path to the file>
     ```

     Par exemple :

     ```
     hostname=192.168.0.1 port=8090 useMutualAuth=true kmo=serverkmo rootFile='/
     home/cacert.b64'
     ```

     Utilisez la syntaxe suivante pour keystore :

     ```
     hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true keystore=<absolute
     path to the keystore file> storepass=<keystore password> key=<alias name>
     keypass= <password for the key>
     ```

     Par exemple :

```
hostname=192.168.0.1 port=8097 useMutualAuth=true keystore='/home/certs/
serverkmo_server.ks' storepass='dirxml' key='serverkmo' keypass='dirxml'
```

3d (Facultatif) Dans le champ **Mot de passe du chargeur distant**, spécifiez le mot de passe que le moteur Identity Manager (ou le module d'interface du chargeur distant) utilise pour s'authentifier auprès du chargeur distant.

3e Cliquez sur **Appliquer**, puis sur **OK**.

Configuration du chargeur distant pour les instances de pilote

Vous devez configurer l'instance de pilote dans le fichier de configuration du chargeur distant. Veillez à spécifier le chemin d'accès absolu au répertoire contenant le fichier de clé, le fichier de certificat et le fichier de racine inclus dans le fichier de configuration du chargeur distant pour un pilote.

Modifiez le fichier de configuration du chargeur distant pour un pilote afin d'inclure le contenu permettant d'activer l'authentification mutuelle. Le fichier se trouve dans le répertoire`/opt/novell/dirxml/doc`.

Pour modifier la configuration :

1. Connectez-vous au serveur sur lequel vous avez installé le pilote et le chargeur distant.
2. Arrêtez le chargeur distant.

   Par exemple, entrez la commande suivante :

   ```
   rdxml -config /home/drivershim.conf -u
   ```

3. Spécifiez le mot de passe Keystore ou de clé en fonction du type de chargeur distant :

   Chargeur distant Java :

   spécifiez la combinaison du mot de passe Keystore et du mot de passe de la clé à l'aide de la syntaxe suivante :

   ```
   dirxml_jremote -config /home/drivershim.conf -ksp <keystorepassword> -kp
   <keypassword>
   ```

   Exemples :

   ```
   dirxml_jremote -config /home/drivershim.conf -ksp dirxml -kp dirxml
   ```

   Chargeur distant natif :

   spécifiez le mot de passe de la clé à l'aide de la syntaxe suivante :

   ```
   dirxml_jremote -config /home/drivershim.conf -kp <keypassword>
   ```

   Exemples :

   ```
   dirxml_jremote -config /home/drivershim.conf -kp dirxml
   ```

4. Dans un éditeur de texte, ouvrez le fichier de configuration du chargeur distant pour le pilote.
5. Ajoutez au fichier le contenu nécessaire pour activer l'authentification mutuelle.
   - Par exemple, pour un pilote Java, ajoutez cette entrée :

     ```
     -connection "port=8090 useMutualAuth=true keystore='/home/certs/
     clientkmo_client.ks' key='clientkmo'
     ```

- Par exemple, pour un pilote natif, ajoutez cette entrée :

  ```
  -connection "useMutualAuth=true port=8090 rootfile='/home/certs/
  trustedcert.b64' certfile='/home/certs/clientkmo_clientcert.pem'
  keyfile='/home/certs/clientkmo_clientkey.pem' certform=PEM keyform=PEM"
  ```

6. Enregistrez et fermez le fichier.
7. Redémarrez le pilote.

11.3.7 Vérification de la configuration

1. Démarrez le chargeur distant. Par exemple :

   ```
   dirxml_remote -config config.txt
   ```

2. Démarrez le module d'interface distant à l'aide d'iManager.
3. Confirmez que le chargeur distant fonctionne correctement.
4. Arrêtez le chargeur distant. Par exemple :

   ```
   dirxml_remote -config config.txt -u
   ```

11.3.8 Démarrage d'une instance de pilote dans le chargeur distant

Vous pouvez configurer chaque plate-forme pour démarrer automatiquement une instance de pilote au démarrage de l'ordinateur hôte. Vous pouvez également démarrer une instance manuellement.

NetIQ propose deux méthodes pour démarrer une instance de pilote pour le chargeur distant :

- « Démarrage automatique des instances de pilote » page 140
- « Utilisation de la ligne de commande pour démarrer des instances de pilote » page 140

Démarrage automatique des instances de pilote

Vous pouvez configurer une instance de pilote pour le chargeur distant afin qu'il démarre automatiquement au démarrage de l'ordinateur. Placez votre fichier de configuration dans le répertoire `/etc/opt/novell/dirxml/rdxml`.

Utilisation de la ligne de commande pour démarrer des instances de pilote

Le composant binaire `rdxml` prend en charge la fonctionnalité de ligne de commande pour le chargeur distant. Par défaut, ce composant se trouve dans le répertoire `/usr/bin/`.

1. Ouvrez une invite de commande.
2. (Conditionnel) Pour spécifier les mots de passe d'authentification de l'instance de pilote auprès du moteur Identity Manager, entrez l'une des commandes suivantes :
   - **Chargeur distant :** `rdxml -config filename –keystorepassword <mot_de_passe_Keystore> - keypassword <mot_de_passe_clé>`
   - **Chargeur distant Java :** `dirxml_jremote -config filename –keystorepassword <mot_de_passe_Keystore> - keypassword <mot_de_passe_clé>`

3 (Conditionnel) Si l'authentification mutuelle est activée entre l'instance de pilote du chargeur distant et le moteur Identity Manager, entrez une des commandes suivantes pour spécifier les mots de passe de certificat :

- **Chargeur distant :** `rdxml -config filename –keystorepassword <mot_de_passe_Keystore> -keypassword <mot_de_passe_clé>`
- **Chargeur distant Java :** `dirxml_jremote -config filename -keypassword <mot_de_passe_clé>`

4 Pour démarrer l'instance de pilote, entrez la commande suivante :

```
rdxml -config nom_fichier
```

5 Connectez-vous à iManager, puis démarrez le pilote.

6 Confirmez que le chargeur distant fonctionne correctement.

Utilisez la commande `ps` ou un fichier de trace pour savoir si la commande et les ports de connexion écoutent.

Le chargeur distant ne charge le module d'interface d'application Identity Manager que lorsqu'il communique avec le module d'interface distant sur le serveur du moteur Identity Manager. Cela signifie notamment que le module d'interface d'application se ferme dès que le chargeur distant perd la communication avec le serveur.

11.3.9 Arrêt d'une instance de pilote dans le chargeur distant

Chaque plate-forme dispose d'une méthode distincte pour arrêter une instance de pilote dans le chargeur distant.

REMARQUE

- Si vous exécutez plusieurs instances du chargeur distant, ajoutez l'option `-cp` *port_commande* pour vous assurer que le chargeur distant puisse arrêter l'instance appropriée.
- Lorsque vous arrêtez une instance de pilote, vous devez disposer de droits suffisants ou indiquer le mot de passe du chargeur distant. Vous avez des droits suffisants pour l'arrêter. Vous saisissez un mot de passe, mais vous vous rendez compte qu'il est incorrect. Le chargeur distant s'arrête tout de même, car il n'accepte pas réellement le mot de passe. En fait, il l'ignore puisqu'il est redondant dans ce cas. Si vous exécutez le chargeur distant comme application et non comme service, le mot de passe est utilisé.

Pour arrêter une instance de pilote, procédez comme suit :

Chargeur distant

Entrez la commande `rdxml -config` *`nom_fichier`* `-u`. Par exemple :

```
rdxml -config config.txt -u
```

Chargeur distant Java

Entrez la commande `dirxml_jremote -config` *`nom_fichier`* `-u`. Par exemple :

```
dirxml_jremote -config config.txt -u
```

11.4 Configuration du coffre-fort d'identité pour les applications d'identité

Les applications d'identité doivent être en mesure d'interagir avec les objets contenus dans le coffre-fort d'identité.

Pour améliorer les performances des applications d'identité, l'administrateur eDirectory doit créer des index de valeur pour les attributs manager, ismanager et srvprvUUID. Sans index de valeur sur ces attributs, les performances des applications d'identité peuvent être réduites, en particulier dans les environnements de grappe.

Vous pouvez créer ces index de valeur automatiquement au cours de l'installation en sélectionnant Advanced > Create eDirectory Indexes (Avancé > Créer des index eDirectory) dans l'utilitaire de configuration de RBPM. Pour plus d'informations sur l'utilisation du gestionnaire d'index pour créer des index de valeur, reportez-vous au *Guide d'administration de NetIQ eDirectory*.

11.5 Configuration du pilote d'application utilisateur pour la mise en grappe

Dans un environnement de grappe, vous pouvez utiliser un seul pilote d'application utilisateur avec plusieurs instances de l'application utilisateur. Le pilote stocke diverses informations (telles que la configuration de workflow et les informations sur la grappe) spécifiques de l'application. Vous devez configurer le pilote pour utiliser le nom d'hôte ou l'adresse IP du répartiteur ou de l'équilibreur de charge de la grappe.

1. Connectez-vous à l'instance d'iManager qui gère votre coffre-fort d'identité.
2. Dans le cadre de navigation, sélectionnez **Identity Manager**.
3. Sélectionnez **Présentation d'Identity Manager**.
4. Utilisez la page de recherche pour afficher l'aperçu Identity Manager de l'ensemble de pilotes contenant votre pilote d'application utilisateur.
5. Cliquez sur l'indicateur d'état arrondi du pilote dans l'angle supérieur droit de l'icône du pilote :
6. Sélectionnez **Modifier les propriétés**.
7. Dans **Paramètres du pilote**, définissez la propriété **Hôte** sur le nom d'hôte ou l'adresse IP du répartiteur.
8. Cliquez sur **OK**.

11.6 Configuration des paramètres pour les applications d'identité

L'utilitaire de configuration des applications d'identité vous permet de gérer les paramètres des pilotes de l'application utilisateur et des applications d'identité. Le programme d'installation des applications d'identité invoque une version de cet utilitaire et vous permet ainsi de configurer rapidement les applications. Vous pouvez également modifier la plupart de ces paramètres une fois l'installation terminée.

Le fichier pour l'exécution de l'utilitaire de configuration (`configupdate.sh`) se trouve par défaut dans le répertoire `/opt/netiq/idm/apps/configupdate` :

REMARQUE

- Vous devez exécuter `configudate.sh` uniquement à partir du répertoire `configupdate`. L'exécution de `configupdate.sh` à partir d'un emplacement personnalisé entraîne des échecs.
- dans une grappe, les paramètres de configuration doivent être identiques pour tous les membres de la grappe.

Cette section décrit les paramètres de l'utilitaire de configuration. Les paramètres sont organisés par onglets. Si vous installez Identity Reporting, le processus ajoute des paramètres de création de rapports à l'utilitaire.

11.6.1 Exécution de l'utilitaire de configuration des applications d'identité

1 Dans le fichier `configupdate.sh.properties`, vérifiez que les options suivantes sont configurées correctement :

```
edit_admin="true"

use_console="false"
```

REMARQUE : configurez la valeur du paramètre `-use_console` sur `true` uniquement si vous voulez exécuter l'utilitaire en mode console.

---

2 Enregistrez et fermez `configupdate.sh`.

3 À l'invite de commande, entrez la commande suivante pour exécuter l'utilitaire de configuration :

```
./configupdate.sh
```

REMARQUE : vous devrez peut-être attendre quelques minutes pour que l'utilitaire démarre.

11.6.2 Paramètres de l'application utilisateur

Lors de la configuration des applications d'identité, cet onglet permet de définir les valeurs utilisées par les applications pour communiquer avec le coffre-fort d'identité. Certains paramètres sont requis pour terminer la procédure d'installation.

Par défaut, l'onglet affiche les options de base. Pour afficher tous les paramètres, cliquez sur **Afficher les options avancées**. En outre, cet onglet comporte les groupes de paramètres suivants :

Paramètres du coffre-fort d'identité

Cette section définit les paramètres qui permettent aux applications d'identité d'accéder aux identités utilisateur et aux rôles dans le coffre-fort d'identité. Certains paramètres sont requis pour terminer la procédure d'installation.

Serveur du coffre-fort d'identité

Requis

Indique le nom d'hôte ou l'adresse IP de votre serveur LDAP. Par exemple : `myLDAPhost`.

Port LDAP

Permet de spécifier le port sur lequel le coffre-fort d'identité doit être à l'écoute des requêtes LDAP en texte clair. La valeur par défaut est 389.

Port sécurisé LDAP

Permet de spécifier le port sur lequel le coffre-fort d'identité doit être à l'écoute des requêtes LDAP à l'aide du protocole SSL (Secure Sockets Layer). La valeur par défaut est 636.

Si un service déjà chargé sur le serveur (avant l'installation d'eDirectory) utilise ce port par défaut, vous devez spécifier un autre port.

Administrateur du coffre-fort d'identité

Requis

Indique les références de l'administrateur LDAP. Par exemple, `cn=admin`. Cet utilisateur doit déjà exister dans le coffre-fort d'identité.

Les applications d'identité utilisent ce compte pour établir une connexion administrative avec le coffre-fort d'identité. Cette valeur est codée, en fonction de la clé principale.

Mot de passe de l'administrateur du coffre-fort d'identité

Requis

Permet de spécifier le mot de passe associé l'administrateur LDAP. Ce mot de passe est codé, en fonction de la clé principale.

Utiliser un compte anonyme public

Permet de spécifier si les utilisateurs non connectés peuvent accéder au compte anonyme public LDAP.

Connexion Admin sécurisée

Indique si RBPM utilise le protocole SSL pour toutes les communications associées au compte administrateur. Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.

REMARQUE : cette option peut affecter les performances.

Connexion utilisateur sécurisée

Indique si RBPM utilise le protocole TLS/SSL pour toutes les communications associées au compte de l'utilisateur connecté. Ce paramètre permet d'effectuer des opérations qui ne nécessitent pas TLS/SSL pour fonctionner sans le protocole.

REMARQUE : cette option peut affecter les performances.

DN du coffre-fort d'identité

Cette section définit les noms distinctifs des conteneurs et des comptes utilisateur qui permettent la communication entre les applications d'identité et les autres composants Identity Manager. Certains paramètres sont requis pour terminer la procédure d'installation.

DN du conteneur racine

Requis

Indique le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire. Exemple : o=mycompany.

DN du conteneur de l'utilisateur

Requis

Si vous affichez les options avancées, l'utilitaire affiche ce paramètre sous Identité de l'utilisateur du coffre-fort d'identité.

Indique le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur utilisateur. Ce paramètre présente les caractéristiques suivantes :

- Les utilisateurs de ce conteneur (et ses sous-conteneurs) sont autorisés à se connecter aux applications d'identité.
- Si vous avez démarré l'instance Tomcat hébergeant les applications d'identité, vous ne pouvez pas modifier ce paramètre à l'aide du fichier `configupdate.sh`.
- Ce conteneur doit inclure l'administrateur de l'application utilisateur que vous avez spécifié lors de la configuration du pilote de l'application utilisateur. Dans le cas contraire, le compte ne peut pas exécuter les workflows.

DN du conteneur du groupe

Requis

Si vous affichez les options avancées, l'utilitaire affiche ce paramètre sous Groupes d'utilisateurs du coffre-fort d'identité.

Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur d'utilisateurs. Ce paramètre présente les caractéristiques suivantes :

- Les définitions d'entité de la couche d'abstraction d'annuaire utilisent ce DN.
- Si vous avez démarré l'instance Tomcat hébergeant les applications d'identité, vous ne pouvez pas modifier ce paramètre à l'aide du fichier `configupdate.sh`.

Pilote d'application utilisateur

Requis

Indique le nom distinctif du pilote de l'application utilisateur.

Par exemple, si votre pilote est UserApplicationDriver et si votre ensemble de pilotes est appelé myDriverSet, et si l'ensemble de pilotes est dans un contexte de o=myCompany, indiquez `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`.

Administrateur de l'application utilisateur

Requis

Permet d'indiquer un compte utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs spécifié de l'application utilisateur. Ce paramètre présente les caractéristiques suivantes :

- Si vous avez démarré l'instance Tomcat hébergeant l'application utilisateur, vous ne pouvez pas modifier ce paramètre à l'aide du fichier `configupdate.sh`.
- Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez les pages **Administration > Sécurité** de l'application utilisateur.
- Ce compte utilisateur est autorisé à utiliser l'onglet **Administration** de l'application utilisateur pour administrer le portail.
- Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, Designer ou l'application utilisateur (onglet **Requêtes et approbations**), vous devez accorder à cet administrateur des autorisations d'ayant droit sur les instances d'objets contenues dans le pilote de l'application utilisateur. Pour plus d'informations, reportez-vous au manuel *User Application Administration Guide* (Guide d'administration de l'application utilisateur).

Administrateur du provisioning

Permet d'indiquer un compte utilisateur existant dans le coffre-fort d'identité qui gère les fonctions de workflow de provisioning disponibles dans l'application utilisateur.

Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page **Administration > Assignations de l'administrateur** de l'application utilisateur.

Administrateur de conformité

Indique un compte existant dans le coffre-fort d'identité qui exécute un rôle système pour permettre aux membres d'exécuter toutes les fonctions de l'onglet **Conformité**. Ce paramètre présente les caractéristiques suivantes :

- Pour modifier cette assignation après avoir déployé les applications d'identité, utilisez la page **Administration > Assignations de l'administrateur** de l'application utilisateur.
- Lors d'une mise à jour de la configuration, les modifications apportées à cette valeur prennent effet uniquement si aucun administrateur de conformité valide n'est assigné. Si un administrateur de conformité valide existe, vos modifications ne sont pas enregistrées.

Administrateur de rôles

Spécifie le rôle qui permet aux membres de créer, de supprimer ou de modifier l'ensemble des rôles, ainsi que d'accorder ou de révoquer les assignations de rôle des utilisateurs, des groupes ou des conteneurs. Il permet également à ses membres d'exécuter des rapports pour n'importe quel utilisateur. Ce paramètre présente les caractéristiques suivantes :

- Par défaut, ce rôle est assigné à l'administrateur de l'application utilisateur.
- Pour modifier cette assignation après avoir déployé les applications d'identité, utilisez la page **Administration > Assignations de l'administrateur** de l'application utilisateur.
- Lors d'une mise à jour de la configuration, les modifications apportées à cette valeur prennent effet uniquement si aucun administrateur de rôles valide n'est assigné. Si un administrateur de rôles valide existe, vos modifications ne sont pas enregistrées.

Administrateur de la sécurité

Spécifie le rôle qui permet aux membres d'accéder à toutes les fonctionnalités du domaine Sécurité. Ce paramètre présente les caractéristiques suivantes :

- L'administrateur de la sécurité peut effectuer toutes les opérations possibles sur tous les objets au sein du domaine Sécurité. Le domaine Sécurité permet également à l'administrateur de la sécurité de configurer des autorisations d'accès pour tous les objets dans tous les domaines de RBPM. L'administrateur de la sécurité peut configurer des équipes et assigner des administrateurs de domaine, des administrateurs délégués et d'autres administrateurs de la sécurité.
- Pour modifier cette assignation après avoir déployé les applications d'identité, utilisez la page **Administration > Assignations de l'administrateur** de l'application utilisateur.

Administrateur de ressources

Spécifie le rôle qui permet aux membres d'accéder à toutes les fonctionnalités du domaine Ressource. Ce paramètre présente les caractéristiques suivantes :

- L'administrateur de ressources peut effectuer toutes les opérations possibles pour tous les objets au sein du domaine Ressource.
- Pour modifier cette assignation après avoir déployé les applications d'identité, utilisez la page **Administration > Assignations de l'administrateur** de l'application utilisateur.

Administrateur de la configuration RBPM

Spécifie le rôle qui permet aux membres d'accéder à toutes les fonctionnalités du domaine Configuration. Ce paramètre présente les caractéristiques suivantes :

- L'administrateur de la configuration RBPM peut effectuer toutes les opérations possibles pour tous les objets au sein du domaine Configuration. L'administrateur de la configuration RBPM contrôle l'accès aux éléments de navigation dans RBPM. En outre, l'administrateur de la configuration RBPM configure le service proxy et de délégation, l'interface utilisateur de provisioning et le moteur de workflow.
- Pour modifier cette assignation après avoir déployé les applications d'identité, utilisez la page **Administration > Assignations de l'administrateur** de l'application utilisateur.

Administrateur de la création de rapports RBPM

Spécifie l'administrateur de la création de rapports. Par défaut, le programme d'installation définit cette valeur sur le même utilisateur que celui renseigné dans les autres champs de sécurité.

Identité de l'utilisateur du coffre-fort d'identité

Cette section définit les valeurs qui permettent aux applications d'identité de communiquer avec un conteneur d'utilisateurs dans le coffre-fort d'identité. Certains paramètres sont requis pour terminer la procédure d'installation.

L'utilitaire n'affiche ces paramètres que lorsque vous sélectionnez **Aff. options avancées**.

DN du conteneur de l'utilisateur

Requis

Lorsque cette option n'est pas présente les options avancées, l'utilitaire affiche ce paramètre sous DN du coffre-fort d'identité.

Indique le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur utilisateur. Ce paramètre présente les caractéristiques suivantes :

- Les utilisateurs de ce conteneur (et ses sous-conteneurs) sont autorisés à se connecter aux applications d'identité.
- Si vous avez démarré l'instance Tomcat hébergeant les applications d'identité, vous ne pouvez pas modifier ce paramètre à l'aide du fichier `configupdate.sh`.
- Ce conteneur doit inclure l'administrateur de l'application utilisateur que vous avez spécifié lors de la configuration du pilote de l'application utilisateur. Dans le cas contraire, le compte ne peut pas exécuter les workflows.

Étendue de la recherche d'utilisateurs

Permet de définir la mesure dans laquelle les utilisateurs du coffre-fort d'identité peuvent effectuer des recherches dans le conteneur.

Classe d'objets Utilisateur

Indique la classe d'objet de l'utilisateur LDAP. La classe est généralement `inetOrgPerson`.

Attribut de connexion

Spécifie l'attribut LDAP qui représente le nom de connexion de l'utilisateur. Exemple : `cn`

Attribut d'assignation de nom

Spécifie l'attribut LDAP utilisé comme identifiant lors de la consultation d'utilisateurs ou de groupes. Ce n'est pas le même que l'attribut de connexion, qui n'est utilisé que lors de la connexion. Exemple : `cn`

Attribut d'adhésion de l'utilisateur

(Facultatif) Spécifie l'attribut LDAP qui représente l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espaces pour le nom.

Groupes d'utilisateurs du coffre-fort d'identité

Cette section définit les valeurs qui permettent aux applications d'identité de communiquer avec un conteneur de groupes dans le coffre-fort d'identité. Certains paramètres sont requis pour terminer la procédure d'installation.

L'utilitaire n'affiche ces paramètres que lorsque vous sélectionnez **Aff. options avancées**.

DN du conteneur du groupe

Requis

Lorsque cette option n'est pas présente les options avancées, l'utilitaire affiche ce paramètre sous DN du coffre-fort d'identité.

Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur d'utilisateurs. Ce paramètre présente les caractéristiques suivantes :

- Les définitions d'entité de la couche d'abstraction d'annuaire utilisent ce DN.
- Si vous avez démarré l'instance Tomcat hébergeant les applications d'identité, vous ne pouvez pas modifier ce paramètre à l'aide du fichier `configupdate.sh`.

Étendue du conteneur de groupes

Permet de définir la mesure dans laquelle les utilisateurs du coffre-fort d'identité peuvent effectuer des recherches dans le conteneur de groupes.

Classe de l'objet Groupe

Indique la classe d'objet du groupe LDAP. La classe est généralement `groupofNames`.

Attribut d'adhésion à un groupe

(Facultatif) Spécifie l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espaces pour le nom.

Utiliser des groupes dynamiques

Indique si vous souhaitez utiliser des groupes dynamiques.

Vous devez aussi spécifier une valeur pour **Classe d'objet Groupe dynamique**.

Classe d'objet Groupe dynamique

Ne s'applique que lorsque vous sélectionnez l'option **Utiliser des groupes dynamiques***.*

Indique la classe d'objet du groupe dynamique LDAP. La classe est généralement `dynamicGroup`.

Certificats du coffre-fort d'identité

Cette section définit le chemin d'accès et le mot de passe pour le keystore du JRE. Certains paramètres sont requis pour terminer la procédure d'installation.

Chemin du fichier Keystore

Requis

Indique le chemin d'accès complet au fichier (`cacerts`) de votre keystore du JRE utilisé par Tomcat. Vous pouvez entrer manuellement le chemin d'accès ou parcourir l'arborescence jusqu'au fichier `cacerts`. Ce paramètre présente les caractéristiques suivantes :

- Dans les environnements, vous devez indiquer le répertoire d'installation de RBPM. La valeur par défaut est définie sur l'emplacement correct.
- Le programme d'installation des applications d'identité modifie le fichier keystore. Sous Linux, l'utilisateur doit avoir l'autorisation d'écrire dans ce fichier.

Mot de passe Keystore

Requis

Spécifie le mot de passe pour le fichier keystore. L'unité par défaut est `changeit`.

Configuration du serveur de messagerie

Cette section décrit les valeurs permettant de configurer des notifications par message électronique que vous pouvez utiliser pour les approbations. Pour plus d'informations, reportez-vous à la section « Enabling Support for Digital Signatures » (Activation de la prise en charge des signatures numériques) du *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager - Guide de l'administrateur des applications d'identité) et à la section « Manage Approvals by Email » (Gestion des approbations par courrier électronique) dans l'*Aide des applications d'identité*.

Hôte du modèle de notification

Spécifie le nom ou l'adresse IP de l'instance Tomcat qui héberge les applications d'identité. Par exemple, `myapplication serverServer`.

Cette valeur remplace le jeton $HOST$ des modèles de courrier électronique. Le programme d'installation utilise ces informations pour créer une URL conduisant aux tâches de requête de provisioning et aux notifications d'approbation.

Port du modèle de notification

Spécifie le numéro de port de l'instance Tomcat qui héberge les applications d'identité.

Cette valeur remplace le jeton $PORT$ dans les modèles de message électronique qui sont utilisés dans des tâches de requête de provisioning et les notifications d'approbation.

Port sécurisé du modèle de notification

Spécifie le numéro de port sécurisé de l'instance Tomcat qui héberge les applications d'identité.

Cette valeur remplace le jeton $SECURE_PORT$ dans les modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.

Protocole du modèle de notification

Indique un protocole non sécurisé inclus dans l'URL lors de l'envoi de courrier électronique à l'utilisateur. Exemple : `http`.

Cette valeur remplace le jeton $PROTOCOL$ dans les modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.

Protocole sécurisé du modèle de notification

Indique le protocole sécurisé inclus dans l'URL lors de l'envoi de courrier électronique à l'utilisateur. Exemple : `https`.

Cette valeur remplace le jeton $SECURE_PROTOCOL$ dans les modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.

Expéditeur du message SMTP de notification

Indique le compte de messagerie électronique utilisé par les applications d'identité pour envoyer des notifications par courrier électronique.

Nom du serveur SMTP

Indique l'adresse IP ou le nom DNS de l'hôte de messagerie SMTP utilisé par les applications d'identité pour les messages électroniques de provisioning. N'utilisez pas `localhost`.

Le serveur requiert une authentification.

Indique si vous souhaitez que le serveur demande une authentification.

Vous devez également spécifier des références pour le serveur de messagerie.

Nom d'utilisateur

Applicable uniquement si vous activez l'option **Le serveur requiert une authentification***.*

Permet d'indiquer le nom d'un compte de connexion au serveur de messagerie.

Mot de passe

Applicable uniquement si vous activez l'option **Le serveur requiert une authentification***.*

Permet d'indiquer le mot de passe d'un compte de connexion pour le serveur de messagerie.

Utiliser SMTP TLS

Indique si vous souhaitez sécuriser le contenu des messages lors de leur transmission entre les serveurs de messagerie.

Emplacement de l'image de notification par message électronique

Indique le chemin d'accès à l'image que vous souhaitez inclure dans les notifications par message électronique. Par exemple, `http://localhost:8080/IDMProv/images`.

Signer le message électronique

Indique si vous souhaitez ajouter une signature numérique aux messages sortants.

Si vous activez cette option, vous devez également spécifier les paramètres du fichier Keystore et de la clé de signature.

Chemin du fichier Keystore

Applicable uniquement lorsque vous activez l'option **Signer le message électronique***.*

Spécifie le chemin d'accès complet au fichier Keystore (`cacerts`) que vous souhaitez utiliser pour ajouter une signature numérique à un message électronique. Vous pouvez entrer manuellement le chemin d'accès ou parcourir l'arborescence jusqu'au fichier `cacerts.`

Par exemple : `/opt/netiq/idm/apps/jre/lib/security/cacerts`.

Mot de passe Keystore

Applicable uniquement lorsque vous activez l'option **Signer le message électronique***.*

Spécifie le mot de passe pour le fichier keystore. Par exemple : `changeit`.

Alias de la clé de signature

Applicable uniquement lorsque vous activez l'option **Signer le message électronique**.

Spécifie l'alias de la clé de signature dans le keystore. Par exemple : `idmapptest`.

Mot de passe de clé de signature

Applicable uniquement lorsque vous activez l'option **Signer le message électronique**.

Spécifie le mot de passe qui protège le fichier contenant la clé de signature. Par exemple : `changeit`.

Banque de clés approuvée

Cette section définit les valeurs du keystore approuvé pour les applications d'identité. L'utilitaire n'affiche ces paramètres que lorsque vous sélectionnez **Aff. options avancées**.

Chemin d'accès à la banque approuvée

Indique le chemin d'accès au keystore approuvé qui contient tous les certificats de signataires approuvés. Si ce chemin est vide, les applications d'identité obtiennent le chemin à partir de la propriété système `javax.net.ssl.trustStore`. Si la propriété système ne peut pas fournir le chemin, le programme d'installation est défini par défaut sur `jre/lib/security/cacerts`.

Mot de passe de la banque approuvée

Spécifie le mot de passe du keystore approuvé. Si ce champ est vide, les applications d'identité obtiennent le mot de passe à partir de la propriété système `javax.net.ssl.trustStorePassword`. Si la propriété système ne peut pas fournir le chemin, le programme d'installation est défini par défaut sur `changeit`.

Ce mot de passe est codé, en fonction de la clé principale.

Type de zone de stockage approuvée

Indique si le chemin d'accès à la zone de stockage approuvée utilise un keystore Java (JKS) ou PKCS12 pour la signature numérique.

Clé et certificat de signature numérique de NetIQ Sentinel

Cette section définit les valeurs qui permettent à Identity Manager de communiquer avec Sentinel pour l'audit des événements. L'utilitaire n'affiche ces paramètres que lorsque vous sélectionnez **Aff. options avancées**.

Certificat de signature numérique de Sentinel

Répertorie les certificats de clé publique personnalisés utilisables par le serveur OAuth pour authentifier les messages d'audit envoyés à Sentinel.

Clé privée de signature numérique de Sentinel

Indique le chemin d'accès au fichier de clé privée personnalisé utilisable par le serveur OAuth pour authentifier les messages d'audit envoyés à Sentinel.

Divers

L'utilitaire n'affiche ces paramètres que lorsque vous sélectionnez **Aff. options avancées**.

URI OCSP

Spécifie l'URI à utiliser lorsque l'installation client utilise le protocole OCSP (On-Line Certificate Status Protocol). Par exemple, `http://host:port/ocspLocal`.

L'URI OCSP met à jour le statut des certificats approuvés en ligne.

Chemin de configuration d'autorisation

Indique le nom complet du fichier de configuration de l'autorisation.

Index du coffre-fort d'identité

Au cours de l'installation, permet d'indiquer si vous souhaitez que le programme d'installation crée des index sur les attributs manager, ismanager, and srvprvUUID attributes. Après l'installation, vous pouvez modifier les paramètres afin qu'ils pointent vers un nouvel emplacement des index. Ce paramètre présente les caractéristiques suivantes :

- En l'absence d'index pour ces attributs, les utilisateurs peuvent être confrontés à des baisses de performances des applications d'identité.
- Vous pouvez créer ces index manuellement à l'aide d'iManager après avoir installé les applications d'identité.
- Pour des performances optimales, nous vous conseillons de créer l'index de l'aide au cours de l'installation.
- Les index doivent être en mode en ligne pour que vous puissiez rendre les applications d'identité accessibles aux utilisateurs.
- Pour créer ou supprimer un index, vous devez aussi spécifier une valeur pour **DN du serveur**.

DN du serveur

Ne s'applique que lorsque vous souhaitez créer ou supprimer un index du coffre-fort d'identité.

Spécifie le serveur eDirectory sur lequel vous voulez créer ou supprimer les index.

Vous ne pouvez spécifier qu'un seul serveur à la fois. Pour configurer des index sur plusieurs serveurs eDirectory, vous devez exécuter l'utilitaire de configuration RBPM plusieurs fois.

Réinitialiser la sécurité RBPM

Indique si vous voulez réinitialiser la sécurité RBPM lorsque l'installation est terminée. Vous devez également redéployer les applications d'identité.

URL IDMReport

Indique l'URL du module de création de rapports d'Identity Manager. Par exemple, `http://hostnamport/IDMRPT`.

Nom du contexte des thèmes personnalisés

Spécifie le nom du thème personnalisé que vous souhaitez utiliser pour l'affichage des applications d'identité dans le navigateur.

Préfixe de l'identificateur du message de journal

Permet de définir la valeur à utiliser dans le modèle de présentation pour les appenders CONSOLE et FILE dans le fichier `idmuserapp_logging.xml`. La valeur par défaut est `RBPM`.

Modifier le nom du contexte RBPM

Indique si vous voulez modifier le nom du contexte de RBPM.

Vous devez également spécifier les nouveaux nom et DN du pilote de rôles et de ressources.

Nom du contexte RBPM

Ne s'applique que lorsque vous sélectionnez **Modifier le nom du contexte RBPM**.

Indique le nouveau nom du contexte pour RBPM.

DN du pilote de rôle

Ne s'applique que lorsque vous sélectionnez **Modifier le nom du contexte RBPM**.

Indique le DN du pilote de rôles et de ressources.

Objet Conteneur

Ces paramètres ne s'appliquent qu'au cours de l'installation.

Cette section vous permet de définir les valeurs des objets Conteneur ou de créer de nouveaux objets Conteneur.

Sélectionné

Indique les types d'objets Conteneur que vous souhaitez utiliser.

Type d'objet Conteneur

Indique le conteneur : lieu, pays, unité organisationnelle, organisation ou domaine.

Vous pouvez également définir vos propres conteneurs dans iManager et les ajouter sous **Ajouter un nouvel objet du conteneur**.

Nom d'attribut du conteneur

Spécifie le nom du type d'attribut associé au type d'objet Conteneur spécifié.

Ajouter un nouvel objet du conteneur : type d'objet Conteneur

Indique le nom LDAP d'une classe d'objets du coffre-fort d'identité pouvant servir de conteneur.

Ajouter un nouvel objet du conteneur : nom d'attribut du conteneur

Spécifie le nom du type d'attribut associé au nouveau type d'objet Conteneur.

11.6.3 Paramètres de création de rapports

Lors de la configuration des applications d'identité, cet onglet permet de définir les valeurs pour la gestion d'Identity Reporting. L'utilitaire ajoute cet onglet lorsque vous installez Identity Reporting.

Par défaut, l'onglet affiche les options de base. Pour afficher tous les paramètres, cliquez sur **Afficher les options avancées**. En outre, cet onglet comporte les groupes de paramètres suivants :

- « Configuration de l'envoi par message électronique » page 155
- « Valeurs de conservation du rapport » page 155
- « Modifier le paramètre local » page 156
- « Configuration du rôle » page 156

Configuration de l'envoi par message électronique

Cette section définit les valeurs pour l'envoi de notifications.

Nom d'hôte du serveur SMTP

Permet de spécifier le nom DNS ou l'adresse IP du serveur de messagerie qu'Identity Reporting doit utiliser pour envoyer des notifications. N'utilisez pas `localhost`.

Port du serveur SMTP

Permet d'indiquer le numéro de port du serveur SMTP.

SMTP utilise SSL

Permet d'indiquer si vous voulez utiliser le protocole TLS/SSL pour les communications avec le serveur de messagerie.

Le serveur nécessite une authentification.

Permet d'indiquer si vous souhaitez utiliser l'authentification pour les communications avec le serveur de messagerie.

Nom d'utilisateur SMTP

Permet de spécifier l'adresse de messagerie à utiliser pour l'authentification.

Vous devez spécifier une valeur. Si le serveur ne nécessite pas d'authentification, vous pouvez spécifier une adresse non valide.

Mot de passe de l'utilisateur SMTP

Ne s'applique que lorsque vous indiquez que le serveur nécessite l'authentification.

Permet d'indiquer le mot de passe du compte utilisateur SMTP.

Adresse électronique par défaut

Permet de spécifier l'adresse électronique à partir de laquelle Identity Reporting envoie les notifications par message électronique.

Valeurs de conservation du rapport

Cette section définit les valeurs associées au stockage des rapports finalisés.

Unité du rapport, Durée de vie du rapport

Permet d'indiquer pendant combien de temps Identity Reporting conserve les rapports avant de les supprimer. Par exemple, pour spécifier six mois, entrez `6` dans le champ **Durée de vie du rapport**, puis sélectionnez **Mois** dans le champ **Unité du rapport**.

Emplacement des rapports

Permet d'indiquer où vous voulez stocker les définitions de rapport. Par exemple, `/opt/netiq/IdentityReporting`.

Modifier le paramètre local

Cette section définit les valeurs pour la langue que doit utiliser Identity Reporting. Identity Reporting utilise ce paramètre local dans les recherches. Pour plus d'informations, reportez-vous au Guide de l'administrateur de NetIQ Identity Reporting.

Configuration du rôle

Cette section définit les valeurs des sources d'authentification utilisées par Identity Reporting pour générer des rapports.

Ajouter une source d'authentification

Permet d'indiquer le type de source d'authentification que vous voulez ajouter pour créer des rapports. Ces sources d'authentification peuvent être les suivantes :

- **Par défaut**
- **Annuaire LDAP**
- **Fichier**

11.6.4 Paramètres d'authentification

Lors de la configuration des applications d'identité, cet onglet permet de définir les valeurs que Tomcat utilise pour diriger les utilisateurs vers les pages de gestion des mots de passe et des applications d'identité.

Par défaut, l'onglet affiche les options de base. Pour afficher tous les paramètres, cliquez sur **Afficher les options avancées**. En outre, cet onglet comporte les groupes de paramètres suivants :

- « Serveur d'authentification » page 156
- « Configuration de l'authentification » page 157
- « Méthode d'authentification » page 158
- « Gestion des mots de passe » page 158
- « Clé et certificat de signature numérique de Sentinel » page 159

Serveur d'authentification

Cette section définit les paramètres des applications d'identité pour vous connecter au serveur d'authentification.

Identificateur de l'hôte du serveur OAuth

Requis

Permet d'indiquer l'URL relative du serveur d'authentification qui émet les jetons pour OSP. Par exemple, 192.168.0.1.

Port TCP du serveur OAuth

Permet de spécifier le port du serveur d'authentification.

Le serveur OAuth utilise TLS/SSL.

Indique si le serveur d'authentification utilise le protocole TLS/SSL pour la communication.

Fichier Truststore TLS/SSL facultatif

S'applique uniquement si vous sélectionnez **Le serveur OAuth utilise TLS/SSL.** *et que l'utilitaire affiche les options avancées.*

Mot de passe Truststore TLS/SSL facultatif

S'applique uniquement si vous sélectionnez **Le serveur OAuth utilise TLS/SSL.** *et que l'utilitaire affiche les options avancées.*

Spécifie le mot de passe utilisé pour charger le fichier keystore pour le serveur d'authentification TLS/SSL.

REMARQUE : Si vous ne spécifiez pas le chemin et le mot de passe du fichier Keystore et si le certificat approuvé pour le serveur d'authentification n'est pas dans le Truststore JRE (cacerts), les applications d'identité ne parviennent pas à se connecter au service d'authentification qui utilise le protocole TLS/SSL.

Configuration de l'authentification

Cette section définit les paramètres pour le serveur d'authentification.

DN LDAP du conteneur des administrateurs

Requis

Spécifie le nom distinctif du conteneur du coffre-fort d'identité qui contient des objets Administrateur à authentifier par OSP. Par exemple, `ou=sa,o=data`.

Attribut d'assignation de nom de résolution en double

Spécifie le nom de l'attribut LDAP utilisé pour différencier plusieurs objets Utilisateur eDirectory avec la même valeur `cn`. La valeur par défaut est `mail`.

Restreindre les sources d'authentification aux contextes

Indique si des recherches dans les conteneurs d'utilisateurs et d'administrateurs du coffre-fort d'identité sont limitées aux objets Utilisateur de ces conteneurs ou si ces recherches doivent également inclure les sous-conteneurs.

Timeout de la session (minutes)

Indique le nombre de minutes d'inactivité dans une session avant que le serveur ne déclenche l'expiration de la session de l'utilisateur. La valeur par défaut est de 20 minutes.

Durée de vie du jeton d'accès (en secondes)

Spécifie le nombre de secondes de validité d'un jeton d'accès OSP. La valeur par défaut est de 60 secondes.

Durée de vie du jeton de rafraîchissement (en heures)

Spécifie le nombre de secondes de validité d'un jeton de rafraîchissement OSP. Le jeton de rafraîchissement est utilisé en interne par OSP. La valeur par défaut est 48 heures.

Méthode d'authentification

Cette section définit les valeurs qui permettent à OSP d'authentifier les utilisateurs qui se connectent aux composants Identity Manager basés sur des navigateurs.

Méthode

Indique le type d'authentification que vous souhaitez qu'Identity Manager emploie lorsqu'un utilisateur se connecte.

- **Nom et mot de passe** : OSP vérifie l'authentification avec le coffre-fort d'identité.
- **Kerberos** : OSP accepte l'authentification de la part d'un serveur de ticket Kerberos et du coffre-fort d'identité. Vous devez aussi spécifier une valeur pour **Nom d'attribut de mappage**.
- **SAML 2.0** : OSP accepte l'authentification de la part d'un fournisseur d'identité SAML et du coffre-fort d'identité. Vous devez également spécifier des valeurs pour **Nom d'attribut de mappage** et **URL des métadonnées**.

Nom d'attribut de mappage

Ne s'applique que lorsque vous indiquez **Kerberos** *ou* **SAML**.

Spécifie le nom de l'attribut qui opère le mappage au serveur du ticket Kerberos ou aux représentations SAML auprès du fournisseur d'identité.

URL des métadonnées

Ne s'applique que lorsque vous indiquez **SAML**.

Indique l'URL utilisée par OSP pour rediriger la requête d'authentification vers SAML.

Gestion des mots de passe

Cette section définit les valeurs qui permettent aux utilisateurs de modifier leur mot de passe en tant qu'opération en self-service

Fournisseur de gestion des mots de passe

Spécifie le type de système de gestion des mots de passe que vous voulez utiliser.

Application utilisateur (héritée) : permet d'utiliser le programme de gestion des mots de passe employé habituellement par Identity Manager. Cette option vous permet d'utiliser un programme de gestion des mots de passe externe.

Mot de passe oublié

Ce paramètre s'applique uniquement lorsque vous souhaitez utiliser SSPR.

Permet d'indiquer si vous souhaitez que les utilisateurs récupèrent un mot de passe oublié sans qu'il soit nécessaire de contacter le centre d'assistance.

Vous devez également configurer les stratégies de réponse de vérification d'identité pour la fonction Mot de passe oublié. Pour plus d'informations, reportez-vous au manuel *NetIQ Self Service Password Reset Administration Guide* (Guide d'administration de NetIQ SSPR)

Mot de passe oublié

Cette liste ne s'applique que lorsque vous sélectionnez **Application utilisateur (héritée)**.

Permet d'indiquer si vous voulez utiliser le système de gestion des mots de passe intégré à l'application utilisateur ou un système externe.

- **Interne** : permet d'utiliser la fonction de gestion des mots de passe interne par défaut, `/jsps/pwdmgt/ForgotPassword.jsp` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.
- **Externe** : permet d'utiliser un fichier WAR de mot de passe oublié externe pour rappeler l'application utilisateur par le biais d'un service Web. Vous devez également définir les paramètres pour le système externe.

Lien Mot de passe oublié

Ne s'applique que si vous souhaitez utiliser un système de gestion des mots de passe externe.

Permet d'indiquer l'URL pointant vers la page de la fonction Mot de passe oublié. Indiquez un fichier `ForgotPassword.jsp` dans un fichier WAR de gestion des mots de passe externe ou interne.

Lien Retour mot de passe oublié

Ne s'applique que si vous souhaitez utiliser un système de gestion des mots de passe externe.

Permet de définir le paramètre **Lien Retour mot de passe oublié** sur lequel l'utilisateur peut cliquer après une opération de type Mot de passe oublié.

URL du service Web de mot de passe oublié

Ne s'applique que si vous souhaitez utiliser un système de gestion des mots de passe externe.

Représente l'URL que le fichier WAR externe de mot de passe oublié utilise pour revenir à l'application utilisateur en vue d'exécuter les fonctions de base de mot de passe oublié. utilisez le format suivant :

```
https://<idmhost>:<sslport>/<idm>/
pwdmgt/service
```

Clé et certificat de signature numérique de Sentinel

Cette section définit les valeurs qui permettent à Identity Manager de communiquer avec Sentinel pour l'audit des événements.

Certificat de signature numérique de Sentinel

Permet de spécifier un certificat de clé publique que vous souhaitez que le serveur OSP utilise pour authentifier les messages d'audit envoyés au système d'audit.

Pour plus d'informations sur la configuration des certificats pour Novell Audit, reportez-vous à la section Managing Certificates (Gestion des certificats) du manuel *Novell Audit Administration Guide* (Guide d'administration de Novell Audit).

Clé privée de signature numérique de Sentinel

Indique le chemin d'accès au fichier de clé privée personnalisé utilisable par le serveur OSP pour authentifier les messages d'audit envoyés au système d'audit.

11.6.5 Paramètres des clients SSO

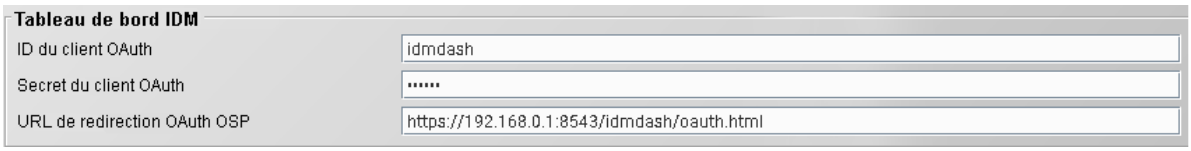
Lors de la configuration des applications d'identité, cet onglet permet de définir les valeurs pour la gestion d'un accès Single Sign-On aux applications.

Par défaut, l'onglet affiche les options de base. Pour afficher tous les paramètres, cliquez sur **Afficher les options avancées**. En outre, cet onglet comporte les groupes de paramètres suivants :

Tableau de bord IDM

Cette section décrit les valeurs d'URL dont les utilisateurs ont besoin pour accéder au tableau de bord Identity Manager, lequel constitue le principal emplacement de connexion pour les applications d'identité.

Figure 11-1 *Tableau de bord IDM*



ID du client OAuth

Requis

Spécifie le nom servant à identifier le client SSO pour le tableau de bord auprès du serveur d'authentification. La valeur par défaut est `idmdash`.

Secret du client OAuth

Requis

Spécifie le mot de passe du client SSO pour le tableau de bord.

URL de redirection OAuth OSP

Requis

Indique l'URL absolue vers laquelle le serveur d'authentification redirige un client de navigateur une fois l'authentification terminée.

Utilisez le format suivant : `protocol//serveur:port/chemin`. Par exemple : `https://192.168.0.1:8543/idmdash/oauth.html`.

Administrateur IDM

Cette section définit les valeurs pour l'URL dont les utilisateurs ont besoin pour accéder à la page de l'administrateur d'Identity Manager.

ID du client OAuth

Requis

Permet d'indiquer le nom servant à identifier le client Single Sign-on pour l'administrateur Identity Manager auprès du serveur d'authentification. La valeur par défaut est `idmadmin`.

Secret du client OAuth

Requis

Permet d'indiquer le mot de passe du client Single Sign-on pour l'administrateur Identity Manager.

URL de redirection OAuth OSP

Requis

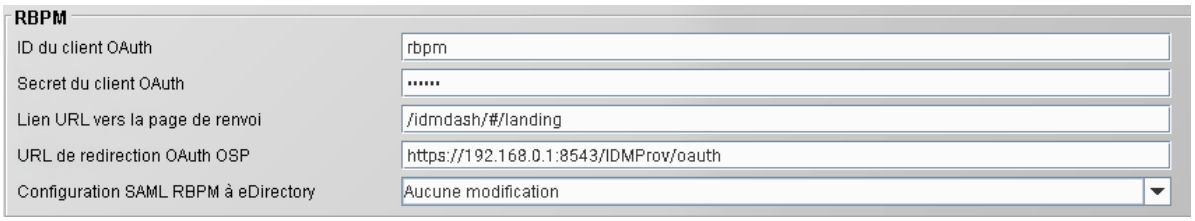
Indique l'URL absolue vers laquelle le serveur d'authentification redirige un client de navigateur une fois l'authentification terminée.

Utilisez le format suivant : `protocol//serveur:port/chemin`. Par exemple : `https://192.168.0.1:8543/idmadmin/oauth.html`.

RBPM

Cette section définit les valeurs pour l'URL dont les utilisateurs ont besoin pour accéder à l'application utilisateur.

Figure 11-2 *RBPM*



ID du client OAuth

Requis

Permet d'indiquer le nom servant à identifier le client SSO pour l'application utilisateur auprès du serveur d'authentification. La valeur par défaut est `rbpm`.

Secret du client OAuth

Requis

Permet d'indiquer le mot de passe du client SSO pour l'application utilisateur.

Lien URL vers la page de renvoi

Requis

Spécifie l'URL relative permettant d'accéder au tableau de bord à partir de l'application utilisateur. La valeur par défaut est `/landing`.

URL de redirection OAuth OSP

Requis

Indique l'URL absolue vers laquelle le serveur d'authentification redirige un client de navigateur une fois l'authentification terminée.

Utilisez le format suivant : `protocol//serveur:port/chemin`. Par exemple : `https://192.168.0.1:8543/IDMProv/oauth`.

Configuration de RBPM à eDirectory SAML

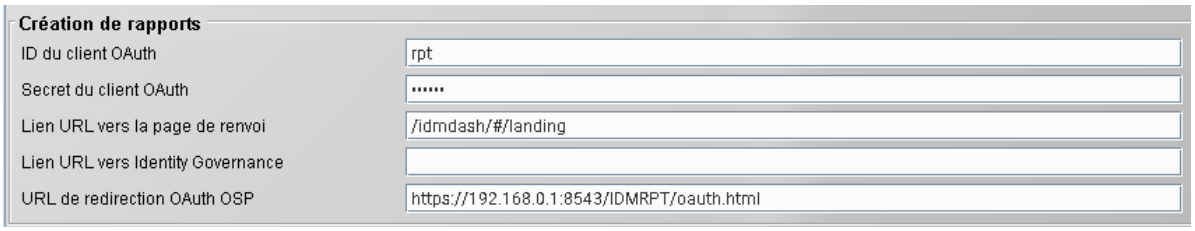
Requis

Indique le RBPM pour les paramètres SAML eDirectory requis pour l'authentification SSO.

Création de rapports

Cette section définit les valeurs pour l'URL dont les utilisateurs ont besoin pour accéder à Identity Reporting. L'utilitaire n'affiche ces valeurs que si vous ajoutez Identity Reporting à votre solution Identity Manager.

Figure 11-3 *Création de rapports*



ID du client OAuth

Requis

Permet d'indiquer le nom servant à identifier le client SSO pour Identity Reporting auprès du serveur d'authentification. La valeur par défaut est `rpt`.

Secret du client OAuth

Requis

Spécifie le mot de passe du client Single Sign-On pour Identity Reporting.

Lien URL vers la page de renvoi

Requis

Spécifie l'URL relative permettant d'accéder au tableau de bord à partir d'Identity Reporting. La valeur par défaut est `/idmdash/#/landing`.

Si vous avez installé Identity Reporting et les applications d'identité dans des serveurs distincts, indiquez une URL absolue. Utilisez le format suivant : `protocol//serveur:port/chemin`. Parr exemple : `https://192.168.0.1:8543/IDMRPT/oauth`.

URL de redirection OAuth OSP

Requis

Indique l'URL absolue vers laquelle le serveur d'authentification redirige un client de navigateur une fois l'authentification terminée.

Utilisez le format suivant : `protocol//serveur:port/chemin`. Parr exemple : `https://192.168.0.1:8543/IDMRPT/oauth`.

Service de collecte de données d'IDM

Cette section définit les valeurs pour l'URL dont les utilisateurs ont besoin pour accéder au service de collecte de données d'Identity Manager.

ID du client OAuth

Requis

Permet d'indiquer le nom que vous souhaitez utiliser pour identifier le client Single Sign-on pour le service de collecte de données d'Identity Manager auprès du serveur d'authentification. La valeur par défaut est `idmdcs`.

Secret du client OAuth

Requis

Permet d'indiquer le mot de passe du client Single Sign-on pour le service de collecte de données d'Identity Manager.

URL de redirection OAuth OSP

Requis

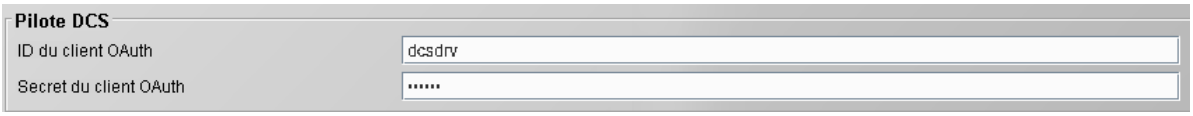
Indique l'URL absolue vers laquelle le serveur d'authentification redirige un client de navigateur une fois l'authentification terminée.

Utilisez le format suivant : `protocol//serveur:port/chemin`. Par exemple : `https://192.168.0.1:8543/idmdcs/oauth.html`.

Pilote DCS

Cette section définit les valeurs pour la gestion du pilote de services de collecte de données.

Figure 11-4



ID du client OAuth

Permet d'indiquer le nom servant à identifier le client SSO pour le pilote du service de collecte de données auprès du serveur d'authentification. La valeur par défaut de ce paramètre est `dcsdrv`.

Secret du client OAuth

Permet d'indiquer le mot de passe du client SSO pour le pilote du service de collecte de données.

Self Service Password Reset

Cette section définit les valeurs pour l'URL dont les utilisateurs ont besoin pour accéder à SSPR.

ID du client OAuth

Requis

Permet d'indiquer le nom servant à identifier le client SSO pour SSPR auprès du serveur d'authentification. La valeur par défaut est `sspr`.

Secret du client OAuth

Requis

Spécifie le mot de passe du client SSO pour SSPR.

URL de redirection OAuth OSP

Requis

Indique l'URL absolue vers laquelle le serveur d'authentification redirige un client de navigateur une fois l'authentification terminée.

Utilisez le format suivant : `protocol//serveur:port/chemin`. Par exemple : `https://192.168.0.1:8543/sspr/public/oauth.html`.

11.6.6 Paramètres de l'audit CEF

Cette section définit les valeurs pour gérer les paramètres d'audit CEF pour le client Single Sign-on.

Envoyer des événements d'audit

Indique si vous souhaitez utiliser CEF pour auditer les événements.

Hôte de destination

Spécifie le nom DNS ou l'adresse IP du serveur d'audit.

Port de destination

Indique le port du serveur d'audit.

Protocole réseau

Indique le protocole réseau utilisé par le serveur d'audit pour recevoir les événements CEF.

Utiliser TLS

S'applique uniquement lorsque vous souhaitez utiliser TCP comme protocole réseau.

Indique si le serveur d'audit est configuré pour utiliser TLS avec TCP.

Répertoire de stockage intermédiaire des événements

Indique l'emplacement du répertoire du cache, avant que les événements CEF soient envoyés au serveur d'audit.

REMARQUE : Assurez-vous que les autorisations `novlua` sont définies pour le répertoire du cache. Dans le cas contraire, vous ne pourrez pas accéder aux applications IDMDash et IDMProv. En outre, aucun des événements OSP ne sera consigné dans le répertoire du cache. Par exemple, vous pouvez modifier l'autorisation et la propriété du répertoire à l'aide de la commande `chown novlua:novlua /<chemin_répertoire>` , dans lequel `<chemin_répertoire>` est le chemin de répertoire du fichier de cache.

11.7 Démarrage des applications d'identité

Veillez à redémarrer les services Tomcat et ActiveMQ après avoir configuré les applications d'identité.

```
systemctl restart netiq-tomcat
```

```
systemctl restart netiq-activemq
```

11.8 Configuration d'OSP et de SSPR pour la mise en grappe

Identity Manager prend en charge la configuration de SSPR dans un environnement de grappe Tomcat.

11.8.1 Configuration de SSPR pour la prise en charge de la mise en grappe

Pour mettre à jour les informations SSPR sur le premier noeud de la grappe, lancez l'utilitaire de configuration à partir de `/opt/netiq/idm/apps/configupdate/configupdate.sh`.

Dans la fenêtre qui s'affiche, cliquez sur **SSO clients** (Clients SSO) > **Self Service Password Reset** et spécifiez des valeurs pour les paramètres **Client ID** (ID de client), **Password** (Mot de passe) et **OSP Auth redirect URL** (URL de redirection de l'authentification OSP).

11.8.2 Configuration des tâches sur les noeuds de grappe

Effectuez les opérations de configuration suivantes sur les noeuds de la grappe :

1. Pour mettre à jour le lien Mot de passe oublié avec l'adresse IP de SSPR, connectez-vous à l'application utilisateur sur le premier noeud, puis cliquez sur **Administration** > **Mot de passe oublié**.

   Pour plus d'informations sur la configuration de SSPR, reportez-vous à la Section 22, « Configuration de la gestion des mots de passe oubliés », page 235.
2. Pour modifier le lien Modifier mon mot de passe, reportez-vous à la Section 22.3, « Mise à jour des liens SSPR dans le tableau de bord pour un environnement distribué ou de grappe », page 239.
3. Vérifiez que les liens Mot de passe oublié et Modifier mon mot de passe ont été mis à jour avec l'adresse IP de SSPR sur les autres noeuds de la grappe.

   REMARQUE : si les liens Modifier mon mot de passe et Mot de passe oublié ont déjà été mis à jour avec l'adresse IP de SSPR, aucune modification n'est nécessaire.
4. Sur le premier noeud, arrêtez Tomcat et générez un nouveau fichier `osp.jks` en spécifiant le nom DNS du serveur de l'équilibreur de charge à l'aide de la commande suivante :

   ```
   /opt/netiq/common/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore
   osp.jks -storepass <mot_de_passe> -keypass <mot_de_passe> -alias osp -validity
   1800 -dname "cn=<IP/DNS_équilibreur_de_charge>"
   ```

   Par exemple : `/opt/netiq/common/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"`

   REMARQUE : assurez-vous que le mot de passe de clé est identique à celui spécifié lors de l'installation d'OSP. Ce mot de passe, de même que le mot de passe Keystore, peut aussi être modifié à l'aide de l'utilitaire de mise à jour de configuration.
5. (Conditionnel) Pour vérifier si le fichier `osp.jks` a été mis à jour avec les modifications, exécutez la commande suivante :

   ```
   /opt/netiq/common/jre/bin/keytool -list -v -keystore osp.jks -storepass
   changeit
   ```

6 Effectuez une sauvegarde du fichier `osp.jks` d'origine situé sous `/opt/netiq/idm/apps/osp` et copiez le nouveau fichier `osp.jks` à cet emplacement. Le nouveau fichier `osp.jks` a été créé à l'étape 3.

7 Copiez le nouveau fichier `osp.jks` situé dans `/opt/netiq/idm/apps/osp` depuis le premier noeud vers tous les autres noeuds d'application utilisateur de la grappe.

8 Lancez l'utilitaire de configuration sur le premier noeud et, sous l'onglet Client SSO, remplacez l'ensemble des paramètres d'URL, notamment le lien URL vers la page de renvoi et l'URL de redirection OAuth, par le nom DNS de l'équilibreur de charge.

8a Enregistrez les modifications dans l'utilitaire de configuration.

8b Pour répercuter cette modification sur tous les autres noeuds de la grappe, copiez le fichier `ism-configuration.properties` situé dans `/TOMCAT_INSTALLED_HOME/conf` depuis le premier noeud vers tous les autres noeuds d'application utilisateur.

REMARQUE : vous avez copié le fichier `ism.properties` depuis le premier noeud vers les autres noeuds de la grappe. Si vous avez spécifié des chemins d'installation personnalisés lors de l'installation de l'application utilisateur, veillez à corriger les chemins d'accès référentiels en utilisant l'utilitaire de mise à jour de configuration sur les noeuds de la grappe.

Dans ce scénario, OSP et l'application utilisateur sont installés sur le même serveur ; dès lors, le même nom DNS est utilisé pour les URL de redirection.

Si OSP et l'application utilisateur sont installés sur des serveurs distincts, remplacez les URL d'OSP par un autre nom DNS pointant vers l'équilibreur de charge. Effectuez cette opération pour tous les serveurs sur lesquels OSP est installé, afin que toutes les requêtes OSP soient distribuées, via l'équilibreur de charge, vers le nom DNS de la grappe OSP. Cela implique d'avoir une grappe distincte pour les noeuds OSP.

---

9 Effectuez les opérations suivantes dans le fichier `setenv.sh` situé dans le répertoire `/TOMCAT_INSTALLED_HOME/bin/` :

9a Pour que la liaison mcast_addr réussisse, JGroups requiert que la propriété `preferIPv4Stack` soit définie sur **true**. Pour ce faire, ajoutez la propriété JVM « -Djava.net.preferIPv4Stack=true » dans le fichier `setenv.sh` sur tous les noeuds.

9b Ajoutez la propriété « -Dcom.novell.afw.wf.Engine-id=Engine » dans le fichier `setenv.sh` sur le premier noeud.

Le nom du moteur doit être unique. Indiquez le nom spécifié lors de l'installation du premier noeud. Si aucun nom n'a été spécifié, le nom par défaut est « Engine ».

De même, ajoutez un nom de moteur unique pour les autres noeuds de la grappe. Par exemple, le nom du deuxième noeud peut être Engine2.

10 Activez la mise en grappe dans l'application utilisateur.

11 Activez l'index des autorisations pour la mise en grappe. Pour plus d'informations, reportez-vous à l'« Activation de l'index des autorisations pour la mise en grappe » page 77.

12 Redémarrez Tomcat sur tous les noeuds.

13 Configurez le pilote d'application utilisateur pour la mise en grappe. Pour plus d'informations, reportez-vous à la Section 11.5, « Configuration du pilote d'application utilisateur pour la mise en grappe », page 142.

11.9 Configuration de l'environnement d'exécution

Cette section fournit des informations à propos des étapes de configuration supplémentaires vous permettant de vous assurer que votre environnement d'exécution fonctionne correctement. Elle indique également des techniques de dépannage, ainsi que des informations sur les tables de base de données qui peuvent vous être utiles.

Cette procédure implique les opérations suivantes :

- Section 11.9.1, « Configuration du pilote du service de collecte de données (DSC) afin de collecter des données à partir des applications d'identité », page 167
- Section 11.9.2, « Migration du pilote du service de collecte de données », page 168
- Section 11.9.3, « Prise en charge des attributs et objets personnalisés », page 170
- Section 11.9.4, « Prise en charge de plusieurs ensembles de pilotes », page 173
- Section 11.9.5, « Configuration des pilotes pour une exécution en mode distant avec SSL », page 174

Si vous rencontrez des problèmes avec un ou plusieurs des pilotes et que vous ne savez pas comment les résoudre, reportez-vous à la section Troubleshooting the Drivers (Dépannage des pilotes) dans le manuel *NetIQ Identity Reporting Module Guide* (Guide du module NetIQ Identity Reporting).

11.9.1 Configuration du pilote du service de collecte de données (DSC) afin de collecter des données à partir des applications d'identité

Pour que les applications d'identité puissent fonctionner correctement avec Identity Reporting, vous devez configurer le pilote DCS pour qu'il prenne en charge le protocole OAuth.

REMARQUE

- Si vous utilisez Identity Reporting dans votre environnement, il vous suffit d'installer et de configurer le pilote DCS.
- Si plusieurs pilotes DCS sont configurés pour votre environnement, vous devez effectuer les étapes suivantes pour chacun d'eux.

---

1. Connectez-vous à Designer.
2. Ouvrez votre projet dans Designer.
3. (Facultatif) Si vous n'avez pas encore mis à niveau votre pilote DCS vers la version de correctif prise en charge, effectuez les étapes suivantes :
   - **3a** Téléchargez la dernière version du fichier de correctif pour le pilote DCS.
   - **3b** Lancez l'extraction du fichier de correctif dans un répertoire sur votre serveur.
   - **3c** Depuis un terminal, accédez à l'emplacement où le RPM du correctif a été extrait pour votre environnement et exécutez la commande suivante :

     ```
     rpm -Uvh novell-DXMLdcs.rpm
     ```

   - **3d** Redémarrez le coffre-fort d'identité.

3e Dans Designer, assurez-vous que la version du paquetage Data Collection Service Base installé est prise en charge. Si nécessaire, installez la dernière version avant de poursuivre. Pour plus d'informations sur la configuration logicielle requise, reportez-vous à la Section 8.6.2, « Conditions préalables à l'installation des composants du module Identity Reporting », page 86.

3f Redéployez et redémarrez le pilote DCS dans Designer.

4 Dans la vue **Mode plan**, cliquez avec le bouton droit de la souris sur le pilote DCS, puis sélectionnez **Propriétés**.

5 Cliquez sur **Configuration du pilote**.

6 Cliquez sur l'onglet **Paramètres du pilote**.

7 Cliquez sur **Show connection parameters** (Afficher les paramètres de connexion), puis sélectionnez **show** (Afficher).

8 Cliquez sur **SSO Service Support** (Support du service SSO), puis sélectionnez **Oui**.

9 Indiquez l'adresse IP et le port du module Identity Reporting.

10 Indiquez un mot de passe pour le client du service SSO. Le mot de passe par défaut est `driver`.

11 Cliquez sur **Appliquer**, puis sur **OK**.

12 Dans la vue **Modélisateur**, cliquez avec le bouton droit de la souris sur le pilote DCS, puis sélectionnez **Pilote > Déployer**.

13 Cliquez sur **Déployer**.

14 Si vous êtes invité à redémarrer le pilote DCS, cliquez sur **Oui**.

15 Cliquez sur **OK**.

11.9.2 Migration du pilote du service de collecte de données

Pour permettre la synchronisation des objets avec l'entrepôt d'informations d'identité, vous devez effectuer la migration du pilote du service de collecte de données.

1 Connectez-vous à iManager.

2 Dans le panneau **Présentation** relatif au pilote du service de collecte de données, sélectionnez **Migrer depuis le coffre-fort d'identité**.

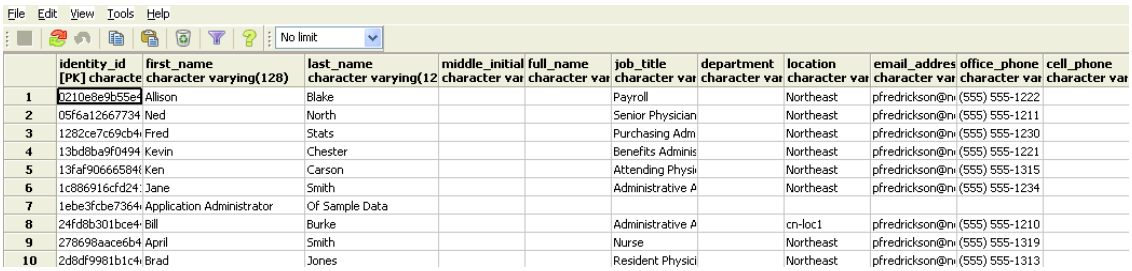
3 Sélectionnez les arborescences contenant des données pertinentes, puis cliquez sur **Démarrer**.

REMARQUE : en fonction du volume de données, la migration peut prendre plusieurs minutes. Veillez à attendre que la migration soit terminée avant de poursuivre.

---

4 Attendez la fin de la procédure de migration.

5 Les tables **idmrpt_identity** et **idmrpt_acct** fournissent des informations sur les identités et comptes figurant dans le coffre-fort d'identité. Assurez-vous qu'elles comportent les types d'informations suivants :

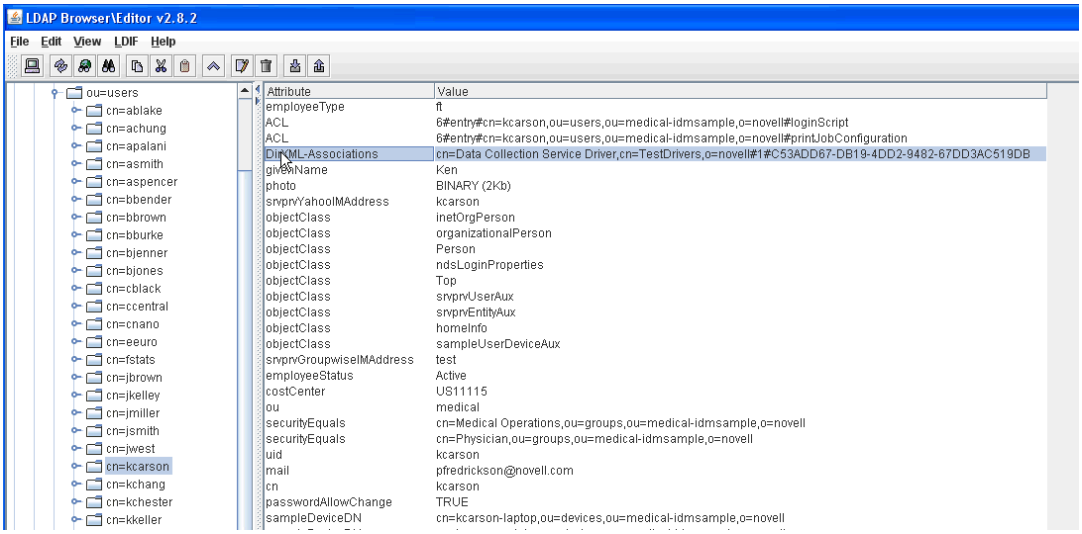

File Edit View Tools Help

No limit

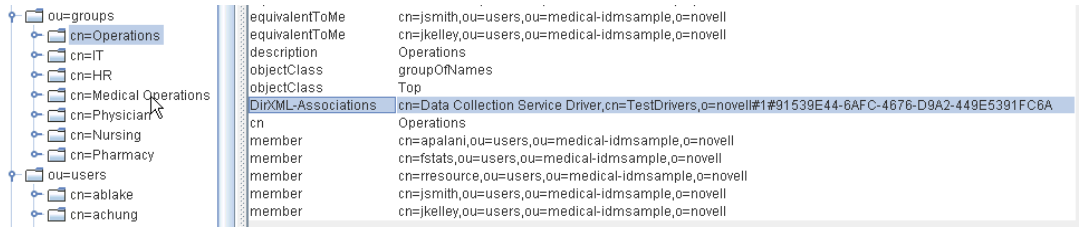
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	Allison	Blake			Payroll		Northeast	pfredrickson@n	(555) 555-1222	
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@n	(555) 555-1211	
3	1282ce7c69cb4	Fred	Stats			Purchasing Adm		Northeast	pfredrickson@n	(555) 555-1230	
4	13bd8ba9f0494	Kevin	Chester			Benefits Adminis		Northeast	pfredrickson@n	(555) 555-1221	
5	13faf906665846	Ken	Carson			Attending Physi		Northeast	pfredrickson@n	(555) 555-1315	
6	1c886916cfd24	Jane	Smith			Administrative A		Northeast	pfredrickson@n	(555) 555-1234	
7	1ebe3fcbe7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@n	(555) 555-1210	
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@n	(555) 555-1319	
10	2d8df9981b1c4	Brad	Jones			Resident Physici		Northeast	pfredrickson@n	(555) 555-1313	

6 Dans le navigateur LDAP, vérifiez que la procédure de migration a ajouté les références suivantes pour les attributs DirXML-Association :

- Pour chaque utilisateur, vérifiez les types d'informations suivants :



- Pour chaque groupe, vérifiez les types d'informations suivants :



7 Assurez-vous que les données de la table **idmrpt_group** sont semblables à ce qui suit :

group_name character var	group_desc character var	dynamic_gro boolean	dynamic_rule character var	nested_group boolean	idmrpt_valid_from timestamp without tin	idmrpt_deleted boolean	idmrpt_syn_state smallint
Pharmacy	Pharmacy	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
IT	Information Tec	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
HR	Human Resourc	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Physician	Physician	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Operations	Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Medical Operatic	Medical Operatic	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Nursing	Nursing	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1

Cette table présente le nom de chaque groupe et l'indicateur associé permettant de savoir s'il s'agit d'un groupe dynamique ou imbriqué. Elle indique également si le groupe a fait l'objet d'une migration. L'état de la synchronisation (idmrpt_syn_state) peut être défini sur 0 si un objet a été modifié dans l'application utilisateur mais que sa migration n'a pas encore été effectuée. Par exemple, si un utilisateur a été ajouté à un groupe mais que la migration du pilote n'a pas encore eu lieu, la valeur indiquée sera 0.

8 (Facultatif) Vérifiez les données dans les tables suivantes :

- idmrpt_approver
- idmrpt_association
- idmrpt_category
- idmrpt_container

- idmrpt_idv_drivers
- idmrpt_idv_prd
- idmrpt_role
- idmrpt_resource
- idmrpt_sod

9 (Facultatif) La table **idmrpt_ms_collect_state** contient les informations relatives à l'état de la collecte des données pour le pilote de la passerelle système gérée. Vérifiez qu'elle comporte désormais des lignes.

Cette table indique notamment quels sont les noeuds d'extrémité REST qui ont été exécutés pour les systèmes gérés. À ce stade, elle ne doit comporter aucune ligne puisque vous n'avez pas démarré le processus de collecte pour ce pilote.

11.9.3 Prise en charge des attributs et objets personnalisés

Vous pouvez configurer le pilote du service de collecte de données afin qu'il recueille et conserve les données relatives aux attributs et objets personnalisés qui ne font pas partie du modèle de collecte de données par défaut. Pour ce faire, vous devez modifier le filtre du pilote du service de collecte de données. La modification du filtre ne déclenche pas immédiatement la synchronisation des objets. En effet, les objets et attributs qui viennent d'être ajoutés sont envoyés vers les services de collecte de données lorsque des événements d'ajout, de modification ou de suppression surviennent au niveau du coffre-fort d'identité.

Pour prendre en charge des attributs et des objets personnalisés, vous devez modifier les rapports afin d'inclure des informations sur les attributs et objets étendus. Les vues suivantes fournissent des données actuelles et historiques sur les objets et les attributs étendus :

- idm_rpt_cfg.idmrpt_ext_idv_item_v
- idm_rpt_cfg.idmrpt_ext_item_attr_v

Cette procédure implique les opérations suivantes :

- « Configuration du pilote pour les objets étendus » page 170
- « Inclusion d'un nom et d'une description dans la base de données » page 171
- « Ajout d'attributs étendus à des types d'objets connus » page 172

Configuration du pilote pour les objets étendus

Vous pouvez ajouter n'importe quel objet ou attribut à la stratégie du filtre du service de collecte de données. Lorsque vous ajoutez un objet ou un attribut, vous devez vous assurer que vous assignez le GUID (avec synchronisation du canal Abonné) et la classe d'objet (avec notification du canal Abonné) comme indiqué dans l'exemple suivant :

```
<filter-class class-name="Device" publisher="ignore" publisher-create-
homedir="true" publisher-track-template-member="false" subscriber="sync">
<filter-attr attr-name="CN" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Description" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="GUID" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Object Class" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="notify"/>
<filter-attr attr-name="Owner" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Serial Number" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="sampleDeviceModel" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
<filter-attr attr-name="sampleDeviceType" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
</filter-class>
```

Inclusion d'un nom et d'une description dans la base de données

Si vous souhaitez que l'objet soit associé à un nom et à une description dans la base de données, vous devez ajouter une stratégie d'assignation de schéma pour _dcsName et _dcsDescription. La stratégie d'assignation de schéma permet d'associer les valeurs d'attribut de l'instance d'objet aux colonnes idmrpt_ext_idv_item.item_name et idmrpt_ext_idv_item.item_desc. Si vous n'ajoutez pas de stratégie d'assignation de schéma, les attributs seront indiqués dans la table enfant idmrpt_ext_item_attr.

Exemple :

```
<attr-name class-name="Device">
<nds-name>CN</nds-name>
<app-name>_dcsName</app-name>
</attr-name>
<attr-name class-name="Device">
<nds-name>Description</nds-name>
<app-name>_dcsDescription</app-name>
</attr-name>
```

L'exemple de code SQL suivant vous permet d'afficher ces valeurs d'objets et d'attributs dans la base de données :

```
SELECT
    item.item_dn,
    item.item_name,
    item.item_desc,
    attr.attribute_name,
    itemAttr.attribute_value,
    item.idmrpt_deleted as item_deleted,
    itemAttr.idmrpt_deleted as attr_deleted,
    item.item_desc,
    obj.object_class
FROM
    idm_rpt_data.idmrpt_ext_idv_item as item, idm_rpt_data.idmrpt_ext_item_attr
itemAttr, idm_rpt_data.idmrpt_ext_attr as attr, idm_rpt_data.idmrpt_ext_obj as obj
WHERE
    item.object_id = obj.object_id and itemAttr.attribute_id = attr.attribute_id
and itemAttr.cat_item_id = item.item_id
ORDER BY
    item.item_dn, item.item_name
```

Ajout d'attributs étendus à des types d'objets connus

Si un attribut est ajouté à la stratégie du filtre pour le pilote du service de collecte de données et qu'il n'est pas explicitement assigné à la base de données de création de rapports dans le fichier de référence XML (`IdmrptIdentity.xml`), la valeur correspondante est indiquée (et mise à jour) dans la table idmrpt_ext_item_attr, avec la référence d'attribut dans la table idmrpt_ext_attr.

L'exemple de code SQL suivant permet d'afficher ces attributs étendus :

```
SELECT
    acct.idv_acct_dn,
    attrDef.attribute_name,
    attribute_value,
    attrVal.idmrpt_valid_from,
    cat_item_attr_id,
    attrVal.idmrpt_deleted,
    attrVal.idmrpt_syn_state
FROM
    idm_rpt_data.idmrpt_ext_item_attr as attrVal, idm_rpt_data.idmrpt_ext_attr as
attrDef, idm_rpt_data.idmrpt_identity as idd, idm_rpt_data.idmrpt_idv_acct as acct
WHERE attrVal.attribute_id = attrDef.attribute_id and idd.identity_id =
acct.identity_id and attrVal.cat_item_id = acct.identity_id and cat_item_type_id =
'IDENTITY'
```

En plus de l'objet User, vous pouvez ajouter des attributs étendus à la stratégie du filtre pour les objets suivants et alimenter la base de données avec ces attributs :

- nrfRole
- nrfResource
- Conteneurs

  REMARQUE : le produit installé prend en charge les conteneurs organizationUnit, Organization et Domain. Les types de conteneur sont tenus à jour dans la table idmrpt_container_types.

- Groupe
- nrfSod

Vous pouvez voir l'association entre les attributs étendus et l'objet ou la table parent en examinant la colonne idmrpt_cat_item_types.idmrpt_table_name. Cette colonne indique comment joindre la colonne idm_rpt_data.idmrpt_ext_item_attr.cat_item_id à la clé primaire de la table parent.

11.9.4 Prise en charge de plusieurs ensembles de pilotes

Le nouveau paquetage relatif à la définition de l'étendue du service de collecte de données (NOVLDCSSCPNG) fournit un ensemble de fonctions permettant la définition statique ou dynamique de l'étendue pour les environnements d'entreprise disposant de plusieurs ensembles de pilotes et paires associant un pilote de service de collecte de données et un pilote de passerelle système gérée.

Pendant ou après l'installation, vous devez déterminer le rôle du pilote du service de collecte de données pour lequel ce paquetage est installé. Vous devez sélectionner l'un des rôles suivants :

- **Primaire** Le pilote synchronise tout, à l'exception des sous-arborescences des autres ensembles de pilotes. Un pilote de service de collecte de données primaire peut tout à fait traiter un coffre-fort d'identité dans son ensemble ou fonctionner en association avec un ou plusieurs pilotes secondaires.
- **Secondaire** Le pilote synchronise uniquement son propre ensemble de pilotes et rien d'autre. Un pilote de service de collecte de données secondaire nécessite généralement qu'un pilote primaire s'exécute sur un autre ensemble de pilotes ou aucune donnée hors de l'ensemble de pilotes local n'est envoyée au service de collecte de données.

  Si vous utilisez la procédure d'installation intégrée afin d'ajouter un deuxième serveur dans l'arborescence, ce serveur reçoit uniquement une copie de la racine et sa propre partition de l'ensemble de pilotes. Si vous utilisez également le pilote du service de collecte de données en tant que pilote primaire sur le serveur secondaire, ce pilote ne peut pas voir les modifications des objets dont il a besoin pour créer les rapports.
- **Personnalisé** Permet à l'administrateur d'indiquer des règles pour définir une étendue personnalisée. La seule étendue implicite correspond à l'ensemble de pilotes local ; tout le reste n'est pas pris en compte, sauf ajout explicite à la liste des étendues personnalisées. Une étendue personnalisée correspond à un conteneur dont le nom distinctif est indiqué en utilisant des barres obliques. Il s'agit d'un conteneur figurant dans le coffre-fort d'identité, dont la sous-arborescence ou les subordonnés doivent être synchronisés.

Le paquetage de définition de l'étendue est uniquement requis dans certains scénarios de configuration, comme décrit ci-dessous :

- **Un seul serveur, avec un seul ensemble de pilotes, pour le coffre-fort d'identité:** Dans ce scénario, vous n'avez pas besoin de définir l'étendue et, par conséquent, il n'est pas nécessaire d'installer le paquetage correspondant.
- **Plusieurs serveurs, avec un seul ensemble de pilotes, pour le coffre-fort d'identité:** Avec un tel scénario, vous devez suivre les instructions ci-dessous :
  - Assurez-vous que le serveur Identity Manager contient les répliques de toutes les partitions à partir desquelles les données doivent être collectées.
  - Dans ce scénario, il n'est pas nécessaire de définir l'étendue, vous n'avez donc pas besoin d'installer le paquetage correspondant.
- **Plusieurs serveurs, avec plusieurs ensembles de pilotes, pour le coffre-fort d'identité:**

  Avec un tel scénario, il existe deux configurations basiques possibles :
  - Tous les serveurs disposent d'une réplique de toutes les partitions à partir desquelles les données doivent être collectées.

Avec une telle configuration, vous devez suivre les instructions ci-dessous :

- Il est nécessaire de définir l'étendue pour éviter qu'une même modification soit traitée par plusieurs pilotes DCS.
- Vous devez installer le paquetage de définition de l'étendue sur tous les pilotes DCS.
- Vous devez sélectionner un pilote DCS comme pilote primaire.
- Vous devez configurer tous les autres pilotes DCS comme pilotes secondaires.

- Tous les serveurs *ne disposent pas* d'une réplique de toutes les partitions à partir desquelles les données doivent être collectées.

  Avec une telle configuration, il y a deux cas possibles :

  - Toutes les partitions à partir desquelles les données doivent être collectées figurent sur *un seul* serveur Identity Manager

    Dans ce cas, vous devez suivre les instructions ci-dessous :

    - Il est nécessaire de définir l'étendue pour éviter qu'une même modification soit traitée par plusieurs pilotes DCS.
    - Vous devez installer le paquetage de définition de l'étendue sur tous les pilotes DCS.
    - Vous devez configurer tous les pilotes DCS comme pilotes primaires.
  - Toutes les partitions à partir desquelles les données doivent être collectées *ne figurent pas* sur un seul serveur Identity Manager (certaines partitions figurent sur plusieurs serveurs Identity Manager).

    Dans ce cas, vous devez suivre les instructions ci-dessous :

    - Il est nécessaire de définir l'étendue pour éviter qu'une même modification soit traitée par plusieurs pilotes DCS.
    - Vous devez installer le paquetage de définition de l'étendue sur tous les pilotes DCS.
    - Vous devez configurer tous les pilotes DCS comme pilotes personnalisés.

      Vous devez définir des règles d'étendue personnalisée pour chaque pilote et vous assurer de ne pas créer des étendues qui se chevauchent.

11.9.5 Configuration des pilotes pour une exécution en mode distant avec SSL

Dans le cadre d'une exécution en mode distant, vous pouvez configurer le pilote du service de collecte de données et celui de la passerelle système gérée afin qu'ils utilisent SSL. Cette section présente les étapes de configuration permettant d'exécuter des pilotes en mode distant avec SSL.

Pour configurer SSL en utilisant un Keystore pour le pilote de la passerelle système gérée :

1. Créez un certificat de serveur dans iManager.
   - **1a** Dans la vue **Roles and Tasks** (Rôles et tâches), cliquez sur **NetIQ Certificate Server > Create Server Certificate** (Créer un certificat de serveur).
   - **1b** Recherchez et sélectionnez l'objet serveur sur lequel le pilote de la passerelle système gérée est installé.
   - **1c** Indiquez le surnom que vous souhaitez attribuer au certificat.
   - **1d** Sélectionnez **Standard** comme méthode de création, puis cliquez sur **Suivant**.
   - **1e** Cliquez sur **Terminer**, puis sur **Fermer**.

2 Exportez le certificat du serveur en utilisant iManager.

2a Dans la vue **Rôles et tâches** (Rôles et tâches), cliquez sur **NetIQ Certificate Server > Server Certificates** (Certificats de serveur).

2b Sélectionnez le certificat créé à l'Étape 1 page 174 et cliquez sur **Exporter**.

2c Dans le menu **Certificats**, sélectionnez le nom de votre certificat.

2d Assurez-vous que l'option **Export private key** (Exporter la clé privée) est cochée.

2e Entrez le mot de passe et cliquez sur **Suivant**.

2f Cliquez sur **Save the exported certificate** (Enregistrer le certificat exporté) et enregistrez le certificat pfx exporté.

3 Importez dans le Keystore Java le certificat pfx exporté à l'Étape 2 page 175.

3a Utilisez le keytool mis à disposition avec Java. Vous devez utiliser JDK 6 ou une version ultérieure.

3b À l'invite, entrez la commande suivante :

```
keytool -importkeystore -srckeystore pfx certificate -srcstoretype
PKCS12 -destkeystore Keystore Name
```

Exemple :

```
keytool -importkeystore -srckeystore cert.pfx -srcstoretype PKCS12
-destkeystore msgw.jks
```

3c Entrez le mot de passe lorsque vous y êtes invité.

4 Modifiez la configuration du pilote de la passerelle système gérée afin d'utiliser le keystore avec iManager.

4a Dans **Présentation d'Identity Manager**, cliquez sur l'ensemble de pilotes qui contient le pilote de la passerelle système gérée.

4b Cliquez sur l'icône d'état du pilote, puis sélectionnez **Modifier les propriétés > Configuration du pilote**.

4c Activez l'option **Show Connection Parameters** (Afficher les paramètres de connexion) et indiquez qu'il s'agit du mode distant dans le champ **Driver configuration mode** (Mode de configuration du pilote).

4d Entrez le chemin d'accès complet du fichier keystore et le mot de passe.

4e Enregistrez les modifications et redémarrez le pilote.

5 Modifiez la configuration du pilote du service de collecte de données afin d'utiliser le keystore avec iManager.

5a Dans **Présentation d'Identity Manager**, cliquez sur l'ensemble de pilotes qui contient le pilote de la passerelle système gérée.

5b Cliquez sur l'icône d'état du pilote, puis sélectionnez **Modifier les propriétés > Configuration du pilote**.

5c Sous l'en-tête **Managed System Gateway Registration** (Enregistrement de la passerelle système gérée), indiquez qu'il s'agit du mode distant dans le champ **Managed System Gateway Driver Configuration Mode** (Mode de configuration du pilote de passerelle système gérée).

5d Entrez le chemin d'accès complet du fichier keystore, le mot de passe et l'alias indiqué à l'Étape 1c page 174.

5e Enregistrez les modifications et redémarrez le pilote.

11.10 Configuration d'Identity Reporting

Une fois l'installation d'Identity Reporting terminée, vous avez toujours la possibilité de modifier de nombreuses propriétés de l'installation. Pour apporter des modifications, exécutez le fichier de l'utilitaire de mise à jour de la configuration (`configupdate.sh`).

Si vous utilisez l'outil de configuration pour modifier l'un des paramètres d'Identity Reporting, vous devez redémarrer Tomcat pour que les modifications soient prises en compte. Toutefois, vous n'avez pas à redémarrer le serveur après avoir effectué des modifications dans l'interface utilisateur Web pour Identity Reporting.

11.10.1 Ajout manuel de la source de données dans la page des services de collecte de données d'identité

1. Connectez-vous à l'application Identity Reporting.
2. Cliquez sur **Sources de données**.
3. Cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Ajouter une source de données**, cliquez sur le bouton d'option **Effectuez la sélection à partir d'une liste prédéfinie**.
5. Sélectionnez **IDMDCSDataSource**.
6. Cliquez sur **Enregistrer**.

11.10.2 Génération de rapports à partir d'une base de données Oracle

Identity Reporting offre la possibilité de générer des rapports à partir de bases de données Oracle à distance. Assurez-vous que le fichier ojbc.jar est bien présent sur le serveur sur lequel vous exécutez la base de données Oracle.

Pour plus d'informations sur les bases de données Oracle prises en charge, reportez-vous à la Section 8.6.4, « Configuration système requise pour Identity Reporting », page 88.

11.10.3 Génération manuelle du schéma de base de données

Pour créer manuellement le schéma de base de données après l'installation, effectuez l'une des procédures suivantes pour votre base de données :

Configuration du schéma create_rpt_roles_and_schemas.sql pour la base de données PostgreSQL

1 Ajoutez les rôles requis à la base de données à l'aide des fichiers SQL create_dcs_roles_and_schemas.sql et `create_rpt_roles_and_schemas.sql` situés dans `/mnt/reporting/sql`.

1. Connectez-vous à PGAdmin en tant qu'utilisateur postgres.
2. Exécutez l'outil de requête.
3. Pour créer les procédures `Create_rpt_roles_and_schemas` et `Create_dcs_roles_and_schemas`, copiez le contenu à partir de ces fichiers SQL vers l'outil de requête et exécutez-le sur la base de données connectée.
4. Pour créer les rôles IDM_RPT_DATA, IDM_RPT_CFG et IDMRPTUSER, exécutez les commandes suivantes dans l'ordre indiqué :

```
Select CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>');

Select CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>', '<Set pwd for IDMRPTUSER>');
```

5. Pour créer le schéma IDM_RPT_DATA, copiez le contenu du fichier `get_formatted_user_dn.sql` à partir de /`mnt/reporting/sql` dans l'outil de requête et exécutez-le sur la base de données connectée.

Configuration du schéma create_rpt_roles_and_schemas.sql pour la base de données Oracle

1 Ajoutez les rôles requis à la base de données à l'aide des fichiers `create_dcs_roles_and_schemas orcale.sql` et `create_rpt_roles_and_schemas orcale.sql` situés dans `/mnt/reporting/sql`.

1. Connectez-vous à SQL Developer en tant qu'administrateur de la base de données.
2. Pour créer les procédures `Create_rpt_roles_and_schemas` et `Create_dcs_roles_and_schemas`, copiez le contenu à partir de ces SQL dans SQL Developer et exécutez-le sur la base de données connectée.
3. Pour créer les rôles IDM_RPT_DATA, IDM_RPT_CFG et IDMRPTUSER, exécutez les commandes suivantes dans l'ordre indiqué :

```
begin
CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>');
end;

begin
CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>', '<Set pwd for IDMRPTUSER>');
end;
```

4. Pour créer des schémas IDM_RPT_DATA, copiez le contenu de `get_formatted_user_dn-oracle.sql` dans SQL Developer à partir de /`mnt/reporting/sql et exécutez-le sur la base de données connectée`.

11.10.4 Effacement des sommes de contrôle de la base de données

1. Recherchez les fichiers `.sql` suivants dans `/opt/netiq/idm/apps/IDMReporting/sql`.
   - `DbUpdate-01-run-as-idm_rpt_cfg.sql`
   - `DbUpdate-02-run-as-idm_rpt_cfg.sql`
   - `DbUpdate-03-run-as-idm_rpt_data.sql`
   - `DbUpdate-04-run-as-idm_rpt_data.sql`
   - `DbUpdate-05-run-as-idm_rpt_data.sql`
   - `DbUpdate-06-run-as-idm_rpt_cfg.sql`
2. Effacez les sommes de contrôle de la base de données.

   2a Pour exécuter la commande clearchsum avec chaque `.sql`, ajoutez la ligne suivante au début de chaque fichier :

   ```
   update DATABASECHANGELOG set MD5SUM = NULL;
   ```

   Le contenu modifié doit ressembler à ce qui suit :

   ```
   -- *********************************************************************
   -- Update Database Script
   -- *********************************************************************
   -- Change Log: IdmDcsDataDropViews.xml
   -- Ran at: 2/23/18 5:17 PM
   -- Against: IDM_RPT_CFG@jdbc:oracle:thin:@192.99.170.20:1521/orcl
   -- Liquibase version: 3.5.1
   -- *********************************************************************
   update databasechangelog set md5sum = null;
   ```

   2b Exécutez chaque fichier `.sql` avec l'utilisateur correspondant.
3. Validez les modifications apportées à la base de données.

11.10.5 Déploiement des API REST pour Identity Reporting

Identity Reporting intègre plusieurs API REST qui permettent d'utiliser différentes fonctionnalités de création de rapports. Ces API REST utilisent le protocole OAuth2 pour l'authentification.

Sous Tomcat, les fichiers `WAR rptdoc` et `WAR dcsdoc` sont automatiquement déployés lorsque Identity Reporting est installé.

11.10.6 Connexion à une base de données PostgreSQL distante

Si votre base de données PostgreSQL est installée sur un serveur distinct, vous devez modifier les paramètres par défaut dans les fichiers `postgresql.conf` et `pg_hba.conf` dans la base de données distante.

1. Modifiez l'adresse d'écoute dans le fichier `postgresql.conf`.

   Par défaut, PostgreSQL permet d'écouter la connexion de l'hôte local, mais n'autorise pas une connexion TCP/IP à distance. Pour autoriser une connexion TCP/IP à distance, ajoutez l'entrée suivante au fichier `/opt/netiq/idm/postgres/data/postgresql.conf` :

   ```
   listen_addresses = '*'
   ```

   Si vous disposez de plusieurs interfaces sur le serveur, vous pouvez spécifier une interface spécifique à écouter.

2 Ajoutez une entrée d'authentification client au fichier `pg_hba.conf`.

Par défaut, PostgreSQL accepte uniquement les connexions provenant de `localhost` (hôte local). Il refuse les connexions à distance. Cela est contrôlé par l'application d'une règle de contrôle d'accès qui permet à un utilisateur de se connecter à partir d'une adresse IP après avoir entré un mot de passe valide (mot clé md5). Pour accepter une connexion à distance, ajoutez l'entrée suivante au fichier `/opt/netiq/idm/postgres/data/pg_hba.conf`.

```
host all all 0.0.0.0/0 md5
```

Par exemple : 192.168.104.24/26 trust

Cela fonctionne uniquement pour les adresses IPv4. Pour les adresses IPv6, ajoutez l'entrée suivante :

```
host all all ::0/0 md5
```

Si vous souhaitez autoriser la connexion à partir de plusieurs ordinateurs client sur un réseau spécifique, indiquez l'adresse réseau au format d'adresse CIDR dans cette entrée.

Le fichier pg_hba.conf prend en charge les formats d'authentification client suivants.

- local database user authentication-method [authentication-option]
- host database user CIDR-address authentication-method [authentication-option]
- hostssl database user CIDR-address authentication-method [authentication-option]
- hostnossl database user CIDR-address authentication-method [authentication-option]

Au lieu du format d'adresse CIDR, vous pouvez spécifier l'adresse IP et le masque de réseau dans des champs distincts à l'aide du format suivant :

- host database user IP-address IP-mask authentication-method [authentication-option]
- hostssl database user IP-address IP-mask authentication-method [authentication-option]
- hostnossl database user IP-address IP-mask authentication-method [authentication-option]

3 Testez la connexion à distance.

3a Redémarrez le serveur PostgreSQL à distance.

3b Connectez-vous au serveur à distance à l'aide du nom d'utilisateur et du mot de passe.

V Installation de Designer

Cette section vous guide dans la procédure d'installation de Designer pour Identity Manager.

12 Planification de l'installation de Designer

Cette section présente les conditions préalables, les considérations et la configuration système requise pour installer Designer.

12.1 Liste de contrôle pour l'installation de Designer

Avant de commencer l'installation, NetIQ recommande de passer en revue la procédure suivante.

	Éléments de la liste de contrôle
❑	1. Passez en revue les considérations relatives à l'installation de Designer pour vous assurer que l'ordinateur répond aux conditions préalables. Pour plus d'informations, reportez-vous à la Section 12.2, « Conditions préalables à l'installation de Designer », page 183.
❑	2. Vérifiez que l'ordinateur sur lequel vous installez Designer remplit les conditions matérielles et logicielles requises. Pour plus d'informations, reportez-vous à la Section 12.3, « Configuration système requise pour Designer », page 184.
❑	3. Installez Designer. Pour plus d'informations, reportez-vous au Section 13, « Installation de Designer », page 185.
❑	4. (Facultatif) Pour démarrer un projet dans votre solution Identity Manager, reportez-vous au manuel NetIQ Designer for Identity Manager (Guide d'administration de NetIQ Designer for Identity Manager).

12.2 Conditions préalables à l'installation de Designer

Cette section présente les conditions préalables et les considérations pour l'installation de Designer.

- Avant d'installer Designer sur un ordinateur exécutant un système d'exploitation Linux, vous devez installer les utilitaires GNU gettext. Ces utilitaires offrent une infrastructure pour les messages internationalisés et multilingues. Pour plus d'informations sur la prise en charge des langues, reportez-vous à la Section 5.10, « Présentation du support linguistique », page 48.
- Avant d'installer Designer sur un ordinateur exécutant le système d'exploitation RHEL 7.4, vous devez installer le module `gtk2-2.24.31-1.el7.x86_64.rpm`. Par exemple, vous pouvez télécharger l'ensemble à partir du site Web du fournisseur du système d'exploitation.

12.3 Configuration système requise pour Designer

Cette section décrit la configuration minimale requise pour le(s) serveur(s) sur le(s)quel(s) vous souhaitez installer Designer. Veuillez passer en revue les conditions préalables requises et les considérations relatives à l'installation, en particulier celles liées au système d'exploitation.

Catégorie	Configuration requise
Processeur	1 GHz
Espace disque	1 Go
Mémoire	1 Go
Systèmes d'exploitation (certifiés)	L'un des systèmes d'exploitation 64 bits suivants : **Serveurs** ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3 ◆ openSUSE Leap 42.1 **génériques** ◆ SLED 12 SP3 ◆ SLED 12 SP2 **REMARQUE :** *Certifié* signifie que le système d'exploitation a été entièrement testé et est pris en charge.
Systèmes d'exploitation (pris en charge)	Dernières versions des Service Packs pour les systèmes d'exploitation certifiés **REMARQUE :** *Pris en charge* signifie que le système d'exploitation n'a pas encore été testé, mais qu'il devrait fonctionner
Système de virtualisation	◆ Hyper-V Server 2012 R2 ◆ VMware ESX 5.5 ou version ultérieure NetIQ prend en charge Identity Manager sur les systèmes de virtualisation d'entreprise qui sont officiellement compatibles avec les systèmes d'exploitation sur lesquels les produits NetIQ s'exécutent. Aussi longtemps que les fournisseurs de systèmes de virtualisation prennent officiellement en charge ces systèmes d'exploitation, NetIQ prend en charge l'intégralité d'Identity Manager sur ces derniers.

13 Installation de Designer

Cette section décrit la procédure d'installation de Designer. Vous pouvez effectuer l'installation en mode Interface graphique (GUI) ou Console.

Pour installer Designer :

1. Téléchargez le fichier `Identity_Manager_Linux_LDAP_Designer.tar.gz` à partir du site Web de téléchargements NetIQ.
2. Accédez au répertoire dans lequel vous souhaitez extraire le fichier.
3. Exécutez la commande suivante :

   ```
   tar -zxvf Identity_Manager_Linux_LDAP_Designer.tar.gz
   ```

4. Exécutez une des commandes suivantes pour installer Designer.

   Console : `./install`

   Interface graphique : `./install -i console`
5. Suivez les invites et effectuez l'installation.

VI Installation d'Analyzer

Cette section vous guide tout au long de la procédure d'installation d'Analyzer pour Identity Manager. Analyzer est un composant client lourd que vous installez sur un poste de travail. Vous pouvez l'utiliser pour contrôler et nettoyer les données des systèmes connectés que vous souhaitez ajouter à votre solution Identity Manager. En utilisant Analyzer pendant la phase de planification, vous pouvez déterminer les modifications à apporter et le meilleur moyen de les réaliser.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous à la Section 14.1, « Liste de contrôle pour l'installation d'Analyzer », page 189.

14 Planification de l'installation d'Analyzer

Cette section fournit des conseils pour la préparation de l'installation d'Analyzer pour Identity Manager. NetIQ recommande de passer en revue la procédure d'installation avant de commencer.

14.1 Liste de contrôle pour l'installation d'Analyzer

Avant d'entamer le processus d'installation, NetIQ vous recommande de passer en revue les étapes suivantes.

	Éléments de la liste de contrôle
❑	1. Renseignez-vous sur les interactions entre les différents composants Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 1, « Aperçu des composants Identity Manager », page 17.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.7, « Configuration de serveur et scénarios d'installation recommandés », page 39.
❑	3. Assurez-vous que votre environnement remplit les conditions nécessaires pour héberger Analyzer. Pour plus d'informations, reportez-vous aux sections suivantes : ◆ Section 14.2, « Conditions préalables à l'installation d'Analyzer », page 190 ◆ Section 14.3, « Configuration système requise pour Analyzer », page 190
❑	4. Pour installer Analyzer, reportez-vous aux sections suivantes : ◆ Pour utiliser l'assistant d'installation, reportez-vous à la Section 15.1, « Utilisation de l'assistant pour installer Analyzer », page 193. ◆ Pour effectuer une installation en mode silencieux, reportez-vous à la Section 15.2, « Installation d'Analyzer en mode silencieux », page 194
❑	5. (Facultatif) Pour recevoir et afficher automatiquement les événements d'audit d'Analyzer, installez le client XDAS. Pour plus d'informations, reportez-vous à la Section 15.4, « Installation d'un client Audit pour Analyzer », page 195.
❑	6. Pour activer Analyzer, reportez-vous à la section Section 24.4.2, « Activation d'Analyzer », page 247.
❑	7. (Facultatif) Pour mettre à niveau Analyzer, reportez-vous à la Section 26.7, « Mise à niveau d'Analyzer », page 282.

14.2 Conditions préalables à l'installation d'Analyzer

Cette section présente les conditions préalables et les considérations pour l'installation d'Analyzer.

- Avant d'installer Analyzer sur un ordinateur exécutant le système d'exploitation SLES 12 SP3, assurez-vous que les bibliothèques suivantes sont installées :
  - `libswt3-gtk2-3.3.0-0.20.8.9mdv2008.0.i586.rpm`
  - `libxcomposite1-0.4.1-1mdv2010.1.i586.rpm`
  - `libgdk_pixbuf2.0_0-2.20.1-1mdv2010.1.i586.rpm`
  - `libgtk+-x11-2.0_0-2.12.1-2.1mdv2008.0.i586.rpm`
- Avant d'installer Analyzer sur un ordinateur exécutant des plates-formes RHEL 7.3 ou version ultérieure, vous devez installer le module `gtk2.i686.rpm`. Par exemple, vous pouvez télécharger l'ensemble à partir du site Web du fournisseur du système d'exploitation.

14.3 Configuration système requise pour Analyzer

Cette section décrit la configuration minimale requise pour les serveurs sur lesquels vous souhaitez installer Analyzer. Veuillez passer en revue les conditions préalables requises et les considérations relatives à l'installation, en particulier celles liées au système d'exploitation.

Catégorie	Configuration requise
Processeur	1 GHz
Mémoire	2 Go
Résolution vidéo	1024*768 (1280*1025 recommandés)
Système d'exploitation (certifié)	L'un des systèmes d'exploitation suivants : ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3 ◆ openSUSE Leap 42.1 **REMARQUE :** *Certifié* signifie que le système d'exploitation a été entièrement testé et est pris en charge.
Systèmes d'exploitation (pris en charge)	Dernières versions des Service Packs pour les systèmes d'exploitation certifiés **REMARQUE :** *Pris en charge* signifie que le système d'exploitation n'a pas encore été testé, mais qu'il devrait fonctionner
Système de virtualisation	◆ Hyper-V Server 2012 R2 ◆ VMware ESX 5.0 et versions ultérieures NetIQ prend en charge Identity Manager sur les systèmes de virtualisation d'entreprise qui sont officiellement compatibles avec les systèmes d'exploitation sur lesquels les produits NetIQ s'exécutent. NetIQ prend en charge l'intégralité de la pile Identity Manager sur les systèmes de virtualisation dont les éditeurs prennent officiellement en charge ces systèmes d'exploitation.

Catégorie	Configuration requise
Logiciels supplémentaires	◆ Utilitaire gettext

15 Installation d'Analyzer

Cette section vous guide tout au long de la procédure d'installation d'Analyzer et de configuration de votre environnement pour Analyzer.

15.1 Utilisation de l'assistant pour installer Analyzer

La procédure suivante décrit comment installer Analyzer sur une plate-forme Linux ou Windows en utilisant un assistant d'installation, au format interface graphique ou à partir de la console. Pour effectuer une installation sans surveillance en mode silencieux, reportez-vous à la Section 15.2, « Installation d'Analyzer en mode silencieux », page 194.

Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise reprises à la Section 14.1, « Liste de contrôle pour l'installation d'Analyzer », page 189.

1. Connectez-vous en tant qu'utilisateur `root` ou administrateur à l'ordinateur sur lequel vous souhaitez installer Analyzer.
2. (Conditionnel) Si vous avez le fichier image `.iso` pour le paquetage d'installation d'Identity Manager, accédez au répertoire contenant les fichiers d'installation d'Analyzer, situé par défaut dans le répertoire `/Analyzer/packages`.
3. (Conditionnel) Si vous avez téléchargé les fichiers d'installation d'Analyzer, procédez comme suit :
   - **3a** Accédez au fichier `.tgz` ou `win.zip` pour l'image téléchargée.
   - **3b** Extrayez le contenu du fichier dans un dossier sur l'ordinateur local.
4. Exécutez le programme d'installation :

   ```
   ./install
   ```
5. Suivez les instructions de l'assistant jusqu'à ce que vous ayez terminé l'installation d'Analyzer.
6. Une fois la procédure d'installation terminée, passez en revue le résumé de post-installation pour vérifier l'état de l'installation et l'emplacement du fichier journal pour Analyzer.
7. Cliquez sur **Terminé**.
8. (Conditionnel) Exécutez les étapes de la Section 15.3, « Ajout de XULrunner au fichier Analyzer.ini », page 194.
9. (Facultatif) Afin de configurer les services basés sur les rôles pour Analyzer sous Windows, ouvrez le lien vers le site Web `gettingstarted.html`, situé par défaut dans le répertoire `C:\Program Files (x86)\NetIQ\Tomcat\webapp\nps\help\en\install`.

   Vous pouvez utiliser iManager pour configurer les services basés sur les rôles.
10. Pour activer Analyzer, reportez-vous à la section « Activation d'Analyzer » page 247.

15.2 Installation d'Analyzer en mode silencieux

Une installation silencieuse (non interactive) n'affiche aucune interface utilisateur et ne pose aucune question à l'utilisateur. À la place, InstallAnywhere utilise des informations contenues dans un fichier par défaut `analzerInstaller.properties`. Vous pouvez exécuter l'installation en mode silencieux avec le fichier par défaut ou modifier le fichier afin de personnaliser la procédure d'installation.

Par défaut, le programme d'installation installe Analyzer dans le répertoire `Program Files (x86)\NetIQ\Analyzer`.

1. Connectez-vous en tant qu'utilisateur `root` ou administrateur à l'ordinateur sur lequel vous souhaitez installer Analyzer.
2. (Conditionnel) Si vous disposez du fichier image `.iso` pour le paquetage d'installation d'Identity Manager, accédez au répertoire contenant les fichiers d'installation d'Analyzer, par défaut dans le répertoire `products/Analyzer/`.
3. (Conditionnel) Si vous avez téléchargé les fichiers d'installation d'Analyzer à partir du site Web de téléchargement NetIQ, procédez comme suit :
   - **3a** Accédez au fichier `.tgz` ou `win.zip` pour l'image téléchargée.
   - **3b** Extrayez le contenu du fichier dans un dossier sur l'ordinateur local.
4. (Facultatif) Pour indiquer un chemin d'installation autre que celui par défaut, procédez comme suit :
   - **4a** Ouvrez le fichier `analyzerInstaller.properties` situé par défaut dans le répertoire `products/Analyzer/`.
   - **4b** Ajoutez le texte suivant dans le fichier de propriétés :

     `USER_INSTALL_DIR=`*`installation_path`*
5. Pour exécuter l'installation en mode silencieux, lancez l'une des commandes suivantes :
   - **Linux** : `install -i silent -f analyzerInstaller.properties`
   - **Windows** : `install.exe -i silent -f analyzerInstaller.properties`
6. (Conditionnel) Sous Linux, effectuez les étapes de la Section 15.3, « Ajout de XULrunner au fichier Analyzer.ini », page 194.
7. Pour activer Analyzer, reportez-vous à la section « Activation d'Analyzer » page 247.

15.3 Ajout de XULrunner au fichier Analyzer.ini

Avant d'exécuter Analyzer sur une plate-forme Linux, vous devez modifier les assignations XULRunner.

REMARQUE : sous SLED 11, la version recommandée de XULrunner est 1.9.0.19. Sous openSUSE 11.4, il s'agit de la version 1.9.0.2. Ces versions sont fournies avec les systèmes d'exploitation.

---

1. Accédez au répertoire d'installation `Analyzer`, se trouvant par défaut aux emplacements suivants :

   `home/admin/analyzer`
2. Ouvrez le fichier `Analyzer.ini` dans l'éditeur gedit.
3. Ajoutez la ligne suivante à la fin de la liste des paramètres :

```
-Dorg.eclipse.swt.browser.XULRunnerPath=/usr/lib/xulrunner-1.9/
```

Par exemple, le fichier `Analyzer.ini` doit se présenter comme suit :

```
-vmargs
-Xms256m
-Xmx1024m
-XX:MaxPermSize=128m
-XX:+UseParallelGC
-XX:ParallelGCThreads=20
-XX:+UseParallelOldGC
-Dorg.eclipse.swt.browser.XULRunnerPath=/usr/lib/xulrunner-1.9/
```

4 Enregistrez le fichier `Analyzer.ini`.

5 Lancez Analyzer.

15.4 Installation d'un client Audit pour Analyzer

Analyzer comprend une bibliothèque XDAS qui génère automatiquement des événements d'audit à partir de l'éditeur Navigateur de données lorsque vous renvoyez des mises à jour de données vers l'application. Pour plus d'informations sur l'utilisation de l'éditeur Navigateur de données pour mettre à jour des données dans l'application source, reportez-vous à la section « Modifying Data » (Modification des données) du manuel *NetIQ Analyzer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Analyzer pour Identity Manager).

Pour afficher ces événements d'audit, installez un client XDAS qui peut recevoir les événements d'audit à partir d'Analyzer. Pour plus d'informations sur XDAS, reportez-vous à la page du projet OpenXDAS (http://openxdas.sourceforge.net).

Analyzer comprend un client XDAS dans son paquetage de téléchargement. Toutefois, le programme d'installation pour Analyzer n'installe pas le client XDAS.

1 Installez Analyzer.

2 Accédez aux fichiers d'installation OpenXDAS, situés par défaut dans le répertoire `products/Analyzer/openxdas/`*`système_exploitation`* du fichier image `.iso`.

3 Lancez le programme d'installation pour le client XDAS à l'aide de la commande rpm.

4 Suivez les invites pour installer le client XDAS.

5 Une fois la procédure d'installation terminée, lancez le client XDAS pour recevoir et afficher automatiquement les événements d'audit d'Analyzer.

VII Configuration de l'accès Single Sign-on dans Identity Manager

Par défaut, Identity Manager utilise OSP pour l'accès Single Sign-on dans Identity Manager. Lorsque vous installez Identity Reporting et les applications d'identité, vous indiquez les réglages de base pour l'authentification des utilisateurs. Toutefois, vous pouvez également configurer le serveur d'authentification OSP pour qu'il accepte l'authentification du serveur des tickets Kerberos ou de SAML IDP. Par exemple, vous pouvez utiliser SAML pour prendre en charge l'authentification de NetIQ Access Manager.

16 Préparation d'un accès Single Sign-on

Par défaut, Identity Manager utilise OSP pour l'accès Single Sign-on dans Identity Manager. Lorsque vous installez Identity Reporting et les applications d'identité, vous indiquez les réglages de base pour l'authentification des utilisateurs. Toutefois, vous pouvez également configurer le serveur d'authentification OSP pour qu'il accepte l'authentification du serveur des tickets Kerberos ou de SAML IDP. Par exemple, vous pouvez utiliser SAML pour prendre en charge l'authentification de NetIQ Access Manager.

NetIQ vous recommande de suivre les étapes de la liste de contrôle suivante.

	Éléments de la liste de contrôle
❑	1. Installez les applications d'identité. Pour plus d'informations, reportez-vous à la Chapitre 9, « Installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting », page 91.
❑	2. (Facultatif) Installez Identity Reporting. Pour plus d'informations, reportez-vous à la Chapitre 9, « Installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting », page 91.
❑	3. Configurez les applications d'identité pour l'accès Single Sign-on à l'aide d'OSP. Pour plus d'informations, reportez-vous au Chapitre 17, « Utilisation d'OSP pour l'accès Single Sign-on dans Identity Manager », page 201.
❑	4. Installez le système d'authentification que vous souhaitez utiliser avec Identity Manager. Par exemple : Access Manager ou Kerberos.
❑	5. (Conditionnel) Configurez Access Manager et OSP. Pour plus d'informations, reportez-vous au Chapitre 18, « Utilisation de l'authentification SAML avec NetIQ Access Manager pour Single Sign-on », page 203.
❑	6. Vérifiez les paramètres Single Sign-on. Pour plus d'informations, reportez-vous au Chapitre 19, « Vérification de l'accès Single Sign-on pour les applications d'identité », page 211.

17 Utilisation d'OSP pour l'accès Single Sign-on dans Identity Manager

Pour fournir un accès Single Sign-on aux applications d'identité, vous devez configurer les paramètres dans l'utilitaire de configuration de RBPM. En principe, vous disposez déjà des certificats et clés nécessaires à l'accès Single Sign-on grâce à l'installation d'OSP.

Cette procédure suppose que votre environnement utilisera un seul certificat pour eDirectory, le contrôleur SSO et le fournisseur OAuth. Si votre organisation requiert des couches supplémentaires de séparation, créez un certificat séparé pour le fournisseur OAuth.

17.1 Préparation d'eDirectory pour l'accès Single Sign-on

Vous devez configurer le coffre-fort d'identité dans le cadre de votre installation d'eDirectory afin qu'il prenne en charge l'accès Single Sign-on pour les applications d'identité et Identity Reporting.

Suivez les étapes de la . Si vous avez déjà étendu le schéma eDirectory pour inclure le schéma SAML et installé les méthodes NMAS requises, vous ne devez pas effectuer ces étapes une seconde fois. Passez alors directement à la sous-section relative à la création du conteneur de racine approuvée.

17.2 Modification des réglages de base pour un accès Single Sign-on

Lorsque vous installez les applications d'identité, vous configurez généralement les réglages de base pour un accès Single Sign-on. Cette section vous permet de vérifier que les paramètres fonctionnent pour votre environnement.

1. Exécutez l'utilitaire de configuration de RBPM. Pour plus d'informations, reportez-vous à la Section 11.6.1, « Exécution de l'utilitaire de configuration des applications d'identité », page 143.
2. Pour modifier les paramètres d'authentification, effectuez les étapes suivantes :
   - **2a** Cliquez sur **Authentification**.
   - **2b** (Conditionnel) Pour indiquer le nom DNS ou l'adresse IP du serveur effectif, changez toutes les instances de `localhost`.
     - L'adresse spécifiée doit pouvoir être résolue par tous les clients. Utilisez `localhost` uniquement si tous les accès à Identity Manager seront locaux, y compris l'accès par le biais d'un navigateur.
     - Cette adresse IP ou ce nom d'hôte « public » doit être identique à la valeur de *`PublicServerName`* que vous avez indiquée lors de l'installation d'OSP.
     - Dans un environnement distribué ou en grappe, toutes les URL OAuth doivent avoir la même valeur. L'URL doit faire passer l'accès client via votre équilibreur de charge ou votre commutateur L4. En outre, les fichiers `osp.war`et les fichiers de configuration doivent être installés dans chaque déploiement de l'environnement.

2c Pour la valeur **DN LDAP du conteneur des administrateurs**, cliquez sur le bouton **Parcourir**, puis sélectionnez le conteneur dans le coffre-fort d'identité qui contient votre administrateur d'applications d'identité.

2d Spécifiez le fichier Keystore OAuth que vous avez créé lors de l'installation d'OSP.

Indiquez le chemin du fichier Keystore, son mot de passe, l'alias de la clé et le mot de passe de cette dernière. Le fichier Keystore par défaut est `osp.jks` et l'alias par défaut de la clé est `osp`.

3 Pour modifier les paramètres Single Sign-on, effectuez les étapes suivantes :

3a Cliquez sur **Clients SSO**.

3b (Conditionnel) Pour indiquer le nom DNS ou l'adresse IP du serveur effectif, changez toutes les instances de `localhost`.

- L'adresse spécifiée doit pouvoir être résolue par tous les clients. Utilisez `localhost` uniquement si tous les accès au tableau de bord seront locaux, y compris l'accès par le biais d'un navigateur.
- Cette adresse IP ou ce nom d'hôte « public » doit être identique à la valeur de *`PublicServerName`* que vous avez indiquée lors de l'installation d'OSP.
- Dans un environnement distribué ou en grappe, toutes les URL de redirection OAuth doivent avoir la même valeur. L'URL doit faire passer l'accès client via votre équilibreur de charge ou votre commutateur L4.

3c (Conditionnel) Si vous utilisez des ports autres que ceux par défaut, mettez à jour les numéros des ports des composants Identity Manager suivants :

- Administration des applications d'identité
- Tableau de bord Identity Manager
- Identity Reporting
- Application utilisateur

4 Cliquez sur **OK** pour enregistrer les modifications, puis fermez l'utilitaire de configuration.

5 Démarrez Tomcat.

17.3 Configuration de SSPR pour l'approbation d'OSP

Pour que l'accès Single Sign-on fonctionne correctement, vous devez configurer une relation de confiance avec des certificats entre OSP et SSPR (Self Service Password Reset). Vous devez exporter un certificat depuis le fichier Keystore d'OSP, à savoir `osp.jks`.

Après avoir exporté le certificat, vous devez l'importer dans le fichier keystore de SSPR.

Pour plus d'informations sur la définition d'un canal sécurisé, reportez-vous à la section « Setting Up a Secure Channel Between the Application Server and the LDAP Server » (Configuration d'un canal sécurisé entre le serveur d'applications et le serveur LDAP) dans le manuel « Self Service Password Reset Administration Guide » (Guide d'administration du module de réinitialisation de mot de passe en self-service).

18 Utilisation de l'authentification SAML avec NetIQ Access Manager pour Single Sign-on

Cette section vous permet de configurer NetIQ Access Manager et OSP pour prendre en charge l'accès Single Sign-on dans Identity Manager à l'aide de l'authentification SAML 2.0. Avant de commencer, vérifiez les points suivants :

- Vous avez installé une nouvelle version d'Access Manager qui est prise en charge.
- Vous avez installé une nouvelle version d'Identity Manager.
- Les deux installations utilisent des noms DNS pour la configuration du nom d'hôte.
- Les deux installations utilisent un protocole SSL pour la communication.
- Vous devez configurer pour Access Manager un environnement en grappe qui utilise le coffre-fort d'identité en tant que magasin d'utilisateurs LDAP. Pour plus d'informations, reportez-vous au *NetIQ Access Manager Administration Guide* (Guide d'administration de NetIQ Access Manager).

18.1 Présentation de l'authentification tierce et de Single Sign-On

Vous pouvez configurer Identity Manager pour qu'il fonctionne avec NetIQ Access Manager à l'aide de l'authentification SAML 2.0. Cette option vous permet d'utiliser une technologie qui n'est pas basée sur un mot de passe pour vous connecter aux applications d'identité via Access Manager. Par exemple, les utilisateurs peuvent se connecter via un certificat utilisateur (client), comme une carte à puce.

Access Manager interagit avec OSP pour assigner l'utilisateur à un DN dans le coffre-fort d'identité. Lorsqu'un utilisateur se connecte aux applications d'identité par le biais d'Access Manager, ce-dernier peut injecter une assertion SAML (avec le DN de l'utilisateur comme identificateur) dans un en-tête HTTP et transférer la requête aux applications d'identité. Les applications d'identité utilisent l'assertion SAML pour établir la connexion LDAP avec le coffre-fort d'identité.

Les portlets d'accessoires qui permettent l'authentification Single Sign-on basée sur des mots de passe ne prennent pas en charge la fonction Single Sign-on lorsque les assertions SAML sont utilisées pour l'authentification des applications d'identité.

18.2 Création et installation de certificats SSL

Pour garantir l'authentification, Access Manager et OSP doivent partager la racine approuvée de leurs certificats SSL. Cette section vous aide à créer un nouveau certificat pour Access Manager et à vous assurer que les Truststores disposent des certificats adéquats.

18.2.1 Création d'un certificat SSL pour Access Manager

Access Manager ne peut pas utiliser son certificat SSL par défaut, `test-connector`, pour communiquer avec Identity Manager. Au lieu de cela, vous devez créer un certificat qui comprend le nom d'hôte dans l'objet du certificat et l'assigner à Access Manager.

Pour plus d'informations, reportez-vous à la section Security and Certificate Management (Sécurité et gestion des certificats) dans le manuel *NetIQ Access Manager Administration Console Guide* (Guide de la console d'administration de NetIQ Access Manager).

1. Ouvrez la console d'administration d'Access Manager.
2. Cliquez sur **Sécurité > Certificats**.
3. Cliquez sur **Nouveau**.
4. Spécifiez un nom pour le nouveau certificat. Par exemple : *`nom_hôte`*`_ssl`.
5. Cliquez sur le bouton d'édition du côté droit de la fenêtre.
6. Pour **Nom commun**, indiquez le nom DNS du serveur qui héberge Access Manager, puis cliquez sur **OK**.
7. Pour **Months valid** (Mois valides), indiquez une valeur inférieure ou égale à 99.
8. Pour **Key size** (Taille de clé), entrez `2048`.
9. Sélectionnez le certificat que vous venez de créer, puis cliquez sur **Actions > Add certificate to Keystores...** (Opérations > Ajouter le certificat aux fichiers Keystore...).
10. Cliquez sur le bouton d'édition à droite de **Keystores** (Fichiers Keystore).
11. Sélectionnez **SSL connector** (Connecteur SSL) et cliquez sur **OK**.
12. Cliquez sur **OK**.
13. Installez le nouveau certificat dans le Truststore OSP. Pour plus d'informations, reportez-vous à la Section 18.2.2, « Installation du certificat Access Manager dans le Truststore Identity Manager », page 205.

18.2.2 Installation du certificat Access Manager dans le Truststore Identity Manager

Le Truststore OSP doit inclure le certificat de sécurité d'Access Manager.

1. Pour exporter le nouveau certificat SSL, procédez comme suit :
   - Sous **Security** (Sécurité) > **Trusted Roots** (Racines approuvées) dans la console d'administration d'Access Manager, exportez le certificat racine du certificat SSL. Nommez le certificat racine **configCA**.
   - Exportez le certificat du serveur SSL.

     Pour plus d'informations, reportez-vous à la section Managing Trusted Roots and Trust Stores (Gestion des racines approuvées et des Truststores) du manuel *NetIQ Access Manager Administration Console Guide* (Guide de la console d'administration de NetIQ Access Manager).
2. Copiez le certificat exporté sur le serveur où s'exécute OSP.
3. Utilisez l'utilitaire keytool disponible avec Java pour importer le fichier dans le fichier Keystore cacerts du JRE.

   Par exemple : `/opt/netiq/common/jre/bin/keytool -importcert -trustcacerts -alias <cert_NAM> -keystore /opt/netiq/common/jre/lib/security -storepass <mot_de_passe> -file custom_location/<fichier_exporté>`
4. Installez le certificat OSP dans le Truststore Access Manager.

   Pour plus d'informations, reportez-vous à la Section 18.2.3, « Installation du certificat du serveur SSL dans le Truststore Access Manager », page 205.

18.2.3 Installation du certificat du serveur SSL dans le Truststore Access Manager

Le Truststore Access Manager doit inclure le certificat de sécurité d'OSP. Pour plus d'informations, reportez-vous à la section Managing Trusted Roots and Trust Stores (Gestion des racines approuvées et des Truststores) du manuel *NetIQ Access Manager Administration Console Guide* (Guide de la console d'administration de NetIQ Access Manager).

Obtenez le certificat de serveur SSL utilisé par l'instance Tomcat exécutant OSP.

1. Copiez le certificat du serveur SSL de l'instance Tomcat qui héberge OSP sur le serveur où vous avez installé Access Manager.
2. Ouvrez la console d'administration d'Access Manager.
3. Pour importer le certificat, cliquez sur **Security > NIDP Trust Store** (Sécurité > Truststore NIDP).
4. Cliquez sur **Ajouter**.
5. Dans la boîte de dialogue **Add** (Ajouter) > **Import** (Importer), sélectionnez Trusted Root (Racine approuvée).
6. Sélectionnez le certificat de racine que vous souhaitez importer, puis cliquez sur **OK**.
7. Assurez-vous qu'OSP reconnaît les assertions d'authentification provenant de SAML.

   Pour plus d'informations, reportez-vous à la Section 18.4.2, « Création d'un ensemble d'attributs pour SAML », page 207.

18.3 Configuration d'Identity Manager pour l'approbation d'Access Manager

Identity Manager a besoin de l'URL des métadonnées SAML afin de rediriger les utilisateurs pour les requêtes d'authentification. Par défaut, Access Manager utilise l'URL suivante pour stocker les métadonnées SAML :

`https://server:port/nidp/saml2/metadata`

où *server*:*port* représente le serveur d'identités d'Access Manager.

1. (Facultatif) Pour afficher un document `.xml` des métadonnées SAML, ouvrez l'URL dans un navigateur.

   Si l'URL ne fournit pas le document, assurez-vous que le lien est correct.
2. Sur le serveur OSP, exécutez l'utilitaire de configuration de RBPM. Pour plus d'informations, reportez-vous à la Section 11.6.1, « Exécution de l'utilitaire de configuration des applications d'identité », page 143.
3. Dans l'utilitaire, sélectionnez **Authentification**.
4. Pour **Méthode d'authentification**, indiquez **SAML 2.0**.
5. Pour **URL des métadonnées**, indiquez l'URL qu'OSP utilise pour rediriger les requêtes d'authentification vers les métadonnées SAML d'Access Manager.

   Par exemple : `https://serveur: port/nidp/saml2/metadata`
6. Dans la section **Serveur d'authentification**, indiquez le nom DNS du serveur qui héberge OSP dans le paramètre **Identificateur de l'hôte du serveur OAuth**.
7. Cliquez sur **OK** pour enregistrer les modifications.
8. Redémarrez l'instance Tomcat qui héberge OSP.

18.4 Configuration d'Access Manager pour fonctionner avec Identity Manager

Pour vérifier qu'Access Manager reconnaît Identity Manager en tant que fournisseur de service approuvé, ajoutez le texte de métadonnées d'OSP au serveur d'identités et configurez un ensemble d'attributs. Ce processus comprend les opérations suivantes :

- Section 18.4.1, « Copie des métadonnées pour Identity Manager », page 206
- Section 18.4.2, « Création d'un ensemble d'attributs pour SAML », page 207
- Section 18.4.3, « Ajout d'Identity Manager en tant que fournisseur de service approuvé », page 207

18.4.1 Copie des métadonnées pour Identity Manager

Access Manager nécessite le texte de métadonnées pour OSP. Copiez le contenu du fichier de métadonnées `.xml` dans un document que vous pouvez ouvrir sur le serveur d'identités d'Access Manager.

1. Dans un navigateur, accédez à l'URL pour les métadonnées d'OSP. Par défaut, Identity Manager utilise l'URL suivante :

   `https://server:port/osp/a/idm/auth/saml2/spmetadata`

où *server*:*port* représente le serveur Tomcat qui héberge OSP.

2. Affichez la source de la page du fichier `spmetadata.xml`.
3. Copiez le contenu du fichier dans un document auquel vous pouvez accéder lors de l'« Ajout d'Identity Manager en tant que fournisseur de service approuvé » page 207.

18.4.2 Création d'un ensemble d'attributs pour SAML

Pour vous assurer que SAML peut effectuer un échange d'assertions entre Access Manager et OSP, créez un ensemble d'attributs dans Access Manager. Les ensembles d'attributs fournissent un modèle commun d'assignation de nom pour l'échange. OSP recherche une valeur d'attribut qui identifie l'objet de l'assertion. Par défaut, l'attribut est `mail`.

Pour plus d'informations, reportez-vous à la section Configuring Attribute Sets (Configuration d'ensembles d'attributs) du *NetIQ Access Manager Administration Guide* (Guide d'administration de NetIQ Access Manager).

1. Ouvrez la console d'administration d'Access Manager.
2. Cliquez sur **Devices > Identity Servers > Shared Settings > Attribute Sets > New** (Périphériques > Serveurs d'identités > Paramètres partagés > Ensembles d'attributs > Nouveau).
3. Indiquez un nom pour l'ensemble d'attributs. Par exemple : `Attributs SAML IDM`.
4. Cliquez sur **Next** (Suivant), puis sur **New** (Nouveau).
5. Pour **Local Attribute**(Attribut local), sélectionnez **Ldap attribute: mail [LDAP Attribute Profile]** (Attribut LDAP : mail [Profil d'attribut LDAP].
6. Pour **Remote Attribute** (Attribut à distance), indiquez `mail`.
7. Cliquez sur **OK**, puis sur **Finish** (Terminer).

18.4.3 Ajout d'Identity Manager en tant que fournisseur de service approuvé

Configurez Access Manager pour qu'il reconnaisse Identity Manager en tant que fournisseur de service approuvé. Pour plus d'informations, reportez-vous à la section Creating a Trusted Service Provider for SAML 2.0 (Création d'un fournisseur de service approuvé pour SAML 2.0) du *NetIQ Access Manager Administration Guide* (Guide d'administration de NetIQ Access Manager).

1. Ouvrez la console d'administration d'Access Manager.
2. Cliquez sur **Devices > Identity Servers > Edit > SAML 2.0**(Périphériques > Serveurs d'identités > Éditer > SAML 2.0).
3. Cliquez sur **New > Service Provider** (Nouveau > Fournisseur de service).
4. Pour **Provider Type** (Type de fournisseur), spécifiez **General** (Général).
5. Pour **Source**, indiquez **Metadata Text** (Texte de métadonnées).
6. Dans le champs **Text** (Texte), collez le contenu du fichier `spmetadata.xml` que vous avez copié à la section « Copie des métadonnées pour Identity Manager » page 206.
7. Indiquez un nom pour le nouveau fournisseur de service OSP.
8. Cliquez sur **Suivant**, puis sur **Terminer**.
9. Sous l'onglet **SAML 2.0**, sélectionnez le fournisseur de service OSP que vous avez créé à l'Étape 7.
10. Cliquez sur **Attributes** (Attributs).

11 Sélectionnez l'ensemble d'attributs que vous avez créé à la section « Création d'un ensemble d'attributs pour SAML » page 207. Par exemple : `Attributs SAML IDM`.

12 Déplacez les attributs disponibles pour le fournisseur de service OSP vers le panneau **Send with authentication** (Envoyer avec authentification) sur le côté gauche de la page.

Les attributs que vous déplacez vers le panneau **Send with authentication** (Envoyer avec authentification) sont ceux que vous souhaitez obtenir lors de l'authentification.

13 Cliquez deux fois sur **OK**.

14 Pour mettre à jour le serveur d'identités, cliquez sur **Devices > Identity Servers > Update > Update All Configuration** (Périphériques > Serveurs d'identités > Mise à jour > Mettre à jour toute la configuration).

18.5 Mise à jour des pages de connexion pour Access Manager

Les pages de connexion par défaut pour Access Manager utilisent des éléments HTML iFrame qui entrent en conflit avec les éléments utilisés pour les applications d'identité. Cette section fournit des instructions pour éliminer ce conflit en créant une nouvelle méthode de connexion et un nouveau contrat pour Access Manager. Les fichiers `.jsp` référencés dans cette section sont situés par défaut dans le répertoire `/opt/novell/idm/apps`.

Pour plus d'informations, reportez-vous à la section Customizing the Identity Server Login Page (Personnalisation de la page de connexion du serveur d'identités) du *NetIQ Access Manager Administration Guide* (Guide d'administration de NetIQ Access Manager).

1 Modifiez le fichier `top.jsp` selon les documents TID 7004020 et TID 7018468.

2 (Facultatif) À des fins de sauvegarde, copiez et renommez le fichier `login.jsp`. Par exemple, renommez-le `idm_login.jsp`.

3 Ouvrez la console d'administration d'Access Manager.

4 Pour créer une nouvelle méthode de connexion, procédez comme suit :

4a Cliquez sur **Devices > Identity Servers > Edit > Local > Methods** (Périphériques > Serveurs d'identités > Éditer > Local > Méthodes).

4b Cliquez sur **New** (Nouveau), puis indiquez la valeur **Display Name** (Nom d'affichage) de la nouvelle méthode. Par exemple : `Nom IDM/Mot de passe`.

4c Pour **Class** (Classe), indiquez **Name/Password-Form**.

4d Pour **Magasin d'utilisateurs**, indiquez le coffre-fort d'identité en tant que magasin d'utilisateurs LDAP.

4e Dans la section **Properties** (Propriétés), cliquez sur **New** (Nouveau), puis indiquez les propriétés suivantes :

Nom	Valeur
JSP	idm_login
MainJSP	true

4f Cliquez sur **OK**.

5 Pour créer un contrat qui utilise la nouvelle méthode de connexion, procédez comme suit :

5a Cliquez sur **Contracts > New** (Contrats > Nouveau).

5b Sous l'onglet **Configuration**, indiquez la valeur **Display Name** (Nom d'affichage) du nouveau contrat. Par exemple : `Nom IDM/Mot de passe`.

5c Pour **URI**, indiquez `name/password/uri/idm`.

5d Sous **Methods** (Méthodes), ajoutez la méthode que vous avez créée à l'Étape 4. Par exemple : `Nom IDM/Mot de passe`.

5e Sous l'onglet **Authentication Card** (Carte d'authentification), indiquez un **ID** pour la carte. Par exemple : `IDM_Nom_Motdepasse`.

5f Indiquez une image pour la carte.

5g Cliquez sur **OK**.

6 Pour spécifier les valeurs par défaut pour la façon dont le système traite le nouveau contrat d'authentification, procédez comme suit :

6a Sous l'onglet **Local**, cliquez sur **Defaults** (Valeurs par défaut).

6b Pour le magasin d'utilisateurs, indiquez le coffre-fort d'identité en tant que magasin d'utilisateurs LDAP.

6c Pour **Authentication Contract** (Contrat d'authentification), indiquez le contrat que vous avez créé à l'Étape 5. Par exemple : `Nom IDM/Mot de passe`.

6d Cliquez sur **OK**.

7 Pour mettre à jour le serveur d'identités, cliquez sur **Devices > Identity Servers > Update > Update All Configuration** (Périphériques > Serveurs d'identités > Mise à jour > Mettre jour toute la configuration).

19 Vérification de l'accès Single Sign-on pour les applications d'identité

Une fois que vous avez installé les applications d'identité et configuré les paramètres de Single Sign-on, vous devez vérifier que vous pouvez vous connecter aux différentes applications et basculer de l'une à l'autre sans vous déconnecter. Par défaut, les applications utilisent le suffixe suivant dans le lien URL :

- Administration des applications d'identité : `/idmadmin`
- Tableau de bord Identity Manager : `/idmdash`
- Application utilisateur : `/IDMProv`
- Identity Reporting : `/IDMRPT`

Pour personnaliser le suffixe, utilisez l'utilitaire de configuration RBPM. Pour plus d'informations, reportez-vous au Chapitre 11.6, « Configuration des paramètres pour les applications d'identité », page 143.

Pour vérifier la fonctionnalité Single Sign-on :

1. Dans une nouvelle fenêtre de navigateur sur votre serveur d'applications d'identité, entrez l'URL du tableau de bord :

   `https://server:port/idmdash`

   Ne vous connectez pas au tableau de bord.
2. Dans votre navigateur, accédez à l'application utilisateur :

   `https://server:port/IDM-context`
3. Vérifiez que l'application utilisateur affiche la même page de connexion que celle de l'Étape 1.
4. Connectez-vous à l'application utilisateur.
5. Dans le coin supérieur droit, cliquez sur l'icône **Accueil** et vérifiez que vous pouvez accéder au tableau de bord sans vous connecter à nouveau.

20 Utilisation de SSL pour une communication sécurisée

Les applications d'identité et Identity Reporting utilisent des formulaires HTML pour l'authentification. Par conséquent, le processus de connexion peut exposer les références de l'utilisateur. NetIQ vous recommande d'activer le protocole SSL pour protéger les informations sensibles. Le protocole SSL garantit que les communications gérées entre les composants Identity Manager sont sécurisées.

Vous devez disposer de certificats pour configurer le serveur Tomcat de manière à ce qu'il communique via SSL. Vous pouvez obtenir des certificats de deux manières :

- Certificat émis par une autorité de certification (CA) approuvée externe
- Certificat auto-signé

Le programme d'installation configure automatiquement les composants Applications d'identité et Identity Reporting avec une connexion sécurisée (HTTPS) à l'aide du certificat émis par le coffre-fort d'identité. Pour un environnement de production, il est recommandé d'utiliser un certificat émis par une autorité de certification externe.

20.1 Liste de contrôle pour garantir des connexions SSL

Pour garantir des connexions sécurisées entre les applications d'identité, Identity Reporting, SSPR et OSP, NetIQ vous recommande d'effectuer les étapes de la liste de contrôle suivante :

	Éléments de la liste de contrôle
❑	1. Utilisez le Keystore pour stocker les certificats d'authentification. Pour plus d'informations, reportez-vous au Section 20.2, « Création d'un fichier Keystore et d'une demande de signature de certificat », page 214.
❑	2. (Conditionnel) Vous pouvez utiliser un certificat auto-signé ou un certificat délivré par une autorité de certification externe dans votre environnement. Pour plus d'informations, reportez-vous au Section 20.4, « Activation de SSL avec un certificat auto-signé », page 216. Pour un environnement de production, il est recommandé d'utiliser un certificat émis par une autorité de certification externe.
❑	3. (Conditionnel) Dans un environnement de production, importez un certificat signé. Pour plus d'informations, reportez-vous à la Section 20.3, « Activation de SSL avec un certificat signé d'une autorité de certification externe », page 215.
❑	4. Configurez le serveur d'authentification, les applications d'identité et Identity Reporting pour qu'ils prennent en charge les communications SSL. Pour plus d'informations, reportez-vous à la section Section 20.6, « Mise à jour des paramètres SSL pour le serveur d'applications », page 222 et au Section 20.7, « Mise à jour des paramètres SSL dans l'utilitaire de configuration », page 223.

20.2 Création d'un fichier Keystore et d'une demande de signature de certificat

Un Keystore est un fichier Java qui contient des clés de chiffrement et, le cas échéant, des certificats de sécurité. Pour créer un Keystore, vous avez besoin de l'utilitaire Java Keytool inclus dans le JRE. Pour créer le fichier `.jks`, générez un certificat dans le Keystore. Chaque certificat est associé à un alias unique. Le fichier Keystore doit être placé dans le répertoire `conf` du serveur d'applications qui héberge les applications d'identité et Identity Reporting.

Par défaut, le programme d'installation crée un fichier Keystore, à savoir `tomcat.ks` dans `/opt/netiq/idm/apps/tomcat/conf` et l'utilise pour configurer la connexion `https`. Si vous créez un fichier Keystore portant le même nom, remplacez ce fichier dans ce répertoire.

1. Dans une invite de commande, accédez au répertoire `conf` du serveur d'applications sur lequel vous avez déployé les applications d'identité. Par exemple : `/opt/netiq/idm/apps/tomcat/conf`.

   Le chemin `tomcat/conf` est l'emplacement par défaut des applications installées sur un serveur Tomcat. Le chemin d'accès peut varier en fonction de la manière dont vous avez installé l'application et Tomcat.

2. Définissez le chemin de l'environnement pour la création du Keystore à l'aide de la commande suivante :

   ```
   cd /opt/netiq/idm/apps/tomcat/conf
   export PATH=/opt/netiq/common/jre/bin:$PATH
   ```

3. Créez le Keystore à l'aide de la commande suivante :

   ```
   keytool -genkey -alias keystore_name -keyalg RSA -keystore
   keystore_name.keystore -validity 3650 -keysize 2048
   ```

   Par exemple :

   ```
   keytool -genkey -alias IDMkey -keyalg RSA -keystore IDMkey.keystore -validity
   3650 -keysize 2048
   ```

4. À l'invite, indiquez les valeurs des paramètres en tenant compte des considérations suivantes :
   - En guise de prénom et de nom, indiquez le nom complet du serveur. Par exemple :

     ```
     MyTomcatServer.NetIQ.com
     ```

   - Utilisez une orthographe correcte. Si vous écrivez mal des mots, vous obtiendrez des erreurs lorsque vous générerez votre certificat signé à partir de l'autorité de signature.

5. (Facultatif) Créez un simple fichier texte pour enregistrer une copie des informations que vous fournissez pour les valeurs de paramètres.

   Enregistrer ces informations permet de vous assurer de fournir les mêmes lorsque vous introduisez une demande auprès de l'autorité de signature et lorsque vous importez votre certificat.

6. Copiez le fichier Keystore dans le répertoire `/tomcat/conf` de chaque instance du serveur d'applications sur laquelle vous avez déployé les composants Identity Manager et SSPR.

7. Pour générer une requête de certificat auprès d'une autorité de certification, procédez comme suit :

   7a Dans le répertoire `conf`, créez un simple fichier texte nommé `votre_requête.csr`. Par exemple : `IDMcertrequest.csr`.

   7b Exécutez la commande suivante :

```
keytool -certreq -v -alias keystore_name -file your_request.csr -keypass
keystore_password -keystore your.keystore -storepass your_password
```

Exemples :

```
keytool -certreq -v -alias IDMkey.keystore -file IDMcertrequest.csr -
keypass IDMkeypass -keystore IDMkey.keystore -storepass IDMpass
```

Lorsque vous exécutez la commande, l'utilitaire Keytool remplit le fichier .csr avec les données appropriées pour la demande d'un certificat.

8 (Conditionnel) Pour obtenir un certificat signé, soumettez le fichier .csr à une autorité de certification valide.

9 Copiez le certificat dans le répertoire de configuration de votre serveur d'applications.

Par exemple : `/opt/netiq/idm/apps/tomcat/conf`.

10 Arrêtez Tomcat.

Après la création d'un Keystore et la génération d'une requête de certificat auprès d'une autorité de certification. Suivez les procédures ci-dessous pour importer des certificats dans le Keystore :

- Pour le certificat signé par une autorité de certification externe, reportez-vous à la Section 20.3, « Activation de SSL avec un certificat signé d'une autorité de certification externe », page 215.
- Pour le certificat auto-signé, reportez-vous à la Section 20.4, « Activation de SSL avec un certificat auto-signé », page 216.

20.3 Activation de SSL avec un certificat signé d'une autorité de certification externe

Pour un environnement de production, il convient d'utiliser un certificat signé émis par une autorité de certification valide. Cette section explique comment importer un certificat signé sur le serveur d'applications Tomcat par défaut pour les applications d'identité.

Cette procédure suppose que vous disposez d'un certificat signé provenant d'une autorité de certification valide. Pour plus d'informations, reportez-vous à la Section 20.2, « Création d'un fichier Keystore et d'une demande de signature de certificat », page 214.

Pour utiliser un certificat signé et SSL :

1 Copiez le certificat dans le répertoire de configuration de votre serveur d'applications. Par exemple : `/opt/netiq/idm/apps/tomcat/conf`.

2 Pour convertir le certificat racine au format DER, procédez comme suit :

2a Double-cliquez sur le certificat stocké dans le répertoire `conf`.

2b Dans la boîte de dialogue Certificate (Certificat), cliquez sur **Certificate Path** (Chemin du certificat).

2c Sélectionnez le certificat racine que vous avez reçu de l'autorité de signature.

2d Cliquez sur **View Certificate** (Afficher le certificat).

2e Cliquez sur **Details > copy to file** (Détails > Copier dans le fichier).

2f Dans l'assistant d'exportation de certificat, cliquez sur **Next** (Suivant).

2g Sélectionnez **DER encoded binary for X.509** (Binaire DER codé pour X.509), puis cliquez sur **Next** (Suivant).

2h Créez un nouveau fichier pour y stocker le certificat nouvellement formaté et enregistrez-le dans le répertoire `conf` de votre serveur d'applications.

Par exemple : `/opt/netiq/idm/apps/tomcat/conf`.

2i Cliquez sur **Finish** (Terminer).

3 Pour importer les certificats convertis, procédez comme suit :

3a Dans une invite de commande, accédez au répertoire `conf` de votre serveur d'applications.

3b Saisissez la commande suivante :

```
keytool -import -trustcacerts -alias root -keystore your.keystore -file
yourRootCA.der
```

Par exemple :

```
keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file
IDMTESTREE.der
```

REMARQUE : vous devez indiquer **root** comme alias.

Après avoir importé le certificat, le serveur affiche **Certificate was added to keystore** (Certificat ajouté au Keystore).

3c Vérifiez que le certificat signé est importé correctement dans le répertoire `conf` à l'aide de la commande suivante :

```
keytool -list -v -alias root -keystore your.keystore
```

Par exemple :

```
keytool -list -v -alias root -keystore IDMkey.keystore
```

Le serveur répertorie vos certificats.

4 NetIQ vous recommande d'importer les certificats signés dans idm.jks. Il s'agit d'un fichier Keystore centralisé qui stocke tous les certificats utilisés par les applications d'identité et Identity Reporting. Par exemple :

```
keytool -import -trustcacerts -alias root -keystore /opt/netiq/idm/apps/tomcat/
conf/idm.jks -file IDMTESTREE.der
```

5 Mettez à jour les paramètres SSL pour le serveur d'applications. Pour ce faire, reportez-vous à la Section 20.6, « Mise à jour des paramètres SSL pour le serveur d'applications », page 222.

6 Mettez à jour les paramètres SSL dans l'utilitaire de configuration. Pour plus d'informations, reportez-vous à la Section 20.7, « Mise à jour des paramètres SSL dans l'utilitaire de configuration », page 223.

7 Mettez à jour les paramètres SSL pour Self Service Password Reset. Pour plus d'informations, reportez-vous à la Section 20.8, « Mise à jour des paramètres SSL pour SSPR », page 225

8 Relancez Tomcat.

20.4 Activation de SSL avec un certificat auto-signé

Il se peut que vous souhaitiez utiliser un certificat auto-signé dans votre environnement de test, puisque ce type de certificat est plus facile à obtenir qu'un certificat signé par une autorité de certification valide.

20.4.1 Exportation de l'autorité de certification

Vous pouvez utiliser iManager pour exporter l'autorité de certification (CA) à partir de votre serveur eDirectory afin de générer votre certificat auto-signé.

1. Connectez-vous à iManager avec le nom d'utilisateur et le mot de passe de l'administrateur eDirectory.
2. Cliquez sur **Administration > Modify Object** (Administration > Modifier un objet).
3. Dans le conteneur de sécurité, recherchez l'objet CA appelé *nom_arborescence* `CA.Security`. Par exemple : `IDMTESTTREE CA.Security`.
4. Cliquez sur **OK**.
5. Cliquez sur **Certificates > Self-Signed Certificate** (Certificats > Certificat auto-signé).
6. Sélectionnez les certificats auto-signés à utiliser.

   Exemple : **RSA du certificat auto-signé**

   6a. Cochez **RSA du certificat auto-signé**.

   6b. Cliquez sur **Validate** (Valider).
7. Cliquez sur **Export** (Exporter).
8. Effacez **Export private key** (Exporter la clé privée).
9. Cliquez sur **Export format > DER** (Format d'exportation > DER).
10. Cliquez sur **Next** (Suivant).
11. Cliquez sur **Save the exported certificate** (Enregistrer le certificat exporté).
12. Cliquez sur **Save File** (Enregistrer le fichier).

    iManager enregistre le fichier sous le nom *nom_arborescence* `cert.der`. Par exemple : `IDMTESTREE cert.der`.
13. Cliquez sur **Close** (Fermer).
14. Copiez le certificat dans le répertoire de configuration de votre serveur d'applications (`cert.der`).

    Par exemple : `/opt/netiq/idm/apps/tomcat/conf`.
15. Pour importer le certificat racine, procédez comme suit :

    15a. Dans une invite de commande, accédez au répertoire conf de votre serveur d'applications à l'aide de la commande suivante :

    ```
    keytool -import -trustcacerts -alias root -keystore <keystore
    file>.keystore -file exported_certificate_filename.der
    ```

    Exemple :

    ```
    keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file
    cert.der
    ```

    REMARQUE : vous devez indiquer **root** comme alias.

    Après avoir importé le certificat, le serveur affiche **Certificate was added to keystore** (Certificat ajouté au Keystore).

    15b. NetIQ vous recommande d'importer également le certificat racine à l'emplacement du fichier cacerts Java.

    Par exemple :

```
keytool -import -trustcacerts -alias root -keystore /opt/netiq/common/jre/
lib/security/cacerts -file cert.der
```

15c Vérifiez que le certificat signé est importé correctement dans le répertoire `conf` à l'aide de la commande suivante :

```
keytool -list -v -alias root -keystore your.keystore
```

Exemples :

```
keytool -list -v -alias root -keystore IDMkey.keystore
```

Le serveur répertorie les certificats.

20.4.2 Génération du certificat auto-signé

Avant de générer le certificat auto-signé, assurez-vous que vous disposez d'un fichier Keystore et d'un fichier de demande de certificat. Pour plus d'informations, reportez-vous à, Section 20.2, « Création d'un fichier Keystore et d'une demande de signature de certificat », page 214

1. Connectez-vous à iManager.
2. Accédez à **Certificate Server > Issue Certificate** (Serveur de certificat > Émettre un certificat).
3. Recherchez le fichier `.csr` créé à l'Étape 7 de la Section 20.2, « Création d'un fichier Keystore et d'une demande de signature de certificat », page 214.

   Exemple : `IDMcertrequest.csr`
4. Cliquez sur **Next** (Suivant) deux fois.
5. Pour le type de certificat, cliquez sur **Unspecified** (Non spécifié).
6. Cliquez sur **Next** (Suivant) deux fois.

   iManager enregistre le fichier en tant que `csr_request_name.der`. Exemple : `IDMcertrequest.der`
7. Copiez le certificat dans le répertoire de configuration de votre serveur d'applications (`IDMcertrequest.der`).

   Par exemple : `/opt/netiq/idm/apps/tomcat/conf`.
8. Pour importer le certificat auto-signé généré, procédez comme suit :

   8a Dans une invite de commande, accédez au répertoire `conf` de votre serveur d'applications à l'aide de la commande suivante :

   ```
   keytool -import -alias keystore_name -keystore <keystore_file> -file
   <signed_certificate_filename>.der
   ```

   Exemple :

   ```
   keytool -import -alias IDMkey -keystore IDMkey.keystore -file
   IDMcertrequest.der
   ```

   REMARQUE : Vous devez spécifier le nom du Keystore comme étant votre alias.

   Après avoir importé le certificat, le serveur affiche **Certificate was added to keystore** (Certificat ajouté au Keystore).

   8b NetIQ recommande d'importer aussi le certificat auto-signé à l'emplacement du fichier cacerts de Java.

   Par exemple :

```
keytool -import -alias IDMkey -keystore
/opt/netiq/common/jre/lib/security/cacerts -file IDMcertrequest.der
```

8c Vérifiez que le certificat signé est importé correctement dans le répertoire `conf` à l'aide de la commande suivante :

```
keytool -list -v -alias keystore_name -keystore your.jks
```

Exemples :

```
keytool -list -v -alias IDMkey -keystore IDMkey.jks
```

Le serveur répertorie les certificats.

9 Mettez à jour les paramètres SSL pour le serveur d'applications. Pour plus d'informations, reportez-vous au Section 20.6, « Mise à jour des paramètres SSL pour le serveur d'applications », page 222.

10 Mettez à jour les paramètres SSL dans l'utilitaire de configuration. Pour plus d'informations, reportez-vous à la Section 20.7, « Mise à jour des paramètres SSL dans l'utilitaire de configuration », page 223.

11 Mettez à jour les paramètres SSL pour Self Service Password Reset. Pour plus d'informations, reportez-vous à la Section 20.8, « Mise à jour des paramètres SSL pour SSPR », page 225

12 Relancez Tomcat.

20.5 Activation de la communication SSL entre les composants Sentinel et Identity Manager

Vous pouvez créer et exporter un certificat de serveur auto-signé pour garantir une communication sécurisée entre les composants Sentinel et Identity Manager. Utilisez un certificat signé émis par une autorité de certification valide.

- Section 20.5.1, « Activation de la communication SSL entre Sentinel et le moteur/chargeur distant Identity Manager », page 219
- Section 20.5.2, « Activation de la communication SSL entre Sentinel et l'application utilisateur », page 221

20.5.1 Activation de la communication SSL entre Sentinel et le moteur/chargeur distant Identity Manager

1 Pour créer un nouveau certificat, procédez comme suit :

1a Connectez-vous à iManager.

1b Cliquez sur **NetIQ Certificate Server** (Serveur de certificats NetIQ) > **Create Server Certificate** (Créer un certificat de serveur).

1c Sélectionnez le serveur approprié.

1d Indiquez un alias pour le serveur.

1e Acceptez les autres paramètres par défaut du certificat.

2 Pour exporter le certificat de serveur au format `.pfx`, procédez comme suit :

2a Dans iManager, sélectionnez **Directory Administration** (Administration des répertoires) > **Modify Object** (Modifier l'objet).

2b Recherchez et sélectionnez l'objet KMO (Key Material Object).

2c Cliquez sur **Certificates** (Certificats) > **Export** (Exporter).

2d Spécifiez un mot de passe.

2e Enregistrez le certificat de serveur en tant que PKCS#12. Par exemple, `certificat.pfx`.

3 Extrayez la clé privée du certificat exporté dans le fichier `dxipkey.pem` à l'aide de la commande suivante :

```
openssl pkcs12 -in certificate.pfx -nocerts -out dxipkey.pem –nodes
```

4 Extrayez le certificat dans le fichier `dxicert.pem`.

```
openssl pkcs12 -in certificate.pfx -nokeys -out dxicert.pem
```

5 Pour exporter le certificat de l'autorité de certification du serveur eDirectory créé à l'Étape 1 au format Base64, procédez comme suit :

5a Dans iManager, accédez à **Rôles et tâches** > **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **User Certificates** (Certificats de l'utilisateur).

5b Recherchez et sélectionnez le certificat créé.

5c Cliquez sur **Exporter**.

5d Dans le menu déroulant, sélectionnez **OU=organizationCA.O=TREENAME** comme **certificat d'autorité de certification**.

5e Comme **format d'exportation**, sélectionnez **BASE64** dans le menu déroulant.

5f Cliquez sur **Next** (Suivant) et enregistrez le certificat. Par exemple, `cacert.b64`.

6 Importez le certificat de l'autorité de certification dans un fichier Keystore à l'aide de la commande suivante :

```
keytool -import -alias <nom_alias> -file <fichier_b64> -keystore
<fichier_keystore> –noprompt
```

Exemples :

```
keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks –
noprompt
```

7 Pour importer le certificat dans le Truststore du connecteur d'audit, procédez comme suit :

7a Connectez-vous à l'interface principale de Sentinel en tant qu'administrateur.

7b Dans l'écran principal d'ESM, recherchez le serveur d'audit.

7c Cliquez avec le bouton droit de la souris sur le **serveur d'audit**, puis cliquez sur **Éditer**.

7d Sous l'onglet Sécurité, sélectionnez **Strict**.

REMARQUE : par défaut, le système est configuré pour utiliser le mode **Ouvert** (non sécurisé) pour permettre la connectivité initiale. Toutefois, si vous travaillez dans un environnement de production, veillez à définir le mode sur **Strict**.

7e Cliquez sur **Importer** et recherchez le certificat que vous avez créé à l'Étape 6. Par exemple, `idmkeystore.ks`.

7f Cliquez sur **Ouvrir**, puis sur **Enregistrer**.

7g Redémarrez le serveur d'audit.

8 Redémarrez les services Identity Manager.

20.5.2 Activation de la communication SSL entre Sentinel et l'application utilisateur

1 Pour créer un nouveau certificat, procédez comme suit :

1a Connectez-vous à iManager.

1b Cliquez sur **NetIQ Certificate Server** (Serveur de certificats NetIQ) > **Create User Certificate** (Créer un certificat utilisateur).

1c Sélectionnez l'utilisateur approprié.

1d Indiquez un surnom pour l'utilisateur.

1e Dans **Creation Method** (Méthode de création), sélectionnez **Custom** (Personnalisée).

1f Acceptez les autres paramètres par défaut du certificat.

1g Cliquez sur **Suivant**.

1h Dans **Custom Extensions** (Extensions personnalisées-, sélectionnez **New DER Encoded Extensions** (Nouvelles extensions chiffrées au format DER).

1i Accédez à l'extension personnalisée `\products\RBPM\ext.der`.

1j (Facultatif) Spécifiez l'adresse électronique.

1k Passez en revue les paramètres de certificat, puis cliquez sur **Terminer**.

2 Pour exporter le certificat utilisateur, procédez comme suit :

2a Cliquez sur **NetIQ Certificate Access** (Accès au certificat NetIQ) > **User Certificates** (Certificats utilisateur).

2b Sélectionnez le certificat utilisateur importé à l'Étape 1.

2c Sélectionnez le certificat utilisateur valide et cliquez sur **Exporter**.

2d Spécifiez un mot de passe.

2e Enregistrez le certificat utilisateur en tant que PKCS #12. Par exemple, `certificat.pfx`.

3 Extrayez la clé privée du certificat exporté dans le fichier `key.pem` à l'aide de la commande suivante :

```
openssl pkcs12 -in certificate.pfx -nocerts -out key.pem –nodes
```

4 Extrayez le certificat dans le fichier `cert.pem`.

```
openssl pkcs12 -in certificate.pfx -nokeys -out cert.pem
```

5 Arrêtez l'application utilisateur.

6 Ajoutez la clé privée et le certificat à l'utilitaire configupdate.

6a Ouvrez l'utilitaire configupdate.

6b Cliquez sur **Afficher les options avancées**.

6c Dans le champ **Certificat de signature numérique de NetIQ Sentinel**, copiez le fichier `cert.pem`.

6d Dans le champ **Clé privée de signature numérique de NetIQ Sentinel**, naviguez jusqu'à l'emplacement où vous avez extrait la clé privée (`key.pem`) et importez la clé.

6e Enregistrez les modifications apportées à l'utilitaire configupdate.

7 Redémarrez les applications utilisateur.

8 Pour exporter le certificat de l'autorité de certification du serveur eDirectory créé à l'Étape 1 au format Base64, procédez comme suit :

8a Dans iManager, accédez à **Rôles et tâches** > **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **User Certificates** (Certificats de l'utilisateur).

8b Sélectionnez le certificat créé.

8c Cliquez sur **Exporter** et désactivez la case à cocher Export private key (Exporter la clé privée).

8d Comme **format d'exportation**, sélectionnez **BASE64** dans le menu déroulant.

8e Cliquez sur **Next** (Suivant) et enregistrez le certificat. Par exemple, `cacert.b64`.

9 Importez le certificat de l'autorité de certification dans un fichier Keystore à l'aide de la commande suivante :

```
keytool -import -alias <nom_alias> -file cacert.b64 -keystore
<fichier_keystore> –noprompt
```

Exemples :

```
keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks –
noprompt
```

10 Pour importer le certificat dans le Truststore du connecteur d'audit, procédez comme suit :

10a Connectez-vous à l'interface principale de Sentinel en tant qu'administrateur.

10b Dans l'écran principal d'ESM, recherchez le serveur d'audit.

10c Cliquez avec le bouton droit de la souris sur le **serveur d'audit**, puis cliquez sur **Éditer**.

10d Sous l'onglet Sécurité, sélectionnez **Strict**.

REMARQUE : par défaut, le système est configuré pour utiliser le mode **Ouvert** (non sécurisé) pour permettre la connectivité initiale. Toutefois, si vous travaillez dans un environnement de production, veillez à définir le mode sur **Strict**.

10e Cliquez sur **Importer** et recherchez le certificat que vous avez créé à l'Étape 9. Par exemple, `idmKeystore.ks`.

10f Cliquez sur **Ouvrir**, puis sur **Enregistrer**.

10g Redémarrez le serveur d'audit.

11 Redémarrez les applications utilisateur.

20.6 Mise à jour des paramètres SSL pour le serveur d'applications

Le programme d'installation configure automatiquement le serveur d'applications qui héberge les applications d'identité et Identity Reporting pour prendre en charge les communications SSL. Il crée le connecteur par défaut dans le fichier `server.xml` situé dans le répertoire `/opt/netiq/idm/apps/tomcat/conf/`.

```
<Connector port="https_port" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLSv1.2" keystoreFile="path_to_keystore_file"
keystorePass="keystore_password" sslEnabledProtocols="TLSv1.2" />
```

où:

keystoreFile

Spécifie le chemin du fichier Keystore, par exemple, le fichier `idmapps.keystore`. Placez le fichier dans le répertoire `/opt/netiq/idm/apps/tomcat/conf/`.

keystorePass

Spécifie le mot de passe du fichier `tomcat.ks`.

Vous devez vous assurer que le mot de passe Keystore et le chemin du fichier Keystore sont corrects dans le fichier `server.xml`.

Pour modifier les valeurs fournies par l'installation, procédez comme suit :

1. Arrêtez Tomcat, s'il est en cours d'exécution.
2. Accédez au répertoire `conf` de Tomcat, situé par défaut sous `/opt/netiq/idm/apps/tomcat/conf`.
3. Vérifiez que le répertoire `conf` contient un fichier Keystore. Par exemple : `tomcat.ks`.

   Si vous créez le fichier Keystore après l'exécution de cette procédure, veillez à utiliser le même nom de fichier que celui spécifié au cours de la procédure. Pour plus d'informations, reportez-vous à la Section 20.2, « Création d'un fichier Keystore et d'une demande de signature de certificat », page 214.
4. Dans un éditeur de texte, ouvrez le fichier `server.xml` situé dans le répertoire `conf`.
5. Configurez le port SSL du serveur Tomcat.

   Par exemple, le port connecteur pour SSL est `8543`.

   De même, mettez à jour l'attribut `redirectPort` sur `8543` et enregistrez le fichier `server.xml`.

   Par exemple :

   ```
   <Connector port="8543" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="/opt/netiq/idm/apps/tomcat/conf/idmapps.keystore"
   keystorePass="encrypted_password"
   ```
6. Démarrez Tomcat.

   Par exemple : `systemctl start netiq-tomcat.service`

20.7 Mise à jour des paramètres SSL dans l'utilitaire de configuration

Le programme d'installation configure automatiquement les paramètres SSL. Pour modifier les valeurs fournies par l'installation, procédez comme suit :

1. Arrêtez Tomcat, s'il est en cours d'exécution, à l'aide du fichier `services.msc`.

   Par exemple : `systemctl status netiq-tomcat.service`.
2. Accédez à l'utilitaire de configuration de RBPM, situé par défaut dans le répertoire d'installation des applications d'identité.
3. À l'invite de commande, exécutez l'utilitaire de configuration (`configupdate.sh`) :

   REMARQUE : vous devrez peut-être attendre quelques minutes pour que l'utilitaire démarre.
4. (Conditionnel) Si vous configurez SSL dans l'utilitaire configupdate, accédez à l'onglet **Authentification** et remplacez toutes les références mentionnées dans l'onglet **Clients SSO**.

`https://<IP address>:<SSL Port number>`

Exemples :

`https://192.168.0.1:8543`

5 Cliquez sur **Authentification**, puis modifiez les paramètres suivants :

Port TCP du serveur OAuth

Permet de spécifier le port du serveur d'authentification.

Par exemple : `8543`

Le serveur OAuth utilise TLS/SSL.

Indique que vous souhaitez que le serveur d'authentification utilise le protocole TLS/SSL pour les communications.

Fichier keystore TLS/SSL facultatif

Indique le chemin et le nom du fichier de keystore JKS Java qui contient le certificat approuvé du serveur d'authentification. Ce paramètre s'applique lorsque le serveur d'authentification utilise le protocole TLS/SSL et que le certificat approuvé du serveur d'authentification n'est pas dans le Truststore JRE (`cacerts`).

Mot de passe du fichier keystore TLS/SSL facultatif

Spécifie le mot de passe utilisé pour charger le fichier keystore pour le serveur d'authentification TLS/SSL.

Fichier Keystore OAuth

Indique le chemin d'accès au fichier keystore JKS Java que vous souhaitez utiliser pour l'authentification. Le fichier keystore doit contenir au moins une paire de clés publique/privée.

Mot de passe du fichier keystore OAuth

Spécifie le mot de passe utilisé pour charger le fichier keystore OAuth.

Alias de la clé qui doit être utilisée par OAuth

Spécifie le nom de la paire de clés publique/privée dans le fichier keystore OSP que vous souhaitez utiliser pour la génération de la clé symétrique.

Clé de mot de passe qui doit être utilisée par OAuth

Spécifie le mot de passe de la clé privée utilisée par le serveur d'authentification.

6 Cliquez sur **Clients SSO**.

7 Mettez à jour l'ensemble des paramètres d'URL, tels que le **lien URL vers la page de renvoi** et l'**URL de redirection OAuth**.

Ces paramètres spécifient l'URL absolue vers laquelle le serveur d'authentification dirige un client de navigateur une fois l'authentification terminée.

Utilisez le format suivant :`https://nom_DNS:port_SSL/chemin`. Par exemple : `https://nqserver.testsite:8543/landing/com.netiq.test`.

8 Enregistrez les modifications dans l'utilitaire de configuration.

9 Démarrez Tomcat.

20.8 Mise à jour des paramètres SSL pour SSPR

Pour modifier les paramètres SSL de SSPR, vous devez être connecté à l'application.

1 Dans un navigateur, entrez l'URL `https` que vous avez indiquée dans l'utilitaire de configuration pour la page de renvoi. Par exemple : `https://myserver.host:8543/landing`.

2 Connectez-vous à l'aide des références de l'administrateur pour les applications d'identité.

L'application affiche un message d'avertissement indiquant que vous devez modifier l'URL de la liste blanche de redirection.

3 Pour modifier l'URL de la liste blanche de redirection, suivez les instructions de la page.

4 Accédez à **Paramètres > SSO Oauth**.

5 Pour les trois URL, indiquez le protocole et le port `https`.

6 Accédez à **Paramètres > Application**.

7 Pour les trois URL, indiquez le protocole et le port `https`.

8 Cliquez sur **Enregistrer**, puis sur **OK**.

9 Vérifiez que toutes les URL pour les applications d'identité utilisent à présent le protocole `https`.

Astuce de dépannage

Après la mise à jour des paramètres SSL pour SSPR, si vous ne parvenez pas à accéder à la page de renvoi de SSPR, effectuez les étapes suivantes pour mettre à jour les URL nécessaires dans le fichier `SSPRConfiguration.xml`.

1 Accédez au fichier `SSPRConfiguration.xml` à l'emplacement suivant :

```
/opt/netiq/idm/apps/sspr/sspr_data
```

2 Mettez à jour toutes les URL avec une adresses IP et des numéros de port appropriés.

```
https://<IP address>:<SSL Port number>
```

Exemple :

```
https://192.168.0.1:8543
```

VIII Tâches de post-installation

Après l'installation d'Identity Manager, vous devez configurer les pilotes installés conformément aux stratégies et exigences définies par vos processus métiers. Vous devez également configurer Sentinel Log Management for IGA pour collecter les événements d'audit. Les tâches post-installation comprennent généralement les éléments suivants :

21 Configuration d'un système connecté

Identity Manager permet aux applications, répertoires et bases de données de partager des informations. Pour des instructions concernant la configuration de pilotes spécifiques, reportez-vous à la documentation relative aux pilotes Identity Manager.

21.1 Création et configuration d'un ensemble de pilotes

Un ensemble de pilotes est un conteneur qui regroupe des pilotes Identity Manager. Vous ne pouvez activer qu'un seul ensemble de pilotes à la fois sur un serveur. Pour créer un ensemble de pilotes, vous pouvez utiliser l'outil Designer.

Pour que la synchronisation des mots de passe avec le coffre-fort d'identité soit prise en charge, Identity Manager requiert que les ensembles de pilotes aient une stratégie de mot de passe. Vous pouvez utiliser le paquetage de stratégie de mot de passe universel par défaut d'Identity Manager ou créer une stratégie de mot de passe en fonction des besoins de votre organisation. Toutefois, la stratégie de mot de passe doit inclure l'objet `DirXML-PasswordPolicy`. Si l'objet Stratégie n'existe pas dans le coffre-fort d'identité, vous pouvez le créer.

21.1.1 Création d'un ensemble de pilotes

Designer pour Identity Manager inclut de nombreux paramètres permettant de créer et de configurer un ensemble de pilotes. Ces paramètres permettent de spécifier des valeurs de configuration globales, des paquetages d'ensemble de pilotes, des mots de passe nommés pour des ensembles de pilotes, des niveaux de consignation, des niveaux de trace et des valeurs d'environnement Java. Pour plus d'informations, reportez-vous à la section « Configuring Driver Sets » (Configuration d'ensembles de pilotes) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).

21.1.2 Assignation de la stratégie de mot de passe par défaut aux ensembles de pilotes

Vous devez assigner l'objet DirXML-PasswordPolicy à chaque ensemble de pilotes présent dans le coffre-fort d'identité. Le paquetage de stratégie de mot de passe universel par défaut d'Identity Manager inclut cet objet Stratégie. La stratégie par défaut installe et assigne une stratégie de mot de passe universel pour contrôler la façon dont le moteur Identity Manager génère automatiquement des mots de passe aléatoires pour les pilotes.

En revanche, si vous souhaitez utiliser une stratégie de mot de passe personnalisée, vous devez créer l'objet Stratégie de mot de passe et la stratégie. Pour plus d'informations, reportez-vous à la Section 21.1.3, « Création de l'objet Stratégie de mot de passe dans le coffre-fort d'identité », page 230 et à la Section 21.1.4, « Création d'une stratégie de mot de passe personnalisée », page 231.

1. Ouvrez votre projet dans Designer.
2. Dans le volet Mode plan, développez votre projet.
3. Développez **Catalogue de paquetages > Commun** pour vérifier que le paquetage de stratégie de mot de passe universel par défaut existe.
4. (Conditionnel) Si le paquetage de stratégie de mot de passe n'est pas répertorié dans Designer, procédez comme suit :
   - **4a** Cliquez avec le bouton droit de la souris sur **Catalogue de paquetages**.
   - **4b** Sélectionnez **Importer le paquetage**.
   - **4c** Sélectionnez **Stratégie de mot de passe universel par défaut Identity Manager**, puis cliquez sur **OK**.

     Pour que le tableau affiche bien tous les paquetages disponibles, vous devrez peut-être désélectionner l'option **Afficher les paquetages de base uniquement**.
5. Sélectionnez chaque ensemble de pilotes et assignez la stratégie de mot de passe.

21.1.3 Création de l'objet Stratégie de mot de passe dans le coffre-fort d'identité

Si l'objet `DirXML-PasswordPolicy` n'existe pas dans le coffre-fort d'identité, vous pouvez le créer à l'aide de Designer ou de l'utilitaire ldapmodify. Pour plus d'informations sur la procédure à suivre dans Designer, reportez-vous à la section « Configuring Driver Sets » (Configuration d'ensembles de pilotes) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager). Pour utiliser l'utilitaire ldapmodify, procédez comme suit :

1. Dans un éditeur de texte, créez un fichier LDIF (LDAP Data Interchange Format) avec les attributs suivants :

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: <driverset LDAP dn>
```

REMARQUE : si vous copiez le contenu tel quel, vous risquez d'introduire des caractères spéciaux masqués dans le fichier. Si un message d'erreur de type `ldif_record() = 17` s'affiche lors de l'ajout de ces attributs au coffre-fort d'identité, insérez un espace supplémentaire entre les deux DN.

2 Pour ajouter l'objet DirMXL-PasswordPolicy dans le coffre-fort d'identité, importez les attributs du fichier en effectuant l'opération suivante :

Accédez au répertoire contenant l'utilitaire ldapmodify et entrez la commande suivante :

```
ldapmodify -x -c -h hostname_or_IP_address -p 389 -D "cn=admin,ou=sa,o=system"
-w password -f path_to_ldif_file
```

Par exemple :

```
ldapmodify -x -ZZ -c -h server1.test.com -p 389 -D "cn=admin,ou=sa,o=system" -
w test123 -f /root/dirxmlpasswordpolicy.ldif
```

Par défaut, l'utilitaire ldapmodify est situé dans le répertoire `/opt/novell/eDirectory/bin`.

21.1.4 Création d'une stratégie de mot de passe personnalisée

Au lieu d'utiliser la stratégie de mot de passe par défaut d'Identity Manager, vous pouvez créer une nouvelle stratégie adaptée aux exigences de votre organisation. Vous pouvez assigner une stratégie de mot de passe à la totalité de l'arborescence, à un conteneur racine de partition, à un conteneur, voire à un utilisateur particulier. Pour simplifier la gestion, NetIQ recommande d'assigner des stratégies de mot de passe au niveau le plus élevé possible de l'arborescence. Pour plus d'informations, reportez-vous à la section Creating Password Policies (Création de stratégies de mot de passe) du manuel *Password Management 3.3.2 Administration Guide* (Guide d'administration 3.3.2 pour la gestion des mots de passe).

REMARQUE : vous devez également assigner l'objet DirXML-PasswordPolicy aux ensembles de pilotes. Pour plus d'informations, reportez-vous à la Section 21.1.3, « Création de l'objet Stratégie de mot de passe dans le coffre-fort d'identité », page 230.

21.1.5 Création de l'objet Collection de notification par défaut dans le coffre-fort d'identité

La Collection de notification par défaut est un objet du coffre-fort d'identité qui contient un ensemble de modèles de notification par message électronique et un serveur SMTP utilisé lors de l'envoi des messages électroniques générés à partir des modèles. Si l'objet Collection de notification par défaut n'existe pas dans le coffre-fort d'identité, créez-le à l'aide de Designer.

1. Ouvrez votre projet dans Designer.
2. Dans le volet Mode plan, développez votre projet.
3. Cliquez avec le bouton droit de la souris sur le coffre-fort d'identité, puis cliquez sur **Propriétés** du coffre-fort d'identité.
4. Cliquez sur **Paquetages**, puis sur l'icône d'**ajout de paquetages**.
5. Sélectionnez tous les paquetages de modèles de notification, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer** pour installer les paquetages à l'aide de l'opération **Installer**.
7. Déployez les modèles de notification dans le coffre-fort d'identité.

21.2 Création d'un pilote

Pour créer des pilotes, utilisez la fonctionnalité de gestion de paquetages incluse dans Designer. Pour chaque pilote Identity Manager que vous envisagez d'utiliser, créez un objet Pilote et importez une configuration. L'objet Pilote contient des paramètres et des stratégies de configuration pour ce pilote. Lors de la création d'un objet Pilote, installez les paquetages du pilote, puis modifiez sa configuration en fonction de votre environnement.

Les paquetages de pilote contiennent un ensemble de stratégies par défaut. Il permet de commencer dans de bonnes conditions l'implémentation de votre modèle de partage de données. La plupart du temps, vous configurez un pilote à l'aide de la configuration par défaut, puis vous modifiez cette configuration en fonction des besoins de votre environnement. Une fois le pilote créé et configuré, déployez-le dans le coffre-fort d'identité et démarrez-le. En règle générale, le processus de création d'un pilote inclut les opérations suivantes :

1. Importation des paquetages du pilote
2. Installation des paquetages du pilote
3. Configuration de l'objet Pilote
4. Déploiement de l'objet Pilote
5. Démarrage de l'objet Pilote

Pour obtenir des informations supplémentaires et propres à des pilotes spécifiques, reportez-vous au guide de mise en oeuvre des pilotes correspondants sur le site Web des pilotes Identity Manager.

21.3 Définition de stratégies

Les stratégies permettent de personnaliser le flux d'informations entrant et sortant du coffre-fort d'identité pour un environnement particulier. Par exemple, une société peut utiliser inetorgperson en tant que classe d'utilisateur principal, et une autre société peut utiliser Utilisateur. Pour cela, une

stratégie doit être créée afin d'indiquer au moteur Identity Manager comment est appelé l'utilisateur dans chacun des systèmes. Chaque fois que des opérations affectant les utilisateurs circulent entre les systèmes connectés, Identity Manager applique la stratégie permettant cette modification.

Les stratégies créent aussi de nouveaux objets, mettent à jour des valeurs d'attributs, apportent des transformations aux schémas, définissent des critères de correspondance, gèrent des associations Identity Manager, etc.

NetIQ recommande d'utiliser Designer afin de définir, pour les pilotes, des stratégies répondant aux besoins de votre entreprise. Pour plus d'informations sur les stratégies, reportez-vous aux manuels *NetIQ Identity Manager - Using Designer to Create Policies* (NetIQ Identity Manager - Utilisation de Designer pour la création de stratégies) et *NetIQ Identity Manager Understanding Policies Guide* (Guide de présentation des stratégies NetIQ Identity Manager). Pour plus d'informations sur les définitions de type de document (DTD) utilisées par Identity Manager, reportez-vous à la documentation Identity Manager DTD Reference (Référence des DTD d'Identity Manager). Ces ressources incluent :

- une description détaillée de chaque stratégie disponible ;
- un guide et des références approfondis pour le Générateur de stratégies, y compris des exemples et une syntaxe pour chaque situation, opération, nom et verbe ;
- des informations relatives à la création de stratégies via les feuilles de style XSLT.

22 Configuration de la gestion des mots de passe oubliés

Le programme d'installation d'Identity Manager comprend une fonction de réinitialisation des mots de passe en self-service pour vous aider à gérer le processus de réinitialisation des mots de passe oubliés. Sinon, vous pouvez utiliser un système de gestion des mots de passe externe.

22.1 Utilisation de Self Service Password Reset pour la gestion des mots de passe oubliés

Dans la plupart des cas, vous pouvez activer la fonctionnalité de gestion des mots de passe oubliés lors de l'installation de SSPR et des applications d'identité. Toutefois, vous n'avez peut-être pas spécifié l'URL de la page de renvoi pour les applications d'identité vers laquelle SSPR renvoie les utilisateurs après une modification de mot de passe. Vous devrez peut-être également activer la gestion de mot de passe oublié. Cette section contient les informations suivantes :

22.1.1 Configuration d'Identity Manager pour l'utilisation de SSPR

Cette section fournit des informations sur la configuration d'Identity Manager pour l'utilisation de SSPR.

1. Connectez-vous au serveur sur lequel vous avez installé les applications d'identité.
2. Exécutez l'utilitaire de configuration de RBPM. Pour plus d'informations, reportez-vous à la Section 11.6.1, « Exécution de l'utilitaire de configuration des applications d'identité », page 143.
3. Dans l'utilitaire, accédez à **Authentification > Gestion des mots de passe**.
4. Pour **Fournisseur de gestion des mots de passe**, indiquez **SSPR**.
5. Sélectionnez **Mot de passe oublié**.
6. Accédez à **Clients SSO > Réinitialisation de mot de passe en self-service**.
7. Pour l'**ID du client OSP**, spécifiez le nom à utiliser pour identifier le client Single Sign-On pour SSPR vis-à-vis du serveur d'authentification. La valeur par défaut est `sspr`.
8. Pour le **secret du client OSP**, indiquez le mot de passe pour le client Single Sign-On pour SSPR.

9 Pour l'**URL de redirection OSP**, spécifiez l'URL absolue vers laquelle le serveur d'authentification redirige un client de navigateur une fois l'authentification effectuée.

   Utilisez le format suivant : `protocole://serveur:port/chemin`. Par exemple : `http://10.10.10.48:8180/sspr/public/oauth`.

10 Enregistrez les modifications, puis fermez l'utilitaire.

22.1.2 Configuration de SSPR pour Identity Manager

Cette section fournit des informations sur la configuration de SSPR afin que cet utilitaire fonctionne avec Identity Manager. Par exemple, vous pouvez modifier les stratégies de mot de passe et de questions de vérification d'identité.

Lorsque vous avez installé SSPR avec Identity Manager, vous avez spécifié un mot de passe qu'un administrateur peut utiliser pour configurer l'application. NetIQ vous recommande de modifier les paramètres de SSPR, puis de spécifier le compte d'administrateur ou le groupe en mesure de configurer SSPR.

REMARQUE : Si vous installez SSPR sur un serveur différent de celui du serveur d'applications utilisateur, assurez-vous que le certificat de l'application SSPR est ajouté à l'application utilisateur `cacerts`.

---

1 Connectez-vous à SSPR à l'aide du mot de passe de configuration que vous avez spécifié au cours de l'installation.

2 Sur la page Paramètres, modifiez les paramètres de la stratégie de mot de passe et de questions de vérification d'identité. Pour plus d'informations sur la configuration des valeurs par défaut des paramètres SSPR, reportez-vous à la section Configuring Self Service Password Reset (Configuration de la réinitialisation de mot de passe en self-service) du manuel *NetIQ Self Service Password Reset Administration Guide* (Guide d'administration de NetIQ SSPR).

3 Verrouillez le fichier de configuration de SSPR (`SSPRConfiguration.xml`). Pour plus d'informations sur le verrouillage du fichier de configuration, reportez-vous à la section « Verrouillage de la configuration de SSPR » page 236.

4 (Facultatif) Pour modifier les paramètres de SSPR après avoir verrouillé la configuration, vous devez définir le paramètre `configIsEditable` sur `true` dans le fichier `SSPRConfiguration.xml`.

5 Déconnectez-vous de SSPR.

6 Pour que les modifications prennent effet, redémarrez Tomcat.

22.1.3 Verrouillage de la configuration de SSPR

1 Accédez à **http://<IP/nom DNS>:<port>/sspr**. Ce lien vous permet d'accéder au portail SSPR.

2 Connectez-vous à Identity Manager avec un compte d'administrateur ou connectez-vous avec vos références de connexion existantes.

3 Cliquez sur **Gestionnaire de configuration** en haut de la page et entrez le mot de passe de configuration spécifié au cours de l'installation.

4 Cliquez sur **Éditeur de configuration** et accédez à **Paramètres > Paramètres LDAP**.

5 Verrouillez le fichier de configuration de SSPR (`SSPRConfiguration.xml`).

   5a Dans la section relative aux autorisations d'administrateur, définissez un filtre au format LDAP pour un utilisateur ou un groupe qui dispose de droits d'administrateur pour SSPR dans le coffre-fort d'identité. Par défaut, le filtre est défini sur `groupMembership=cn=Admins,ou=Groups,o=example`.

   Par exemple, réglez-le sur `uaadmin` (`cn=uaadmin`) pour l'administrateur de l'application utilisateur.

   Cela empêche les utilisateurs de modifier la configuration de SSPR, à l'exception de l'administrateur SSPR qui dispose de droits d'accès complets pour modifier les paramètres.

   5b Pour garantir que la requête LDAP renvoie des résultats, cliquez sur **View Matches** (Afficher les correspondances).

   Si le paramètre présente une erreur, vous ne pouvez pas passer à l'option de configuration suivante. SSPR affiche les détails de l'erreur afin de vous aider à résoudre le problème.

   5c Cliquez sur **Enregistrer**.

   5d Dans la fenêtre de confirmation qui s'affiche, cliquez sur **OK**.

   Lorsque SSPR est verrouillé, l'administrateur peut afficher d'autres options dans l'interface utilisateur d'administration, telles que le tableau de bord, l'activité de l'utilisateur, l'analyse des données, etc., qui n'étaient pas disponibles avant le verrouillage de SSPR.

6 (Facultatif) Pour modifier les paramètres de SSPR après avoir verrouillé la configuration, vous devez définir le paramètre `configIsEditable` sur `true` dans le fichier `SSPRConfiguration.xml`.

7 Déconnectez-vous de SSPR.

8 Reconnectez-vous ensuite à SSPR avec les références d'administrateur définies à l'Étape 3.

9 Cliquez sur **Close Configuration** (Fermer la configuration), puis sur **OK** pour confirmer les modifications.

10 Pour que les modifications prennent effet, redémarrez Tomcat.

22.2 Utilisation d'un système externe pour la gestion des mots de passe oubliés

Pour utiliser un système externe, vous devez spécifier l'emplacement d'un fichier WAR contenant la fonction de mot de passe oublié. Ce processus comprend les opérations suivantes :

- Section 22.2.1, « Spécification d'un fichier WAR externe de gestion des mots de passe oubliés », page 238
- Section 22.2.2, « Test de la configuration du fichier externe pour les mots de passe oubliés », page 239
- Section 22.2.3, « Configuration de la communication SSL entre serveurs d'applications », page 239

22.2.1 Spécification d'un fichier WAR externe de gestion des mots de passe oubliés

Si vous ne spécifiez pas cette valeur lors de l'installation et que vous souhaitez modifier les paramètres, vous pouvez utiliser l'utilitaire de configuration de RBPM ou apporter les modifications dans l'application utilisateur en tant qu'administrateur.

1. (Facultatif) Pour modifier les paramètres de l'utilitaire de configuration de RBPM, procédez comme suit :
   - **1a** Connectez-vous au serveur sur lequel vous avez installé les applications d'identité.
   - **1b** Exécutez l'utilitaire de configuration de RBPM. Pour plus d'informations, reportez-vous à la Section 11.6.1, « Exécution de l'utilitaire de configuration des applications d'identité », page 143.
   - **1c** Dans l'utilitaire, accédez à **Authentification > Gestion des mots de passe**.
   - **1d** Pour **Fournisseur de gestion des mots de passe**, spécifiez **Application utilisateur (héritée)**.
2. (Facultatif) Pour modifier les paramètres dans l'application utilisateur, procédez comme suit :
   - **2a** Connectez-vous en tant qu'administrateur de l'application utilisateur.
   - **2b** Accédez à **Administration > Configuration de l'application > Config. module mot de passe > Login**.
3. Pour **Mot de passe oublié**, spécifiez **Externe**.
4. Pour **Lien Mot de passe oublié**, spécifiez le lien affiché lorsque l'utilisateur clique sur **Mot de passe oublié** sur la page de connexion. Lorsque l'utilisateur clique sur ce lien, l'application dirige l'utilisateur vers le système de gestion des mots de passe externe. Exemple :

   ```
   http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp
   ```

5. Pour l'option **Lien Retour mot de passe oublié**, indiquez le lien qui s'affiche lorsque l'utilisateur a terminé la procédure de mot de passe oublié. Lorsque l'utilisateur clique sur ce lien, il est redirigé vers le lien spécifié. Exemple :

   ```
   http://localhost/IDMProv
   ```

6. Pour l'option **URL du service Web de mot de passe oublié**, indiquez l'URL du service Web utilisée par le fichier WAR externe de mot de passe oublié pour revenir aux applications d'identité. Utilisez le format suivant :

   ```
   https://idmhost:sslport/idm/pwdmgt/service
   ```

   Le lien de retour doit utiliser SSL pour assurer une communication sécurisée des services Web avec les applications d'identité. Pour plus d'informations, reportez-vous à la section « Configuration de la communication SSL entre serveurs d'applications » page 239.
7. Copiez manuellement `ExternalPwd.war` dans le répertoire de déploiement du serveur d'applications distant qui exécute la fonction WAR de mots de passe externe.

22.2.2 Test de la configuration du fichier externe pour les mots de passe oubliés

Si vous disposez d'un fichier WAR de mots de passe externe et souhaitez y accéder pour tester la fonction Mot de passe oublié, vous le trouverez à l'emplacement suivant :

- Directement dans un navigateur. Accédez à la page Mot de passe oublié dans le fichier WAR de mots de passe externe. Exemple : `http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`.
- Sur la page de connexion de l'application utilisateur, cliquez sur le lien **Mot de passe oublié**.

22.2.3 Configuration de la communication SSL entre serveurs d'applications

Si vous utilisez un système externe de gestion des mots de passe, vous devez configurer la communication SSL entre les instances Tomcat sur lesquelles vous déployez les applications d'identité et le fichier WAR externe de gestion des mots de passe oubliés. Pour plus d'informations, reportez-vous à la documentation Tomcat.

22.3 Mise à jour des liens SSPR dans le tableau de bord pour un environnement distribué ou de grappe

La procédure d'installation suppose que vous déployez SSPR sur le même serveur d'applications que les applications d'identité et Identity Reporting. Par défaut, les liens intégrés sur la page **Applications** du tableau de bord utilisent une URL relative pointant vers SSPR sur le système local. Par exemple : `\sspr\private\changepassword`. Si vous installez les applications dans un environnement en grappe ou distribué, vous devez mettre à jour les URL des liens SSPR.

Pour plus d'informations, reportez-vous à l'*Aide relative aux applications d'identité*.

1. Connectez-vous au tableau de bord en tant qu'administrateur. Par exemple, connectez-vous en tant que `uaadmin`.
2. Cliquez sur **Éditer**.
3. Sur la page Modifier les éléments d'accueil, pointez sur l'élément que vous souhaitez mettre à jour, puis cliquez sur l'icône d'édition. Par exemple, sélectionnez **Modifier mon mot de passe**.
4. Pour **Lien**, indiquez l'URL absolue. Par exemple : `http://10.10.10.48:8180/sspr/changepassword`.
5. Cliquez sur **Enregistrer**.
6. Répétez cette opération pour chaque lien SSPR à mettre à jour.
7. Une fois l'opération terminée, cliquez sur **J'ai terminé**.
8. Déconnectez-vous, puis reconnectez-vous en tant qu'utilisateur normal pour tester les modifications.

23 Gestion des activités de pilote

Pour effectuer des opérations d'administration et de configuration de pilotes Identity Manager, utilisez Designer ou iManager. Ces opérations sont décrites en détail dans le manuel *NetIQ Identity Manager Driver Administration Guide* (Guide d'administration des pilotes NetIQ Identity Manager).

23.1 Arrêt et démarrage des pilotes Identity Manager

Vous devrez peut-être démarrer ou arrêter les pilotes Identity Manager pour vous assurer qu'une installation ou une mise à niveau peut modifier ou remplacer les fichiers corrects. Cette section explique les opérations suivantes :

- Section 23.1.1, « Arrêt des pilotes », page 241
- Section 23.1.2, « Lancement des pilotes », page 242

23.1.1 Arrêt des pilotes

Avant de modifier les fichiers d'un pilote, vous devez arrêter les pilotes.

- « Utilisation de Designer pour arrêter les pilotes » page 241
- « Utilisation d'iManager pour arrêter les pilotes » page 241

Utilisation de Designer pour arrêter les pilotes

1. Dans Designer, sélectionnez l'objet Coffre-fort d'identité sous l'onglet **Mode plan**.
2. Dans la barre d'outils Modélisateur, cliquez sur l'icône **Arrêter tous les pilotes**.

   Ceci arrête tous les pilotes faisant partie du projet.
3. Configurez les pilotes en mode démarrage manuel pour qu'ils ne démarrent pas tant que la procédure de mise à niveau n'est pas terminée :
   - **3a** Double-cliquez sur l'icône du pilote sous l'onglet **Mode plan**.
   - **3b** Sélectionnez **Configuration du pilote > Options de démarrage**.
   - **3c** Sélectionnez **Manuel**, puis cliquez sur **OK**.
   - **3d** Répétez la procédure de l'Étape 3a à l'Étape 3c pour chaque pilote.

Utilisation d'iManager pour arrêter les pilotes

1. Dans iManager, sélectionnez **Identity Manager > Présentation d'Identity Manager**.
2. Recherchez et sélectionnez l'emplacement de l'arborescence où rechercher les objets Ensemble de pilotes, puis cliquez sur l'icône de recherche.
3. Cliquez sur l'objet Ensemble des pilotes.
4. Cliquez sur **Pilotes > Arrêter tous les pilotes**.
5. Répétez la procédure de l'Étape 2 à l'Étape 4 pour chaque objet Ensemble des pilotes.

6 Configurez les pilotes en mode démarrage manuel pour qu'ils ne démarrent pas tant que la procédure de mise à niveau n'est pas terminée :

6a Dans iManager, sélectionnez **Identity Manager > Présentation d'Identity Manager**.

6b Recherchez et sélectionnez l'emplacement de l'arborescence où rechercher les objets Ensemble de pilotes, puis cliquez sur l'icône de recherche .

6c Cliquez sur l'objet Ensemble des pilotes.

6d Dans l'angle supérieur droit de l'icône du pilote, cliquez sur **Modifier les propriétés**.

6e Sur la page Configuration du pilote, sous **Options de démarrage**, sélectionnez **Manuel**, puis cliquez sur **OK**.

6f Répétez la procédure de l'Étape 6a à l'Étape 6e pour chaque pilote dans l'arborescence.

23.1.2 Lancement des pilotes

Une fois tous les composants Identity Manager mis à jour, redémarrez les pilotes. NetIQ recommande de tester les pilotes après leur exécution pour vérifier que toutes les stratégies continuent à fonctionner.

- « Utilisation de Designer pour lancer les pilotes » page 242
- « Utilisation d'iManager pour démarrer les pilotes » page 242

Utilisation de Designer pour lancer les pilotes

1 Dans Designer, sélectionnez l'objet Coffre-fort d'identité sous l'onglet **Mode plan**.

2 Cliquez sur l'icône **Démarrer tous les pilotes** dans la barre d'outils Modélisateur. Ceci lance tous les pilotes du projet.

3 Définissez les options de démarrage des pilotes :

3a Double-cliquez sur l'icône du pilote sous l'onglet **Mode plan**.

3b Sélectionnez **Configuration du pilote > Option de démarrage**.

3c Sélectionnez **Démarrage auto** ou choisissez votre méthode préférée pour lancer le pilote, puis cliquez sur **OK**.

3d Répétez la procédure de l'Étape 3a à l'Étape 3c pour chaque pilote.

4 Testez les pilotes pour vérifier que les stratégies fonctionnent comme prévu. Pour plus d'informations sur la manière de tester vos stratégies, reportez-vous à la section « Testing Policies with Policy Simulator » (Test des stratégies avec le simulateur de stratégies) dans la documentation *NetIQ Identity Manager - Using Designer to Create Policies* (NetIQ Identity Manager - Utilisation de Designer pour la création de stratégies).

Utilisation d'iManager pour démarrer les pilotes

1 Dans iManager, sélectionnez **Identity Manager > Présentation d'Identity Manager**.

2 Recherchez et sélectionnez l'emplacement de l'arborescence où rechercher les objets Ensemble de pilotes, puis cliquez sur l'icône de recherche .

3 Cliquez sur l'objet Ensemble des pilotes.

4 Cliquez sur **Pilotes > Démarrer tous les pilotes** pour lancer tous les pilotes simultanément.

ou

Dans la partie supérieure droite de l'icône du pilote, cliquez sur **Lancer le pilote** pour lancer chaque pilote individuellement.

5 Si vous disposez de plusieurs pilotes, répétez la procédure de l'Étape 2 à l'Étape 4.

6 Définissez les options de démarrage des pilotes :

6a Dans iManager, sélectionnez **Identity Manager > Présentation d'Identity Manager**.

6b Recherchez et sélectionnez l'emplacement de l'arborescence où rechercher les objets Ensemble de pilotes, puis cliquez sur l'icône de recherche  .

6c Cliquez sur l'objet Ensemble des pilotes.

6d Dans l'angle supérieur droit de l'icône du pilote, cliquez sur **Modifier les propriétés**.

6e Sur la page Configuration du pilote, sous **Options de démarrage**, sélectionnez **Démarrage auto** ou choisissez votre méthode préférée de lancement du pilote, puis cliquez sur **OK**.

6f Répétez la procédure de l'Étape 6b à l'Étape 6e pour chaque pilote.

7 Testez les pilotes pour vérifier que les stratégies fonctionnent comme prévu.

Il n'existe pas de simulateur de stratégie dans iManager. Pour tester les stratégies, faites intervenir des événements qui les exécutent. Vous pouvez, par exemple, créer un utilisateur, le modifier ou le supprimer.

24 Activation d'Identity Manager

Certains composants Identity Manager s'activent automatiquement lors de votre première connexion. D'autres composants requièrent une procédure d'activation.

24.1 Installation d'une référence d'activation de produit

NetIQ vous recommande d'utiliser iManager pour installer les références d'activation du produit.

REMARQUE : Pour chaque pilote que vous souhaitez activer, activez le module d'intégration contenant le pilote.

---

1. Une fois la licence achetée, NetIQ vous envoie un message électronique avec votre ID client. Ce courrier électronique contient également un lien sous la section Détail de la commande vers le site sur lequel vous pouvez obtenir votre référence. Cliquez sur le lien pour aller sur le site.
2. Cliquez sur le lien de téléchargement de licence et effectuez l'une des opérations suivantes :
   - Ouvrez le fichier de référence d'activation du produit, puis copiez son contenu dans le Presse-papiers.
   - Enregistrez le fichier de référence d'activation du produit.
   - Si vous avez choisi de copier le contenu, n'incluez pas d'espaces ni de lignes supplémentaires. Vous devez commencer la copie à partir du premier tiret (-) de la référence (`----DÉBUT DE LA RÉFÉRENCE D'ACTIVATION DU PRODUIT`) jusqu'au dernier tiret (-) (`FIN DE LA RÉFÉRENCE D'ACTIVATION DU PRODUIT-----`).
3. Connectez-vous à iManager.
4. Sélectionnez **Identity Manager > Présentation d'Identity Manager**.
5. Pour sélectionner un ensemble de pilotes dans l'arborescence, cliquez sur l'icône Parcourir ().
6. Sur la page **Présentation d'Identity Manager**, cliquez sur l'ensemble de pilotes qui contient le pilote à activer.
7. Sur la page **Présentation de l'ensemble de pilotes**, cliquez sur **Activation** > **Installation**.
8. Sélectionnez l'ensemble de pilotes dans lequel vous voulez activer un composant Identity Manager, puis cliquez sur **Suivant**.
9. (Conditionnel) Si vous avez enregistré le fichier de référence d'activation du produit, indiquez l'emplacement auquel il est enregistré.
10. (Conditionnel) Si vous avez copié le contenu du fichier de référence d'activation du produit, collez le contenu dans la zone de texte.
11. Cliquez sur **Next** (Suivant).
12. Cliquez sur **Terminer**.

24.2 Vérification des activations de produits pour Identity Manager et les pilotes

Pour chaque ensemble de pilotes, vous pouvez afficher les références d'activation de produit installées pour le serveur du moteur et les pilotes Identity Manager. Vous pouvez également supprimer une référence d'activation.

REMARQUE : après l'installation de références d'activation du produit valides pour un ensemble de pilotes, il est possible que la mention « Activation nécessaire » apparaisse encore en regard du nom du pilote. Si tel est le cas, redémarrez le pilote. Le message doit disparaître.

1. Connectez-vous à iManager.
2. Cliquez sur **Identity Manager** > **Présentation d'Identity Manager.**
3. Pour sélectionner un ensemble de pilotes dans l'arborescence, utilisez l'icône Parcourir () et l'icône Rechercher ().
4. Sur la page **Présentation d'Identity Manager**, cliquez sur l'ensemble de pilotes pour lequel vous voulez vérifier les informations d'activation.
5. Sur la page **Présentation de l'ensemble de pilotes**, cliquez sur **Activation > Information**.

   Vous pouvez afficher le texte de la référence d'activation ou, si une erreur est signalée, vous pouvez supprimer une référence d'activation.

24.3 Activation des pilotes Identity Manager

Lorsque vous activez le moteur Identity Manager, vous activez également les pilotes suivants :

Pilotes de service	Pilotes courants
Service de collecte de données	Active Directory
Fournisseur d'ID	Pilote bidirectionnel pour eDirectory
Passerelle système gérée	eDirectory
Service de rôles et de ressources	GroupWise 2014
Application utilisateur	LDAP
	Lotus Notes

Pour activer d'autres pilotes Identity Manager, vous devez acheter des modules d'intégration Identity Manager supplémentaires, qui peuvent contenir un ou plusieurs pilotes. Vous recevez une référence d'activation de produit pour chaque module d'intégration Identity Manager acheté. Après avoir reçu la référence, effectuez la procédure décrite à la Section 24.1, « Installation d'une référence d'activation de produit », page 245. Pour plus d'informations à propos des pilotes, reportez-vous au site Web de documentation des pilotes Identity Manager.

24.4 Activation de composants spécifiques Identity Manager

Cette section fournit des informations sur l'activation de composants spécifiques pour Identity Manager.

24.4.1 Activation de Designer

Lorsque vous activez le moteur Identity Manager ou les pilotes Identity Manager, vous activez également Designer et l'administrateur de catalogue.

24.4.2 Activation d'Analyzer

Lorsque vous lancez la perspective Analyzer sans licence, Analyzer ouvre la page d'activation, l'analyseur à partir de laquelle vous pouvez gérer les licences Analyzer.

REMARQUE : si vous fermez la boîte de dialogue Activation, Analyzer reste verrouillé jusqu'à ce que vous fournissiez une licence pour l'activer. Lorsque vous êtes prêt à ajouter une licence, cliquez sur **Activate Analyzer** (Activer Analyzer) dans la `Project View` (Vue du projet) pour ouvrir la boîte de dialogue Activation.

---

1. Lancez Analyzer.
2. Dans la fenêtre d'**activation d'Analyzer**, vous pouvez ajouter une nouvelle licence ou accéder au Customer Center pour en obtenir une.
3. (Conditionnel) Pour ajouter une nouvelle licence :
   - **3a** Cliquez sur **Add a new license** (Ajouter une nouvelle licence).
   - **3b** Dans la fenêtre **License** (Licence), tapez le code d'activation que vous avez téléchargé à partir du portail du service clients NetIQ, puis cliquez sur **OK**.
4. (Conditionnel) Pour accéder au Customer Center pour obtenir une licence :
   - **4a** Cliquez sur **Access Customer Center for license**. (Accéder au Customer Center pour obtenir une licence).
   - **4b** Cliquez sur **Visit the NetIQ Customer Center** (Visiter le NetIQ Customer Center) à partir de la page **Micro Focus Customer Center**.
   - **4c** Recherchez et sélectionnez la licence Analyzer.
   - **4d** Copiez le code d'activation, puis fermez le portail du service clients.
   - **4e** Dans la fenêtre **Licence** , tapez le code d'activation, puis cliquez sur **OK**.
5. Dans la fenêtre **Analyzer Activation** (Activation d'Analyzer), passez en revue les détails de la licence que vous venez d'installer.
6. Cliquez sur **OK** pour commencer à utiliser Analyzer.

24.4.3 Activation de Sentinel Log Management for IGA

Vous pouvez ajouter une clé de licence lors de l'installation de Sentinel. Cette section fournit des informations sur l'ajout de la clé de licence après l'installation de Sentinel.

Si vous utilisez une clé de licence d'évaluation installée par défaut, vous devez activer Sentinel avant l'expiration de la clé d'évaluation pour éviter toute interruption dans les fonctionnalités de Sentinel. Pour plus d'informations sur l'achat de la licence, consultez le site Web du produit Identity Manager.

Vous pouvez ajouter une clé de licence à l'aide de l'interface principale de Sentinel ou de la ligne de commande.

- « Ajout d'une clé de licence à l'aide de l'interface principale de Sentinel » page 248
- « Ajout d'une clé de licence par l'intermédiaire de la ligne de commande » page 248

Ajout d'une clé de licence à l'aide de l'interface principale de Sentinel

1. Connectez-vous à l'interface principale de Sentinel en tant qu'administrateur.
2. Cliquez sur **À propos de > Licences**.
3. Dans la section Licences, cliquez sur **Ajouter une licence**.
4. Indiquez la clé de licence dans le champ **Clé.**

   Une fois que vous avez indiqué la licence, les informations suivantes sont affichées dans la section Aperçu :

   - **Fonctions:** fonctionnalités disponibles avec la licence.
   - **Nom d'hôte :** champ réservé à l'usage interne de NetIQ.
   - **Série:** champ réservé à l'usage interne de NetIQ.
   - **EPS :** taux d'événement intégré dans la clé de licence. Au-delà de ce taux, Sentinel génère des avertissements, mais continue à collecter des données.
   - **Expiration :** date d'expiration de la licence. Vous devez indiquer une clé de licence valide avant la date d'expiration afin d'éviter toute interruption de la fonctionnalité.
5. Cliquez sur **Enregistrer**.

Ajout d'une clé de licence par l'intermédiaire de la ligne de commande

Si vous utilisez l'installation traditionnelle de Sentinel, vous pouvez ajouter la licence par le biais de la ligne de commande à l'aide du script `softwarekey.sh`.

1. Connectez-vous au serveur Sentinel en tant qu'utilisateur root.
2. Placez-vous dans le répertoire `/opt/novell/sentinel/bin`.
3. Entrez la commande suivante pour prendre l'identité de l'utilisateur Novell :

   ```
   su novell
   ```
4. Entrez la commande suivante pour exécuter le script `softwarekey.sh`.

   ```
   ./softwarekey.sh
   ```
5. Entrez **1** pour insérer la clé de licence.
6. Spécifiez la clé de licence, puis appuyez sur **Entrée**.

IX Mise à niveau d'Identity Manager

Cette section fournit des informations pour la mise à niveau des composants Identity Manager.

25 Préparation à la mise à niveau d'Identity Manager

Cette section fournit des informations pour vous aider à préparer la mise à niveau de votre solution Identity Manager vers la version la plus récente. Vous pouvez mettre à niveau la plupart des composants Identity Manager à l'aide d'un fichier exécutable, d'un fichier binaire ou en mode texte, en fonction de l'ordinateur cible. Pour effectuer la mise à niveau, vous devez télécharger et dézipper ou décompresser le kit d'installation d'Identity Manager.

25.1 Liste de contrôle pour la mise à niveau d'Identity Manager

Pour effectuer la mise à niveau, NetIQ vous recommande d'exécuter les différentes étapes de la liste de contrôle ci-après.

	Éléments de la liste de contrôle
❑	1. Comprenez le processus de mise à niveau. Pour plus d'informations, reportez-vous au Section 25.2, « Présentation du processus de mise à niveau », page 253.
❑	2. Passez en revue les chemins pris en charge pour la mise à niveau d'Identity Manager vers la version 4.7. Pour plus d'informations sur les chemins de mise à niveau pris en charge, reportez-vous à la Section 25.3, « Chemins de mise à niveau pris en charge », page 253.
❑	3. Assurez-vous que vous disposez du kit d'installation pour mettre à niveau Identity Manager.
❑	4. Renseignez-vous sur les interactions entre les différents composants Identity Manager. Pour plus d'informations, reportez-vous au Partie I, « Introduction », page 15.
❑	5. Assurez-vous que votre ordinateur dispose des prérequis logiciels et matériels pour une version plus récente d'Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 5.9, « Préparation de l'installation », page 43 et aux notes de publication de la version vers laquelle vous voulez effectuer la mise à niveau.
❑	6. Sauvegardez le projet actuel, la configuration du pilote, ainsi que les bases de données. Pour plus d'informations, reportez-vous à la Section 25.4, « Sauvegarde de la configuration actuelle », page 258.
❑	7. Effectuez la mise à niveau vers la version la plus récente de Designer. Pour plus d'informations, reportez-vous à la Section 26.2, « Mise à niveau de Designer », page 261.
❑	8. Effectuez la mise à niveau de Sentinel Log Management for IGA vers la dernière version. Pour plus d'informations, reportez-vous au Section 26.6.3, « Mise à niveau de Sentinel Log Management for IGA », page 279.

	Éléments de la liste de contrôle
❑	9. Sur le serveur exécutant Identity Manager, effectuez la mise à niveau du coffre-fort d'identité (eDirectory) vers la version 9.1. Il s'agit de la première étape du processus de mise à niveau du moteur Identity Manager. Pour plus d'informations, reportez-vous à la Section 26.3.1, « Mise à niveau du coffre-fort d'identité », page 262. La mise à niveau d'eDirectory arrête ndsd qui, à son tour, stoppe tous les pilotes. Pour plus d'informations, reportez-vous au *Guide d'installation de NetIQ eDirectory*.
❑	10. Arrêtez les pilotes associés au serveur sur lequel vous avez installé le moteur Identity Manager. Pour plus d'informations, reportez-vous au Section 23.1.1, « Arrêt des pilotes », page 241.
❑	11. Mettez à niveau le moteur Identity Manager. Pour plus d'informations, reportez-vous à la Section 26.3, « Mise à niveau du moteur Identity Manager », page 262. **REMARQUE :** si vous migrez le moteur Identity Manager vers un nouveau serveur, vous pouvez utiliser les mêmes répliques eDirectory que celles figurant sur le serveur Identity Manager actuel. Pour plus d'informations, reportez-vous à la Section 29.4, « Migration du moteur Identity Manager vers un nouveau serveur », page 297.
❑	12. (Conditionnel) Si l'un des pilotes de l'ensemble de pilotes du moteur Identity Manager est un pilote de chargeur distant, mettez à niveau les serveurs de chargeur distant pour chaque pilote. Pour plus d'informations, reportez-vous à la Section 26.3.3, « Mise à niveau du chargeur distant », page 263.
❑	13. Effectuez la mise à niveau d'iManager vers la version 3.1. Pour plus d'informations, reportez-vous à la Section 26.3.4, « Mise à niveau d'iManager », page 264.
❑	14. Mettez à jour les plug-ins iManager en fonction de la version d'iManager. Pour plus d'informations, reportez-vous au « Mise à jour des plug-ins iManager après une mise à niveau ou une réinstallation » page 266.
❑	15. (Conditionnel) Si vous utilisez des paquetages, mettez à niveau les paquetages sur les pilotes existants afin d'obtenir de nouvelles stratégies. Pour plus d'informations, reportez-vous à la Section 26.4, « Mise à niveau des pilotes Identity Manager », page 266. Cette action n'est requise que si une version plus récente d'un paquetage est disponible et qu'une nouvelle fonction est incluse dans les stratégies d'un pilote que vous souhaitez ajouter à votre ensemble de pilotes existant.
❑	16. Mettez à niveau les applications d'identité. Pour plus d'informations, reportez-vous au Section 26.5, « Mise à niveau des applications d'identité », page 268.
❑	17. Mettez à niveau Identity Reporting. Pour plus d'informations, reportez-vous au Section 26.6, « Mise à niveau d'Identity Reporting », page 278.
❑	18. Démarrez les pilotes associés aux applications d'identité et le moteur Identity Manager. Pour plus d'informations, reportez-vous à la Section 23.1.2, « Lancement des pilotes », page 242.
❑	19. (Conditionnel) Si vous avez déplacé le moteur Identity Manager ou les applications d'identité sur un nouveau serveur, ajoutez le nouveau serveur à l'ensemble de pilotes. Pour plus d'informations, reportez-vous au Section 26.8, « Ajout de nouveaux serveurs à l'ensemble de pilotes », page 282.
❑	20. (Conditionnel) Si vous disposez de stratégies et de règles personnalisées, restaurez vos paramètres personnalisés. Pour plus d'informations, reportez-vous au Section 26.9, « Restauration de stratégies et de règles personnalisées sur le pilote », page 284.
❑	21. Mise à niveau d'Analyzer. Pour plus d'informations, reportez-vous au Section 26.7, « Mise à niveau d'Analyzer », page 282.

	Éléments de la liste de contrôle
❑	22. Activez votre solution Identity Manager mise à niveau. Pour plus d'informations, reportez-vous à la Section 24, « Activation d'Identity Manager », page 245.

25.2 Présentation du processus de mise à niveau

Lorsque vous souhaitez installer une version plus récente d'une installation Identity Manager existante, vous effectuez généralement une **mise à niveau**. Si la nouvelle version d'Identity Manager ne fournit pas de chemin de mise à niveau pour vos données existantes, vous devez toutefois effectuer une migration. NetIQ définit la **migration** comme processus consistant à installer Identity Manager sur un nouveau serveur, puis à migrer les données existantes vers ce nouveau serveur.

Au cours de la période d'évaluation du produit ou après l'activation de l'édition avancée, vous souhaiterez peut-être **passer** à l'édition standard, si vous ne voulez pas utiliser les fonctionnalités de la version avancée dans votre environnement. Identity Manager vous permet de passer de l'édition avancée à l'édition standard en suivant une procédure simple.

Passage de l'édition avancée à l'édition standard

Identity Manager vous permet de passer de l'édition avancée à l'édition standard au cours de la période d'évaluation du produit, ou après avoir activé l'édition avancée.

IMPORTANT : si vous avez déjà activé l'édition avancée, il est inutile de passer à l'édition standard dans la mesure où toutes les fonctionnalités de l'édition standard sont disponible dans l'édition avancée. Vous ne devez basculer vers l'édition standard que si vous ne souhaitez pas utiliser les fonctionnalités de la version avancée dans votre environnement et souhaitez réduire votre déploiement Identity Manager. Pour plus d'informations, reportez-vous à la section « Passage de l'édition avancée à l'édition standard » page 287.

25.3 Chemins de mise à niveau pris en charge

Identity Manager 4.7 prend en charge la mise à niveau à partir des versions 4.6.x et 4.5.6. Avant d'entamer la mise à niveau, NetIQ vous recommande de passer en revue les informations des notes de version correspondant à votre version actuelle.

- Section 25.3.1, « Mise à niveau à partir des versions 4.6.x d'Identity Manager », page 253
- Section 25.3.2, « Mise à niveau à partir des versions 4.5.x d'Identity Manager », page 255

25.3.1 Mise à niveau à partir des versions 4.6.x d'Identity Manager

Le tableau suivant répertorie les chemins de mise à niveau relatifs aux composants pour les versions 4.6.x d'Identity Manager :

Composant	Version de base	Version mise à jour
Moteur Identity Manager	4.6.x	1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Mettez à niveau le coffre-fort d'identité vers la version 9.1. 3. Mettez à niveau le moteur Identity Manager vers la version 4.7.
Chargeur distant/Agent de dissémination (fan-out)	4.6.x	Installez la version 4.7 du chargeur distant/ de l'agent de dissémination (fan-out).
Designer	4.6.x	1. Installez Designer 4.7. 2. Convertissez votre espace de travail de NCP vers LDAP. Designer 4.7 est basé sur LDAP. Avant d'utiliser cette version, reportez-vous aux *Notes de version de NetIQ Identity Manager LDAP Designer*.
Applications d'identité	4.6.x	Avant de mettre à niveau les applications d'identité, assurez-vous que le coffre-fort d'identité et le moteur Identity Manager sont respectivement mis à niveau vers la version 9.1 et 4.7. 1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Mettez à niveau la base de données vers une version prise en charge. Pour les versions de la base de données prises en charge, reportez-vous à la Section 8.5.3, « Configuration système requise pour les applications d'identité », page 83. 3. (Conditionnel) Si SSPR est installé sur un serveur distinct, mettez à niveau le composant vers la version 4.7. 4. Mettez à jour les paquetages de pilote d'application utilisateur et de pilote de rôles et de ressources. 5. Mettez à niveau les applications d'identité vers la version 4.7. 6. Arrêtez Tomcat.

Composant	Version de base	Version mise à jour
Identity Reporting	4.6.x	1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Mettez à niveau la base de données vers une version prise en charge. Pour plus d'informations sur les versions de base de données prises en charge, reportez-vous à la Section 8.6.4, « Configuration système requise pour Identity Reporting », page 88. 3. Mettez à niveau SLM for IGA vers une version prise en charge. 4. Mettez à jour les paquetages de pilote de passerelle de services gérés et des services de collecte de données. 5. Effectuez la mise à niveau d'Identity Reporting 4.7. 6. (Conditionnel) Créez une stratégie de synchronisation des données à partir de la page Services de collecte de données d'Identity Manager.

Avant d'entamer la mise à niveau, NetIQ vous recommande de passer en revue les informations des notes de version relatives à votre version :

- Notes de version de NetIQ Identity Manager 4.6 Service Pack 2
- Notes de version de NetIQ Identity Manager 4.6 Service Pack 1
- Notes de version de NetIQ Identity Manager 4.6

25.3.2 Mise à niveau à partir des versions 4.5.x d'Identity Manager

Le tableau suivant répertorie les chemins de mise à niveau relatifs aux composants pour les versions 4.5.x d'Identity Manager :

Composant	Version de base	Étape intermédiaire	Version mise à jour
Moteur Identity Manager	Identity Manager 4.5.x (où x est compris entre 0 et 5) avec eDirectory 8.8.8.x (où x est compris entre 3 et 9)	Appliquez le correctif 4.5.6.	1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Mettez à niveau le coffre-fort d'identité vers la version 9.1. 3. Mettez à niveau le moteur Identity Manager vers la version 4.7.
Chargeur distant/ Agent de dissémination (fan-out)	4.5.x, où x est compris entre 0 et 5	Appliquez le correctif 4.5.6.	Installez la version 4.7 du chargeur distant/de l'agent de dissémination (fan-out).

Composant	Version de base	Étape intermédiaire	Version mise à jour
Designer	4.5.x, où x est compris entre 0 et 5	Appliquez le correctif 4.5.6.	1. Installez Designer 4.7. 2. Convertissez votre espace de travail de NCP vers LDAP. Designer 4.7 est basé sur LDAP. Avant d'utiliser cette version, reportez-vous aux *Notes de version de NetIQ Identity Manager LDAP Designer*.
Applications d'identité	4.5.x, où x est compris entre 0 et 5	◆ Si vous utilisez JBoss ou Websphere, migrez vers le serveur d'applications de Tomcat. ◆ Appliquez le correctif 4.5.6.	Avant de mettre à niveau les applications d'identité, assurez-vous que le coffre-fort d'identité et le moteur Identity Manager sont respectivement mis à niveau vers la version 9.1 et 4.7. 1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Mettez à jour les paquetages de pilote d'application utilisateur et de pilote de rôles et de ressources. 3. Mettez à niveau la base de données vers une version prise en charge. Pour les versions de la base de données prises en charge, reportez-vous à la Section 8.5.3, « Configuration système requise pour les applications d'identité », page 83. 4. (Conditionnel) Si SSPR est installé sur un serveur distinct, mettez à niveau le composant vers la version 4.7. 5. Mettez à niveau les applications d'identité vers la version 4.7. 6. Arrêtez Tomcat.

Composant	Version de base	Étape intermédiaire	Version mise à jour
Identity Reporting	4.5.x, où x est compris entre 0 et 5	◆ Si vous utilisez JBoss ou Websphere, migrez vers le serveur d'applications de Tomcat. ◆ Appliquez le correctif 4.5.6.	1. Mettez à niveau le système d'exploitation vers une version prise en charge. 2. Mettez à niveau la base de données vers une version prise en charge. Pour plus d'informations sur les versions de base de données prises en charge, reportez-vous à la Section 8.6.4, « Configuration système requise pour Identity Reporting », page 88. 3. Migrez les données du service d'audit des événements vers une version prise en charge d'une base de données PostgreSQL ou Oracle. 4. Installez SLM for IGA. 5. Mettez à jour les paquetages de pilote de passerelle de services gérés et des services de collecte de données. 6. Migrez Identity Reporting vers la version 4.7. Pour plus d'informations, reportez-vous à la Section 29.8, « Migration d'Identity Reporting », page 301. 7. (Conditionnel) Créez une stratégie de synchronisation des données à partir de la page Services de collecte de données d'Identity Manager.

Avant d'entamer la mise à niveau, NetIQ vous recommande de passer en revue les informations des notes de version relatives à votre version :

- Notes de version de NetIQ Identity Manager 4.5 Service Pack 6
- Notes de version de NetIQ Identity Manager 4.5 Service Pack 5
- Notes de version de NetIQ Identity Manager 4.5 Service Pack 4
- Notes de version de NetIQ Identity Manager 4.5 Service Pack 3
- Notes de version de NetIQ Identity Manager 4.5 Service Pack 2
- Notes de version de NetIQ Identity Manager 4.5 Service Pack 1
- Notes de version de NetIQ Identity Manager 4.5

25.4 Sauvegarde de la configuration actuelle

Avant la mise à niveau, NetIQ recommande de sauvegarder la configuration actuelle de votre solution Identity Manager. Aucune autre étape n'est requise pour sauvegarder l'application utilisateur. Toute la configuration de l'application utilisateur est stockée dans le pilote de cette application. Pour créer la sauvegarde, vous pouvez procéder de plusieurs façons :

- Section 25.4.1, « Exportation du projet Designer », page 258
- Section 25.4.2, « Exportation de la configuration des pilotes », page 259

25.4.1 Exportation du projet Designer

Un projet Designer contient le schéma ainsi que toutes les informations de configuration de pilote. La création d'un projet de votre solution Identity Manager vous permet d'exporter tous les pilotes en une seule fois plutôt que de créer un fichier d'exportation distinct pour chaque pilote.

- « Exportation du projet actuel » page 258
- « Création d'un nouveau projet à partir du coffre-fort d'identité » page 258

Exportation du projet actuel

Si vous avez déjà un projet Designer, vérifiez que les informations contenues dans ce projet sont synchronisées avec celles contenues dans le coffre-fort d'identité.

1. Dans Designer, ouvrez votre projet.
2. Dans Modeler, cliquez avec le bouton droit sur le coffre-fort d'identité, puis sélectionnez **Activité en direct > Comparer**.
3. Évaluez le projet et actualisez toutes les différences, puis cliquez sur **OK**.

   Pour plus d'informations, reportez-vous à la section « Using the Compare Feature When Deploying » (Utilisation de la fonction de comparaison lors du déploiement) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer for Identity Manager).
4. Dans la barre d'outils, sélectionnez **Projet > Exporter**.
5. Cliquez sur **Sélectionner tout** pour sélectionner toutes les ressources à exporter.
6. Sélectionnez l'emplacement où vous voulez sauvegarder le projet et son format, puis cliquez sur **Terminer**.

   Sauvegardez le projet à n'importe quel emplacement, sauf sur l'espace de travail actuel. Lorsque vous effectuez une mise à niveau vers Designer, vous devez créer un nouvel emplacement d'espace de travail. Pour plus d'informations, reportez-vous à la section « Exporting a Project » (Exportation d'un projet) du manuel NetIQ Designer for Identity Manager Administration Guide (Guide d'administration de NetIQ Designer pour Identity Manager).

Création d'un nouveau projet à partir du coffre-fort d'identité

Si vous ne disposez pas d'un projet Designer de votre solution Identity Manager actuelle, vous devez en créer un afin de sauvegarder votre solution actuelle.

1. Installez Designer.
2. Lancez Designer, puis déterminez un emplacement pour votre espace de travail.
3. Sélectionnez s'il faut rechercher des mises à niveau en ligne, puis cliquez sur **OK**.

4 Sur la page de bienvenue, cliquez sur **Lancer Designer**.

5 Dans la barre d'outils, sélectionnez **Projet > Importer un projet > Coffre-fort d'identité**.

6 Indiquez un nom pour le projet, puis sélectionnez soit l'emplacement par défaut pour votre projet, soit un emplacement différent que vous définirez.

7 Cliquez sur **Suivant**.

8 Indiquez les valeurs suivantes pour la connexion au coffre-fort d'identité :

- **Nom d'hôte**, qui correspond à l'adresse IP ou au nom DNS du serveur de coffre-fort d'identité
- **Nom d'utilisateur**, qui correspond au DN de l'utilisateur employé pour l'authentification auprès du coffre-fort d'identité
- **Mot de passe**, qui correspond au mot de passe de l'utilisateur d'authentification

9 Cliquez sur **Suivant**.

10 Laissez le schéma de coffre-fort d'identité et la collection de notification par défaut cochés.

11 Développez la collection de notification par défaut et décochez les langues dont vous n'avez pas besoin.

Les collections de notification par défaut sont traduites vers beaucoup de langues différentes. Vous pouvez importer toutes les langues ou sélectionner seulement celles que vous utilisez.

12 Cliquez sur **Parcourir**, puis naviguez jusqu'à un ensemble de pilotes à importer et sélectionnez-le.

13 Répétez l'Étape 12 pour chaque ensemble de pilotes dans ce coffre-fort d'identité, puis cliquez sur **Terminer**.

14 Une fois l'importation du projet terminée, cliquez sur **OK**.

15 Si vous n'avez qu'un seul coffre-fort d'identité, vous avez terminé. Si vous avez plusieurs coffres-forts d'identité, passez à l'Étape 16.

16 Dans la barre d'outils, cliquez sur **Activité en direct > Importer**.

17 Répétez la procédure de l'Étape 8 à l'Étape 14 pour chaque coffre-fort d'identité supplémentaire.

25.4.2 Exportation de la configuration des pilotes

La création d'une exportation des pilotes réalise une sauvegarde de votre configuration actuelle. Toutefois, Designer ne crée actuellement pas de sauvegarde des pilotes de droits basés sur les rôles et les stratégies. Utilisez iManager pour vérifier l'exportation du pilote de droits basés sur les rôles.

- « Utilisation de Designer pour exporter les configurations de pilote » page 259
- « Utilisation d'iManager pour créer une exportation du pilote » page 260

Utilisation de Designer pour exporter les configurations de pilote

1 Vérifiez que votre projet dans Designer dispose de la dernière version en date de votre pilote. Pour plus d'informations, reportez-vous à la section « Importing a Library, a Driver Set, or a Driver from the Identity Vault » (Importation d'une bibliothèque, d'un ensemble de pilotes ou d'un pilote depuis le coffre-fort d'identité) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).

2 Dans le modélisateur, cliquez avec le bouton droit sur la ligne du pilote que vous mettez à niveau.

3 Sélectionnez **Exporter dans un fichier de configuration**.

4 Naviguez jusqu'à l'emplacement dans lequel enregistrer le fichier de configuration, puis cliquez sur **Enregistrer**.

5 Cliquez sur **OK** sur la page des résultats.

6 Répétez la procédure de l'Étape 1 à l'Étape 5 pour chaque pilote.

Utilisation d'iManager pour créer une exportation du pilote

1 Dans iManager, sélectionnez **Identity Manager > Présentation d'Identity Manager**.

2 Recherchez et sélectionnez l'emplacement de l'arborescence où rechercher les objets Ensemble de pilotes, puis cliquez sur l'icône de recherche  .

3 Cliquez sur l'objet Ensemble des pilotes contenant le pilote à mettre à niveau.

4 Cliquez sur le pilote à mettre à niveau, puis cliquez sur **Exporter**.

5 Cliquez sur **Suivant**, puis choisissez **Exporter toutes les stratégies contenues, qu'elles soient liées ou non à la configuration**.

6 Cliquez sur **Suivant**, puis sur **Enregistrer sous**.

7 Sélectionnez **Enregistrer sur le disque**, puis cliquez sur **OK**.

8 Cliquez sur **Terminer**.

9 Répétez la procédure de l'Étape 1 à l'Étape 8 pour chaque pilote.

26 Mise à niveau des composants Identity Manager

Cette section fournit des informations spécifiques pour la mise à niveau de certains composants Identity Manager. Cette section décrit également des procédures susceptibles d'être nécessaires après une mise à niveau.

26.1 Séquence de mise à niveau

Vous devez mettre à niveau les composants Identity Manager dans l'ordre suivant :

1. Designer
2. Sentinel Log Management for IGA
3. Coffre-fort d'identité
4. Moteur Identity Manager
5. Chargeur distant
6. Agent Fan-out
7. iManager
8. Applications d'identité (pour l'édition avancée)
9. Identity Reporting
10. Analyzer

REMARQUE : vous ne pouvez mettre à niveau qu'un seul composant à la fois.

26.2 Mise à niveau de Designer

1 Connectez-vous en tant qu'administrateur au serveur sur lequel Designer est installé.

2 Pour créer une copie de sauvegarde de vos projets, exportez-les.

Pour plus d'informations sur l'exportation, reportez-vous à la section « Exporting a Project » (Exportation d'un projet) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).

3 Lancez le programme d'installation de Designer. Pour plus d'informations, reportez-vous à la Chapitre 13, « Installation de Designer », page 185.

Après la mise à niveau vers la version actuelle de Designer, vous devez importer tous les projets de l'ancienne version. Lorsque vous lancez le processus d'importation, Designer exécute l'assistant Convertisseur de projet qui convertit les anciens projets dans la version actuelle. Dans l'assistant, sélectionnez **Copier le projet dans l'espace de travail**. Pour plus d'informations sur le convertisseur de projet, reportez-vous au manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).

26.3 Mise à niveau du moteur Identity Manager

Veillez à effectuer la mise à niveau du coffre-fort d'identité avant de mettre à niveau le moteur Identity Manager. La procédure de mise à niveau du moteur Identity Manager met à jour les fichiers du module d'interface du pilote stockés dans le système de fichiers sur l'ordinateur hôte.

26.3.1 Mise à niveau du coffre-fort d'identité

1 Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` comme indiqué dans la Section 5.11, « Téléchargement des fichiers d'installation », page 49.

2 Montez le fichier `.iso` téléchargé.

3 À partir du répertoire racine du fichier `.iso`, accédez au répertoire `IDVault/setup`.

4 Exécutez la commande suivante :

```
./nds-install
```

5 Acceptez l'accord de licence et poursuivez l'installation.

6 Spécifiez la valeur **adminDN**. Par exemple : `cn=admin.ou=sa.o=system`.

7 Spécifiez y à l'invite pour arrêter les instances d'eDirectory et mettre à niveau NICI.

8 Indiquez si vous voulez configurer **l'authentification EBA**.

REMARQUE : si la mise à niveau de la DIB échoue et que `nds-install` vous demande d'y procéder, exécutez `ndsconfig` après `nds-install`. Si les services eDirectory ne démarrent pas après une mise à niveau, exécutez la commande ndsconfig upgrade. Pour plus d'informations, reportez-vous au Guide d'installation de NetIQ eDirectory.

26.3.2 Mise à niveau du moteur Identity Manager

Vérifiez que les pilotes sont bien arrêtés. Pour plus d'informations, reportez-vous à la Section 23.1.1, « Arrêt des pilotes », page 241.

Assurez-vous que le fichier de cache ne contient aucun événement avant de commencer le processus de mise à niveau. Lorsque vous mettez à niveau le moteur Identity Manager vers la version 4.7, le programme d'installation du moteur nettoie les fichiers de cache de travail du pilote

MapDB (dx *) existants. Toutefois, vous devez supprimer manuellement les fichiers de cache de l'état MapDB existants après la mise à niveau du pilote. Dans le cas contraire, le pilote peut ne pas démarrer. Les pilotes Identity Manager suivants utilisent MapDB 3.0.5 :

- MS Azure
- JDBC
- DCS
- MSGW
- LDAP
- Salesforce
- ServiceNow

Procédez comme suit pour mettre à niveau le moteur Identity manager :

1. Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.
2. Montez le fichier `.iso` téléchargé.
3. Exécutez la commande suivante :

   ```
   ./install.sh
   ```
4. Lisez le contrat de licence.
5. Entrez `o` pour accepter l'accord de licence.
6. Indiquez si vous souhaitez mettre à niveau les composants Identity Manager. Les options disponibles sont **`y`** (oui) et **`n`** (non).
7. Sélectionnez le moteur Identity Manager.
8. Spécifiez les informations suivantes :

   Administrateur du coffre-fort d'identité: Indiquez le nom de l'administrateur du coffre-fort d'identité.

   Mot de passe de l'administrateur du coffre-fort d'identité: Indiquez le mot de passe de l'administrateur du coffre-fort d'identité.

26.3.3 Mise à niveau du chargeur distant

Si vous exécutez le chargeur distant, vous devez mettre à niveau ses fichiers.

1. Créez une sauvegarde des fichiers de configuration du chargeur distant.
2. Vérifiez que les pilotes sont bien arrêtés. Pour connaître les instructions, reportez-vous à la Section 23.1.1, « Arrêt des pilotes », page 241.
3. Arrêtez le service ou le daemon du chargeur distant pour chaque pilote.
   - **Chargeur distant :** `rdxml -config` *`chemin_vers_fichier_config`* `-u`
   - **Chargeur distant Java :** `dirxml_jremote -config` *`chemin_vers_fichier_config`* `-u`
4. Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.
5. Montez le fichier `.iso` téléchargé.
6. Exécutez la commande suivante :

   ```
   ./install.sh
   ```
7. Lisez le contrat de licence.

8 Entrez o pour accepter l'accord de licence.

9 Indiquez si vous souhaitez mettre à niveau les composants Identity Manager. Les options disponibles sont **y** (oui) et **n** (non).

10 Sélectionnez le chargeur distant.

11 Une fois l'installation terminée, vérifiez que vos fichiers de configuration contiennent bien les informations de votre environnement.

12 (Conditionnel) Si vous rencontrez un problème lié au fichier de configuration, copiez le fichier de sauvegarde créé à l'étape 1. Sinon, passez à l'étape suivante.

13 Lancez le service ou le daemon du chargeur distant pour chaque pilote.

- **Chargeur distant** : `rdxml -config` *`chemin_fichier_configuration`*
- **Chargeur distant Java** : `dirxml_jremote -config` *`chemin_accès_fichier_configuration`*

26.3.4 Mise à niveau d'iManager

En général, la procédure de mise à niveau pour iManager utilise les valeurs de configuration figurant dans le fichier `configiman.properties`, telles que les valeurs de port et les utilisateurs autorisés. Avant la mise à niveau, NetIQ vous recommande de sauvegarder les fichiers de configuration `server.xml` et `context.xml` si vous les avez modifiés.

Avant de mettre à niveau iManager vers la version 3.1, vérifiez que votre version d'eDirectory a été mise à niveau vers 9.1.

La procédure de mise à niveau inclut les tâches suivantes :

- « Mise à niveau d'iManager » page 264
- « Mise à jour des services basés sur le rôle » page 265
- « Réinstallation ou migration des plug-ins pour Plug-in Studio » page 265
- « Mise à jour des plug-ins iManager après une mise à niveau ou une réinstallation » page 266

Mise à niveau d'iManager

Avant la mise à niveau d'iManager, assurez-vous que l'ordinateur répond aux conditions préalables et à la configuration système requise.

REMARQUE : la procédure de mise à niveau utilise les valeurs de port HTTP et de port SSL configurées dans la version précédente d'iManager.

---

1 Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` comme indiqué dans la Section 5.11, « Téléchargement des fichiers d'installation », page 49.

2 Montez le fichier `.iso` téléchargé.

3 Exécutez la commande suivante :

```
./install.sh
```

4 Lisez le contrat de licence.

5 Entrez o pour accepter l'accord de licence.

6 Spécifiez iManager pour poursuivre la mise à niveau.

Mise à jour des services basés sur le rôle

La première fois que vous utilisez iManager pour vous connecter à une arborescence eDirectory qui contient déjà une collection de services basés sur les rôles (RBS), vous risquez de ne pas voir toutes les informations sur les rôles. Ce comportement est normal car vous devez mettre à jour certains plug-ins pour qu'ils fonctionnent avec la dernière version d'iManager. NetIQ vous recommande de mettre à jour vos modules RBS vers la dernière version pour pouvoir voir et utiliser toutes les fonctionnalités disponibles d'iManager. Le tableau de configuration RBS liste les modules RBS qui doivent être mis à jour.

N'oubliez pas que vous pouvez avoir plusieurs rôles portant le même nom. À partir de la version iManager 2.5, certains développeurs de plug-ins ont modifié des ID de tâche ou des noms de module tout en conservant le même nom d'affichage. En conséquence, les rôles semblent dupliqués alors qu'en réalité, une instance concerne une version et l'autre, une version plus récente.

REMARQUE

- Lors de la mise à jour ou de la réinstallation d'iManager, le programme d'installation ne met pas à jour les plug-ins existants. Pour mettre à jour les plug-ins manuellement, lancez iManager et accédez à **Configurer** > **Installation de plug-ins** > **Modules de plug-in Novell disponibles**.
- En fonction de l'installation d'iManager, le nombre de plug-ins installés localement peut être différent. Par conséquent, il se peut que vous constatiez des différences dans le rapport de module pour une collection donnée de la page **Services basés sur le rôle** > **Configuration RBS**. Pour que les nombres coïncident entre les différentes installations d'iManager, assurez-vous d'installer le même sous-ensemble de plug-ins sur chaque instance d'iManager dans l'arborescence.

Pour trouver les objets RBS périmés et les mettre à jour :

1. Loguez-vous à iManager.
2. Dans la vue Configurer, cliquez sur **Services basés sur le rôle > Configuration RBS**.

   Consultez le tableau de la page à onglets Collections 2.*x* pour les modules périmés.
3. (Facultatif) Pour mettre à jour un module, procédez comme suit :
   - **3a** Pour la collection à mettre à jour, sélectionnez le numéro dans la colonne **Périmé**.

     iManager affiche la liste des modules périmés.
   - **3b** Sélectionnez le module à mettre à jour.
   - **3c** Cliquez sur **M à jour** dans la partie supérieure du tableau.

Réinstallation ou migration des plug-ins pour Plug-in Studio

Vous pouvez migrer ou répliquer des plug-ins Plug-in Studio vers une autre instance d'iManager, ainsi que vers une nouvelle version d'iManager ou une version mise à jour.

1. Loguez-vous à iManager.
2. Dans la vue de configuration d'iManager, sélectionnez **Services basés sur le rôle > Plug-in Studio**.

   Le cadre de contenu affiche la liste des plug-ins personnalisés installés, ainsi que l'emplacement de la collection RBS à laquelle les plug-ins appartiennent.
3. Sélectionnez le plug-in à réinstaller ou migrer, puis cliquez sur **Éditer**.

REMARQUE : vous ne pouvez éditer qu'un plug-in à la fois.

4 Cliquez sur **Installer**.

5 Répétez cette procédure pour chaque plug-in à réinstaller ou à migrer.

Mise à jour des plug-ins iManager après une mise à niveau ou une réinstallation

Lorsque vous mettez à niveau ou réinstallez iManager, le programme d'installation ne met pas à jour les plug-ins existants. Assurez-vous que les plug-ins correspondent à la bonne version d'iManager.

1 Ouvrez iManager.

2 Accédez à **Configurer > Installation de plug-ins > Modules de plug-in Novell disponibles**.

3 Mettez à jour les plug-ins.

26.4 Mise à niveau des pilotes Identity Manager

NetIQ fournit du nouveau contenu de pilote par le biais de **paquetages**. Vous gérez, mettez à jour et créez des paquetages dans Designer. Bien qu'iManager soit axé sur des paquetages, Designer ne répercute pas les changements que vous apportez au contenu des pilotes dans iManager. Pour plus d'informations sur la gestion des paquetages, reportez-vous à la section « Managing Packages » (Gestion des paquetages) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).

Vous pouvez mettre à niveau vos pilotes vers des paquetages de l'une des manières suivantes :

- Section 26.4.1, « Création d'un nouveau pilote », page 266
- Section 26.4.2, « Remplacement du contenu existant par du contenu issu de paquetages », page 267
- Section 26.4.3, « Conservation du contenu actuel et ajout de nouveau contenu avec des paquetages », page 267

26.4.1 Création d'un nouveau pilote

La manière la plus simple et la plus propre de mettre à niveau un pilote vers un paquetage consiste à supprimer le pilote existant et à en créer un nouveau à l'aide d'un paquetage. Ajoutez toutes les fonctionnalités que vous souhaitez au nouveau pilote. La procédure est différente pour chaque pilote. Pour connaître la procédure, reportez-vous aux guides des différents pilotes sur le site Web de documentation des pilotes Identity Manager. Le pilote fonctionne à présent comme auparavant, mais son contenu est issu de paquetages et non plus d'un fichier de configuration.

26.4.2 Remplacement du contenu existant par du contenu issu de paquetages

Si vous devez conserver les associations créées par le pilote, vous ne devez pas supprimer ni recréer le pilote. Vous pouvez conserver les associations et remplacer le contenu de pilote par des paquetages.

Pour remplacer le contenu existant par le contenu des paquetages :

1. Créez une sauvegarde du pilote et de tout son contenu personnalisé.

   Pour obtenir des instructions, reportez-vous à la Section 25.4.2, « Exportation de la configuration des pilotes », page 259.

2. Dans Designer, supprimez tous les objets stockés dans le pilote. Supprimez les stratégies, les filtres, les droits et tous les autres éléments stockés dans le pilote.

   REMARQUE : Designer propose une fonction d'importation automatique pour importer les paquetages les plus récents. Vous ne devez pas importer manuellement les paquetages de pilotes dans le catalogue de paquetages.

   Pour plus d'informations, reportez-vous à la section « Importing Packages into the Package Catalog » (Importation de paquetages dans le catalogue de paquetages) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).

   ---

3. Installez les paquetages les plus récents sur le pilote.

   Ces étapes sont spécifiques à chaque pilote. Pour connaître la procédure, reportez-vous au guide de chaque pilote sur le site Web de documentation des pilotes Identity Manager.

4. Restaurez toutes les stratégies et règles personnalisées sur le pilote. Pour connaître la procédure, reportez-vous à la Section 26.9, « Restauration de stratégies et de règles personnalisées sur le pilote », page 284.

26.4.3 Conservation du contenu actuel et ajout de nouveau contenu avec des paquetages

Vous pouvez garder le pilote tel qu'il est actuellement et lui ajouter de nouvelles fonctionnalités par le biais de paquetages, pour autant que celles-ci n'empiètent pas sur la fonction actuelle du pilote.

Avant d'installer un paquetage, créez une sauvegarde du fichier de configuration du pilote. Lorsque vous installez un paquetage, il est possible qu'il écrase les stratégies existantes et empêche ainsi le pilote de fonctionner. Si une stratégie est écrasée, vous pouvez la recréer en important le fichier sauvegardé de configuration du pilote.

Avant de commencer, assurez-vous que les stratégies personnalisées disposent de noms différents de ceux des stratégies par défaut. Quand une configuration de pilote est déposée avec un nouveau fichier de pilote, les stratégies existantes sont écrasées. Si elles ne possèdent pas de nom unique, vos stratégies personnalisées seront perdues.

Pour ajouter du contenu nouveau au pilote à l'aide de paquetages :

1. Créez une sauvegarde du pilote et de tout son contenu personnalisé.

   Pour obtenir des instructions, reportez-vous à la Section 25.4.2, « Exportation de la configuration des pilotes », page 259.

REMARQUE : Designer propose une fonction d'importation automatique pour importer les paquetages les plus récents. Vous ne devez pas importer manuellement les paquetages de pilotes dans le catalogue de paquetages.

Pour plus d'informations, reportez-vous à la section « Importing Packages into the Package Catalog » (Importation de paquetages dans le catalogue de paquetages) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).

2 Installez les paquetages sur le pilote.

Pour connaître la procédure, consultez le guide de chaque pilote sur le site Web de documentation des pilotes Identity Manager.

3 Ajoutez les paquetages souhaités au pilote. Ces étapes sont spécifiques à chaque pilote.

Pour plus d'informations, reportez-vous au site Web de documentation des pilotes Identity Manager.

Le pilote contient la nouvelle fonctionnalité ajoutée par les paquetages.

26.5 Mise à niveau des applications d'identité

Cette section fournit des informations sur la mise à niveau des applications d'identité et des logiciels de support, ce qui inclut la mise à jour des composants suivants :

- Application utilisateur Identity Manager
- One SSO Provider (OSP)
- Self-Service Password Reset (SSPR)
- Tomcat, JDK et ActiveMQ
- Base de données PostgreSQL

Après la mise à niveau, les composants sont mis à niveau vers les versions suivantes :

- Tomcat – `8.5.27`
- ActiveMQ – `5.15.2`
- Java – `1.8.0_162`
- One SSO Provider – `6.2.1`
- Self-Service Password Reset – `4.2.0.4`

Cette section fournit des informations concernant les rubriques suivantes :

26.5.1 Présentation du programme de mise à niveau

La procédure de mise à niveau lit les valeurs de configuration à partir des composants existants. Ces informations incluent les fichiers `ism-configuration.properties`, `server.xml`, `SSPRConfiguration` ainsi que d'autres fichiers de configuration. À l'aide de ces fichiers de configuration, la procédure de mise à niveau appelle en interne le programme de mise à niveau des composants. Ce programme crée en outre une sauvegarde de l'installation actuelle.

26.5.2 Conditions préalables et considérations relatives à la mise à niveau

Avant d'effectuer une mise à niveau, passez en revue les considérations suivantes :

- **Identity Manager est mis à niveau vers la version 4.5.6 :** vous ne pouvez pas effectuer la mise à niveau ou la migration vers la version 4.7 à partir de versions antérieures à 4.5.6. Pour plus d'informations sur la mise à niveau vers Identity Manager 4.7, reportez-vous à la Section 25.3, « Chemins de mise à niveau pris en charge », page 253.
- **Configuration système requise:** La procédure de mise à niveau requiert au moins 3 Go d'espace disque pour stocker la configuration actuelle et les fichiers temporaires créés pendant la mise à niveau. Assurez-vous que votre serveur dispose de suffisamment d'espace pour stocker la sauvegarde et d'espace libre supplémentaire pour la mise à niveau.

  Si vous avez installé les applications d'identité sur une partition distincte de la partition racine, vérifiez que la partition dispose de suffisamment d'espace pour stocker la configuration de sauvegarde. En outre, assurez-vous que le répertoire `/tmp` comporte suffisamment d'espace pour stocker les journaux et les fichiers temporaires. Si ce répertoire ne dispose pas de l'espace requis, définissez la variable d'environnement `IATEMPDIR` sur un répertoire d'une partition qui dispose de suffisamment d'espace. Le programme de mise à niveau sera redirigé vers ce répertoire pour stocker les fichiers de ce répertoire.

  Pour définir `IATEMPDIR` sur un répertoire :

  1. Ouvrez un terminal et entrez la commande suivante :

     ```
     export IATEMPDIR=/opt/custom_tmp
     ```

     où `/opt/custom_tmp` est le chemin d'accès au répertoire qui dispose de suffisamment d'espace.

     REMARQUE : Sauvegardez les certificats des applications d'identité (`cacerts`).

     ---

  2. Démarrez le programme de mise à niveau à partir de la ligne de commande.
- **Tomcat en tant que serveur d'applications :** cette version d'Identity Manager prend uniquement en charge Tomcat en tant que serveur d'applications.

  Si vos applications d'identité sont en cours d'exécution sur un serveur d'applications autre que Tomcat, migrez le serveur d'applications vers Tomcat avant d'effectuer une mise à niveau. Pour plus d'informations, reportez-vous à la section Migration de Websphere ou JBoss vers Tomcat.
- **La plate-forme de base de données est mise à niveau :** ce programme ne met pas à niveau la plate-forme de base de données des applications d'identité. Mettez à niveau manuellement votre version actuelle de la base de données vers une version prise en charge. Pour mettre à niveau la base de données PostgreSQL, reportez-vous à la section Section 26.5.4, « Mise à niveau de la base de données PostgreSQL », page 270.

- **Le paquetage du pilote du service de rôles et ressources est mis à niveau :** pour plus d'informations, reportez-vous à la section Upgrading Installed Packages (Mise à niveau des paquetages installés) du *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).
- **Self Service Password Reset :** si vous effectuez la mise à niveau à partir de SSPR 4.0, assurez-vous d'avoir mis à jour la propriété `CATALINA_OPTS` et d'avoir défini `-Dsspr.application.Path` sur le dossier hébergeant votre configuration SSPR.

  Exemples :

  ```
  export CATALINA_OPTS="-Dsspr.applicationPath=/home/sspr_data
  ```

  Sauvegardez votre base de données LocalDB SSPR avant la mise à niveau. Pour exporter ou télécharger la base de données locale (LocalDB), effectuez les opérations suivantes :

  1. Connectez-vous au portail SSPR en tant qu'administrateur.
  2. Dans le menu déroulant situé dans le coin supérieur droit de la page, cliquez sur **Configuration Manager** (Gestionnaire de configuration).
  3. Cliquez sur **LocalDB**.
  4. Cliquez sur **Download LocalDB** (Télécharger la base de données locale).

26.5.3 Configuration système requise

La procédure de mise à niveau crée une sauvegarde de la configuration actuelle des composants installés. Assurez-vous que votre serveur dispose de suffisamment d'espace pour stocker la sauvegarde et d'espace libre supplémentaire pour la mise à niveau.

26.5.4 Mise à niveau de la base de données PostgreSQL

La procédure suivante doit être effectuée avant la mise à niveau de la base de données PostgreSQL.

1. Arrêtez le service PostgreSQL.

   ```
   su -s /bin/sh - postgres -c "/opt/netiq/idm/apps/postgres/bin/pg_ctl stop -w -D /opt/netiq/idm/apps/postgres/data"
   ```

2. Désactivez le fichier d'unité existant pour le service PostgreSQL.

   ```
   systemctl disable postgresql-9.6.service
   ```

3. Nettoyez le fichier d'unité existant pour le service PostgreSQL.

   ```
   rm /usr/lib/systemd/system/postgresql-9.6.service
   systemctl daemon-reload
   systemctl reset-failed
   ```

4. Créez un répertoire de sauvegarde et réalisez une sauvegarde du répertoire PostgreSQL existant.

   Par exemple :

   ```
   mkdir -p /home/backup
   cp -rvf /opt/netiq/idm/apps/postgres/ /home/backup/
   ```

5. Accédez à l'emplacement où vous avez monté le fichier `Identity_Manager_4.7_Linux.iso`.
6. Accédez au répertoire `/common/packages/postgres/`.
7. Installez la nouvelle version de PostgreSQL.

   ```
   rpm -ivh netiq-postgresql-9.6.6-0.noarch.rpm
   ```

REMARQUE : le répertoire privé de PostgreSQL est déplacé de l'emplacement d'installation personnalisé précédent vers `/opt/netiq/idm/postgres/`.

8 Créez un répertoire `data` à l'emplacement d'installation de PostgreSQL.

`mkdir -p <répertoire_privé_POSTGRES>/data`, où `<répertoire_privé_POSTGRES>` correspond à `/opt/netiq/idm/postgres`.

Par exemple :

```
mkdir -p /opt/netiq/idm/postgres/data
```

9 Changez les autorisations du répertoire de l'instance PostgreSQL qui vient d'être installée.

```
chown -R postgres:postgres <chemin_répertoire_postgres>
```

Par exemple :

```
chown -R postgres:postgres /opt/netiq/idm/postgres
```

10 Créez un répertoire privé pour l'utilisateur `postgres`.

Par exemple : `mkdir -p /home/users/postgres`

11 Changez les autorisations du répertoire privé pour l'utilisateur de l'instance PostgreSQL qui vient d'être installée.

```
chown -R postgres:postgres <chemin_répertoire_privé_postgres>
```

Par exemple :

```
chown -R postgres:postgres /home/users/postgres
```

12 Exportez le répertoire `privé` de PostgreSQL.

```
export PGHOME=<chemin_répertoire_privé_postgres>
```

Par exemple :

```
export PG_HOME=/opt/netiq/idm/postgres
```

13 Exportez le mot de passe PostgreSQL :

```
export PGPASSWORD=<entrer mot de passe base de données>
```

14 Initialisez la base de données.

```
su -s /bin/sh - postgres -c "LANG=en_US.UTF-8 <répertoire privé_POSTGRES>/bin/
initdb -D <répertoire privé_POSTGRES>/data"
```

Par exemple :

```
su -s /bin/sh - postgres -c "LANG=en_US.UTF-8 /opt/netiq/idm/postgres/bin/
initdb -D /opt/netiq/idm/postgres/data"
```

15 Remplacez le chemin du répertoire privé de l'utilisateur postgres par `/opt/netiq/idm/postgres/` dans le fichier `/etc/passwd`.

15a Accédez au répertoire `/etc/`.

15b Modifiez le fichier `passwd`.

```
vi /etc/passwd
```

15c Déplacez le répertoire privé de l'utilisateur postgres vers `/opt/netiq/idm/postgres/`.

16 Accédez au répertoire `/opt/netiq/idm/postgres/`.

17 Connectez-vous en tant qu'utilisateur `postgres`.

Par exemple :

```
su postgres
```

18 Migrez les données existantes.

Par exemple :

```
/opt/netiq/idm/postgres/bin/pg_upgrade --old-datadir /opt/netiq/idm/apps/
postgres/data/ --new-datadir /opt/netiq/idm/postgres/data/ --old-bindir /opt/
netiq/idm/apps/postgres/bin --new-bindir /opt/netiq/idm/postgres/bin/
```

19 Déconnectez-vous de la session d'utilisateur `postgres`.

20 Mettez à jour le fichier `pg_hba.conf` de manière à approuver le réseau du serveur :

20a Accédez au répertoire `/opt/netiq/idm/postgres/data/`.

20b Modifiez le fichier `pg_hba.conf` :

```
vi pg_hba.conf
```

20c Ajoutez la ligne suivante au fichier `pg_hba.conf` :

```
host all all 0.0.0.0/0 trust
```

21 Pour vous assurer que votre instance de PostgreSQL écoute sur les instances du réseau autres que `localhost`, mettez à jour le fichier de configuration :

21a Accédez au répertoire `/opt/netiq/idm/postgres/data/`.

21b Modifiez le fichier `postgresql.conf` :

```
vi postgresql.conf
```

21c Ajoutez la ligne suivante au fichier `postgresql.conf` :

```
listen_addresses = '*'
```

REMARQUE : Pour écouter sur certaines interfaces réseau, spécifiez une liste d'adresses IP séparées par des virgules.

---

22 Créez le répertoire `pg_log` sous `<chemin_répertoire_privé_postgres>/data`.

Par exemple :

```
mkdir -p /opt/netiq/idm/postgres/data/pg_log
```

23 Modifiez les autorisations pour le répertoire `pg_log`.

```
chown -R postgres:postgres <chemin_répertoire_postgres>/data/pg_log
```

Par exemple :

```
chown -R postgres:postgres /opt/netiq/idm/postgres/data/pg_log
```

24 Démarrez le service PostgreSQL.

```
systemctl start netiq-postgresql
```

Cela lancera le nouveau service PostgreSQL.

25 (Facultatif) Lancez la nouvelle application pgAdmin à partir de l'interface graphique :

25a Copiez le répertoire `scripts` de l'ancien répertoire privé `postgres` vers le nouveau répertoire privé `postgres`.

Par exemple :

```
cp -rvf /opt/netiq/idm/apps/postgres/scripts /opt/netiq/idm/postgres
```

25b Accédez au répertoire `/opt/netiq/idm/postgres/scripts`.

25c Modifiez le fichier `launchpgadmin.sh` et remplacez l'ancien chemin de PostgreSQL par le nouveau.

Remplacez `/opt/netiq/idm/apps/postgres/` avec `/opt/netiq/idm/postgres`.

25d Accédez au répertoire `/usr/share/application` et modifiez l'application `.desktop` pour fournir le nouveau chemin pour `launchpgadmin.sh`.

SLES : modifiez l'application `pgadmin-pg-9_6.desktop` et remplacez la valeur `EXEC` par le nouveau chemin du fichier `launchpgadmin.sh`.

Par exemple :

Remplacez la valeur de `"Exec=/opt/netiq/idm/apps/postgres/scripts/launchpgadmin.sh"` par :`"Exec=/opt/netiq/idm/postgres/scripts/launchpgadmin.sh"`.

RHEL : accédez à `/usr/share/application` et créez le fichier `pgadmin-pg-9_6.desktop` avec les détails suivants :

Par exemple :

```
[Desktop Entry]
Version=1.0
Encoding=UTF-8
Name=pgAdmin 4
Exec=/opt/netiq/idm/postgres/scripts/launchpgadmin.sh
Icon=pg-pgadmin-9_6.png
Terminal=false
Type=Application
```

25e Supprimez l'ancien répertoire privé postgres du système.

```
rm -rf /opt/netiq/idm/apps/postgres/
```

25f Redémarrez le système pour que les modifications prennent effet.

26.5.5 Mise à niveau des paquetages de pilotes pour les applications d'identité

Cette section explique comment mettre à jour les paquetages pour le pilote d'application utilisateur et les pilotes du service Rôles et ressource vers la dernière version. Vous devez effectuer cette tâche avant de mettre à niveau les applications d'identité.

1. Dans Designer, ouvrez votre projet en cours.
2. Cliquez avec le bouton droit sur **Catalogue de paquetages > Importer le paquetage**.
3. Sélectionnez le paquetage approprié. Par exemple, **paquetage de base du pilote de l'application utilisateur**.
4. Cliquez sur **OK**.
5. Dans la vue Développeur, cliquez avec le bouton droit sur le pilote, puis cliquez sur **Propriétés**.
6. Accédez à l'onglet **Paquetages** sur la page **Propriétés**.
7. Cliquez sur le symbole d'**ajout de paquetage (+)** dans le coin supérieur droit.
8. Sélectionnez le paquetage, puis cliquez sur **OK**.
9. Répétez la même procédure pour mettre à niveau le paquetage pour le pilote du service Rôles et ressource.

REMARQUE : assurez-vous que le pilote d'application utilisateur et le pilote du service Rôles et ressource sont connectés à la version mise à niveau d'Identity Manager.

26.5.6 Mise à niveau des applications d'identité

REMARQUE : si vos applications d'identité et SSPR sont installés sur des serveurs différents, vous devez mettre à niveau SSPR manuellement. Pour plus d'informations, reportez-vous à la « Mise à niveau de SSPR » page 274.

Mise à niveau des applications d'identité

La procédure suivante décrit comment mettre à niveau les applications d'identité.

1. Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.
2. Montez le fichier `.iso` téléchargé.
3. Exécutez la commande suivante :

   ```
   ./install.sh
   ```
4. Lisez le contrat de licence.
5. Entrez o pour accepter l'accord de licence.
6. Indiquez si vous souhaitez mettre à niveau les composants Identity Manager. Les options disponibles sont **y** (oui) et **n** (non).
7. Sélectionnez les applications d'identité pour poursuivre la mise à niveau.
8. Spécifiez les informations suivantes :

   Dossier d'installation de SSPR : spécifiez le dossier d'installation de SSPR.

   Dossier de l'application utilisateur : spécifiez le dossier de l'application utilisateur.

   Mot de passe du service SSO One des applications d'identité : spécifiez le mot de passe SSO One.

   Fichier JAR JDBC de la base de données des applications d'identité : spécifiez le fichier JAR de la base de données. L'emplacement par défaut du fichier JAR de la base de données existante est `/opt/netiq/idm/apps/postgres/postgresql-9.4.1212.jar`.

   Créer le schéma pour les applications d'identité : indique si vous souhaitez créer le schéma de base de données. Les options disponibles sont **Maintenant**, **Démarrage** et **Fichier**.

Mise à niveau de SSPR

REMARQUE : si SSPR est installé sur un serveur différent de celui des applications d'identité et d'OSP, vous devez mettre à niveau SSPR séparément.

1. Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` comme indiqué dans la Section 5.11, « Téléchargement des fichiers d'installation », page 49.
2. Montez le fichier `.iso` téléchargé.
3. À partir du répertoire racine du fichier `.iso`, accédez au répertoire `SSPR`.
4. Exécutez la commande suivante :

   ```
   ./install.sh
   ```

5 Lisez le contrat de licence.

6 Entrez o pour accepter l'accord de licence.

26.5.7 Tâches postérieures à la mise à niveau

- Vérifiez que le paramètre **Configuration SAML RBPM à eDirectory** dans l'utilitaire configupdate est défini sur **Auto**.
  1. Lancez l'utilitaire ConfigUpdate.
  2. Accédez à **Clients SSO** > **RBPM** et définissez **Configuration SAML RBPM à eDirectory** sur `Auto`.
  3. Enregistrez les modifications apportées.
  4. Démarrez Tomcat.
- Modifiez l'autorisation et la propriété du répertoire OSP :

  ```
  chmod +x novlua:novlua /opt/netiq/idm/apps/osp
  ```
- Supprimez manuellement la version précédente de Tomcat et des services ActiveMQ.

  ```
  /etc/init.d/idmapps_tomcat_init
  ```

  ```
  /etc/init.d/idmapps_activemq_init
  ```

Vous devez également restaurer manuellement les paramètres personnalisés pour Tomcat, SSPR, OSP ou les applications d'identité.

- « Java » page 275
- « Tomcat » page 276
- « Applications d'identité » page 277
- « One SSO Provider » page 278
- « Kerberos » page 278

Java

Vérifiez que l'emplacement du JRE mis à niveau (`jre/lib/security/cacerts`) contient tous les certificats de l'emplacement de l'ancien JRE. Si un certificat est manquant, importez-le manuellement dans le fichier `cacerts` du JRE mis à niveau.

1 Importez le fichier `java cacerts` à l'aide de la commande `keytool` :

```
keytool -import -trustcacerts -file Cerificate_Path -alias ALIAS_NAME -keystore cacerts
```

REMARQUE : après la mise à niveau, JRE est stocké à l'emplacement d'installation des applications identité. Par exemple : `/opt/netiq/idm/apps/jre`.

---

2 Vérifiez l'emplacement d'origine du JRE.

```
tomcat/bin/setenv.sh
```

3 Lancez l'utilitaire de **mise à jour de la configuration** et vérifiez le chemin de votre fichier `cacerts`.

Tomcat

1 (Conditionnel) Pour restaurer les fichiers personnalisés à partir de la sauvegarde effectuée précédemment dans le cadre de la procédure de mise à niveau, effectuez les tâches suivantes :

- Restaurez les certificats https personnalisés. Pour restaurer ces certificats, copiez le contenu Java Secure Sockets Extension (JSSE) du fichier `server.xml` sauvegardé vers le nouveau fichier `server.xml` situé dans le répertoire `/tomcat/conf`.
- Ne copiez pas les fichiers de configuration présents dans le répertoire Tomcat sauvegardé vers le nouveau répertoire Tomcat. Commencez avec la configuration par défaut de la nouvelle version et procédez aux éventuelles modifications nécessaires. Pour plus d'informations, reportez-vous au site Web d'Apache.

  Vérifiez que le nouveau fichier `server.xml` comporte les entrées suivantes :

  ```
  <Connector port="8543" protocol="HTTP/1.1"
         maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
         clientAuth="false" sslProtocol="TLS"
         keystoreFile="path_to_keystore_file"
         keystorePass="keystore_password" />
  <!--
        <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
   -->
  ```

  ou

  ```
  <Connector port="8543"
  protocol="org.apache.coyote.http11.Http11NioProtocol"
         maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
         clientAuth="false" sslProtocol="TLS"
         keystoreFile="path_to_keystore_file"
         keystorePass="keystore_password" />
  <!--
        <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
   -->
  ```

  REMARQUE : dans un environnement en grappe, supprimez manuellement le commentaire de la balise `Cluster` dans le fichier `server.xml` et copiez le fichier `osp.jks` sur tous les noeuds à partir du premier noeud situé à l'emplacement `/opt/netiq/idm/apps/osp_backup_<date>`.

- Si vous disposez de fichiers Keystore personnalisés, incluez le chemin d'accès correct dans le nouveau fichier `server.xml`.
- Importez les certificats des applications d'identité dans le coffre-fort d'identité dans `/opt/novell/eDirectory/lib64/nds-modules/jre/lib/security/cacerts`.

  Par exemple, vous pouvez utiliser la commande keytool suivante pour importer des certificats dans le coffre-fort d'identité :

  ```
  keytool -importkeystore -alias <keyalias> -srckeystore  <backup cacert> -
  srcstorepass changeit -destkeystore /opt/novell/eDirectory/lib64/nds-
  modules/jre/lib/security/cacerts
   -deststorepass changeit
  ```

2 (Conditionnel) Accédez à l'application utilisateur et restaurez les paramètres personnalisés manuellement en consultant la configuration sauvegardée.

Applications d'identité

Restaurez les configurations personnalisées des applications d'identité à partir de la sauvegarde effectuée pendant la procédure de mise à niveau.

Si vous avez renommé le nom du dossier de contexte personnalisé `IDMProv` avant d'exécuter le programme de mise à niveau, vous devez restaurer le nom d'origine du dossier de contexte à l'aide de l'utilitaire `configupdate`. Par exemple, le nom de contexte personnalisé d'origine est `IDMDev` et il a été renommé `IDMProv`.

Effectuez les étapes suivantes pour restaurer le nom d'origine du contexte :

1. Accédez au répertoire de l'application utilisateur situé dans `/opt/netiq/idm/apps/UserApplication`.
2. (Facultatif) Pour lancer l'utilitaire configupdate en mode GUI, assurez-vous que l'option `use_console` est définie sur `false` dans le fichier `configupdate.sh.properties`.

   Cette étape est nécessaire, car l'utilitaire de mise à niveau modifie la valeur de cette option sur `true`.

   Vous pouvez également lancer l'utilitaire configupdate et transmettre un argument de ligne de commande supplémentaires sous Linux.

   ```
   ./configupdate.sh use_console=false
   ```

3. Lancez l'utilitaire `ConfigUpdate`.

   ```
   configupdate.sh
   ```

4. Sous l'onglet **Application utilisateur**, cliquez sur **Aff. options avancées** et effectuez les opérations suivantes :
   - **4a** Cochez la case **Modifier le nom du contexte RBPM**.
   - **4b** Remplacez le nom du contexte RBPM par le nom du contexte d'origine.
   - **4c** Recherchez et sélectionnez le **DN du pilote des rôles**, puis cliquez sur **OK**.
   - **4d** Modifiez l'autorisation et la propriété du fichier `WAE` à l'aide de la commande suivante.

     ```
     chmod 755 <Original_Context_Name>.war; chown -R novlua:novlua
     <Original_Context_Name>.war
     ```

     Par exemple, si le nom d'origine du contexte personnalisé est `IDMDev` :

     ```
     chmod 755 IDMDev.war; chown -R novlua:novlua IDMDev.war
     ```

5. (Conditionnel) Si vous avez terminé toutes les tâches postérieures à la mise à niveau, démarrez le service Tomcat pour les applications d'identité.

One SSO Provider

Si OSP et l'application utilisateur sont déployés sur des serveurs distincts, mettez à jour le paramètre du client SSO à l'aide de l'utilitaire de mise à jour de la configuration. Pour plus d'informations, reportez-vous à la « Tableau de bord IDM » page 160 de la Section 11.6.5, « Paramètres des clients SSO », page 160.

Par défaut, l'entrée `LogHost` située dans le fichier `/etc/logevent.conf` est définie sur `localhost`.

Pour modifier l'entrée `LogHost`, restaurez manuellement les configurations OSP personnalisées à partir de la sauvegarde effectuée pendant la procédure de mise à niveau.

Kerberos

L'utilitaire de mise à niveau crée un nouveau dossier Tomcat sur votre ordinateur. Si des fichiers Kerberos tels que `keytab` et `Kerberos_login.config` se trouvaient dans l'ancien dossier Tomcat, copiez ces fichiers dans le nouveau dossier Tomcat à partir du dossier sauvegardé.

26.6 Mise à niveau d'Identity Reporting

Identity Reporting inclut deux pilotes. Effectuez la mise à niveau dans l'ordre suivant :

REMARQUE : assurez-vous que votre base de données est mise à niveau vers une version prise en charge.

---

1. Mettez à niveau votre base de données vers une version prise en charge. Pour plus d'informations sur la mise à niveau de la base de données PostgreSQL, reportez-vous à la Section 26.5.4, « Mise à niveau de la base de données PostgreSQL », page 270.
2. Mettez à niveau les paquetages de pilote. Pour plus d'informations, reportez-vous à la Section 26.6.2, « Mise à niveau des paquetages de pilotes pour Identity Reporting », page 279.
3. Effectuez une mise à niveau/migration vers Sentinel Log Management for IGA.

   Si vous effectuez une mise à niveau à partir d'Identity Reporting 4.6.x, mettez à niveau Sentinel Log Management for IGA vers la version 4.7. Pour plus d'informations, reportez-vous à la Section 26.6.3, « Mise à niveau de Sentinel Log Management for IGA », page 279.

   Si vous effectuez une migration depuis Identity Reporting 4.5.x, migrez à partir d'EAS vers Sentinel Log Management for IGA. Pour plus d'informations, reportez-vous à la Section 29.8.1, « Migration d'Event Auditing Service vers Sentinel Log Management for IGA », page 302.
4. Mettez à niveau Identity Reporting. Pour plus d'informations, reportez-vous à la Section 26.6.5, « Mise à niveau d'Identity Reporting », page 280.

26.6.1 Conditions préalables et considérations relatives à la mise à niveau

Avant d'effectuer une mise à niveau, tenez compte des considérations suivantes :

- Au cours de la mise à niveau, veillez à spécifier le bon emplacement pour le fichier `postgresql-9.4.1212.jar`. L'emplacement par défaut est `/opt/netiq/idm/postgres/`. La connexion de base de données échoue dans les scénarios suivants :
  - Si vous indiquez un chemin incorrect.
  - Si vous indiquez un fichier JAR incorrect.

- Si le pare-feu est activé.
- Si la base de données n'accepte pas les connexions à partir de machines distantes.

- Si votre base de données est configurée sur SSL, supprimez `ssl=true` du fichier `server.xml` de la variable PATH située à l'emplacement :

  `/opt/netiq/idm/apps/tomcat/conf/`

  Par exemple, remplacez

  `jdbc:postgresql://<postgres db>:5432/idmuserappdb?ssl=true`

  par

  `jdbc:postgresql://<postgres db>:5432/idmuserappdb`

26.6.2 Mise à niveau des paquetages de pilotes pour Identity Reporting

Cette section explique comment mettre à jour les paquetages pour les pilotes de la passerelle système gérée et le service de collecte de données vers la version la plus récente. Vous devez effectuer cette opération avant de mettre à niveau Identity Reporting.

1. Dans Designer, ouvrez votre projet en cours.
2. Cliquez avec le bouton droit sur **Catalogue de paquetages > Importer le paquetage**.
3. Sélectionnez le paquetage approprié. Par exemple : **Paquetage Base de la passerelle système gérée**.
4. Cliquez sur **OK**.
5. Dans la vue Développeur, cliquez avec le bouton droit sur le pilote, puis cliquez sur **Propriétés**.
6. Accédez à l'onglet **Paquetages** sur la page **Propriétés**.
7. Cliquez sur le symbole d'**ajout de paquetage (+)** dans le coin supérieur droit.
8. Sélectionnez le paquetage, puis cliquez sur **OK**.
9. Répétez la même procédure pour mettre à niveau le paquetage pour le pilote du service de collecte des données.

REMARQUE : Assurez-vous que les pilotes de la passerelle système gérée et du service de collecte de données sont connectés à la version d'Identity Manager mise à niveau.

26.6.3 Mise à niveau de Sentinel Log Management for IGA

1. Téléchargez le fichier `SentinelLogManagementForIGA8.1.1.0.tar.gz` à partir du site Web des téléchargements NetIQ.
2. Accédez au répertoire dans lequel vous souhaitez extraire le fichier.
3. Exécutez la commande suivante pour extraire le fichier :

   ```
   tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
   ```

4. Accédez au répertoire `SentinelLogManagementforIGA`.
5. Pour installer SLM for IGA, exécutez la commande suivante :

   ```
   ./install.sh
   ```

6 Spécifiez la langue à utiliser dans le cadre de l'installation, puis appuyez sur la touche `Entrée`.

7 Entrez `o` pour accepter l'accord de licence.

REMARQUE : une fois SLM pour IGA mis à niveau, vous devez importer manuellement les derniers collecteurs.

1. Accédez au site Web de téléchargements NetIQ.
2. Téléchargez le fichier `SentinelLogManagementForIGA8.1.1.0.tar.gz`.
3. Extrayez le fichier et accédez au répertoire `/content/`.
4. Importez le collecteur d'Identity Manager.

26.6.4 Mise à niveau du système d'exploitation

Lorsque vous mettez à niveau le système d'exploitation depuis SLES 11 vers SLES 12, la procédure supprime certains RPM de SLM for IGA.

Les commandes suivantes permettent de garantir le bon fonctionnement de SLM for IGA une fois le système d'exploitation mis à niveau.

REMARQUE : vous devez effectuer la mise à niveau de SLM for IGA avant celle du système d'exploitation.

Utilisez les étapes suivantes pour mettre à niveau votre système d'exploitation :

1 Accédez au répertoire dans lequel le fichier d'installation de Sentinel a été extrait.

2 Arrêtez les services Sentinel :

```
rcsentinel stop
```

3 Exécutez la commande suivante :

```
./install.sh --preosupgrade
```

4 Mettez à niveau votre système d'exploitation

5 Exécutez la commande suivante :

```
./install.sh --postosupgrade
```

6 Redémarrez le service Sentinel :

```
rcsentinel restart
```

26.6.5 Mise à niveau d'Identity Reporting

1 Téléchargez le fichier `Identity_Manager_4.7_Linux.iso` à partir du site Web de téléchargement de NetIQ.

2 Montez le fichier `.iso` téléchargé.

3 Exécutez la commande suivante :

```
./install.sh
```

4 Lisez le contrat de licence.

5 Entrez `o` pour accepter l'accord de licence.

6 Indiquez si vous souhaitez mettre à niveau les composants Identity Manager. Les options disponibles sont **`y`** (oui) et **`n`** (non).

7 Sélectionnez Identity Reporting pour poursuivre la mise à niveau.

8 Spécifiez les informations suivantes :

OSP est-il installé : indiquez si OSP est installé.

Dossier d'installation d'Identity Reporting pour la sauvegarde : spécifiez le dossier d'installation d'Identity Reporting.

Créer le schéma pour Identity Reporting : indiquez quand vous souhaitez créer le schéma de votre base de données.

Fichier JAR JDBC de la base de données d'Identity Reporting : spécifiez le fichier JAR de base de données d'Identity Reporting. L'emplacement par défaut du fichier JAR de la base de données existante est `/opt/netiq/idm/apps/postgres/postgresql-9.4.1212.jar`.

Utilisateur de la base de données d'Identity Reporting : indiquez le nom de l'utilisateur de la base de données de création de rapports.

Mot de passe du compte de la base de données d'Identity Reporting : indiquez le mot de passe associé à la base de données de création de rapports.

26.6.6 Étapes postérieures à la mise à niveau pour la création de rapports

---

REMARQUE : les rapports d'Identity Manager 4.6.1 ne fonctionnent pas après avoir effectué une mise à niveau. Vous pouvez uniquement utiliser les rapports d'Identity Manager 4.7.

Au cours de la mise à niveau, si vous avez sélectionné comme option de création du **schéma de base de données** la valeur **Démarrage** ou **Fichier**, veillez à effectuer les opérations suivantes :

1. Connectez-vous à Identity Reporting.
2. Supprimez la source de données et les définitions de rapport existantes du dépôt Identity Reporting.
3. Ajoutez la nouvelle source de données Services de collecte de données Identity Manager.

26.6.7 Vérification de la mise à niveau d'Identity Reporting

1 Lancez Identity Reporting.

2 Vérifiez que les anciens et les nouveaux rapports s'affichent dans l'outil.

3 Consultez l'**Agenda** pour vérifier si vos rapports planifiés s'affichent.

4 Assurez-vous que la page **Paramètres** affiche vos paramètres précédents pour les applications gérées et non gérées.

5 Vérifiez que tous les autres paramètres semblent corrects.

6 Vérifiez si l'application répertorie vos rapports finalisés.

26.7 Mise à niveau d'Analyzer

Pour mettre à niveau Analyzer, NetIQ fournit des fichiers de correctif au format `.zip`. Avant la mise à niveau d'Analyzer, assurez-vous que l'ordinateur répond aux conditions préalables et à la configuration système requise. Pour plus d'informations, consultez les notes de version accompagnant la mise à niveau.

1. Téléchargez le fichier `Identity_Manager_4.7_Linux_Analyzer.tar.gz` à partir du site Web de téléchargements NetIQ.
2. Extrayez le fichier `.zip` dans le répertoire qui contient les fichiers d'installation d'Analyzer, comme les plug-ins, le script de désinstallation, ainsi que d'autres fichiers Analyzer.
3. Redémarrez Analyzer.
4. Pour vérifier que vous avez correctement appliqué le nouveau correctif, procédez comme suit :
   - **4a** Lancez Analyzer.
   - **4b** Cliquez sur **Aide > À propos d'Analyzer**.
   - **4c** Vérifiez si le programme affiche la nouvelle version.

26.8 Ajout de nouveaux serveurs à l'ensemble de pilotes

Lorsque vous mettez à niveau ou migrez Identity Manager vers de nouveaux serveurs, vous devez mettre à jour les informations de l'ensemble de pilotes. Cette section vous guide tout au long du processus. Vous pouvez utiliser Designer ou iManager pour mettre à jour l'ensemble de pilotes.

26.8.1 Ajout du nouveau serveur à l'ensemble de pilotes

Si vous utilisez iManager, vous devez ajouter le nouveau serveur à l'ensemble de pilotes. Designer contient un assistant de migration de serveur qui accomplit cette tâche pour vous. Si vous utilisez iManager, exécutez la procédure suivante :

1. Dans iManager, cliquez sur  pour afficher la page d'administration d'Identity Manager.
2. Cliquez sur **Présentation d'Identity Manager**.
3. Naviguez jusqu'au conteneur dans lequel se trouve l'ensemble de pilotes et sélectionnez-le.
4. Cliquez sur le nom de l'ensemble de pilotes pour accéder à la page Présentation de l'ensemble de pilotes.
5. Cliquez sur **Serveurs > Ajouter un serveur**.
6. Recherchez et sélectionnez le nouveau serveur Identity Manager, puis cliquez sur **OK**.

26.8.2 Suppression de l'ancien serveur de l'ensemble de pilotes

Une fois que le nouveau serveur exécute tous les pilotes, vous pouvez supprimer l'ancien serveur de l'ensemble de pilotes.

- « Utilisation de Designer pour retirer l'ancien serveur de l'ensemble de pilotes » page 283
- « Utilisation d'iManager pour retirer l'ancien serveur de l'ensemble de pilotes » page 283
- « Déclassement de l'ancien serveur » page 283

Utilisation de Designer pour retirer l'ancien serveur de l'ensemble de pilotes

1. Dans Designer, ouvrez votre projet.
2. Dans Modeler, cliquez avec le bouton droit sur l'ensemble de pilotes, puis sélectionnez **Propriétés**.
3. Sélectionnez **Liste de serveurs**.
4. Sélectionnez l'ancien serveur Identity Manager dans la liste **Serveurs sélectionnés**, puis cliquez sur le signe **<** pour le retirer de la liste **Serveurs sélectionnés**.
5. Cliquez sur **OK** pour enregistrer les modifications.
6. Déployez les modifications vers le coffre-fort d'identité.

   Pour plus d'informations, reportez-vous à la section « Deploying a Driver Set to an Identity Vault » (Déploiement d'un ensemble de pilotes dans un coffre-fort d'identité) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).

Utilisation d'iManager pour retirer l'ancien serveur de l'ensemble de pilotes

1. Dans iManager, cliquez sur pour afficher la page d'administration d'Identity Manager.
2. Cliquez sur **Présentation d'Identity Manager**.
3. Naviguez jusqu'au conteneur dans lequel se trouve l'ensemble de pilotes et sélectionnez-le.
4. Cliquez sur le nom de l'ensemble de pilotes pour accéder à la page Présentation de l'ensemble de pilotes.
5. Cliquez sur **Serveurs > Supprimer le serveur**.
6. Sélectionnez l'ancien serveur d'Identity Manager, puis cliquez sur **OK**.

Déclassement de l'ancien serveur

À ce stade, le serveur n'héberge aucun pilote. Si vous n'avez plus besoin de ce serveur, vous devez suivre des étapes supplémentaires pour le déclasser :

1. Supprimez les répliques d'eDirectory de ce serveur.

   Pour plus d'informations, reportez-vous à la section Deleting Replicas (Suppression de répliques) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8).
2. Supprimez eDirectory de ce serveur.

   Pour plus d'informations, reportez-vous au document TID 10056593, Removing a Server From an NDS Tree Permanently (Suppression définitive d'un serveur dans une arborescence NDS).

26.9 Restauration de stratégies et de règles personnalisées sur le pilote

Après avoir installé de nouveaux paquetages pour vos pilotes ou effectué une mise à niveau vers ces derniers, vous devez restaurer les éventuelles stratégies ou règles personnalisées sur le pilote après avoir installé le fichier de configuration du nouveau pilote. Si ces stratégies ont des noms différents, elles restent stockées dans le pilote mais leurs liens sont cassés et doivent être rétablis.

26.9.1 Utilisation de Designer pour restaurer les stratégies et les règles personnalisées sur le pilote

Vous pouvez ajouter des stratégies à l'ensemble de stratégies. Il est conseillé d'exécuter cette procédure dans un environnement de test, avant de déplacer le pilote mis à niveau dans votre environnement de production.

1. Dans la vue **Mode plan**, sélectionnez le pilote mis à niveau, puis cliquez sur l'icône **Afficher le flux de stratégie** .
2. Cliquez avec le bouton droit de la souris sur l'ensemble de stratégies dans lequel vous devez restaurer la stratégie personnalisée sur le pilote, puis choisissez **Ajouter une stratégie > Copier existant**.
3. Naviguez jusqu'à la stratégie personnalisée, puis sélectionnez-la et cliquez sur **OK**.
4. Indiquez le nom de la stratégie personnalisée, puis cliquez sur **OK**.
5. Cliquez sur **Oui** dans le message de conflit de fichier pour enregistrer votre projet.
6. Lorsque le Générateur de stratégies ouvre la stratégie, vérifiez que les informations sont correctes dans la stratégie copiée.
7. Répétez la procédure de l'Étape 2 à l'Étape 6 pour chaque stratégie personnalisée à restaurer pour le pilote.
8. Lancez le pilote et testez-le.

   Pour plus d'informations sur le lancement du pilote, reportez-vous à la Section 23.1.2, « Lancement des pilotes », page 242. Pour plus d'informations sur le test du pilote, reportez-vous à la section « Testing Policies with Policy Simulator » (Test des stratégies avec le simulateur de stratégie) dans la documentation *NetIQ Identity Manager Policies - Using Designer to Create Policies* (NetIQ Identity Manager - Utilisation de Designer pour la création de stratégies).
9. Une fois que vous avez vérifié que les stratégies fonctionnent, déplacez le pilote vers l'environnement de production.

26.9.2 Utilisation d'iManager pour restaurer les stratégies et les règles personnalisées sur le pilote

Exécutez cette procédure dans un environnement de test avant de déplacer le pilote mis à niveau dans votre environnement de production.

1. Dans iManager, sélectionnez **Identity Manager > Présentation d'Identity Manager**.
2. Recherchez et sélectionnez l'emplacement de l'arborescence où rechercher les objets Ensemble de pilotes, puis cliquez sur l'icône de recherche  .
3. Cliquez sur l'objet Ensemble des pilotes contenant le pilote mis à niveau.
4. Cliquez sur l'icône du pilote, puis choisissez l'ensemble de stratégies dans lequel restaurer la stratégie personnalisée.
5. Cliquez sur **Insérer**.
6. Sélectionnez **Utiliser une stratégie existante**, puis naviguez jusqu'à la stratégie personnalisée et sélectionnez-la.
7. Cliquez sur **OK**, puis sur **Fermer**.
8. Répétez la procédure de l'Étape 3 à l'Étape 7 pour chaque stratégie personnalisée à restaurer pour le pilote.
9. Lancez le pilote et testez-le.

   Pour plus d'informations sur le lancement du pilote, reportez-vous à la Section 23.1.2, « Lancement des pilotes », page 242. Il n'existe pas de simulateur de stratégie dans iManager. Pour tester les stratégies, faites intervenir des événements qui les exécutent. Vous pouvez, par exemple, créer un utilisateur, le modifier ou le supprimer.
10. Une fois que vous avez vérifié que les stratégies fonctionnent, déplacez le pilote vers l'environnement de production.

27 Passage de l'édition avancée à l'édition standard

Vous ne devez basculer vers l'édition standard que si vous ne souhaitez pas utiliser les fonctionnalités de la version avancée dans votre environnement et souhaitez réduire votre déploiement Identity Manager.

1. (Conditionnel) Si vous avez déjà activé l'édition avancée, supprimez l'activation.
2. (Conditionnel) Pour basculer vers le mode d'évaluation de l'édition standard, procédez comme suit :
   - **2a** Accédez au répertoire du coffre-fort d'identité `dib`.

     `/var/opt/novell/eDirectory/data/dib`
   - **2b** Créez un nouveau fichier, appelez-le `.idme` et ajoutez 2 (en chiffre) dans le fichier.
   - **2c** Redémarrez eDirectory.
   - **2d** Passez à l'étape 4.
3. (Conditionnel) Si vous avez déjà acheté une activation de Standard Edition, appliquez-la.
4. Arrêtez Tomcat.
5. Supprimez les fichiers WAR et le dossier Webapps du répertoire `/opt/netiq/idm/apps/tomcat/webapps` :
   - `IDMProv*`
   - `IDMRPT*`
   - `dash*`
   - `idmdash*`
   - `landing*`
   - `rra*`
   - `rptdoc*`
6. Déplacez les dossiers existants suivants vers un répertoire de sauvegarde :
   - `IDMReporting`
   - `UserApplication`
7. Copiez le fichier `ism-configuration.properties` à partir du répertoire `<dossier_installation="">/tomcat/conf` vers un répertoire de sauvegarde.
8. Installez Identity Reporting à partir du support Identity Manager 4.6.
9. Démarrez le fichier `configupdate.sh` à partir du répertoire `<dossier installation reporting> /bin` et spécifiez des valeurs pour les paramètres suivants :

   Onglet Création de rapports : Spécifiez les paramètres dans les sections suivantes :
   - Coffre-fort d'identité
   - Identité de l'utilisateur du coffre-fort d'identité

- Administrateurs de rapports
  - **DN du conteneur du rôle d'administrateur de création de rapports**. Par exemple, `ou=sa,o=data`
  - **Administrateurs de rapports**. Par exemple, `cn=admin,ou=sa,o=system`

Sous l'onglet Authentification : spécifiez les paramètres dans les sections suivantes :

- Serveur d'authentification
  - **Identificateur de l'hôte du serveur OAuth**. Par exemple, adresse IP ou nom DNS du serveur d'authentification tel que `192.168.0.1`
  - **Port TCP du serveur OAuth**
  - **Le serveur OAuth utilise TLS/SSL.**
- Configuration de l'authentification
  - **Fichier Keystore OAuth**. Par exemple, `/opt/netiq/idm/apps/osp/osp.jks`
  - **Alias de la clé qui doit être utilisé par OAuth**
  - **Mot de passe de la clé qui doit être utilisé par OAuth**
  - **Timeout de la session (minutes)**. Par exemple, 60 minutes.

Onglet Clients SSO : spécifiez les paramètres dans les sections suivantes :

- Création de rapports
  - **Lien URL vers la page de renvoi**. Par exemple, `http://192.168.0.1:8180/idmrpt`
- SSPR (réinitialisation du mot de passe en self-service)
  - **ID du client OAuth**. Par exemple, *sspr*
  - Secret du client OAuth Par exemple, *<sspr client secret>*
  - **URL de redirection OAuth OSP**. Par exemple, `http://192.168.0.1:8180/sspr/public/oauth`

Pour plus d'informations sur l'utilitaire de configuration, reportez-vous à la section « Exécution de l'utilitaire de configuration des applications d'identité » page 143.

10 Enregistrez les modifications et quittez l'utilitaire de configuration.

11 Démarrez Tomcat.

X Migration des données Identity Manager vers une nouvelle installation

Cette section fournit des informations sur la migration de données existantes dans des composants Identity Manager vers une nouvelle installation. La plupart des tâches de migration s'appliquent aux applications d'identité. Pour mettre à niveau les composants Identity Manager, reportez-vous à la Partie IX, « Mise à niveau d'Identity Manager », page 249. Pour plus d'informations sur la différence entre la mise à niveau et la migration, reportez-vous à la Section 25.2, « Présentation du processus de mise à niveau », page 253.

28 Préparation à la migration d'Identity Manager

Cette section fournit des informations pour vous aider à préparer la migration de votre solution Identity Manager vers la nouvelle installation.

28.1 Liste de contrôle pour l'exécution d'une migration

Si vous souhaitez effectuer une migration, NetIQ vous recommande de suivre les étapes de la liste de contrôle suivante.

	Éléments de la liste de contrôle
❑	1. Déterminez si vous devez effectuer une mise à niveau ou une migration. Pour plus d'informations, reportez-vous à la Section 25.2, « Présentation du processus de mise à niveau », page 253.
❑	2. Assurez-vous que vous disposez de la dernière version du kit d'installation pour migrer les données Identity Manager.
❑	3. Renseignez-vous sur les interactions entre les différents composants Identity Manager. Pour plus d'informations, reportez-vous au Partie I, « Introduction », page 15.
❑	4. Assurez-vous que votre ordinateur dispose des prérequis logiciels et matériels pour une version plus récente d'Identity Manager. Pour plus d'informations, reportez-vous au Section 5.9, « Préparation de l'installation », page 43 et aux notes de publication de la version vers laquelle vous voulez effectuer la mise à niveau.
❑	5. Mettez eDirectory à niveau vers la dernière version prise en charge pour le coffre-fort d'identité. Pour plus d'informations, reportez-vous à la Section 26.3.1, « Mise à niveau du coffre-fort d'identité », page 262.
❑	6. Ajoutez au nouveau serveur les répliques qui figurent sur le serveur d'Identity Manager actuel. Pour plus d'informations, reportez-vous à la Section 29.4, « Migration du moteur Identity Manager vers un nouveau serveur », page 297.
❑	7. Installez Identity Manager sur le nouveau serveur. Pour plus d'informations, reportez-vous à la « Planification de l'installation d'Identity Manager » page 31.
❑	8. (Conditionnel) Si l'un des pilotes dans l'ensemble de pilotes est un pilote de chargeur distant, mettez à niveau le serveur de chargeur distant pour chaque pilote. Pour plus d'informations, reportez-vous à la Section 26.3.3, « Mise à niveau du chargeur distant », page 263.
❑	9. (Conditionnel) Si vous exécutez l'application utilisateur sur votre ancien serveur, mettez à jour le composant et ses pilotes. Pour plus d'informations, reportez-vous à la Section 29.1, « Liste de contrôle pour la migration d'Identity Manager », page 293.
❑	10. Modifiez les informations spécifiques du serveur pour chaque pilote. Pour plus d'informations, reportez-vous à la Section 29.3.1, « Copie des informations spécifiques au serveur dans Designer », page 295.

	Éléments de la liste de contrôle
❑	11. (Conditionnel) Si vous avez RBPM, mettez à jour les informations spécifiques au serveur de l'ancien vers le nouveau serveur pour l'application utilisateur. Pour plus d'informations, reportez-vous à la section Section 29.3, « Copie des informations spécifiques du serveur pour l'ensemble de pilotes », page 295.
❑	12. Mettez à jour vos pilotes au format du paquetage. Pour plus d'informations, reportez-vous à la Section 26.4, « Mise à niveau des pilotes Identity Manager », page 266.
❑	13. (Conditionnel) Si vous disposez de stratégies et de règles personnalisées, restaurez vos paramètres personnalisés. Pour plus d'informations, reportez-vous à la Section 26.9, « Restauration de stratégies et de règles personnalisées sur le pilote », page 284.
❑	14. Installez Identity Reporting et les pilotes associés. Pour plus d'informations, reportez-vous au Section 29.8, « Migration d'Identity Reporting », page 301.
❑	15. Supprimez l'ancien serveur de l'ensemble de pilotes. Pour plus d'informations, reportez-vous à la Section 26.8.2, « Suppression de l'ancien serveur de l'ensemble de pilotes », page 282.
❑	16. Activez votre solution Identity Manager mise à niveau. Pour plus d'informations, reportez-vous à la Section 24, « Activation d'Identity Manager », page 245.

28.2 Arrêt et démarrage des pilotes Identity Manager au cours de la migration

Lorsque vous mettez à niveau ou procédez à la migration d'Identity Manager, vous devez démarrer et arrêter les pilotes pour vous assurer que le processus peut modifier ou remplacer les fichiers corrects. Cette section explique les activités suivantes : Pour plus d'informations, reportez-vous aux sections suivantes :

- Section 23.1.1, « Arrêt des pilotes », page 241
- Section 23.1.2, « Lancement des pilotes », page 242

29 Migration d'Identity Manager vers un nouveau serveur

Cette section fournit des informations sur la migration de l'application utilisateur vers les applications d'identité d'un nouveau serveur. Il est également possible que vous deviez effectuer une migration lorsque vous ne pouvez pas effectuer la mise à niveau d'une installation existante. Cette section explique les activités suivantes :

29.1 Liste de contrôle pour la migration d'Identity Manager

NetIQ vous recommande de suivre les étapes de la liste de contrôle suivante :

	Éléments de la liste de contrôle
❑	1. Sauvegardez les répertoires et les bases de données de votre solution Identity Manager.
❑	2. Assurez-vous que vous avez installé les versions les plus récentes des composants Identity Manager, à l'exception des applications d'identité. Pour plus d'informations, reportez-vous à la Section 5.7.4, « Configuration recommandée pour le serveur », page 40 et aux dernières notes de version des composants. **REMARQUE :** pour continuer à utiliser la base de données de votre application utilisateur actuelle, spécifiez **Base de données existante** dans le programme d'installation. Pour plus d'informations, reportez-vous à la Chapitre 9, « Installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting », page 91.
❑	3. Vérifiez l'état de santé du coffre-fort d'identité pour vous assurer que le schéma s'étend correctement. Pour la procédure de vérification de l'état de santé, reportez-vous au document TID 3564075.
❑	4. Importez vos pilotes d'application utilisateur existants dans Designer.
❑	5. Archivez le projet Designer. Il correspond à l'état des pilotes avant la migration. Pour plus d'informations, reportez-vous à la Section 29.2, « Préparation de votre projet Designer pour la migration », page 294.

	Éléments de la liste de contrôle
❑	6. (Conditionnel) Pour migrer le moteur Identity Manager vers un nouveau serveur, copiez les répliques eDirectory sur le nouveau serveur. Pour plus d'informations, reportez-vous à la Section 29.4, « Migration du moteur Identity Manager vers un nouveau serveur », page 297.
❑	7. Créez un projet Designer dans la version la plus récente du concepteur, puis importez le pilote d'application utilisateur en vue de la préparation à la migration.
❑	8. Procédez à la migration du pilote d'application utilisateur. Pour plus d'informations, reportez-vous au Section 29.5, « Migration du pilote d'application utilisateur », page 297.
❑	9. Mettez à niveau les applications d'identité. Pour plus d'informations, reportez-vous au Section 26.5, « Mise à niveau des applications d'identité », page 268.
❑	10. (Conditionnel) Pour mettre à niveau une base de données Oracle avec un fichier SQL créé par le processus d'installation, préparez l'environnement Oracle. Pour plus d'informations, reportez-vous à la Section 29.7.1, « Préparation d'une base de données Oracle pour le fichier SQL », page 299.
❑	11. Assurez-vous que vos navigateurs n'incluent pas de contenu des versions précédentes d'Identity Manager. Pour plus d'informations, reportez-vous à la Section 29.7.2, « Vidage du cache du navigateur », page 300.
❑	12. (Conditionnel) Restaurez vos paramètres personnalisés pour SharedPagePortlet. Pour plus d'informations, reportez-vous à la Section 29.7.3, « Mise à jour du paramètre Timeout maximum pour SharedPagePortlet », page 300.
❑	13. Assurez-vous que l'option de recherche de groupes n'affiche pas d'informations tant que l'utilisateur n'a pas fourni les paramètres de filtre. Pour plus d'informations, reportez-vous à la Section 29.7.4, « Désactivation du paramètre de requête automatique pour les groupes », page 301.

29.2 Préparation de votre projet Designer pour la migration

Avant de procéder à la migration du pilote, vous devez effectuer certaines opérations de configuration pour préparer le projet Designer à la migration.

REMARQUE : si vous n'avez pas de projet Designer existant à migrer, créez un projet à l'aide des options suivantes : **Fichier > Importer > Projet (depuis le coffre-fort d'identité)**.

1. Lancez Designer.
2. (Conditionnel) Si un de vos projets Designer existant contient l'application utilisateur que vous souhaitez migrer, sauvegardez le projet :
   - **2a** Cliquez avec le bouton droit sur le nom du projet dans la vue Projet, puis sélectionnez **Copier un projet**.
   - **2b** Indiquez un nom pour le projet, puis cliquez sur **OK**.
3. Pour mettre à jour le schéma de votre projet existant, procédez comme suit :
   - **3a** Dans la vue Modélisateur, sélectionnez le coffre-fort d'identité.
   - **3b** Sélectionnez **En direct > Schéma > Importer**.

4 (Facultatif) Pour vérifier que le numéro de version d'Identity Manager est correct dans votre projet, procédez comme suit :

4a Dans la vue Modélisateur, sélectionnez le coffre-fort d'identité, puis cliquez sur **Propriétés**.

4b Dans le menu de navigation de gauche, sélectionnez **Liste de serveurs**.

4c Sélectionnez un serveur, puis cliquez sur **Éditer**.

Le champ **version d'Identity Manager** doit afficher la version la plus récente.

29.3 Copie des informations spécifiques du serveur pour l'ensemble de pilotes

Vous devez copier toutes les informations spécifiques au serveur stockées dans chaque pilote et dans chaque ensemble de pilotes vers les informations du nouveau serveur. Cela inclut également les valeurs de configuration globales et d'autres données sur l'ensemble de pilotes qui ne seraient pas présentes sur le nouveau serveur et devraient donc être copiées. Les informations spécifiques du serveur sont contenues dans :

- Les valeurs de configuration globale
- Les valeurs de contrôle du moteur
- Les mots de passe nommés
- Les informations d'authentification de pilote
- Les options de démarrage de pilote
- Les paramètres de pilote
- Les données d'ensemble de pilotes

Cela peut être fait dans Designer ou dans iManager. Si vous utilisez Designer, le processus est automatisé. Si vous utilisez iManager, vous devez le faire manuellement. Si vous effectuez la migration à partir d'une version d'un serveur Identity Manager antérieure à 3.5 vers une version égale ou supérieure à 3.5, vous devez utiliser iManager. Pour tous les autres chemins de migration pris en charge, vous pouvez utiliser Designer.

- Section 29.3.1, « Copie des informations spécifiques au serveur dans Designer », page 295
- Section 29.3.2, « Modification des informations spécifiques au serveur dans iManager », page 296
- Section 29.3.3, « Modification des informations spécifiques au serveur pour l'application utilisateur », page 297

29.3.1 Copie des informations spécifiques au serveur dans Designer

Cette procédure affecte tous les pilotes stockés dans l'ensemble de pilotes.

1 Dans Designer, ouvrez votre projet.

2 Dans l'onglet **Aperçu**, cliquez avec le bouton droit sur le serveur, puis sélectionnez **Migrer**.

3 Lisez la présentation pour savoir quels éléments sont migrés vers le nouveau serveur, puis cliquez sur **Suivant**.

4 Sélectionnez le serveur cible dans la liste des serveurs disponibles, puis cliquez sur **Suivant**.

Les serveurs répertoriés sont ceux qui ne sont actuellement pas associés à un ensemble de pilotes et qui sont équivalent à la version d'Identity Manager du serveur source ou plus récents que celle-ci.

5 Choisissez l'une des options suivantes :

- **Activer le serveur cible :** les paramètres du serveur source sont copiés vers le serveur cible et les pilotes désactivés sur le serveur source. NetIQ recommande l'utilisation de cette option.
- **Garder le serveur source actif :** les paramètres ne sont pas copiés et tous les pilotes sont désactivés sur le serveur cible.
- **Les serveurs source et cible sont tous deux activés :** les paramètres du serveur source sont copiés vers le serveur cible sans désactiver les pilotes sur les serveurs source et cible. Cette option n'est pas recommandée. En cas de démarrage des deux pilotes, les mêmes informations sont écrites dans deux files d'attente, ce qui peut provoquer des altérations.

6 Cliquez sur **Migrer**.

7 Déployer les pilotes modifiés vers le coffre-fort d'identité.

Pour plus d'informations, reportez-vous à la section « Deploying a Driver to an Identity Vault » (Déploiement d'un pilote dans un coffre-fort d'identité) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer for Identity Manager).

8 Démarrez les pilotes.

Pour plus d'informations, reportez-vous à la Section 23.1.2, « Lancement des pilotes », page 242.

29.3.2 Modification des informations spécifiques au serveur dans iManager

1 Dans iManager, cliquez sur  pour afficher la page d'administration d'Identity Manager.

2 Cliquez sur **Présentation d'Identity Manager**.

3 Naviguez jusqu'au conteneur dans lequel se trouve l'ensemble de pilotes et sélectionnez-le.

4 Cliquez sur le nom de l'ensemble de pilotes pour accéder à la page Présentation de l'ensemble de pilotes.

5 Cliquez dans l'angle supérieur droit, puis cliquez sur **Arrêter le pilote**.

6 Cliquez dans l'angle supérieur droit, puis cliquez sur **Modifier les propriétés**.

7 Copiez ou migrez l'ensemble des paramètres de pilote spécifiques au serveur, valeurs de configuration globale, valeurs de contrôle du moteur, mots de passe nommés, données d'authentification de pilote et options de démarrage de pilote qui contiennent les informations de l'ancien serveur vers les informations du nouveau serveur. Les valeurs de configuration globale et autres paramètres de l'ensemble de pilotes, tels que la taille de tas maximale, les paramètres Java, etc., doivent être identiques à ceux de l'ancien serveur.

8 Cliquez sur **OK** pour sauvegarder toutes les modifications.

9 Cliquez dans l'angle supérieur droit du pilote pour le démarrer.

10 Répétez la procédure de l'Étape 5 à l'Étape 9 pour chaque pilote dans l'ensemble de pilotes.

29.3.3 Modification des informations spécifiques au serveur pour l'application utilisateur

Vous devez reconfigurer l'application utilisateur pour qu'elle reconnaisse le nouveau serveur. Exécutez `configupdate.sh`.

1. Accédez à l'utilitaire de mise à jour de la configuration situé par défaut dans le sous-répertoire d'installation de l'application utilisateur.
2. À l'invite de commande, lancez l'utilitaire de mise à jour de la configuration :

   ```
   configupdate.sh
   ```

3. Spécifiez les valeurs telles que décrites au Chapitre 11.6, « Configuration des paramètres pour les applications d'identité », page 143.

29.4 Migration du moteur Identity Manager vers un nouveau serveur

Lors de la migration du moteur Identity Manager vers un nouveau serveur, vous pouvez conserver les répliques eDirectory que vous utilisez actuellement sur l'ancien serveur.

1. Installez une version prise en charge d'eDirectory sur le nouveau serveur.
2. Copiez sur le nouveau serveur les répliques d'eDirectory qui figurent sur le serveur d'Identity Manager actuel.

   Pour plus d'informations, reportez-vous à la section Gestion des répliques du *Guide d'administration de NetIQ eDirectory*.
3. Installez le moteur Identity Manager sur le nouveau serveur.

   Pour plus d'informations, reportez-vous à la Chapitre 9, « Installation du moteur Identity Manager, des applications d'identité et d'Identity Reporting », page 91.

29.5 Migration du pilote d'application utilisateur

Lors de la mise à niveau vers une nouvelle version d'Identity Manager ou de la migration vers un autre serveur, vous devrez peut-être importer un nouveau paquetage de base pour le pilote d'application utilisateur ou effectuer la mise à niveau du paquetage existant. Par exemple, la **version 2.2.0.20120516011608 de base de l'application utilisateur**.

Lorsque vous commencez à utiliser un projet Identity Manager, Designer vous invite automatiquement à importer de nouveaux paquetages dans le projet. Vous pouvez également importer manuellement le paquetage à ce moment-là.

29.5.1 Importation d'un nouveau paquetage de base

1. Ouvrez votre projet dans Designer.
2. Cliquez avec le bouton droit sur **Catalogue de paquetages > Importer le paquetage**, puis sélectionnez le paquetage approprié.

3 (Conditionnel) Si la boîte de dialogue Importer le paquetage ne répertorie pas le paquetage de base de l'application utilisateur, procédez comme suit :

3a Cliquez sur le bouton Parcourir.

3b Accédez à *racine_Designer*/packages/eclipse/plugins/NOVLUABASE_*version_dernier_paquetage*.jar.

3c Cliquez sur **OK**.

4 Cliquez sur **OK**.

29.5.2 Mise à niveau d'un paquetage de base existant

1 Ouvrez votre projet dans Designer.

2 Cliquez avec le bouton droit sur le pilote d'application utilisateur.

3 Cliquez sur **Pilote > Propriétés > Paquetages**.

Si le paquetage de base peut être mis à niveau, l'application présente une coche dans la colonne **Mises à niveau**.

4 Cliquez sur **Sélectionnez une opération** pour le paquetage pour lequel une mise à niveau est disponible.

5 Dans la liste déroulante, cliquez sur **Mettre à niveau**.

6 Sélectionnez la version que vous voulez mettre à niveau. Cliquez ensuite sur **OK**.

7 Cliquez sur **Appliquer**.

8 Remplissez les champs avec les informations appropriées pour mettre à niveau le paquetage. Cliquez ensuite sur **Suivant**.

9 Lisez le résumé de l'installation. Cliquez ensuite sur **Terminer**.

10 Fermez la page Gestion des paquetages.

11 Désélectionnez l'option **Afficher uniquement les versions de paquetage applicables**.

29.5.3 Déploiement du pilote migré

La migration du pilote n'est pas terminée tant que vous n'avez pas déployé le pilote de l'application utilisateur dans le coffre-fort d'identité. Après la migration, le projet se trouve dans un état dans lequel seule la totalité de la configuration migrée peut être déployée. Vous ne pouvez pas importer de définitions dans la configuration migrée. Une fois que la totalité de la configuration migrée a été déployée, cette restriction est levée et vous pouvez déployer des objets individuels et importer des définitions.

1 Ouvrez le projet dans Designer et exécutez le contrôleur de projet sur les objets migrés.

Pour plus d'informations, reportez-vous à la section « Validating Provisioning Objects » (Validation d'objets de provisioning) du manuel *NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications* (NetIQ Identity Manager - Guide de l'administrateur pour la conception des applications d'identité). En cas d'erreurs de validation pour la configuration, vous en êtes informé. Vous devez corriger ces erreurs avant de pouvoir déployer le pilote.

2 Dans la vue **Mode plan**, cliquez avec le bouton droit sur le pilote d'application utilisateur.

3 Sélectionnez **Déployer**.

4 Répétez cette procédure pour chaque pilote d'application utilisateur de l'ensemble de pilotes.

29.6 Mise à niveau des applications d'identité

Lorsque vous exécutez le programme de mise à niveau des applications d'identité, veillez à prendre en compte les considérations suivantes :

- Utilisez la même base de données que celle employée pour l'application utilisateur précédente. Il s'agit de l'installation à partir de laquelle vous effectuez la migration. Dans le programme d'installation, renseignez la **Base de données existante** pour le type de base de données.
- (Conditionnel) Si votre base de données existante s'exécute sur Oracle et si vous demandez au programme d'installation d'écrire un fichier SQL pour mettre à jour le schéma, vous devez effectuer des opérations supplémentaires. Pour plus d'informations, reportez-vous à la Section 29.7.1, « Préparation d'une base de données Oracle pour le fichier SQL », page 299.
- Vous pouvez indiquer un autre nom pour le contexte de l'application utilisateur.
- Spécifiez un emplacement d'installation différent de celui de l'installation précédente.
- Pointez vers une version prise en charge de Tomcat.
- N'utilisez pas de classement insensible à la casse pour votre base de données. Le classement ne tenant pas compte de la casse n'est pas pris en charge. Si vous utilisez ce classement, vous risquez d'être confronté à des erreurs de clé dupliquée lors de la migration. Si tel est le cas, vérifiez le classement et corrigez-le, puis réinstallez les applications d'identité.
- Comprenez les différences entre les fournisseurs pour la gestion des mots de passe. Le fournisseur par défaut est SSPR. Pour utiliser le fournisseur hérité d'Identity Manager ou un fournisseur externe, vous devez mettre à jour la configuration des applications d''identité après la mise à niveau.

Pour plus d'informations sur la mise à niveau des applications d'identité, reportez-vous à la Section 26.5, « Mise à niveau des applications d'identité », page 268.

29.7 Fin de la migration des applications d'identité

Après la mise à niveau ou la migration des applications d'identité, terminez le processus de migration.

29.7.1 Préparation d'une base de données Oracle pour le fichier SQL

Pendant du processus d'installation, il se peut que vous ayez choisi d'écrire un fichier SQL pour mettre à jour la base de données des applications d'identité. Si votre base de données s'exécute sur une plate-forme Oracle, vous devez effectuer quelques opérations avant de pouvoir exécuter le fichier SQL.

1 Dans la base de données, exécutez la commande suivante pour traiter les instructions SQL :

```
ALTER TABLE DATABASECHANGELOG ADD ORDEREXECUTED INT;
UPDATE DATABASECHANGELOG SET ORDEREXECUTED = -1;
ALTER TABLE DATABASECHANGELOG MODIFY ORDEREXECUTED INT NOT NULL;
ALTER TABLE DATABASECHANGELOG ADD EXECTYPE VARCHAR(10);
UPDATE DATABASECHANGELOG SET EXECTYPE = 'EXECUTED';
ALTER TABLE DATABASECHANGELOG MODIFY EXECTYPE VARCHAR(10) NOT NULL;
```

2 Exécutez la commande `updateSQL` suivante :

```
/opt/novell/idm/jre/bin/java -Xms256m -Xmx256m  -Dwar.context.name=IDMProv
-jar /opt/novell/idm/liquibase.jar
--databaseClass=com.novell.soa.persist.liquibase.OracleUnicodeDatabase
--driver=oracle.jdbc.driver.OracleDriver
--classpath=/root/ojdbc8.jar:/opt/novell/idm/tomcat/server/IDMProv/deploy/
IDMProv.war
--changeLogFile=DatabaseChangeLog.xml
--url="jdbcURL" --logLevel=debug
--logFile=/opt/novell/idm/db.out --contexts="prov,updatedb" --username=xxxx
--password=xxxx updateSQL  > /opt/novell/idm/db.sql
```

3 Dans un éditeur de texte, ouvrez le fichier SQL qui se trouve par défaut dans le répertoire *chemin_installation*/userapp/sql.

4 Insérez une barre oblique (/) après la définition de la fonction CONCAT_BLOB. Par exemple

```
  -- Changeset icfg-data-load.xml::700::IDMRBPM
CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB AS
                C BLOB;
            BEGIN
                DBMS_LOB.CREATETEMPORARY(C, TRUE);
                DBMS_LOB.APPEND(C, A);
                DBMS_LOB.APPEND(C, B);
                RETURN c;
            END;
/
```

5 Exécutez le fichier SQL.

REMARQUE : n'utilisez pas SQL*Plus pour exécuter le fichier SQL. La longueur des lignes du fichier dépasse 4 000 caractères.

29.7.2 Vidage du cache du navigateur

Avant de vous connecter aux applications d'identité, vous devez vider le cache du navigateur. Si vous ne videz pas le cache, vous risquez de rencontrer des erreurs d'exécution.

29.7.3 Mise à jour du paramètre Timeout maximum pour SharedPagePortlet

Si vous avez personnalisé l'un des paramètres ou l'une des préférences par défaut de SharedPagePortlet, il a été enregistré dans votre base de données et ce paramètre est écrasé. Par conséquent, l'accès à l'onglet Self-service d'identité ne permet pas toujours de mettre en surbrillance la page partagée correcte. Pour vous assurer que vous n'avez pas ce problème, procédez comme suit :

1 Connectez-vous en tant qu'administrateur de l'application utilisateur.

2 Accédez à **Administration > Administration des portlets**.

3 Développez **Navigation dans les pages partagées**.

4 Dans l'arborescence de portlets à gauche, cliquez sur **Navigation dans les pages partagées**.

5 À droite de la page, cliquez sur **Paramètres**.

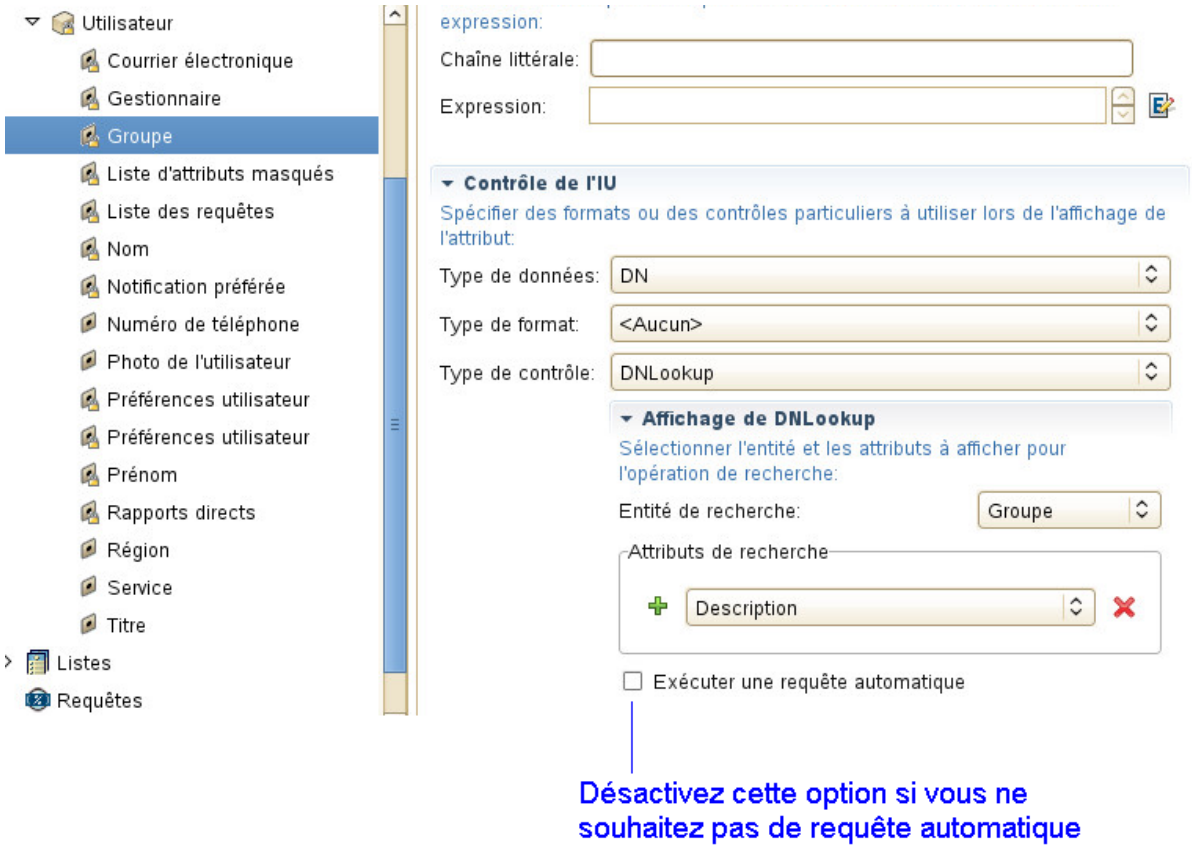
6 Assurez-vous que **Timeout maximum** soit défini sur 0.

7 Cliquez sur **Enregistrer les paramètres**.

29.7.4 Désactivation du paramètre de requête automatique pour les groupes

Par défaut, Affichage de DNLookup est activé pour l'entité Groupe dans la couche d'abstraction d'annuaire. Cela signifie que chaque fois que le sélecteur d'objet est ouvert pour une affectation de groupe, tous les groupes s'affichent par défaut sans qu'il ne soit nécessaire de les rechercher. Vous devez modifier ce paramètre, étant donné que la fenêtre de recherche de groupes doit s'afficher sans résultats tant que l'utilisateur n'a pas fourni d'entrée pour la recherche.

Pour modifier ce paramètre dans Designer, désélectionnez **Exécuter une requête automatique**, comme illustré ci-dessous :



29.8 Migration d'Identity Reporting

Une migration à partir d'une version précédente d'Identity Manager implique la migration d'Identity Reporting. Veillez à tenir compte des considérations suivantes :

- Migrez manuellement les données EASvers la base de données PostgreSQL.
- Nettoyez l'installation existante d'Identity Reporting.
- Effectuez une nouvelle installation d'Identity Reporting 4.7 sur le nouveau serveur.
- Indiquez l'emplacement d'installation du service d'authentification et du coffre-fort d'identité existants pour la nouvelle version d'Identity Reporting installée.

29.8.1 Migration d'Event Auditing Service vers Sentinel Log Management for IGA

Cette section explique comment migrer des données SIEM à partir de la base de données EAS vers une base de données PostgreSQL prise en charge.

Vous devez créer les rôles et espaces de table requis pour éviter tout échec de la migration.

Préparation de la nouvelle base de données PostgreSQL

1. Arrêtez EAS pour veiller à ce qu'aucun événement ne soit envoyé au serveur EAS.
2. À l'aide d'iManager, arrêtez le pilote DCS :
   - **2a** Connectez-vous à iManager.
   - **2b** Arrêtez le pilote DCS.
   - **2c** Changez les propriétés du pilote pour modifier l'option de démarrage sur **Manuel**.

     Cette étape permet d'éviter que le pilote ne démarre automatiquement.
3. Exécutez les commandes SQL suivantes pour créer les rôles requis, l'espace de table et la base de données à l'aide de `PGAdmin`.

   Cette étape permet d'éviter tout échec lors de la migration.

   - **3a** Exécutez les commandes suivantes pour créer les rôles requis :

```
CREATE ROLE esec_app
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE esec_user
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE admin LOGIN
  ENCRYPTED PASSWORD '<specify the password for admin>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO admin;

CREATE ROLE appuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for appuser>'
  NOSUPERUSER INHERIT NOCREATEDB CREATEROLE;
GRANT esec_app TO appuser;

CREATE ROLE dbauser LOGIN
  ENCRYPTED PASSWORD '<specify the password for dbauser>'
  SUPERUSER INHERIT CREATEDB CREATEROLE;

CREATE ROLE idmrptsrv LOGIN
  ENCRYPTED PASSWORD '<specify the password for idmrptsrv>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO idmrptsrv;

CREATE ROLE idmrptuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for idmrptuser>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE rptuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for rptuser>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO rptuser;
```

3b Exécutez la commande suivante pour créer des espaces de table :

```
CREATE TABLESPACE sendata1
 OWNER dbauser
 LOCATION '<provide the location where table space has to be created>';
```

Exemples :

```
CREATE TABLESPACE sendata1
  OWNER dbauser
  LOCATION '</opt/netiq/idm/apps/postgres/data>';
```

3c Exécutez la commande suivante pour créer une base de données SIEM :

```
CREATE DATABASE "SIEM"
  WITH OWNER = dbauser
       ENCODING = 'UTF8'
       TABLESPACE = sendata1
       CONNECTION LIMIT = -1;
```

Exportation des données à partir d'EAS

1. Arrêtez EAS pour veiller à ce qu'aucun événement ne soit envoyé au serveur EAS.
2. À l'aide d'iManager, arrêtez le pilote DCS :
   - **2a** Connectez-vous à iManager.
   - **2b** Arrêtez le pilote DCS.
   - **2c** Changez les propriétés du pilote pour modifier l'option de démarrage sur **Manuel**.

     Cette étape permet d'éviter que le pilote ne démarre automatiquement.
3. Exportez les données de la base de données EAS vers un fichier :
   - **3a** Connectez-vous au compte utilisateur EAS :

     ```
     # su - novleas
     ```
   - **3b** Spécifiez un emplacement auquel l'utilisateur EAS a totalement accès, par exemple, `/home/novleas`.
   - **3c** Accédez au répertoire d'installation PostgreSQL et exécutez les commandes suivantes :

     Exemples :

     ```
     export PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/bin/:$PATH
     ```

     ```
     export LD_LIBRARY_PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/lib/
     :$LD_LIBRARY_PATH
     ```
   - **3d** Exportez les données dans un fichier `.sql` à l'aide de la commande suivante :

     ```
     ./pg_dump -p <numéro_port> -U <nom_utilisateur> -d <nom_bd> -f
     <emplacement_exportation>
     ```

     Exemples :

     ```
     ./pg_dump -p 15432 -U dbauser SIEM -f /home/novleas/SIEM.sql
     ```

Importation des données dans la nouvelle base de données PostgreSQL

1. Arrêtez EAS pour veiller à ce qu'aucun événement ne soit envoyé au serveur EAS.
2. À l'aide d'iManager, arrêtez le pilote DCS :
   - **2a** Connectez-vous à iManager.
   - **2b** Arrêtez le pilote DCS.

2c Changez les propriétés du pilote pour modifier l'option de démarrage sur **Manuel**.

Cette étape permet d'éviter que le pilote ne démarre automatiquement.

3 Importez les données dans la nouvelle base de données PostgreSQL:

3a (Conditionnel) Créez un utilisateur `postgres`.

Ceci est spécifique à Windows uniquement. Un utilisateur est créé automatiquement sous Linux.

3b Copiez le fichier exporté à l'Étape 3d à un emplacement auquel l'utilisateur postgres a totalement accès. Par exemple, `/opt/netiq/idm/postgres`

3c Exécutez la commande suivante pour importer des données dans la base de données PostgreSQL.

```
psql -d <nom_Bdd> -U <nom_utilisateur> -f
<chemin_complet_emplacement_fichier_exporté>
```

Exemples :

```
psql -d SIEM -U postgres -f /opt/netiq/idm/apps/postgres/SIEM.sql
```

4 Recherchez les éventuelles erreurs dans le journal de migration et résolvez-les.

REMARQUE : les rapports Identity Manager 4.7 n'utilisent pas les données d'audit migrées d'EAS vers SLM for IGA, mais les données d'audit synchronisées directement à partir de SLM for IGA.

29.8.2 Configuration du nouveau serveur de création de rapports

Après avoir importé les données EAS dans la nouvelle base de données PostgreSQL, installez une nouvelle application de création de rapports sur un autre serveur et faites-le pointer vers le coffre-fort d'identité et le service d'authentification existants.

1 Arrêtez le service Tomcat existant (qui s'exécute sur votre application de création de rapports existante).

2 Créez une sauvegarde de vos fichiers WAR Identity Reporting à partir du répertoire `tomcat/webapps` et du répertoire privé de `Reporting` situé à l'emplacement `/opt/netiq/idm/apps/` en dehors du chemin d'installation de `Tomcat`.

3 Supprimez les entrées EAS du fichier `server.xml` existant.

4 Créez une nouvelle base de données dans la base de données PostgreSQL vers laquelle les données EAS ont été migrées.

5 Installez et configurez Identity Reporting sur le nouveau serveur et faites-le pointer vers le service Single Sign-on et le coffre-fort d'identité existants. Pour plus d'informations, reportez-vous à la Chapitre 10, « Configuration des composants installés », page 101.

6 Faites pointer le service Single Sign-on existant sur la nouvelle version installée d'Identity Reporting, modifiez les entrées de configuration d'Identity Reporting à l'aide de l'utilitaire de mise à jour de la configuration.

7 Redémarrez le serveur Tomcat exécutant le service Single Sign-on existant.

29.8.3 Création de la stratégie de synchronisation des données

Après avoir configuré le serveur de création de rapports, vous devez créer la stratégie de synchronisation des données pour transférer des événements SLM for IGA vers la base de données de création de rapports. Les considérations suivantes s'appliquent lors de la mise à niveau vers Identity Reporting 4.7.

REMARQUE

- Si vous effectuez une mise à niveau à partir d'Identity Reporting 4.5.6 vers Identity Reporting 4.7, vous devez créer une nouvelle stratégie sur la page Services de collecte de données d'Identity Manager. Pour plus d'informations, reportez-vous à la section About the Data Sync Policies tab (À propos de l'onglet Stratégies de synchronisation des données) du Administrator Guide to NetIQ Identity Reporting (Guide de l'administrateur de NetIQ Identity Reporting).
- Si vous mettez à niveau Identity Reporting 4.6.x vers Identity Reporting 4.7, suivez la procédure de la section Problèmes de mise à niveau d'Identity Manager des Notes de version de NetIQ Identity Manager 4.7.

30 Désinstallation des composants Identity Manager

Cette section décrit la procédure de désinstallation des composants Identity Manager. Certains composants présentent des conditions préalables à la désinstallation. Veillez à lire la section complète pour chaque composant avant de commencer la procédure de désinstallation.

REMARQUE : vous devez arrêter tous les services tels que Tomcat, PostgreSQL et ActiveMQ avant de désinstaller les composants Identity Manager.

30.1 Suppression d'objets du coffre-fort d'identité

La première étape de la désinstallation d'Identity Manager consiste à effacer tous les objets Identity Manager du coffre-fort d'identité. Lorsque l'ensemble de pilotes est créé, l'assistant vous invite à convertir l'ensemble de pilotes en partition. Si des objets Ensemble de pilotes sont des objets Racine de partition dans eDirectory, vous devez fusionner la partition avec la partition parente avant de pouvoir supprimer l'objet Ensemble de pilotes.

Pour supprimer des objets du coffre-fort d'identité :

1. Vérifiez l'état de santé de la base de données eDirectory, puis corrigez les erreurs qui se produisent avant de poursuivre.

   Pour plus d'informations, reportez-vous à la section « Préservation de l'état de santé d'eDirectory » du *Guide d'administration de NetIQ eDirectory*.
2. Connectez-vous à iManager en tant qu'administrateur avec tous les droits dans l'arborescence eDirectory.
3. Sélectionnez **Partitions et répliques > Fusionner la partition**.
4. Naviguez jusqu'à l'objet Ensemble des pilotes qui soit l'objet racine de partition et sélectionnez-le, puis cliquez sur **OK**.
5. Attendez que la procédure de fusion soit terminée, puis cliquez sur **OK**.
6. Effacez l'objet Ensemble des pilotes.

   Lorsque vous supprimez l'objet Ensemble des pilotes, le processus supprime tous les objets Pilote associés à cet ensemble des pilotes.
7. Répétez la procédure de l'Étape 3 jusqu'à l'Étape 6 pour chaque objet Ensemble des pilotes se trouvant dans la base de données eDirectory, jusqu'à ce qu'ils soient supprimés.
8. Répétez l'Étape 1 pour vous assurer que toutes les fusions ont été réalisées et que tous les objets ont été supprimés.

30.2 Désinstallation du moteur Identity Manager

Le programme d'installation fournit un script de désinstallation d'Identity Manager. Ce script vous permet de supprimer tous les services, paquetages et répertoires créés lors de l'installation.

REMARQUE : avant de désinstaller le moteur Identity Manager, préparez le coffre-fort d'identité. Pour plus d'informations, reportez-vous à la Section 30.1, « Suppression d'objets du coffre-fort d'identité », page 307.

Pour désinstaller le moteur Identity Manager :

1. Accédez à l'emplacement où vous avez monté le fichier ISO lors de l'installation.
2. À partir du répertoire racine du fichier `.iso`, exécutez la commande suivante :

   ```
   ./uninstall.sh
   ```

3. Spécifiez les composants à désinstaller.

   Par exemple, spécifiez *1* pour désinstaller le moteur Identity Manager. Vous pouvez également désinstaller plusieurs composants simultanément. Par exemple, spécifiez *1, 2, 3* pour désinstaller respectivement le moteur Identity Manager, le chargeur distant et l'agent de dissémination (fan-out).

30.3 Désinstallation des applications d'identité

1. Accédez à l'emplacement où vous avez monté le fichier `.iso` lors de l'installation.
2. À partir du répertoire racine du fichier `.iso`, exécutez la commande suivante :

   ```
   ./uninstall.sh
   ```

3. Spécifiez les composants à désinstaller.

   Par exemple, spécifiez *1* pour désinstaller les applications d'identité.

30.4 Désinstallation des composants du Identity Reporting

Vous devez désinstaller les composants Identity Reporting dans l'ordre suivant :

1. Supprimez les pilotes. Pour plus d'informations, reportez-vous à la Section 30.4.1, « Suppression des pilotes de création de rapports », page 309.
2. Supprimez Identity Reporting. Pour plus d'informations, reportez-vous à la Section 30.4.2, « Désinstallation d'Identity Reporting », page 309.
3. Supprimez Sentinel. Pour plus d'informations, reportez-vous à la Section 30.4.3, « Désinstallation de Sentinel », page 309.

REMARQUE : pour économiser de l'espace disque, les programmes d'installation d'Identity Reporting n'installent pas de machine virtuelle java (JVM). Par conséquent, pour désinstaller un ou plusieurs composants, assurez-vous qu'une machine virtuelle Java est disponible et qu'elle figure dans la variable PATH. Si une erreur se produit au cours d'une désinstallation, ajoutez l'emplacement d'une machine virtuelle Java dans la variable d'environnement PATH locale, puis réexécutez le programme de désinstallation.

30.4.1 Suppression des pilotes de création de rapports

Vous pouvez utiliser Designer ou iManager pour supprimer les pilotes du service de collecte de données et de la passerelle système gérée.

1. Arrêtez les pilotes. En fonction du composant utilisé, effectuez l'une des opérations suivantes :
   - **Designer :** pour chaque pilote, cliquez avec le bouton droit sur la ligne du pilote, puis cliquez sur **En direct > arrêter le pilote**.
   - **iManager :** sur la page Présentation de l'ensemble de pilotes, cliquez dans le coin supérieur droit de l'image de chaque pilote, puis cliquez sur **Arrêter le pilote**.
2. Supprimez les pilotes. En fonction du composant utilisé, effectuez l'une des opérations suivantes :
   - **Designer :** pour chaque pilote, cliquez avec le bouton droit sur la ligne du pilote, puis cliquez sur **Supprimer**.
   - **iManager :** sur la page Présentation de l'ensemble de pilotes, cliquez sur **Pilotes > Supprimer le pilote**, puis sur le pilote à supprimer.

30.4.2 Désinstallation d'Identity Reporting

Avant de supprimer Identity Reporting, assurez-vous d'avoir supprimé les pilotes du service de collecte de données et de la passerelle système gérée. Pour plus d'informations, reportez-vous à la Section 30.4.1, « Suppression des pilotes de création de rapports », page 309.

1. Accédez à l'emplacement où vous avez monté le fichier `.iso` lors de l'installation.
2. À partir du répertoire racine du fichier `.iso`, exécutez la commande suivante :

   ```
   ./uninstall.sh
   ```
3. Spécifiez les composants à désinstaller.

   Par exemple, spécifiez *1* pour désinstaller Identity Reporting.

30.4.3 Désinstallation de Sentinel

1. Connectez-vous au serveur Sentinel.
2. Accédez au répertoire contenant le script de désinstallation :

   ```
   /opt/novell/sentinel/setup/
   ```
3. Exécutez la commande suivante :

   ```
   ./uninstall.sh
   ```
4. Lorsque vous êtes invité à confirmer que vous souhaitez procéder à la désinstallation, appuyez sur y (oui).

   Le script arrête d'abord le service et le supprime ensuite complètement.

30.5 Désinstallation de Designer

1. Fermez Designer.
2. Désinstallez Designer.

Accédez au répertoire contenant le script de désinstallation, qui est par défaut `<répertoire_installation>/designer/UninstallDesigner/Uninstall Designer for Identity Manager`.

Pour exécuter le script, saisissez `./uninstall`

30.6 Désinstallation d'Analyzer

1. Fermez Analyzer.
2. Désinstallez Analyzer en fonction du système d'exploitation :

   Accédez au script `Uninstall Analyzer for Identity Manager`, situé par défaut dans le répertoire `<répertoire_installation>/analyzer/UninstallAnalyzer`.

   Pour exécuter le script, saisissez `./Désinstaller`

31 Dépannage

Cette section fournit des informations utiles pour le dépannage des problèmes liés à l'installation d'Identity Manager. Pour plus d'informations sur le dépannage d'Identity Manager, reportez-vous au guide du composant spécifique.

31.1 Dépannage concernant l'installation de l'application utilisateur et de RBPM

Le tableau suivant répertorie les problèmes susceptibles de se poser et les actions suggérées pour les résoudre. Si le problème persiste, contactez votre représentant NetIQ.

Point	Actions suggérées
Lorsque vous activez l'audit CEF pour OSP à partir de l'utilitaire configupdate (`configupdate.sh`), vos tentatives de connexion à IDMRPT échouent.	Procédez comme suit pour résoudre ce problème : 1. Accédez aux fichiers `ism-configuration.properties` et `idmrptcore_logging.xml` situés dans le répertoire `/opt/netiq/idm/apps/tomcat/conf`. 2. Modifiez respectivement les fichiers `ism-configuration.Properties` et `idmrptcore_logging.xml`. 3. Modifiez les valeurs de **com.netiq.ism.audit.cef.protocol** et **<protocole>** de **tcp** en **TCP** respectivement dans les fichiers `ism-configuration.properties` et `idmrptcore_logging.xml`. 4. Relancez Tomcat.
Si vos applications d'identité et Identity Reporting sont installés sur le même serveur et que vous sélectionnez l'option **Startup** (Au démarrage) lors de la création de la base de données, vous remarquerez que le journal contient quelques exceptions.	Pour effacer les exceptions, redémarrez Tomcat manuellement.
Vous souhaitez modifier un ou plusieurs des paramètres de configuration suivants de l'application utilisateur créés pendant l'installation : ◆ Connexions et certificats du coffre-fort d'identité ◆ Paramètres de messagerie électronique ◆ Groupes d'utilisateurs et identité de l'utilisateur du moteur Identity Manager ◆ Paramètres Access Manager ou iChain	Exécutez l'utilitaire de configuration indépendamment du programme d'installation. **Linux** : exécutez la commande suivante à partir du répertoire d'installation (par défaut, `/opt/netiq/idm/apps/configupdate/`) : `./configupdate.sh`

Point	Actions suggérées
Le démarrage de Tomcat provoque l'exception suivante : `port 8180 already in use`	Arrêtez toutes les instances de Tomcat (ou autre logiciel de serveur) qui pourraient déjà être en cours d'exécution. Si vous reconfigurez Tomcat de façon à ce qu'il utilise un autre port que le port 8180, modifiez les paramètres `config` du pilote de l'application utilisateur.
Au démarrage de Tomcat, l'application signale qu'elle ne trouve pas de certificats approuvés.	Veillez à démarrer Tomcat en utilisant le JDK spécifié pendant l'installation de l'application utilisateur.
Impossible de se connecter à la page d'administration du portail.	Assurez-vous que le compte administrateur de l'application utilisateur existe bien. Ce compte est différent de votre compte administrateur iManager.
Impossible de créer de nouveaux utilisateurs, même avec le compte administrateur.	L'administrateur de l'application utilisateur doit être un ayant droit du conteneur maître et avoir des droits de superviseur. Vous pouvez essayer de configurer les droits de l'administrateur de l'application utilisateur pour qu'ils soient équivalents à ceux de l'administrateur LDAP (via iManager).
Le démarrage du serveur d'applications génère des erreurs de keystore.	Votre serveur d'applications n'utilise pas le JDK spécifié pendant l'installation de l'application utilisateur. Utilisez la commande `keytool` pour importer le fichier de certificat : `keytool -import -trustcacerts -alias` *`aliasName`* `-file` *`certFile`* `-keystore ..\lib\security\cacerts -storepass changeit` ◆ Remplacez *aliasName* par un nom unique de votre choix pour ce certificat. ◆ Remplacez *certFile* par le chemin complet et le nom de votre fichier de certificat. ◆ Le mot de passe du keystore par défaut est `changeit` (si vous avez un mot de passe différent, indiquez-le).
La notification par message électronique n'est pas envoyée.	Exécutez l'utilitaire `configupdate` pour vérifier si vous avez fourni des valeurs pour les paramètres de configuration suivants de l'application utilisateur : **Expéditeur du message électronique** et **Hôte du message électronique**. **Linux** : exécutez la commande suivante à partir du répertoire d'installation (par défaut, `/opt/netiq/idm/apps/UserApplication/`) : `./configupdate.sh`

31.2 Dépannage des problèmes de connexion

Le tableau suivant répertorie les problèmes susceptibles de se poser et les actions suggérées pour les résoudre. Si le problème persiste, contactez votre représentant NetIQ.

Point	Actions suggérées
L'utilisateur ne parvient pas à se connecter à un environnement à grande échelle (> 2 millions d'objets)	Ajoutez un index pour l'attribut `mail(adresse de messagerie Internet)` avec la règle définie comme `Value` sur le serveur maître et le serveur de répliques d'eDirectory.
Lorsque vous vous déconnectez de la page des applications d'identité, SSPR affiche une erreur `5053 ERROR_APP_UNAVALIABLE`.	Ignorez cette erreur. Elle ne provoque aucune perte de fonctionnalité.
Aucune réponse de vérification d'identité n'est demandée lors de la première connexion aux applications d'identité	1. Vérifiez que le serveur SSPR possède un certificat créé à l'aide du nom de domaine complet. 2. Connectez-vous au serveur de l'application utilisateur et lancez l'utilitaire ConfigUpdate (`/opt/netiq/idm/apps/configupdate/`). 3. Accédez à **Clients SSO > Self Service Password Reset** et assurez-vous que les paramètres sont corrects. Si SSPR est installé sur un serveur distinct, assurez-vous que le certificat SSPR est importé dans le fichier `idm.jks` situé sur le serveur de l'application utilisateur à l'emplacement `/opt/netiq/idm/apps/tomcat/conf`.

Point	Actions suggérées
Le navigateur affiche une page vierge lors de l'accès à l'URL de SSPR	Cela se produit lorsque SSPR n'est pas configuré correctement avec OSP. Le journal SSPR affiche les informations suivantes : `2018-01-24T22:24:02Z, ERROR, oauth.OAuthConsumerServlet, 5071 ERROR_OAUTH_ERROR (unexpected error communicating with oauth server: password.pwm.error.PwmUnrecoverableException : 5071 ERROR_OAUTH_ERROR (io error during oauth code resolver http request to oauth server: Certificate for <IP> doesn't match any of the subject alternative names: [IP]))` 1. Vérifiez que le serveur Tomcat sur lequel OSP est en cours d'exécution dispose d'un certificat valide créé à l'aide d'un nom de domaine complet. Connectez-vous au serveur de l'application utilisateur et lancez l'utilitaire ConfigUpdate. Accédez à **Clients SSO > Self Service Password Reset** et assurez-vous que les paramètres sont corrects. 2. Connectez-vous à SSPR en ignorant la méthode de connexion OSP. (par exemple, `https://<IP serveur SSPR>:<port>/sspr/private/Login?sso=false`) 3. Accédez à **Configuration Editor** (Éditeur de configuration) dans le coin supérieur droit de la page. 4. Spécifiez **Configure Password** (Configurer le mot de passe), puis cliquez sur **Sign In** (Connexion). 5. Accédez à **LDAP > LDAP Directories > Default > Connection** (LDAP > Annuaires LDAP > Valeur par défaut > Connexion). 6. Si le certificat LDAP n'est pas correct, cliquez sur **Clear** (Effacer). 7. Pour réimporter le certificat, cliquez sur **Import From Server** (Importer à partir du serveur). 8. Accédez à **Settings >Single Sign On (SSO)Client > OAuth** (Paramètres > Client Single Sign-on (SSO) > OAuth) et vérifiez que le certificat sous **OAUTH Web Service Server Certificate** (Certificat de serveur du service Web OAUTH) est correct. 9. Si le certificat n'est pas correct, cliquez sur **Clear** (Effacer). 10. Pour réimporter le certificat, cliquez sur **Import From Server** (Importer à partir du serveur).

Point	Actions suggérées
Erreur lorsque l'utilitaire ConfigUpdate est lancé à partir d'un autre répertoire	L'utilitaire ConfigUpdate signale des erreurs. Il n'enregistre aucune modification. Par exemple, si vous lancez l'utilitaire configupdate à l'aide de la commande `/opt/netiq/idm/apps/configupdate/configupdate.sh` , il ne se lance pas. À la place, accédez au répertoire `/opt/netiq/idm/apps/configupdate/`, puis exécutez la commande `./configupdate.sh`.

31.3 Dépannage en cas de désinstallation

Le tableau suivant répertorie les problèmes susceptibles de se poser et les actions suggérées pour les résoudre. Si le problème persiste, contactez votre représentant NetIQ.

Point	Actions suggérées
Un message indique que la procédure de désinstallation est incomplète, mais le fichier journal n'indique aucun échec.	La procédure n'a pas pu supprimer le répertoire `netiq` qui contient les fichiers d'installation par défaut. Vous pouvez supprimer ce répertoire si vous avez supprimé tous les logiciels NetIQ de votre ordinateur.

A Utilisation de plusieurs Instances du coffre-fort d'identité

Cette section décrit les conditions préalables, les considérations, ainsi que la configuration système requise pour installer le coffre-fort d'identité. Tout d'abord, consultez la liste de contrôle pour comprendre la procédure d'installation.

A.1 Présentation des objets Identity Manager dans eDirectory

La liste ci-dessous décrit les principaux objets Identity Manager stockés dans eDirectory et les relations qui les unissent. La procédure d'installation ne crée pas d'objets Identity Manager. C'est vous qui devez les créer lors de la configuration de la solution Identity Manager.

- **Ensemble de pilotes :** un ensemble de pilotes est un conteneur pour les pilotes Identity Manager et les objets de bibliothèque. Vous ne pouvez activer qu'un seul ensemble de pilotes à la fois sur un serveur. Cependant, plusieurs serveurs peuvent être associés à un même ensemble de pilotes. De plus, un pilote peut être associé à plus d'un serveur à la fois. Toutefois, le pilote ne doit être exécuté que sur un serveur à la fois. Il doit être à l'état désactivé sur les autres serveurs. Le serveur Identity Manager doit être installé sur tous les serveurs associés à un ensemble de pilotes.
- **Bibliothèque :** l'objet Bibliothèque est un espace de stockage des stratégies souvent utilisées et pouvant être référencées depuis plusieurs sites. La bibliothèque est stockée dans l'ensemble de pilotes. Vous pouvez placer une stratégie dans la bibliothèque, de façon à ce qu'elle puisse être référencée par chaque pilote de l'ensemble.
- **Pilote :** un pilote assure la connexion entre une application et le coffre-fort d'identité. Il permet également de synchroniser et de partager des données entre différents systèmes. Le pilote est conservé dans l'ensemble de pilotes.
- **Travail :** un travail automatise une tâche récurrente. Par exemple, un travail peut configurer un système afin qu'il désactive un compte un jour donné ou qu'il initie un workflow pour demander l'extension de l'accès d'une personne à une ressource de l'entreprise. Le travail est stocké dans l'ensemble de pilotes.

A.2 Réplication des objets nécessaires à Identity Manager sur le serveur

Si votre environnement Identity Manager nécessite plusieurs serveurs afin d'exécuter plusieurs pilotes Identity Manager, votre plan doit garantir que certains objets eDirectory sont répliqués sur les serveurs sur lesquels vous voulez exécuter ces pilotes.

Vous pouvez utiliser des répliques filtrées, à condition que tous les objets et attributs dont le pilote a besoin pour lire ou synchroniser soient inclus dans la réplique filtrée.

N'oubliez pas que vous devez donner à l'objet du pilote Identity Manager des droits eDirectory suffisants sur tout objet qu'il doit synchroniser, soit en lui accordant explicitement des droits soit en rendant la sécurité de l'objet du pilote équivalente à un objet qui dispose des droits souhaités.

Un serveur eDirectory exécutant un pilote Identity Manager (ou auquel le pilote fait référence si vous utilisez le chargeur distant) doit contenir une réplique maîtresse ou lecture-écriture des éléments suivants :

- L'objet Ensemble des pilotes de ce serveur.

  Vous devez avoir un objet Ensemble des pilotes pour chaque serveur qui exécute Identity Manager. À moins d'avoir des besoins particuliers, n'associez pas plusieurs serveurs au même objet Ensemble des pilotes.

  REMARQUE : lorsque vous créez un objet Ensemble de pilotes, une partition distincte est créée par défaut. NetIQ recommande la création d'une partition séparée sur l'objet Ensemble des pilotes. Pour que Identity Manager fonctionne, le serveur doit comporter une réplique complète de l'objet Ensemble des pilotes. La partition n'est pas obligatoire si le serveur dispose d'une réplique complète de l'emplacement d'installation de l'objet Ensemble des pilotes.

- L'objet Serveur de ce serveur.

  L'objet Serveur est nécessaire car il permet au pilote de générer des paires clés pour les objets. Il est également important pour l'authentification du chargeur distant.

- Les objets que vous souhaitez que cette instance du pilote synchronise.

  Le pilote ne peut pas synchroniser des objets à moins qu'une réplique de ces objets se trouve sur le même serveur que le pilote. En fait, un pilote Identity Manager synchronise les objets dans *tous* les conteneurs qui sont répliqués sur le serveur à moins que vous ne créiez des règles pour le filtrage des étendues indiquant autre chose.

  Ainsi, si vous souhaitez qu'un pilote synchronise tous les objets utilisateur, la manière la plus simple consiste à utiliser une instance du pilote sur un serveur détenant une réplique maîtresse ou lecture-écriture de tous vos utilisateurs.

  Cependant, de nombreux environnements n'ont pas de serveur avec une réplique de tous les utilisateurs. L'ensemble des utilisateurs est plutôt réparti sur plusieurs serveurs. Dans ce cas, vous disposez de trois options :

  - **Regrouper les utilisateurs sur un seul serveur.** Pour créer un seul serveur avec tous les utilisateurs, ajoutez des répliques sur un serveur existant. Les répliques filtrées peuvent être utilisées pour réduire la taille de la base de données eDirectory si nécessaire, à condition que les objets et attributs utilisateur nécessaires fassent partie de la réplique filtrée.
  - **Utilisez plusieurs instances du pilote sur plusieurs serveurs, avec un filtrage des étendues.** Si vous ne voulez pas regrouper les utilisateurs sur un seul serveur, vous devez déterminer l'ensemble de serveurs qui contiendra tous les utilisateurs et configurer une instance du pilote Identity Manager sur chacun de ces serveurs.

Pour éviter que les instances séparées d'un pilote tentent de synchroniser les mêmes utilisateurs, vous devez utiliser le filtrage des étendues pour définir les utilisateurs que chaque instance du pilote doit synchroniser. Le filtrage des étendues signifie que vous ajoutez des règles à chaque pilote pour limiter l'étendue de la gestion du pilote à des conteneurs spécifiques. Reportez-vous à la section « Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents » page 319.

- **Utilisez plusieurs instances du pilote sur plusieurs serveurs, sans filtrage des étendues.** Si vous voulez exécuter plusieurs instances d'un pilote sur différents serveurs sans utiliser de répliques filtrées, vous devez définir des stratégies sur les différentes instances du pilote qui permettent au pilote de traiter différents ensembles d'objets au sein du même coffre-fort d'identité.

- Les objets Modèle que vous voulez que le pilote utilise lors de la création d'utilisateurs, si vous choisissez d'utiliser des modèles.

  Les pilotes Identity Manager n'exigent pas que vous indiquiez des objets Modèle eDirectory pour créer des utilisateurs. Cependant, si vous indiquez qu'un pilote doit utiliser un modèle lors de la création d'utilisateurs dans eDirectory, l'objet Modèle doit être répliqué sur le serveur sur lequel le pilote est exécuté.

- Tout conteneur que vous voulez que le pilote Identity Manager utilise pour la gestion des utilisateurs.

  Par exemple, si vous avez créé un conteneur nommé Utilisateurs inactifs qui contient les comptes utilisateur désactivés, vous devez avoir une réplique maîtresse ou lisible/inscriptible (de préférence une réplique maîtresse) de ce conteneur sur le serveur sur lequel le pilote est exécuté.

- Tout autre objet auquel le pilote doit se rapporter (par exemple, les objets Bon de travail pour le pilote).

  Si les autres objets ne doivent être que lus par le pilote, la réplique de ces objets sur le serveur peut être une réplique en lecture seule.

A.3 Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents

Le filtrage des étendues signifie l'ajout de règles à chaque pilote pour limiter l'étendue des actions du pilote à des conteneurs spécifiques. Voici deux situations dans lesquelles vous devez utiliser le filtrage des étendues :

- Vous voulez que le pilote ne synchronise que les utilisateurs d'un conteneur particulier.

  Par défaut, un pilote Identity Manager synchronise les objets de tous les conteneurs répliqués sur le serveur sur lequel il est exécuté. Pour limiter cette étendue, vous devez créer des règles de filtrage des étendues.

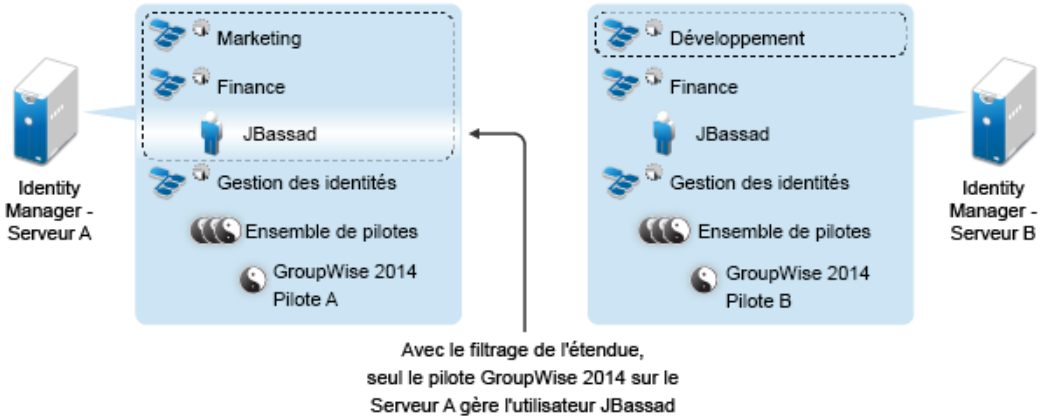
- Vous voulez qu'un pilote Identity Manager synchronise tous les utilisateurs, mais vous ne voulez pas que tous les utilisateurs soient répliqués sur le même serveur.

  Pour synchroniser tous les utilisateurs sans les répliquer sur un seul serveur, vous devez déterminer l'ensemble de serveurs qui contient tous les utilisateurs, puis créer une instance du pilote Identity Manager sur chacun de ces serveurs. Pour éviter que deux instances du pilote tentent de synchroniser les mêmes utilisateurs, vous devez utiliser le filtrage des étendues pour définir les utilisateurs que chaque instance du pilote doit synchroniser.

REMARQUE : vous devez utiliser le filtrage des étendues même si les répliques de votre serveur ne sont pas en chevauchement pour l'instant. À l'avenir, des répliques peuvent être ajoutées à vos serveurs et un chevauchement peut être créé involontairement. Si le filtrage des étendues est en place, vos pilotes Identity Manager ne tentent pas de synchroniser les mêmes utilisateurs, même si des répliques sont ajoutées à vos serveurs à l'avenir.

La Figure A-1 page 320 montre un coffre-fort d'identité avec trois conteneurs d'utilisateurs : Marketing, Finance et Développement. Elle montre également un conteneur Identity Manager conservant les ensembles des pilotes. Chacun de ces conteneurs constitue une partition distincte. Dans cet exemple, l'administrateur d'Identity Manager a deux serveurs de coffre-fort d'identité, à savoir les serveurs A et B. Aucun d'eux ne contient une copie de tous les utilisateurs. Chaque serveur contient deux des trois partitions, l'étendue de ce que les serveurs peuvent contenir est donc en chevauchement.

Figure A-1 *Le filtrage des étendues définit les pilotes qui synchronisent chaque conteneur*



L'administrateur souhaite que tous les utilisateurs de l'arborescence soient synchronisés par le pilote GroupWise 2014, mais ne veut pas regrouper les répliques des utilisateurs sur un seul serveur. Il choisit plutôt d'utiliser deux instances du pilote GroupWise 2014, une sur chaque serveur. Il installe Identity Manager et configure le pilote GroupWise 2014 sur chaque serveur Identity Manager.

Le serveur A contient des répliques des conteneurs Marketing et Finance. Il contient également une réplique du conteneur Gestion des identités, dans lequel figurent l'ensemble des pilotes pour le serveur A et l'objet Pilote GroupWise 2014 pour le serveur A.

Le serveur B contient, quant à lui, des répliques des conteneurs Développement et Finance ainsi que le conteneur Gestion des identités, dans lequel figurent l'ensemble des pilotes pour le Serveur B et l'objet Pilote GroupWise 2014 pour le serveur B.

Comme le serveur A et le serveur B contiennent une réplique du conteneur Finance, ils contiennent tous deux l'utilisateur JBassad, qui est dans le conteneur Finance. Sans filtrage des étendues, le pilote GroupWise 2014 A et le pilote GroupWise 2014 B synchroniseraient tous les deux l'utilisateur JBassad. Le filtrage des étendues empêche les deux instances du pilote de gérer le même utilisateur, car il définit les pilotes qui synchronisent chaque conteneur.

Identity Manager comporte des règles prédéfinies. Deux règles facilitent le filtrage des étendues : **Transformation de l'événement - Filtrage de l'étendue - Inclure la/les sous-arborescence(s)** et **Transformation de l'événement - Filtrage de l'étendue - Exclure la/les sous-arborescence(s)**. Pour plus d'informations, reportez-vous au manuel *NetIQ Identity Manager Understanding Policies Guide* (Guide de présentation des stratégies de NetIQ Identity Manager).

Dans cet exemple, vous utiliseriez la règle prédéfinie Inclure les sous-arborescences pour le serveur A et le serveur B. Vous définiriez l'étendue de chaque pilote différemment de façon à ce qu'ils ne synchronisent que les utilisateurs des conteneurs indiqués. Le serveur A synchroniserait le conteneur Marketing et Finance. Le serveur B synchroniserait le conteneur Développement.

A.4 Présentation des paquetages Linux du kit d'installation du coffre-fort d'identité

NetIQ eDirectory contient un système de paquetages Linux. Il s'agit d'une collection d'outils visant à simplifier l'installation et la désinstallation de différents composants d'eDirectory. Ces paquetages contiennent des fichiers `makefile` qui décrivent les paramètres à prendre en compte pour installer un composant défini d'eDirectory. Ces paquetages contiennent également des fichiers de configuration, des utilitaires, des bibliothèques, des daemons et des pages de manuel utilisant les outils Linux standard installés avec l'OS.

Certains paquetages dépendent d'autres paquetages ou de composants Identity Manager, comme NICI. Pour garantir le bon fonctionnement de la solution, vous devez installer tous les paquetages dépendants.

Le tableau suivant fournit des informations sur les paquetages Linux inclus dans eDirectory. Tous les paquetages ont comme préfixe *novell-*. Par exemple, NDSserv s'appelle `novell-NDSserv`.

Paquetage	Description
`NOVLice`	Contient l'utilitaire NetIQ d'importation/de conversion/d'exportation. Ce paquetage dépend des paquetages `NOVLmgnt`, `NOVLxis` et `NLDAPbase`.
`NOVbase`	Représente l'agent utilisateur d'annuaire. Ce paquetage dépend du paquetage NICI. Ce paquetage contient les éléments suivants : ◆ Boîte à outils contenant l'authentification RSA nécessaire à eDirectory. ◆ Bibliothèque d'abstraction de système indépendante de la plate-forme, bibliothèque contenant toutes les fonctions définies de l'agent utilisateur d'annuaire et bibliothèque d'extension du schéma. ◆ Utilitaire de configuration combiné et utilitaire de test de l'agent utilisateur d'annuaire. ◆ Fichier de configuration et pages de manuel d'eDirectory.
`NDScommon`	Contient les pages du manuel du fichier de configuration et des utilitaires d'installation et de désinstallation d'eDirectory. Ce paquetage dépend du paquetage NDSbase.
`NDSmasv`	Contient les bibliothèques requises pour le service MASV (Mandatory Access Control).

Paquetage	Description
NDSserv	Contient tous les fichiers binaires et bibliothèques dont le serveur eDirectory a besoin. Il contient également les utilitaires permettant de gérer le serveur eDirectory sur le système. Ce paquetage dépend des paquetages NDSbase, NDScommon, NDSmasv, NLDAPsdk, NOVLpkia et NOVLpkit. Il contient également les éléments suivants : ◆ Bibliothèque d'installation NDS, bibliothèque FLAIM, bibliothèque de trace, bibliothèque NDS, bibliothèque de serveur LDAP, bibliothèque d'installation LDAP, bibliothèque d'éditeur d'index, bibliothèque DNS, bibliothèque de fusion et bibliothèque d'extension LDAP pour SDK LDAP. ◆ Daemon de serveur eDirectory. ◆ Fichier binaire pour DNS et fichier binaire pour le chargement et le déchargement de LDAP. ◆ L'utilitaire nécessaire pour créer l'adresse MAC, l'utilitaire de trace du serveur et de modification de certaines variables globales du serveur, l'utilitaire de sauvegarde et de restauration d'eDirectory et l'utilitaire de fusion d'arborescences eDirectory. ◆ Scripts de démarrage de DNS, NDSD et NLDAP. ◆ Pages du manuel.
NDSrepair	Contient les bibliothèques d'exécution ainsi que l'utilitaire permettant de corriger les problèmes liés à la base de données eDirectory. Ce paquetage dépend du paquetage NDSbase.
NLDAPbase	Contient les bibliothèques LDAP, leurs extensions et les outils LDAP suivants : ◆ ldapdelete ◆ ldapmodify ◆ ldapmodrdn ◆ ldapsearch Ce paquetage dépend du paquetage NLDAPsdk.
NOVLnmas	Contient l'ensemble des bibliothèques NMAS, ainsi que les fichiers binaires nmasinst requis par le serveur NMAS. Ce paquetage dépend des paquetages NICI et NDSmasv.
NLDAPsdk	Contient les extensions NetIQ des bibliothèques d'exécution LDAP et de sécurité (Client NICI).
NOVLsubag	Contient les utilitaires et bibliothèques d'exécution du sous-agent SNMP d'eDirectory. Ce paquetage dépend des paquetages NICI, NDSbase et NLDAPbase.
NOVLpkit	Fournit des services PKI indépendants de eDirectory. Ce paquetage dépend des paquetages NICI et NLDAPsdk.
NOVLpkis	Fournit le service PKI Server. Ce paquetage dépend des paquetages NICI, NDSbase et NLDAPsdk.
NOVLsnmp	Utilitaires et bibliothèques d'exécution pour SNMP. Ce paquetage dépend du paquetage NICI.

Paquetage	Description
NDSdexvnt	Contient la bibliothèque qui gère les événements générés dans NetIQ eDirectory vers d'autres bases de données.
NOVLpkia	Fournit des services PKI. Ce paquetage dépend des paquetages NICI, NDSbase et NLDAPsdk.
NOVLembox	Fournit l'infrastructure eMBox et les outils eMTools.
NOVLlmgnt	Contient les bibliothèques d'exécution pour NetIQ Language Management.
NOVLxis	Contient les bibliothèques d'exécution pour NetIQ XIS.
NOVLsas	Contient les bibliothèques SAS de NetIQ.
NOVLntls	Contient la bibliothèque TLS de NetIQ. Ce paquetage est également identifié sous le nom ntls.
NOVLldif2	Contient l'utilitaire de chargement en bloc hors connexion de NetIQ et dépend des paquetages NDSbase, NDSserv, NOVLntls, NOVLlmgnt et NICI.
NOVLncp	Contient les services NCP chiffrés de NetIQ pour Linux. Ce paquetage dépend du paquetage NDScommon.

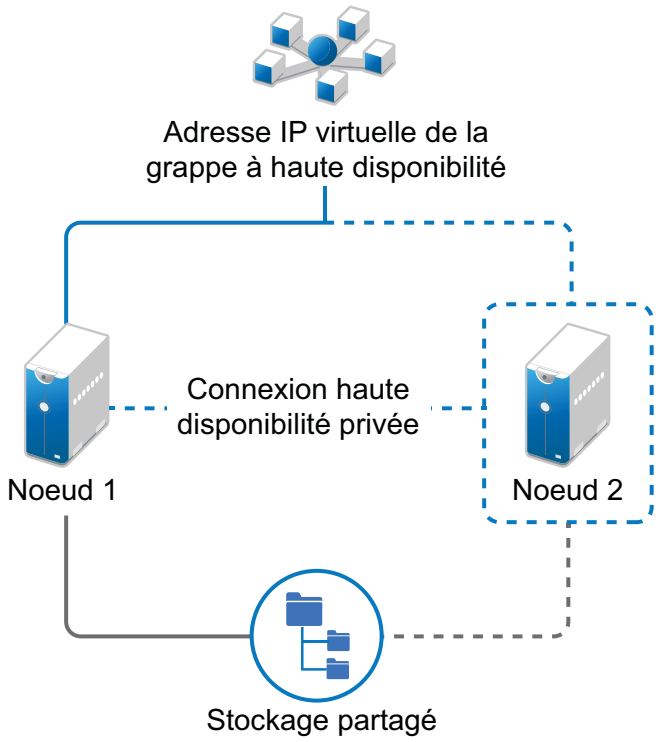
B Exemple de solution de déploiement en grappe d'Identity Manager sous SLES 12 SP2

L'annexe fournit des instructions étape par étape concernant la procédure de configuration d'eDirectory et d'Identity Manager dans un environnement en grappe SUSE Linux Enterprise Server (SLES) pris en charge avec stockage partagé et un exemple de déploiement en grappe d'Identity Manager.

Pour une solution de production haute disponibilité Linux avec stockage partagé, il est recommandé de mettre en place un mécanisme d'isolation dans la grappe. Bien qu'il existe différentes méthodes pour installer des mécanismes d'isolation dans la grappe, dans notre exemple, nous utilisons une ressource STONITH qui utilise le détecteur de vues de grappe divergentes (SBD).

La Figure B-1 page 325 présente un exemple de solution de déploiement en grappe.

Figure B-1 *Exemple de solution de déploiement en grappe*



B.1 Conditions préalables

- Deux serveurs exécutant SLES 12 SP2 64 bits pour les noeuds

- Un serveur exécutant SLES 12 SP2 64 bits pour le serveur iSCSI
- Fichier image ISO de l'extension Haute disponibilité SLES 12 SP2 64 bits
- Six adresses IP statiques :
  - Deux adresses IP statiques pour chaque noeud.
  - Une adresse IP statique pour la grappe. Cette adresse IP est assignée de façon dynamique au noeud qui exécute eDirectory.
  - Une adresse IP pour le serveur iSCSI.

B.2 Procédure d'installation

Cette section explique la procédure à suivre pour installer et paramétrer ce qui suit afin de configurer l'environnement en grappe. Pour plus d'informations sur la configuration de SLES High Availability Extension, reportez au Guide de SUSE Linux Enterprise High Availability Extension.

B.2.1 Configuration du serveur iSCSI

Une cible iSCSI est un périphérique configuré en tant que périphérique de stockage commun pour tous les noeuds de la grappe. Il s'agit d'un disque virtuel créé sur le serveur Linux afin de permettre l'accès à distance via une connexion Ethernet par un initiateur iSCSI. Tout noeud de la grappe configuré pour contacter la cible (iSCSI) pour des services est un initiateur iSCSI. La cible iSCSI doit toujours être active et en cours d'exécution de sorte que n'importe quel hôte agissant en tant qu'initiateur puisse atteindre la cible. Avant de procéder à l'installation de la cible iSCSI sur le serveur iSCSI, assurez-vous que celle-ci dispose de suffisamment d'espace pour un stockage commun. Installez les paquetages de l'initiateur iSCSI sur les deux autres noeuds après avoir installé SLES 12 SP2.

Pendant l'installation de SLES 12 SP2 :

1. Créez une partition distincte et indiquez son chemin comme partition de stockage partagé iSCI.
2. Installez les paquetages cibles iSCSI.

Pour configurer le serveur iSCSI :

1. Créez un périphérique de bloc sur le serveur cible.
2. Entrez la commande `yast2 disk` sur le terminal.
3. Créez une nouvelle partition Linux et sélectionnez **Do not format** (Ne pas formater).
4. Sélectionnez **Do not mount the partition** (Ne pas monter la partition).
5. Définissez la taille de la partition.
6. Entrez la commande `yast2 iscsi-server` ou `yast2 iscsi-lio-server` dans le terminal.
7. Cliquez sur l'onglet **Service**, puis sélectionnez When Booting **(Au démarrage) dans Service Start (Lancement du service).**
8. Sous l'onglet **Targets** (Cibles), cliquez sur **Add** (Ajouter) pour entrer le chemin de la partition (tel que créé lors de l'installation de SLES).
9. Sur la page **Modify iSCSI Target Initiator Setup** (Modifier la configuration de l'initiateur cible iSCSI), spécifiez les noms d'hôte de l'initiateur du client iSCSI pour le serveur cible, puis cliquez sur **Suivant**.

   Par exemple, *iqn.sles12sp2node2.com* et *iqn.sles12sp2node3.com*.

10 Cliquez sur **Finish** (Terminer).

11 Exécutez la commande `cat /proc/net/iet/volume` sur le terminal pour vérifier que la cible iSCSI est installée.

B.2.2 Configuration de l'initiateur iSCSI sur tous les noeuds

Vous devez configurer l'initiateur iSCSI sur tous les noeuds de la grappe pour qu'il se connecte à la cible iSCSI.

Pour configurer l'initiateur iSCSI :

1 Installez les paquetages de l'initiateur iSCSI.

2 Exécutez le client `yast2 iscsi-client` sur le terminal.

3 Cliquez sur l'onglet **Service** et sélectionnez When Booting **(Au démarrage) dans Service Start (Lancement du service).**

4 Cliquez sur l'onglet **Connected Targets** (Cibles connectées), puis sur **Add** (Ajouter) pour entrer l'adresse IP du serveur cible iSCSI.

5 Sélectionnez **No Authentication** (Aucune authentification).

6 Cliquez sur **Next** (Suivant), puis sur **Connect** (Se connecter).

7 Cliquez sur **Toggle Start-up** (Changer le démarrage) pour passer du démarrage manuel au démarrage automatique, puis cliquez sur **Next** (Suivant).

8 Cliquez sur **Next** (Suivant), puis sur **OK**.

9 Pour vérifier l'état de l'initiateur connecté sur le serveur cible, exécutez la commande `cat /proc/net/iet/session` sur le serveur cible. La liste des initiateurs connectés au serveur iSCSI s'affiche.

B.2.3 Partitionnement du stockage partagé

Créez deux partitions de stockage partagé : l'une pour le détecteur de vues de grappe divergentes (SBD) et l'autre pour le système de fichiers en grappe.

Pour partitionner le stockage partagé :

1 Exécutez la commande `yast2 disk` sur le terminal.

2 Dans la boîte de dialogue **Expert Partitioner** (Partitionneur en mode expert), sélectionnez le volume partagé. Dans notre exemple, sélectionnez **sdb** dans la boîte de dialogue **Expert Partitioner** (Partitionneur en mode expert).

3 Cliquez sur **Add** (Ajouter), sélectionnez l'option **Primary partition** (Partition principale), puis cliquez sur **Next** (Suivant).

4 Sélectionnez **Custom size** (Taille personnalisée), puis cliquez sur **Next** (Suivant). Dans notre exemple, la taille personnalisée est 100 Mo.

5 Sous **Formatting options** (Options de formatage), sélectionnez **Do not format partition** (Ne pas formater la partition). Dans notre exemple, l'ID du système de fichiers est 0x83 Linux.

6 Sous **Mounting options** (Options de montage), sélectionnez **Do not mount partition** (Ne pas monter la partition), puis cliquez sur **Finish** (Terminer).

7 Cliquez sur **Add** (Ajouter), puis sélectionnez **Primary partition** (Partition principale).

8 Cliquez sur **Next** (Suivant), puis sélectionnez **Maximum Size** (Taille maximale) et cliquez sur **Next** (Suivant).

9 Dans **Formatting options** (Options de formatage), cliquez sur **Do not format partition** (Ne pas formater la partition). Dans notre exemple, définissez l'ID du système de fichiers comme 0x83 Linux.

10 Dans **Mounting options** (Options de montage), sélectionnez **Do not mount partition** (Ne pas monter la partition), puis cliquez sur **Finish** (Terminer).

B.2.4 Installation de l'extension Haute disponibilité

Pour installer l'extension Haute disponibilité :

1 Accédez au site Web des téléchargements SUSE.

SLE HA (SUSE Linux Enterprise High Availability Extension) est disponible au téléchargement pour chaque plate-forme disponible en tant que deux images ISO. Media 1 contient les paquetages binaires et Media 2 contient le code source.

REMARQUE : sélectionnez et installez le fichier ISO d'extension Haute disponibilité adapté à votre architecture système.

---

2 Téléchargez le fichier ISO Media 1 sur chaque serveur.

3 Ouvrez la boîte de dialogue **Centre de contrôle YaST** et cliquez sur **Produits complémentaires > Ajouter**.

4 Cliquez sur **Parcourir** et sélectionnez le DVD ou l'image ISO locale, puis cliquez sur **Suivant**.

5 Sous l'onglet **Patterns** (Modèles), sélectionnez **High Availability** (Haute disponibilité) sous **Primary Functions** (Fonctions principales).

Vérifiez que tous les composants en haute disponibilité sont installés.

6 Cliquez sur **Accepter**.

B.2.5 Configuration de la surveillance logicielle (softdog)

Dans l'extension Haute disponibilité de SLES, la prise en charge de la surveillance dans le kernel est activée par défaut. Cette fonctionnalité est fournie avec différents modules de kernel qui proposent des pilotes de surveillance spécifiques au matériel. Le pilote de surveillance correspondant à votre matériel est automatiquement chargé au démarrage du système.

1 Activez la surveillance logicielle :

```
echo softdog > /etc/modules-load.d/watchdog.conf
```

```
systemctl restart systemd-modules-load
```

2 Vérifiez si le module de surveillance logicielle est chargé correctement :

```
lsmod | grep dog
```

B.2.6 Configuration de la grappe haute disponibilité

Cet exemple part du principe que vous configurez deux noeuds dans une grappe.

Configuration du premier noeud :

1 Connectez-vous en tant qu'utilisateur root à la machine physique ou virtuelle que vous souhaitez utiliser comme noeud de grappe.

2 Exécutez la commande suivante :

`ha-cluster-init`

La commande vérifie la configuration NTP et la présence d'un service de surveillance matérielle. Il génère les clés SSH publiques et privées utilisées pour l'accès SSH et la synchronisation Csync2, et démarre les services respectifs.

3 Configurez la couche de communication de grappe:

3a Spécifiez une adresse réseau pour la liaison.

3b Spécifiez une adresse de multidiffusion. Le script propose une adresse aléatoire que vous pouvez utiliser comme adresse par défaut.

3c Spécifiez un port de multidiffusion. Le port par défaut est 5405.

4 Configurez SBD comme mécanisme d'isolation de noeud :

4a Appuyez sur *y* (oui) pour utiliser SBD.

4b Entrez un chemin d'accès persistant à la partition du périphérique de bloc pour lequel vous souhaitez utiliser SBD. Le chemin doit être cohérent sur les deux noeuds de la grappe.

5 Configurez une adresse IP virtuelle pour l'administration de la grappe :

5a Appuyez sur *y* pour configurer une adresse IP virtuelle.

5b Spécifiez une adresse IP inutilisée à employer comme adresse IP d'administration pour l'interface graphique de SUSE Hawk. Par exemple, *192.168.1.3*.

Au lieu de vous connecter à un noeud de grappe individuel, vous pouvez vous connecter à l'adresse IP virtuelle.

Une fois que le premier noeud est opérationnel et en cours d'exécution, ajoutez le deuxième noeud de grappe à l'aide de la commande `ha-cluster-join`.

Configuration du second noeud :

1 Connectez-vous en tant qu'utilisateur root à la machine physique ou virtuelle à l'aide de laquelle vous souhaitez vous connecter à la grappe.

2 Exécutez la commande suivante :

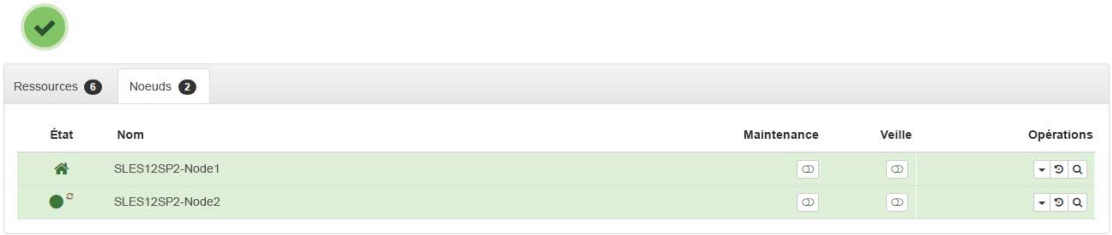
`ha-cluster-join`

Si le protocole NTP n'est pas configuré, un message s'affiche. La commande recherche un périphérique de surveillance matérielle et vous avertit s'il n'en trouve aucun.

3 Entrez l'adresse IP du premier noeud.

4 Entrez le mot de passe root du premier noeud.

5 Connectez-vous à l'interface graphique de SUSE Hawk, puis cliquez sur **État** > **Noeuds**. Par exemple : `https://192.168.1.3:7630/cib/live`.



B.2.7 Installation et configuration d'eDirectory et d'Identity Manager sur les noeuds de grappe

1 Installez eDirectory sur les noeuds de grappe :

Installez une version prise en charge d'eDirectory. Pour des instructions étape par étape pour configurer eDirectory sur une grappe haute disponibilité, reportez-vous à la section Déploiement de eDirectory sur les grappes haute disponibilité du *Guide d'installation d'eDirectory*.

IMPORTANT : assurez-vous que l'adresse IP virtuelle est configurée sur le noeud 1 avant d'installer eDirectory sur ce dernier.

---

2 Installez Identity Manager sur le noeud 1 via l'option Serveur méta-annuaire.

3 Installez le moteur Identity Manager sur le serveur du noeud 2 via l'option `DCLUSTER_INSTALL`.

Exécutez la commande `./install.bin -DCLUSTER_INSTALL="true"` sur le terminal.

Le programme d'installation installe les fichiers Identity Manager sans aucune interaction avec eDirectory.

B.2.8 Configuration de la ressource eDirectory

1 Connectez-vous à l'interface graphique de SUSE Hawk.

2 Cliquez sur **Add Resource** (Ajouter une ressource) et créez un nouveau groupe.

2a Cliquez sur ⊕ en regard de **Group** (Groupe).

2b Spécifiez un ID de groupe. Par exemple, *Groupe-1*.

Assurez-vous que les ressources enfants suivantes sont sélectionnées lorsque vous créez un groupe :

- *stonith-sbd*
- *admin_addr (adresse IP de la grappe)*

3 Sous l'onglet **Meta Attributes** (Méta attributs), définissez le champ **target-role** (rôle cible) sur *Started* (Démarré) et le champ **is-managed** (est géré) sur *Oui*.

4 Cliquez sur **Edit Configuration** (Modifier la configuration), puis cliquez sur ✎ en regard du groupe que vous avez créé à l'étape 2.

5 Dans le champ **Children** (Enfants), ajoutez les ressources enfants suivantes :

- *Shared-storage* (stockage partagé)
- *eDirectory-resource* (ressource eDirectory)

Par exemple, les ressources doivent être ajoutées dans l'ordre suivant au sein du groupe :

- *stonith-sbd*
- *admin_addr (adresse IP de la grappe)*
- *Shared-storage* (stockage partagé)
- *eDirectory-resource* (ressource eDirectory)

Vous pouvez modifier les noms de ressource si nécessaire. Chaque ressource possède un ensemble de paramètres que vous devez définir. Pour plus d'informations à propos des exemples de stockage partagé et de ressources eDirectory, reportez-vous à la section Primitives pour les ressources eDirectory et les ressources enfants du stockage partagé.

B.2.9 Primitives pour les ressources eDirectory et les ressources enfants du stockage partagé

Les ressources *stonith sbd* et admin_addr sont configurées par les commandes de grappe haute disponibilité par défaut lors de l'initialisation du noeud de grappe.

Tableau B-1 *Exemple de stockage partagé*

ID de la ressource	Nom de la ressource de stockage partagé
Classe	ocf
Provider	heartbeat
Type	Système de fichiers
Périphérique	/dev/sdc1
répertoire	/shared
fstype	xfs
operations	◆ start (60, 0) ◆ stop (60, 0) ◆ monitor (40, 20)
is-managed	Oui
resource-stickiness	100
target-role	Commencé

Tableau B-2 *Exemple de la ressource eDirectory*

ID de la ressource	Nom de la ressource eDirectory
Classe	systemd
Type	ndsdtmpl-shared-conf-nds.conf@-shared-conf-env
operations	◆ start (100, 0) ◆ stop (100, 0) ◆ monitor (100, 60)
target-role	Commencé
is-managed	Oui
resource-stickiness	100
failure-timeout	125
migration-threshold	0

B.2.10 Modification du score de contrainte d'emplacement

Modifiez le score de contrainte d'emplacement sur 0.

1. Connectez-vous à l'interface graphique de SUSE Hawk.
2. Cliquez sur **Edit Configuration**. (Modifier la configuration)
3. Sous l'onglet **Constraints** (Contraintes), cliquez sur en regard du noeud 1 de votre grappe.
4. Sous l'onglet **Simple**, définissez le score sur *0*.
5. Cliquez sur **Appliquer**.

Assurez-vous d'avoir défini le score sur *0* pour tous les noeuds de la grappe.

REMARQUE : lorsque vous migrez les ressources d'un noeud à l'autre de l'interface utilisateur graphique de SUSE Hawk à l'aide des options **Status** (État) > **Resources** (Ressources) > **Migrate** (Migrer), le score de contrainte d'emplacement passe de *Infinity* (Infini) à - *Infintity* (Infinité négative). Cela accordera la préférence à un seul des noeuds de la grappe et entraînera des retards dans les opérations d'eDirectory.

C Exemple de solution de déploiement en grappe d'applications d'identité sur un serveur d'applications Tomcat

Cette annexe explique, sur la base d'un exemple de déploiement, comment configurer les applications d'identité dans un environnement de grappe sur le serveur d'applications Tomcat.

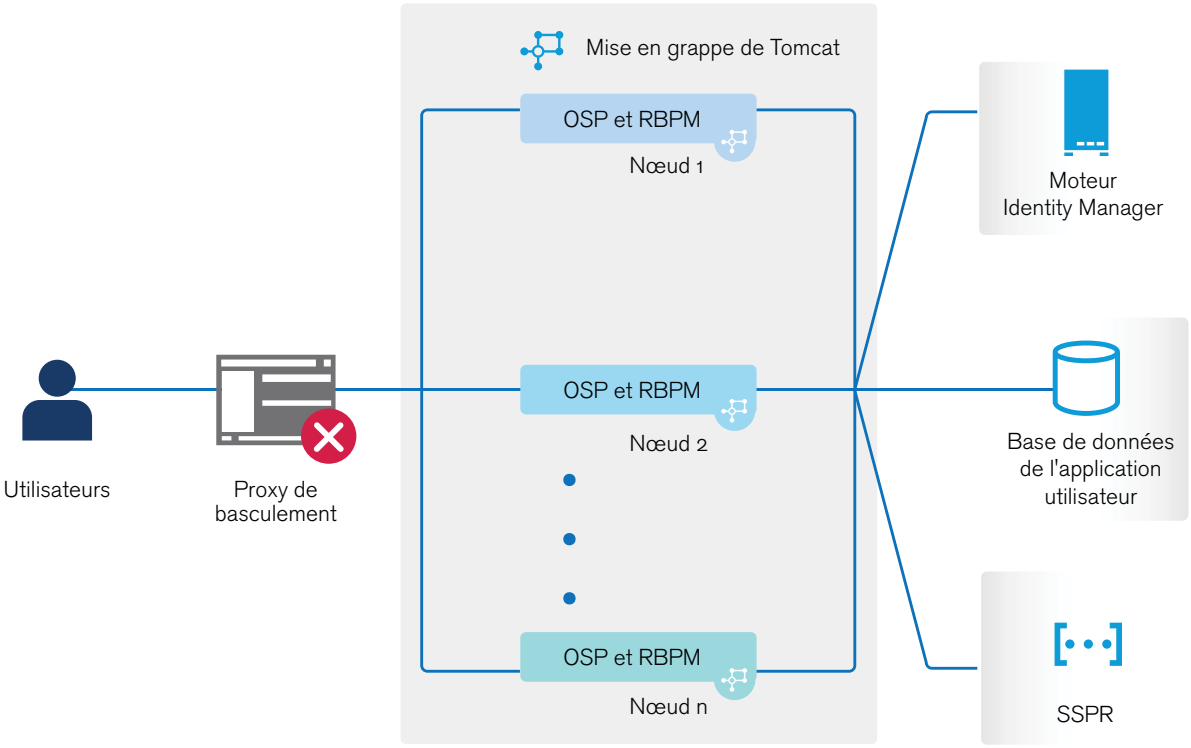
La mise en grappe permet d'exécuter les applications d'identité sur plusieurs serveurs en parallèle (noeuds de grappe) pour optimiser la disponibilité. Pour créer une grappe, vous devez regrouper plusieurs instances (noeuds) de Tomcat. La charge est répartie entre plusieurs serveurs, si bien qu'en cas de défaillance de l'un des serveurs, les applications d'identité continuent d'être accessibles via les autres nœuds de la grappe. Pour le basculement, vous pouvez créer une grappe d'applications d'identité et les configurer pour qu'elles agissent comme un seul serveur. Toutefois, cette configuration n'inclut pas Identity Reporting.

Il est recommandé d'utiliser un logiciel d'équilibrage de la charge qui traite toutes les demandes des utilisateurs et les distribue entre les noeuds de serveur de la grappe. L'équilibreur de charge fait généralement partie de la grappe. Il comprend la configuration de la grappe, ainsi que les stratégies de basculement. Vous pouvez choisir une solution adaptée à vos besoins.

La Figure C-1 montre un exemple de déploiement avec une grappe à deux nœuds, reposant sur les hypothèses suivantes :

- Toutes les communications sont routées via l'équilibreur de charge.
- Les composants tels que le moteur Identity Manager et l'application utilisateur sont installés sur des serveurs distincts. Cette approche est recommandée pour un déploiement au niveau de la production.
- Vous connaissez bien les procédures d'installation d'eDirectory, du moteur Identity Manager, des applications d'identité, du serveur d'applications Tomcat et des bases de données pour l'application utilisateur.
- SSPR (Single Sign-On Password Reset) est installé sur un ordinateur distinct. Il s'agit de l'approche recommandée pour un déploiement en production.
- PostgreSQL est utilisé comme base de données pour l'application utilisateur. Toutefois, vous pouvez utiliser n'importe quelle base de données prise en charge, comme Oracle ou MsSQL.
- Tous les noeuds d'application utilisateur communiquent avec la même instance d'eDirectory et la base de données de l'application utilisateur. En fonction de vos besoins, vous pouvez augmenter le nombre d'instances d'application utilisateur.

Figure C-1 *Exemple de solution de déploiement en grappe*



REMARQUE : une grappe à deux noeuds est la configuration minimale utilisée pour la haute disponibilité. Cependant, les concepts de cette section peuvent facilement être appliqués à une grappe comprenant des noeuds supplémentaires.

Pour vous aider à comprendre les différentes étapes de la configuration, cet exemple de déploiement est évoqué tout au long des sections suivantes du présent document.

C.1 Conditions préalables

- Deux serveurs exécutant SUSE Linux Enterprise Server (SLES) 12 SP2 64 bits ou RedHat Enterprise Linux (RHEL) 7.3 64 bits pour les noeuds installés avec toutes les bibliothèques dépendantes. Pour plus d'informations, reportez-vous à la section relative à RHEL.
- Composants Identity Manager 4.7 installés.
- Les horloges de serveur d'applications sont identiques sur tous les noeuds. Le moyen le plus simple de s'en assurer est de configurer les noeuds pour qu'ils utilisent le même serveur horaire réseau pour la synchronisation de l'heure à l'aide du protocole NTP.
- Les noeuds de la grappe résident sur le même sous-réseau.
- Un proxy de basculement ou une solution d'équilibrage de charge est installé sur un ordinateur distinct.

C.2 Procédure d'installation

Cette section explique de façon détaillée comment installer une nouvelle instance des applications d'identité sur le serveur Tomcat et la configurer pour la mise en grappe.

1. Installez le moteur Identity Manager 4.7. Pour obtenir des instructions détaillées, reportez-vous au Section 9.1, « Installation du moteur Identity Manager », page 91. Pour un déploiement en production, il est recommandé d'installer le moteur Identity Manager sur un serveur distinct.
2. Installez la base de données pour les applications d'identité. Vous pouvez utiliser la base de données PostgreSQL installée avec les applications d'identité. Il est toutefois recommandé d'installer la base de données sur un serveur distinct.
3. Installez et configurez les applications d'identité sur le noeud 1.

   Pendant l'installation, veillez à effectuer les opérations suivantes :

   - Sélectionnez l'option Nouvelle de base de données.
   - Indiquez un ID unique pour le moteur de workflow. Par exemple, `Noeud1`.
   - Procurez-vous le fichier JAR de base de données disponible sur tous les noeuds de l'application utilisateur dans la grappe. Pour PostgreSQL, le fichier `postgresql-9.4.1212.jar` se trouve à l'emplacement `/opt/netiq/idm/postgres`.

   Les applications d'identité chiffrent les données sensibles à l'aide d'une clé principale. Le programme d'installation crée une nouvelle clé principale lors de la configuration des applications d'identité. Dans une grappe, la mise en grappe de l'application utilisateur requiert que chaque instance de cette dernière utilise la même clé principale. La clé principale est stockée sous la propriété `com.novell.idm.masterkey` du fichier `ism-configuration.properties` situé dans le répertoire `/opt/netiq/idm/apps/tomcat/conf/`.

   Pour obtenir des instructions détaillées, reportez-vous à la Section 9.3, « Installation des applications d'identité », page 97.
4. Installez et configurez les applications d'identité sur le noeud 2.

   Pendant l'installation, veillez à effectuer les opérations suivantes :

   - Sélectionnez l'option Base de données existante
   - Indiquez un ID unique pour le moteur de workflow. Par exemple, `Noeud2`.
   - Procurez-vous le fichier JAR de base de données disponible sur tous les noeuds de l'application utilisateur dans la grappe. Pour PostgreSQL, le fichier `postgresql-9.4.1212.jar` se trouve à l'emplacement `/opt/netiq/idm/postgres`.

   Après avoir terminé la configuration du noeud 2 de l'application utilisateur, copiez la valeur de la clé principale de du fichier ism-configuration.properties du noeud 1 et remplacez la valeur de la clé principale correspondante du fichier ism-configuration.properties du noeud 2. La clé principale est stockée sous la propriété com.novell.idm.masterkey du fichier ism-configuration.properties (/opt/netiq/idm/apps/tomcat/conf/).
5. Installez SSPR sur un ordinateur distinct.

   Prenez note des paramètres ci-dessous avant de procéder à l'installation et spécifiez-les au cours du processus d'installation :

   Une fois SSPR installé, démarrez Tomcat et lancez SSPR (`http://<IP>:<port>/sspr/private/config/ConfigEditor`) et connectez-vous. Cliquez sur **Configuration Editor** (Éditeur de configuration) > **Settings** (Paramètres) > **Security** (Sécurité) > **Redirect Whitelist** (Liste blanche de redirection).

   a. Cliquez sur **Add value** (Ajouter une valeur) et spécifiez l'URL suivante :

      OSP : `http:<DNS_basculement>:<port>/osp`

b. Enregistrez les modifications apportées.

c. Sur la page de configuration de SSPR, cliquez sur **Settings** (Paramètres) > **OAuth SSO** (SSO OAuth) et modifiez les liens OSP en remplaçant les adresses IP par le nom DNS du serveur sur lequel le logiciel d'équilibrage de charge est installé.

d. Cliquez sur **Settings** (Paramètres) > **Application** et mettez à jour les URL de réacheminement et de déconnexion en remplaçant les adresses IP par le nom DNS du serveur sur lequel le logiciel d'équilibrage de charge est installé.

e. Pour mettre à jour les informations de SSPR sur le noeud 1, lancez l'utilitaire de configuration situé dans `/opt/netiq/idm/apps/UserApplication/configupdate.sh`.

f. Cliquez sur **Clients SSO** > **Self Service Password Reset** et spécifiez des valeurs pour les paramètres **ID du client**, **Mot de passe** et **OSP Auth redirect URL** (URL de redirection de l'authentification OSP). Pour plus d'informations, reportez-vous à la Section 22.3, « Mise à jour des liens SSPR dans le tableau de bord pour un environnement distribué ou de grappe », page 239.

REMARQUE : vérifiez que les valeurs de ces paramètres sont mises à jour sur le noeud 2.

---

6. Sur le noeud 1, arrêtez Tomcat et générez un nouveau fichier `osp.jks` en spécifiant le nom DNS du serveur de l'équilibreur de charge à l'aide de la commande suivante :

   ```
   /opt/netiq/idm/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore
   osp.jks -storepass <mot_de_passe> -keypass <mot_de_passe> -alias osp -validity
   1800 -dname "cn=<IP/DNS_équilibreur_de_charge>"
   ```

   Par exemple : `/opt/netiq/idm/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"`

REMARQUE : assurez-vous que le mot de passe de clé est identique à celui spécifié lors de l'installation d'OSP. Ce mot de passe, de même que le mot de passe Keystore, peut aussi être modifié à l'aide de l'utilitaire de mise à jour de configuration.

---

7. (Conditionnel) Pour vérifier si le fichier `osp.jks` a été mis à jour avec les modifications, exécutez la commande suivante :

   ```
   /opt/netiq/idm/jre/bin/keytool -list -v -keystore osp.jks -storepass changeit
   ```

8. Effectuez une sauvegarde du fichier `osp.jks` d'origine situé sous `/opt/netiq/idm/apps/osp_sspr/osp/` et copiez le nouveau fichier `osp.jks` à cet emplacement.

9. Copiez le nouveau fichier `osp.jks` situé dans `/opt/netiq/idm/apps/osp_sspr/osp/` depuis le noeud 1 vers les autres noeuds d'application utilisateur de la grappe.

10. Lancez l'utilitaire de configuration sur le noeud 1 et, sous l'onglet Client SSO, remplacez l'ensemble des paramètres d'URL, notamment le lien URL vers la page de renvoi et l'URL de redirection OAuth, par le nom DNS de l'équilibreur de charge.

    a. Enregistrez les modifications dans l'utilitaire de configuration.

    b. Pour que cette modification soit prise en compte sur tous les autres noeuds de la grappe, copiez le fichier `ism-configuration.properties` situé sous `/TOMCAT_INSTALLED_HOME/conf` à partir du noeud 1 vers les autres noeuds d'application utilisateur de la grappe.

    REMARQUE : vous avez copié le fichier `ism.properties` depuis le noeud 1 vers les autres noeuds de la grappe. Si vous avez spécifié des chemins d'installation personnalisés lors de l'installation de l'application utilisateur, veillez à corriger les chemins d'accès référentiels en utilisant l'utilitaire de mise à jour de configuration sur les noeuds de la grappe.

Dans ce scénario, OSP et l'application utilisateur sont installés sur le même serveur ; dès lors, le même nom DNS est utilisé pour les URL de redirection.

Si OSP et l'application utilisateur sont installés sur des serveurs distincts, remplacez les URL d'OSP par un autre nom DNS pointant vers l'équilibreur de charge. Effectuez cette opération pour tous les serveurs sur lesquels OSP est installé, afin que toutes les requêtes OSP soient distribuées, via l'équilibreur de charge, vers le nom DNS de la grappe OSP. Cela implique d'avoir une grappe distincte pour les noeuds OSP.

11. Effectuez les opérations suivantes dans le fichier `setenv.sh` situé dans le répertoire `/TOMCAT_INSTALLED_HOME/bin/` :
    a. Pour vérifier la réussite de la liaison `mcast_addr`, JGroups requiert que la `propriété preferIPv4Stack` soit définie sur **true** (vrai). Pour ce faire, ajoutez la propriété JVM « -Djava.net.preferIPv4Stack=true » dans le fichier `setenv.sh` sur tous les noeuds.
    b. Ajoutez `-Dcom.novell.afw.wf.Engine-id="Engine1"` dans le fichier `setenv.sh` sur le noeud 1. De même, ajoutez un nom de moteur unique pour chaque noeud de la grappe. Par exemple, pour le noeud 2, vous pouvez ajouter le nom de moteur *`Moteur2`*.
12. Activez la mise en grappe dans l'application utilisateur.
    a. Démarrez Tomcat sur le noeud 1.

       Ne démarrez aucun autre serveur.
    b. Connectez-vous à l'application utilisateur en tant qu'administrateur.
    c. Cliquez sur l'onglet **Administration**.

       L'application utilisateur affiche le portail Configuration de l'application.
    d. Cliquez sur **Mise en cache**.

       L'application utilisateur affiche la page Gestion de la mise en cache.
    e. Définissez le paramètre **Grappe activée** sur **Vrai**.
    f. Cliquez sur **Enregistrer**.
    g. Relancez Tomcat.

REMARQUE : si vous avez sélectionné les paramètres d'activation locale, répétez cette procédure pour chaque serveur de la grappe.

La grappe d'application utilisateur utilise JGroups pour procéder à la synchronisation du cache sur les nœuds à l'aide du protocole par défaut UDP. Si vous souhaitez modifier ce protocole pour utiliser TCP, reportez-vous à la section Portal Configuration Tasks (Tâches de configuration du portail) du NetIQ Analyzer for Identity Manager Administration Guide (Guide d'administration de NetIQ Analyzer pour Identity Manager).

13. Activez l'index des autorisations pour la mise en grappe.
    a. Connectez-vous à iManager sur le noeud 1 et accédez à **Afficher les objets**.
    b. Sous **Système**, accédez à l'ensemble de pilotes contenant le pilote d'application utilisateur.
    c. Sélectionnez **AppConfig** > **AppDefs** > **Configuration**.
    d. Sélectionnez l'attribut XMLData et définissez la propriété `com.netiq.idm.cis.clustered` sur **true**.

       Par exemple :

       ```
       <property>
       <key>com.netiq.idm.cis.clustered</key>
       <value>true</value>
       ```

```
</property>
```

e. Cliquez sur **OK**.

14. Activez la grappe Tomcat.

    Ouvrez le fichier Tomcat `server.xml` situé dans `/TOMCAT_INSTALLED_HOME/conf/` et supprimez le commentaire de la ligne ci-dessous dans ce fichier sur tous les noeuds de la grappe :

    ```
    <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
    ```

    Pour une configuration avancée de mise en grappe Tomcat, suivez la procédure décrite sur le site https://tomcat.apache.org/tomcat-8.5-doc/cluster-howto.html.

15. Redémarrez Tomcat sur tous les noeuds.

16. Configurez le pilote d'application utilisateur pour la mise en grappe.

    Dans une grappe, le pilote d'application utilisateur doit être configuré pour utiliser le nom DNS de l'équilibreur de charge de la grappe. La configuration du pilote d'application utilisateur s'effectue à l'aide d'iManager.

    a. Connectez-vous à l'instance iManager qui gère votre moteur Identity Manager.

    b. Cliquez sur le **noeud Identity Manager** dans le panneau de navigation d'iManager.

    c. Cliquez sur **Présentation d'Identity Manager**.

    d. Utilisez la page de recherche pour afficher l'aperçu Identity Manager de l'ensemble de pilotes contenant vos pilotes d'application utilisateur et de service de rôles et de ressources.

    e. Cliquez sur l'indicateur d'état arrondi du pilote dans l'angle supérieur droit de l'icône du pilote :

    Un menu contenant les commandes permettant de démarrer et d'arrêter le pilote, ainsi que de modifier ses propriétés, s'affiche :

    f. Sélectionnez **Modifier les propriétés**.

    g. Dans la section Paramètres du pilote, définissez la propriété **Hôte** sur le nom d'hôte ou l'adresse IP du répartiteur.

    h. Cliquez sur **OK**.

    i. Redémarrez le pilote.

17. Pour modifier l'URL du pilote de service de rôles et de ressources, répétez les étapes 18a à 18f, puis cliquez sur **Configuration du pilote** et mettez à jour l'**URL de l'application utilisateur** avec le nom DNS de l'équilibreur de charge.

18. Assurez-vous que la persistance de la session est activée pour la grappe créée dans le logiciel d'équilibrage de charge pour les noeuds d'application utilisateur.

19. Configurez les paramètres du client dans le tableau de bord Identity Manager. Pour plus d'informations, reportez-vous à la section Configuring Client Settings Mode (Mode de configuration des paramètres du client) du NetIQ Identity Manager - Administrator's Guide to the Identity Applications (NetIQ Identity Manager - Guide de l'administrateur des applications d'identité).