NetIQ Identity Manager

Guide d'installation pour Windows

Mars 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.

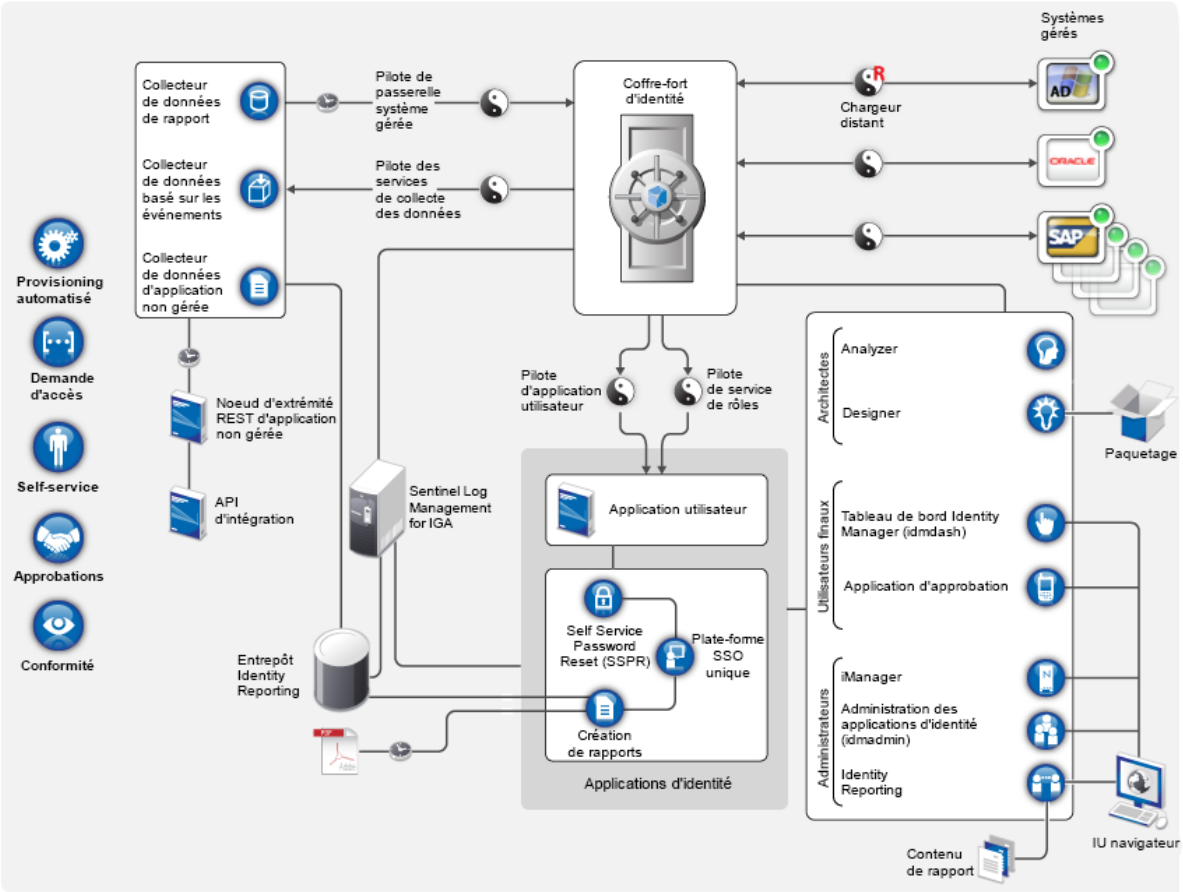
En général, vous pouvez regrouper les composants qui constituent Identity Manager dans les fonctions suivantes :

- 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 21.
- 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 23.
- 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 27.

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 19.

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 *NetIQ iManager Administration Guide* (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
- 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 comptes utilisateur et suppression de comptes existants dans des annuaires comme Active Directory et sur des systèmes tels que PeopleSoft et Lotus Notes. Par exemple, lorsque vous ajoutez un employé à votre système SAP HR, Identity Manager peut créer automatiquement un compte utilisateur dans Active Directory et un compte dans Lotus Notes.

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 NetIQ eDirectory 9.1 Administration Guide (Guide d'administration de NetIQ eDirectory 8.8).

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 faciliter le workload ou la configuration de votre environnement, vous pouvez installer le chargeur distant sur un serveur distinct des serveurs équipés du serveur Tomcat et Identity Manager.

Pour plus d'informations sur le chargeur distant, reportez-vous à la Section 10.1.2, « Présentation du chargeur distant », page 99.

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 25
- « Service de collecte de données » page 26
- « Pilote de passerelle système gérée » page 26

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. 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'application utilisateur. À partir d'Identity Manager 4.7, 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

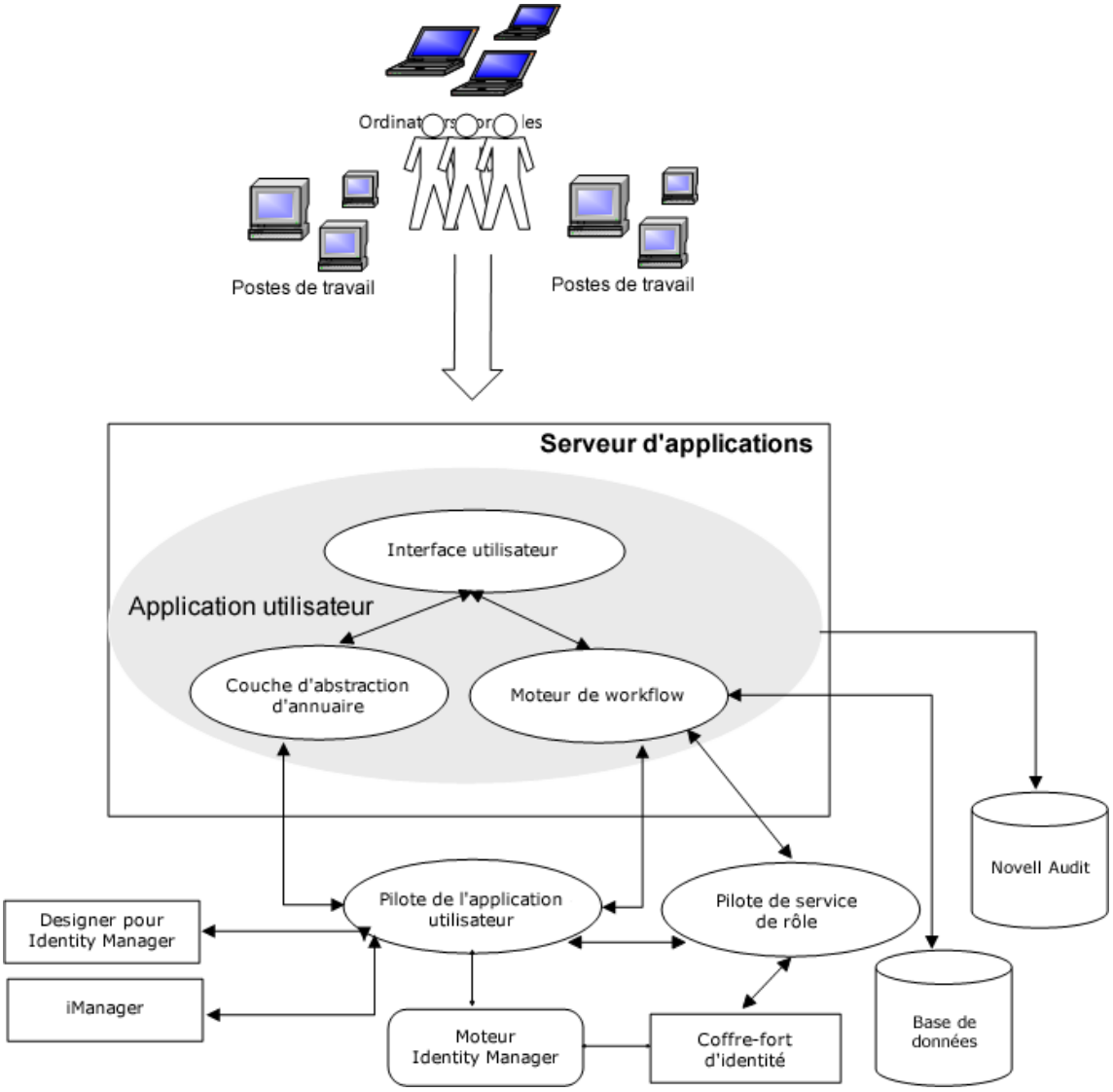
Cette section explique la fonction des composants suivants :

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).

4.4 Utilisation de la gestion des mots de passe en self-service dans Identity Manager

Identity Manager comprend NetIQ Self Service Password Reset (SSPR), un module qui aide les utilisateurs ayant accès à des applications d'identité à réinitialiser leur mot de passe sans demander l'intervention d'un administrateur. La procédure d'installation active SSPR par défaut lors de l'installation ou de la mise à niveau vers la dernière version d'Identity Manager. Dans une nouvelle installation, SSPR utilise un protocole propriétaire pour gérer les méthodes d'authentification. Toutefois, après une mise à niveau, vous pouvez demander à SSPR d'utiliser NMAS (NetIQ Modular Authentication Services), le programme traditionnellement utilisé par Identity Manager pour la gestion des mots de passe hérités.

Selon que vous souhaitiez utiliser la gestion de mots de passe complexes, vous pouvez configurer l'un des modules suivants :

SSPR

NetIQ Self Service Password Reset est l'option par défaut lorsque vous installez ou mettez à niveau Identity Manager. Pour plus d'informations, reportez-vous à la Section 4.4.1, « Présentation du processus de self-service par défaut », page 33.

Fournisseur hérité pour la gestion des mots de passe

Utilise le processus de gestion des mots de passe d'Identity Manager 4.0.2, qui prend en charge l'utilisation de plusieurs stratégies de mot de passe. Pour plus d'informations, reportez-vous à la Section 4.4.2, « Présentation du fournisseur hérité pour la gestion des mots de passe », page 33.

Fournisseur tiers pour la gestion des mots de passe

Vous pouvez utiliser un programme tiers pour gérer les mots de passe oubliés. Pour ce faire, vous devez modifier certains paramètres de configuration d'Identity Manager. Pour plus d'informations, reportez-vous à la section « Utilisation d'un système externe pour la gestion des mots de passe oubliés » page 233.

4.4.1 Présentation du processus de self-service par défaut

SSPR s'intègre automatiquement avec le processus Single Sign-On pour les applications d'identité et NetIQ Identity Reporting. Il s'agit du programme par défaut utilisé par Identity Manager pour la gestion des mots de passe, même si vous n'installez pas SSPR. Lorsqu'un utilisateur demande la réinitialisation d'un mot de passe, SSPR invite l'utilisateur à répondre à une question de stimulation. Si les réponses sont correctes, SSPR réagit de l'une des manières suivantes :

- autorise les utilisateurs à créer un nouveau mot de passe ;
- crée un nouveau mot de passe et l'envoie à l'utilisateur ;
- crée un nouveau mot de passe, l'envoie à l'utilisateur et consigne l'ancien mot de passe comme ayant expiré.

Vous configurez cette réponse dans l'éditeur de configuration SSPR. Après la mise à niveau vers une nouvelle version d'Identity Manager, vous pouvez configurer SSPR de façon à ce qu'il utilise la méthode NMAS traditionnellement utilisée par Identity Manager pour la gestion des mots de passe. Toutefois, SSPR ne reconnaît pas vos stratégies de mot de passe existantes pour la gestion des mots de passe oubliés. Pour continuer à utiliser vos stratégies, reportez-vous à la Section 4.4.2, « Présentation du fournisseur hérité pour la gestion des mots de passe », page 33.

Vous pouvez également configurer SSPR de façon à ce qu'il utilise son protocole propriétaire au lieu de NMAS. Si vous apportez cette modification, vous ne pourrez pas réutiliser NMAS tant que vous n'aurez pas réinitialisé vos stratégies de mot de passe.

Pour plus d'informations sur...	Voir...
Installation de SSPR	Chapitre 14.2, « Installation du composant de gestion des mots de passe pour Identity Manager », page 179
Configuration de la gestion des mots de passe pour les applications d'identité	« Utilisation de Self Service Password Reset pour la gestion des mots de passe oubliés » page 229
Gestion et configuration de SSPR	*NetIQ Self Service Password Reset Administration Guide* (Guide d'administration de NetIQ Self Service Password Reset)

4.4.2 Présentation du fournisseur hérité pour la gestion des mots de passe

REMARQUE : la fonctionnalité de self-service de mot de passe hérité de l'application utilisateur est abandonnée dans cette version. NetIQ recommande vivement que vous commenciez à utiliser SSPR pour toutes les tâches associées au mot de passe. La procédure d'installation active SSPR par défaut. Pour plus d'informations, reportez-vous à la Section 4.2, « Présentation du processus de self-service d'Identity Manager », page 28.

Lorsque vous effectuez une mise à niveau à partir d'une version antérieure d'Identity Manager, les applications d'identité utilisent par défaut SSPR comme programme de gestion des mots de passe. SSPR peut utiliser la méthode NMAS traditionnellement utilisée par Identity Manager pour la gestion des mots de passe. Toutefois, SSPR ne reconnaît pas vos stratégies de mot de passe existantes pour la gestion des mots de passe oubliés. Toutefois, vous pouvez ignorer SSPR et utiliser le fournisseur hérité pour gérer vos mots de passe.

Lorsqu'un utilisateur demande la réinitialisation d'un mot de passe, le fournisseur hérité compare les références de l'utilisateur aux stratégies de mot de passe définies. Par exemple, l'utilisateur sera peut-être invité à fournir une réponse de vérification d'identité. En fonction de la stratégie appliquée à cet utilisateur, le programme réagit de l'une des manières suivantes :

- il réinitialise le mot de passe ;
- il affiche l'indice du mot de passe ;
- il envoie par message électronique l'indice de mot de passe à l'utilisateur ;
- il envoie un nouveau mot de passe à l'utilisateur.

Utilisez le fournisseur hérité si votre entreprise utilise plusieurs stratégies de mots de passe ou si elles sont complexes. Par exemple, vos stratégies de mot de passe sont basées sur les rôles utilisateur. Pour un employé, un mot de passe généré automatiquement ne nécessitant pas de réponse de vérification d'identité suffit. En revanche, pour un manager ayant accès à des données sécurisées, vous pouvez avoir des exigences plus strictes. Cet utilisateur devra peut-être réinitialiser son mot de passe régulièrement. Dans les deux cas, vous souhaitez permettre à vos utilisateurs de gérer leurs demandes de mot de passe en self-service.

Pour utiliser le fournisseur hérité, modifiez les paramètres de configuration des applications d'identité après avoir installé ou mis à niveau Identity Manager. Il n'est pas nécessaire de reconfigurer vos stratégies de mot de passe après la mise à niveau.

Pour plus d'informations sur...	Voir...
Configuration d'Identity Manager pour utiliser le fournisseur hérité	« Utilisation du fournisseur hérité pour la gestion des mots de passe oubliés » page 231
Utilisation du fournisseur hérité pour la gestion des mots de passe	*NetIQ Identity Manager Password Management Guide* (Guide de gestion des mots de passe NetIQ Identity Manager)

4.5 Utilisation de l'accès Single Sign-on dans Identity Manager

Pour fournir un accès Single Sign-on (SSO), Identity Manager utilise le service d'authentification NetIQ One SSO Provider (OSP). Vous devez utiliser OSP pour les composants suivants :

- Administration des applications d'identité
- Tableau de bord Identity Manager
- Identity Reporting
- Self Service Password Reset
- Application utilisateur

L'image `.iso` du programme d'installation d'Identity Manager inclut une méthode d'installation d'OSP. Pour plus d'informations sur l'installation d'OSP, reportez-vous au Chapitre 14.2, « Installation du composant de gestion des mots de passe pour Identity Manager », page 179.

4.5.1 Présentation de l'authentification avec One SSO Provider

OSP prend en charge la spécification OAuth2 et requiert un serveur d'authentification LDAP. Par défaut, Identity Manager utilise le coffre-fort d'identité (eDirectory). OSP peut communiquer d'autres types de **sources d'authentification**, ou **coffres-forts d'identité**, pour gérer les demandes d'authentification. Vous pouvez configurer le type d'authentification qu'OSP doit utiliser : nom d'utilisateur et mot de passe, Kerberos ou SAML. Toutefois, OSP ne prend pas en charge les tickets de connexion MIT Kerberos ni SAP.

Comment OSP et SSO fonctionnent-ils ?

Si vous utilisez le coffre-fort d'identité comme service d'authentification et que les conteneurs spécifiés dans le coffre-fort d'identité comportent des CN et des mots de passe, les utilisateurs autorisés peuvent se connecter à Identity Manager immédiatement après l'installation. Sans ces comptes de connexion, seul l'administrateur que vous spécifiez durant l'installation peut se connecter immédiatement.

Lorsqu'un utilisateur se connecte à l'un des composants de type navigateur, le processus redirige la paire nom d'utilisateur/mot de passe de l'utilisateur vers le service OSP qui interroge le serveur d'authentification. Le serveur valide les références de l'utilisateur. OSP émet ensuite un jeton d'accès OAuth2 pour le composant et le navigateur. Le navigateur utilise le jeton pendant la session de l'utilisateur pour fournir un accès SSO à l'ensemble des composants de type navigateur.

Si vous utilisez Kerberos ou SAML, OSP accepte l'authentification du serveur de tickets Kerberos ou du fournisseur d'identité SAML, puis émet un jeton d'accès OAuth2 pour le composant auquel l'utilisateur s'est connecté.

Comment OSP fonctionne-t-il avec Kerberos ?

OSP et Kerberos veillent à ce que les utilisateurs puissent se connecter une fois pour ouvrir une session à l'aide de l'une des applications d'identité et d'Identity Reporting. Si la session de l'utilisateur expire, l'autorisation se produit automatiquement sans intervention de l'utilisateur. Après la déconnexion, les utilisateurs doivent toujours fermer le navigateur pour clôturer leur session. Dans le cas contraire, l'application redirige l'utilisateur vers la fenêtre de connexion et OSP donne de nouveau accès à la session de l'utilisateur.

Comment puis-je configurer l'authentification et l'accès Single Sign-on ?

Pour qu'OSP et SSO fonctionnent, vous devez installer OSP. Indiquez ensuite l'URL d'accès du client à chaque composant, l'URL qui redirige les requêtes de validation vers OSP ainsi que les paramètres du serveur d'authentification. Vous pouvez fournir ces informations lors de l'installation ou ultérieurement à l'aide de l'utilitaire de configuration RBPM. Vous pouvez également spécifier les paramètres de votre serveur de tickets Kerberos ou de votre fournisseur d'identité SAML.

Pour plus d'informations sur la configuration de l'authentification et de l'accès Single Sign-on, reportez-vous à la Partie VIII, « Configuration de l'accès Single Sign-on dans Identity Manager », page 317.

Dans une grappe, les paramètres de configuration doivent être identiques pour tous les membres de la grappe.

4.5.2 Présentation du fichier Keystore pour One SSO Provider

Identity Manager utilise un fichier Keystore qui prend en charge les communications `http` et `https` entre le service OSP et le serveur d'authentification. Vous créez le fichier Keystore lors de l'installation d'OSP. Vous créez également un mot de passe que le service OSP utilise pour les

interactions autorisées avec le serveur d'authentification. Pour plus d'informations, reportez-vous au Chapitre 14.2, « Installation du composant de gestion des mots de passe pour Identity Manager », page 179.

4.5.3 Présentation des événements d'audit pour One SSO Provider

OSP génère un événement unique pour indiquer qu'un utilisateur se connecte ou se déconnecte de l'application utilisateur ou d'Identity Reporting :

- 003E0204 lors d'une connexion
- 003E0201 lors d'une déconnexion

La taxonomie XDAS interprète ensuite ces événements OSP comme une connexion/déconnexion réussie ou un appel SOAP destiné à l'application utilisateur ou un événement « autre qu'une réussite ».

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.

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 17.
❑	2. Déterminez le type de programme d'installation que vous souhaitez utiliser. Pour plus d'informations, reportez-vous à la Section 5.2, « Présentation de la procédure d'installation », page 41.
❑	3. Déterminez les plates-formes de systèmes d'exploitation les plus adaptées à votre installation. Pour plus d'informations, reportez-vous à la Section 5.3.5, « Sélection d'une plate-forme de système d'exploitation pour Identity Manager », page 44. **REMARQUE :** Identity Manager prend en charge l'installation de Sentinel Log Management for Identity Governance and Administration (Sentinel Log Management for IGA) uniquement sur un serveur Linux. Si vous souhaitez utiliser Sentinel Log Management for IGA dans votre environnement, reportez-vous à aux rubriques Conditions préalables et Configuration système requise pour cette installation dans la section Installation de Sentinel Log Management for Identity Governance and Administration dans le *Guide d'installation de NetIQ Identity Manager pour Linux*. Toutefois, vous pouvez en utiliser un autre si votre solution d'identité est basée sur Windows uniquement.
❑	4. Déterminez l'ordre d'installation des composants et les emplacements d'installation de chacun. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.
❑	5. Assurez-vous que vous disposez d'une licence pour exécuter Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.4, « Présentation des licences et de l'activation », page 45.

	Éléments de la liste de contrôle
❑	6. 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 6.1, « Présentation de la communication dans Identity Manager », page 49.
❑	7. Déterminez si vous pouvez exécuter les programmes d'installation dans la langue de votre choix. Pour plus d'informations, reportez-vous à la Section 6.2, « Présentation du support linguistique », page 50.
❑	8. Vérifiez que vous disposez des fichiers d'installation d'Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.5, « Téléchargement des fichiers d'installation », page 45. **IMPORTANT :** pour que l'installation se déroule sans encombre, n'exécutez pas d'applications monopolisant énormément de ressources processeur lors de l'installation des composants d'Identity Manager. Vous devez arrêter les services Windows tels que le programme d'installation pour les modules Windows ainsi que Windows Update avant de commencer l'installation d'Identity Manager. Ne les démarrez qu'après avoir terminé l'installation.
❑	9. (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 6.3, « Garantie d'une haute disponibilité pour Identity Manager », page 52.
❑	10. 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.
❑	11. Vérifiez que les ordinateurs sur lesquels vous installez les composants Identity Manager répondent aux conditions requises spécifiées. Pour plus d'informations, reportez-vous aux sections suivantes : ◆ **Designer** : « Planification de l'installation de Designer » page 303 ◆ **Applications d'identité pour la gestion des rôles et des ressources** : « Planification de l'installation des applications d'identité » page 189 ◆ **Moteur Identity Manager** : « Planification de l'installation du moteur, des pilotes et des plug-ins » page 83 ◆ **Coffre-fort d'identité** : « Installation du coffre-fort d'identité » page 57 ◆ **iManager** : (Facultatif) « Planification de l'installation d'iManager » page 143 ◆ **SSPR (Self Service Password Reset)** : « Planification de l'installation du composant de gestion des mots de passe pour Identity Manager » page 177 ◆ **PostgreSQL** : « Planification de l'installation de PostgreSQL et de Tomcat » page 161 ◆ **Chargeur distant** : « Planification de l'installation du moteur, des pilotes et des plug-ins » page 83 ◆ **Création de rapports**: « Planification de l'installation du module Identity Reporting » page 259 ◆ **OSP (One SSO Provider)** : « Planification de l'installation du composant de gestion des mots de passe pour Identity Manager » page 177 ◆ **Tomcat** : « Planification de l'installation de PostgreSQL et de Tomcat » page 161 **REMARQUE :** NetIQ vous recommande de prendre note de chaque compte que vous créez durant la procédure d'installation.
❑	12. Activez vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 30.6, « Activation d'Identity Manager », page 359.

5.2 Présentation de la procédure d'installation

NetIQ fournit des programmes d'installation autonome pour les composants Identity Manager de manière à ce que vous disposiez de plus de flexibilité pour la configuration de votre environnement. Par exemple, la plupart des composants Identity Manager contiennent de grandes quantités de données, comme le coffre-fort d'identité, et devraient être installés sur des serveurs distincts.

La procédure d'installation autonome vous propose les fonctionnalités suivantes :

- personnalisation des paramètres des composants, y compris la structure de l'arborescence dans le coffre-fort d'identité ;
- installation dans des environnements distribués ou en grappe ;
- sélection des pilotes et création d'ensembles de pilotes à ajouter à votre solution de gestion des identités ;
- sélection des plug-ins iManager à ajouter à votre solution de gestion des identités ;
- utilisation d'un compte non-administrateur pour installer certains composants ;
- prise en charge de plusieurs plates-formes de base de données ;
- utilisation d'Apache Tomcat pour tous les systèmes d'exploitation pris en charge ;
- création d'un environnement de production pris en charge ;
- mise à niveau d'une version précédente d'Identity Manager.

Pour de meilleurs résultats, exécutez le programme d'installation autonome dans l'ordre indiqué par votre solution de gestion des identités. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.

5.3 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.

5.3.1 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 (non pris en charge sous Windows)

   REMARQUE : NetIQ prend en charge l'installation de ce composant uniquement sur un serveur Linux. Pour obtenir des instructions d'installation, reportez-vous au *Guide d'installation de NetIQ Identity Manager pour Linux*. Toutefois, vous pouvez en utiliser un autre si votre solution d'identité est basée sur Windows uniquement.

2. Coffre-fort d'identité
3. Moteur Identity Manager, pilotes et plug-ins d'iManager
4. (Facultatif) iManager
5. Designer
6. Tomcat et PostgreSQL
7. OSP
8. SSPR
9. Applications d'identité
10. (Facultatif) Analyzer

5.3.2 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. Coffre-fort d'identité
2. Sentinel Log Management for IGA (non pris en charge sous Windows)

   REMARQUE : NetIQ prend en charge l'installation de ce composant uniquement sur un serveur Linux. Pour obtenir des instructions d'installation, reportez-vous au *Guide d'installation de NetIQ Identity Manager pour Linux*. Toutefois, vous pouvez en utiliser un autre si votre solution d'identité est basée sur Windows uniquement.

3. Moteur Identity Manager, pilotes et plug-ins d'iManager
4. (Facultatif) iManager
5. Designer
6. Tomcat et PostgreSQL
7. OSP
8. SSPR
9. Applications d'identité

10. Identity Reporting
11. (Facultatif) Analyzer

5.3.3 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. Coffre-fort d'identité
3. Moteur Identity Manager, pilotes et plug-ins d'iManager
4. (Facultatif) iManager
5. Designer
6. Tomcat et PostgreSQL
7. OSP
8. SSPR
9. Applications d'identité
10. Identity Reporting
11. (Facultatif) Analyzer

5.3.4 Configuration recommandée pour le serveur

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
Serveurs 1 et 2 (réplique d'annuaire entre deux serveurs)	◆ Coffre-fort d'identité ◆ Moteur Identity Manager
Serveurs 3 et 4 (grappe de deux serveurs)	◆ Applications d'identité ◆ iManager ◆ Un fournisseur SSO ◆ Chargeur distant ◆ SSPR (réinitialisation du mot de passe en self-service) **REMARQUE :** NetIQ vous recommande d'installer les applications d'identité et le fournisseur d'authentification unique One sur le même serveur.
Serveur 5 (ou une grappe de serveurs)	Bases de données Identity Manager : ◆ Applications d'identité ◆ Identity Reporting
Serveur 6	Identity Reporting

Configuration de l'ordinateur	Installation du composant
Serveur 7	Sentinel Log Management for IGA
Postes de travail client (1+)	◆ Designer ◆ iManager Workstation ◆ Navigateurs Internet qui accèdent aux applications d'identité et de création de rapports

5.3.5 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
Poste de travail Windows	Designer Poste de travail iManager (client) Accès par navigateur Web aux applications d'identité et à Identity Reporting
Windows Server	Analyzer Designer Applications d'identité Moteur Identity Manager Identity Reporting Coffre-fort d'identité (Serveur) iManager Chargeur distant .NET Un fournisseur SSO PostgreSQL Chargeur distant SSPR (réinitialisation du mot de passe en self-service) Tomcat

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 303
- « Planification de l'installation d'iManager » page 143
- « Installation du coffre-fort d'identité » page 57
- « Planification de l'installation du moteur, des pilotes et des plug-ins » page 83

- « Planification de l'installation des applications d'identité » page 189
- « Planification de l'installation du composant de gestion des mots de passe pour Identity Manager » page 177
- « Planification de l'installation de PostgreSQL et de Tomcat » page 161

5.4 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 30.6, « Activation d'Identity Manager », page 359.

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.

5.5 Téléchargement des fichiers d'installation

NetIQ fournit les fichiers ISO contenant tous les composants d'une installation d'Identity Manager complète. Chaque fichier inclut les versions du produit. Le nom du fichier ISO identifie la plate-forme. Par exemple : `Identity_Manager_version_Windows.iso`.

REMARQUE : les images ISO sont des fichiers volumineux. Veillez à les télécharger sur un volume ou un DVD qui prend en charge leur taille.

Pour télécharger les fichiers d'installation Identity Manager :

1. Accédez au site Web de téléchargement de NetIQ.
2. Dans le menu **Product or Technology** (Produit ou technologie), sélectionnez **Identity Manager**, puis cliquez sur **Search** (Rechercher).
3. Sur la page des téléchargements NetIQ Identity Manager, cliquez sur le bouton **Télécharger** (Download) en regard du fichier ISO à télécharger.

4 Suivez les invites à l'écran pour télécharger le fichier dans un répertoire sur votre ordinateur.

5 Montez le fichier `.iso` téléchargé en tant que volume ou utilisez ce fichier `.iso` pour créer un DVD du logiciel.

5.6 Emplacement des fichiers exécutables et chemins d'installation par défaut

Le tableau suivant fournit des informations sur l'emplacement des fichiers exécutables dans le fichier ISO du produit et les chemins d'installation par défaut des composants sur votre système de fichiers :

Composant Identity Manager	Version (Advanced Edition/Standard Edition)	Emplacement de l'exécutable dans le fichier ISO	Chemin d'installation par défaut
Coffre-fort d'identité	Advanced et Standard	`Setup.exe` situé à l'emplacement `\products\eDirectory\x64\`	`C:\NetIQ`
iManager	Advanced et Standard	◆ **Installation des serveurs :** `iManagerInstall.exe` situé à l'emplacement `\extracted_directory\products\iManager\installs\win\` ◆ **Installation du poste de travail :** `iManager.bat` situé à l'emplacement `imanager\bin`	`C:\Program Files\Novell`
Moteur Identity Manager, pilotes et plug-ins	Advanced et Standard	`idm_install.exe` situé à l'emplacement `\products\IDM\windows\setup`	`C:\Novell`
Chargeur distant	Advanced et Standard	`idm_install.exe` situé à l'emplacement `\products\idm\windows\setup`	`C:\Novell`
PostgreSQL et Tomcat (base de données et serveur d'application pris en charge)	Advanced et Standard	`TomcatPostgreSQL.exe` situé à l'emplacement `products\CommonApplication\postgre_tomcat_install\`	`C:\NetIQ\idm\apps\tomcat`
Single Sign-on (OSP)	Advanced et Standard	`osp-install-win.exe` situé à l'emplacement `\products\CommonApplication\osp_install`	`C:\NetIQ\idm\apps\osp`
Réinitialisation des mots de passe en self-service (SSPR, Self Service Password Reset)	Advanced et Standard	`sspr-install-win.exe` situé à l'emplacement `\products\CommonApplication\sspr_install`	`C:\NetIQ\idm\apps\sspr`
Applications d'identité	Advanced Edition uniquement	`IdmUserApp.exe` situé à l'emplacement `products\UserApplication`	`C:\NetIQ\idm\apps\UserApplication`

Composant Identity Manager	Version (Advanced Edition/Standard Edition)	Emplacement de l'exécutable dans le fichier ISO	Chemin d'installation par défaut
Designer pour Identity Manager	Advanced et Standard	`install.exe` situé à l'emplacement `\products\Designer\`	`c:\NetIQ\idm\apps\Designer`
Identity Reporting	Module complet avec la version Advanced Edition	`rpt-install-win.exe` situé à l'emplacement `\products\Reporting`	`C:\NetIQ\idm\apps\IdentityReporting`
	Module partiel avec la version Standard Edition		
Analyzer pour Identity Manager	Advanced et Standard	`install.exe` situé à l'emplacement `\products\Analyzer\`	`C:\NetIQ\idm\apps\Analyzer`

6 Considérations relatives à 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.

6.1 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
435	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
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

Numéro de port	Composant/ ordinateur	Utilisation du port
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	*N'écoute pas (option par défaut)* 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 Sentinel
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

6.2 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 donnée, changez les paramètres régionaux à l'aide de l'option **Paramètres régionaux**.

6.2.1 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
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.

6.2.2 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 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.

6.3 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 :
  - Coffre-fort d'identité
  - 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 5.3.4, « Configuration recommandée pour le serveur », page 43
Exécution du coffre-fort d'identité dans une grappe	« Conditions préalables à l'installation du coffre-fort d'identité » page 58 Section A.2, « Configuration de NetIQ Identity Manager sur une grappe eDirectory », page 427 Déploiement d'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	Section 14.2.4, « Configuration d'OSP et de SSPR pour la mise en grappe », page 186 Section 15.1.3, « Conditions requises et considérations relatives à l'installation des applications d'identité », page 192 Section 15.4.2, « Activation de l'index des autorisations pour la mise en grappe », page 205 Section 15.4.4, « Préparation d'une grappe pour les applications d'identité », page 206 Section 15.6.2, « Configuration du pilote d'application utilisateur pour la mise en grappe », page 222 « Mise à jour des liens SSPR dans le tableau de bord pour un environnement distribué ou de grappe » page 234

II Installation du moteur Identity Manager

Cette section fournit des informations sur l'installation d'une partie de l'infrastructure de base pour votre serveur Identity Manager. Ce programme d'installation vous permet d'installer les composants suivants :

- Pilotes Identity Manager
- Moteur Identity Manager
- Plug-ins iManager pour Identity Manager

Pour votre confort, NetIQ regroupe les composants dans le même programme d'installation. Vous pouvez choisir de les installer sur le même serveur ou individuellement. Les fichiers d'installation sont situés dans le répertoire `\products\idm` du paquetage d'installation d'Identity Manager. Par défaut, le programme d'installation installe les composants à l'emplacement `C:\NetIQ`.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous à la Section 8.1, « Liste de contrôle pour l'installation du moteur, des pilotes et des plug-ins Identity Manager », page 83.

REMARQUE : ce programme d'installation peut également installer le chargeur distant. Pour plus d'informations, reportez-vous à la Partie 10, « Installation et gestion du chargeur distant », page 97.

---

7 Installation du coffre-fort d'identité

Cette section vous guide tout au long de la procédure d'installation des composants requis pour le coffre-fort d'identité, qui stocke des informations spécifiques à Identity Manager telles que les configurations de pilote, les paramètres et les stratégies.

Les fichiers d'installation sont situés dans le répertoire `\products\eDirectory\`*`type_processeur`*`\` du fichier image `.iso` du paquetage d'installation d'Identity Manager. Par défaut, le programme d'installation installe le coffre-fort d'identité à l'emplacement `C:\NetIQ\Directory`.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous au Chapitre 7.1, « Planification de l'installation du coffre-fort d'identité », page 57.

7.1 Planification de l'installation 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.

7.1.1 Liste de contrôle pour l'installation du coffre-fort d'identité

NetIQ recommande d'effectuer 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 à la Partie I, « Introduction », page 17.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3.4, « Configuration recommandée pour le serveur », page 43.
❑	3. Passez en revue les considérations relatives à l'installation du coffre-fort d'identité pour vous assurer que les ordinateurs remplissent les conditions préalables. Pour plus d'informations, reportez-vous à la Section 7.1.2, « Conditions préalables et considérations relatives à l'installation du coffre-fort d'identité », page 58.
❑	4. Vérifiez la configuration matérielle et logicielle requise pour les ordinateurs qui hébergeront le coffre-fort d'identité. Pour plus d'informations, reportez-vous à la Section 7.1.4, « Configuration système requise pour le coffre-fort d'identité », page 61.

	Éléments de la liste de contrôle
❑	5. Familiarisez-vous avec l'utilisation des caractères d'échappement dans les noms des conteneurs du coffre-fort d'identité qui contiennent un point (« . »). Pour plus d'informations, reportez-vous à la Section 7.2.1, « Utilisation de caractères d'échappement lorsque le nom d'un conteneur comprend un point (« . ») », page 62.
❑	6. Familiarisez-vous avec l'utilisation du coffre-fort d'identité dans un environnement qui utilise des adresses IPv6. Pour plus d'informations, reportez-vous à la Section 7.2.4, « Utilisation d'adresses IPv6 sur le serveur du coffre-fort d'identité », page 68.
❑	7. Familiarisez-vous avec les ports requis pour les communications LDAP. Pour plus d'informations, reportez-vous à la Section 7.2.5, « Utilisation du protocole LDAP pour communiquer avec le coffre-fort d'identité », page 69.
❑	8. Pour obtenir des instructions d'installation, reportez-vous à l'une des sections suivantes : ◆ Pour une installation guidée (assistant), reportez-vous à la Section 7.3.1, « Utilisation de l'assistant pour l'installation du coffre-fort d'identité », page 71. ◆ Pour une installation en mode silencieux (sans surveillance), reportez-vous à la Section 7.3.2, « Installation et configuration silencieuses du coffre-fort d'identité », page 72.
❑	9. (Facultatif) Excluez le répertoire DIB stocké sur votre serveur eDirectory de tous les processus antivirus ou de sauvegarde.
❑	10. (Facultatif) Sauvegardez votre répertoire DIB. Pour plus d'informations, reportez-vous à la section Backing Up and Restoring NetIQ eDirectory (Sauvegarde et restauration de NetIQ¬eDirectory) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).
❑	11. Installez le moteur Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 8, « Planification de l'installation du moteur, des pilotes et des plug-ins », page 83.

7.1.2 Conditions préalables et considérations relatives à l'installation du coffre-fort d'identité

Le coffre-fort d'identité utilise un annuaire pour stocker les objets synchronisés via la solution Identity Manager. Les sections suivantes contiennent des instructions pour vous aider à planifier le déploiement de NetIQ eDirectory en tant que cadre pour le coffre-fort d'identité.

Conditions préalables à l'installation du coffre-fort d'identité

NetIQ recommande de passer en revue les considérations suivantes avant d'installer eDirectory comme cadre pour le coffre-fort d'identité :

- Pour que l'infrastructure eDirectory fonctionne efficacement, vous devez configurer une adresse IP statique sur le serveur. Si vous utilisez des adresses DHCP sur le serveur, eDirectory peut avoir des résultats imprévisibles.
- Synchronisez l'heure de tous les serveurs du réseau. NetIQ recommande l'utilisation de l'option `ntp` de NTP (Network Time Protocol).

- (Conditionnel) Pour installer un serveur secondaire, toutes les répliques de la partition sur laquelle vous installez le produit doivent être activées.
- (Conditionnel) Pour installer un serveur secondaire dans une arborescence existante en tant qu'utilisateur non-administrateur, créez un conteneur, puis partitionnez-le. Vérifiez que vous disposez des droits suivants :
  - droits Superviseur sur la partition dans laquelle ajouter le serveur ;
  - droits Superviseur sur le conteneur dans lequel ajouter le serveur ;
  - tous les droits d'attribut (droits de lecture, de comparaison et d'écriture sur l'objet `W0.KAP.Security`) ;
  - droits d'attributs (droits de lecture et de comparaison sur l'objet Conteneur de sécurité) ;
  - droits d'entrée (droits d'exploration sur l'objet Conteneur de sécurité).

  S'il existe moins de 3 répliques, ces droits sont obligatoires pour pouvoir en ajouter une.
- (Conditionnel) Pour installer un serveur secondaire dans une arborescence existante en tant qu'utilisateur non-administrateur, assurez-vous qu'au moins un des serveurs de l'arborescence a la même version ou une version ultérieure d'eDirectory par rapport à celle du serveur secondaire ajouté en tant qu'administrateur de conteneur. Si la version du serveur secondaire ajouté est ultérieure, l'administrateur de l'arborescence doit étendre le schéma avant d'ajouter le serveur secondaire en tant qu'administrateur de conteneur.
- Lors de la configuration d'eDirectory, vous devez activer un port NCP (NetWare Core Protocol) (port 524 par défaut) dans le pare-feu afin de permettre l'ajout du serveur secondaire. Vous pouvez également activer les ports de service par défaut suivants en fonction de vos besoins :
  - LDAP texte clair - 389
  - LDAP sécurisé - 636
  - HTTP texte clair - 8028
  - HTTP sécurisé - 8030
- Vous devez installer NICI (Novell International Cryptographic Infrastructure) sur tous les postes de travail qui utilisent des utilitaires de gestion pour eDirectory, comme iManager. NICI et eDirectory prennent en charge des tailles de clé de 4 096 bits maximum. Pour plus d'informations, reportez-vous à la section Installation de NICI du *Guide d'installation de NetIQ eDirectory*.
- (Conditionnel) Si les noms des conteneurs de votre arborescence eDirectory contiennent un point, vous devez utiliser des caractères d'échappement pour spécifier les paramètres de nom d'administrateur, de contexte administrateur et de contexte du serveur au cours de l'installation et lors de l'ajout d'un serveur à une arborescence existante. Pour plus d'informations, reportez-vous à la Section 7.2.1, « Utilisation de caractères d'échappement lorsque le nom d'un conteneur comprend un point (« . ») », page 62.
- Vous devez disposer de droits d'administrateur sur le serveur et sur toutes les parties de l'arborescence eDirectory qui contiennent des objets Utilisateur reconnaissant le domaine. Pour procéder à l'installation dans une arborescence existante, vous devez disposer de droits d'administrateur sur l'objet Arborescence afin de pouvoir étendre le schéma et créer des objets.
- Dans la mesure où un système NTFS offre un processus de transaction plus sécurisé qu'un système de fichiers FAT, vous ne pouvez installer eDirectory que sur une partition NTFS. Aussi, si vous disposez uniquement de systèmes de fichiers FAT, effectuez l'une des opérations suivantes :
  - Utilisez l'Administrateur de disques. Pour plus d'informations, reportez-vous à la documentation relative à Windows Server.
  - Créez une partition et attribuez-lui le format NTFS.

- Convertissez un système de fichiers FAT existant au format NTFS à l'aide de la commande CONVERT.
- Pour plus d'informations, reportez-vous à la documentation relative à Windows Server.

Si votre serveur ne dispose que d'un système de fichiers FAT et que vous omettez ce processus, le programme d'installation vous demande de fournir une partition NTFS.

- Vous devez exécuter la version la plus récente du service Windows SNMP.
- Avant de commencer la procédure d'installation, assurez-vous que votre système d'exploitation Windows exécute les derniers service packs.
- Si vous procédez à l'installation sur une machine virtuelle dotée d'une adresse DHCP ou sur une machine physique ou virtuelle sur laquelle SLP n'est pas diffusé, vérifiez que l'agent Annuaire est configuré sur votre réseau.

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'au moins deux serveurs Windows avec un logiciel de grappe.
- 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*.

7.1.3 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 permet d'automatiser 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.

7.1.4 Configuration système requise pour le coffre-fort d'identité

Cette section décrit la configuration minimale requise pour le(s) serveur(s) sur le(s)quel(s) vous souhaitez installer le coffre-fort d'identité. Veuillez passer en revue les conditions préalables requises et les considérations relatives à l'installation, en particulier celles liées au système d'exploitation.

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

Catégorie	Configuration requise
Processeur	1 GHz
Espace disque	◆ 300 Mo pour le coffre-fort d'identité ◆ 150 Mo d'espace disque supplémentaire par tranche de 50 000 utilisateurs
Mémoire	2 Go

Catégorie	Configuration requise
Système d'exploitation (certifié)	L'un des systèmes d'exploitation 64 bits suivants : ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 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.
Système 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 ◆ Virtualisation de Windows Server 2012 R2 avec Hyper-V (prise en charge) 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.
Services Annuaire	NetIQ eDirectory 9.1

7.2 Préparation de l'installation du coffre-fort d'identité

L'environnement d'installation du coffre-fort d'identité doit être configuré correctement. Par exemple, le serveur doit disposer d'une méthode (un service ou un fichier spécifié) pouvant être utilisée pour résoudre les noms d'arborescence du coffre-fort d'identité en adresses de renvoi du serveur. Cette section vous explique comment préparer votre environnement avant d'installer le coffre-fort d'identité.

7.2.1 Utilisation de caractères d'échappement lorsque le nom d'un conteneur comprend un point (« . »)

Vous pouvez ajouter à une arborescence d'annuaire un serveur Windows dont le nom contient un point, par exemple, `O=netiq.com` ou `C=u.s.a`. Toutefois, si les noms de vos conteneurs dans l'arborescence comportent un point (« . »), vous devez utiliser des caractères d'échappement. Passez en revue les considérations suivantes :

- N'utilisez pas de point au début d'un nom de serveur, par exemple, `.netiq`.
- Insérez une barre oblique inverse (« \ ») avant le point dans le nom du conteneur. Par exemple :

  ```
  O=novell\.com
  ```

ou

```
C=a\.b\.c
```

Insérez des caractères d'échappement lorsque vous entrez un nom et un contexte d'administrateur contenant des points pour des utilitaires tels qu'iMonitor, iManager, DHost iConsole, DSRepair, Backup, DSMerge, DSLogin et ldapconfig. Par exemple, lorsque vous vous connectez à iMonitor, si le nom du conteneur Organisation dans votre arborescence est `netiq.com`, entrez `'admin.netiq\.com'` ou `admin.netiq\.com`.

7.2.2 Utilisation d'OpenSLP ou d'un fichier hosts.nds pour résoudre les noms d'arborescence

Avant d'installer l'infrastructure de coffre-fort d'identité, assurez-vous que le serveur dispose d'une méthode (un service ou un fichier spécifié) pouvant être utilisée pour résoudre les noms d'arborescence du coffre-fort d'identité en adresses de renvoi du serveur. NetIQ recommande l'utilisation des services SLP (Service Location Protocol) pour résoudre les noms d'arborescence. Dans les versions précédentes d'eDirectory, OpenSLP était installé automatiquement. Toutefois, à partir de la version 8.8, OpenSLP n'est plus installé automatiquement lors de l'installation d'eDirectory. Vous devez installer séparément un service SLP ou utiliser un fichier `hosts.nds`. Si vous utilisez un service SLP, les agents d'annuaire pour ce service (SLPDA) doivent être stables.

Cette section contient les informations suivantes :

- « Utilisation d'un fichier hosts.nds pour résoudre les noms d'arborescence » page 63
- « Présentation d'OpenSLP » page 64
- « Configuration de SLP pour le coffre-fort d'identité » page 67

Utilisation d'un fichier hosts.nds pour résoudre les noms d'arborescence

Le fichier `hosts.nds` est une table de recherche statique utilisée par les applications de coffre-fort d'identité pour rechercher des partitions et des serveurs de coffre-fort d'identité. Il vous permet d'éviter les délais de multidiffusion SLP lorsqu'aucun SLPDA n'est présent sur le réseau. Pour chaque arborescence ou serveur, vous devez spécifier les informations suivantes dans une seule ligne du fichier `hosts.nds` :

- **Nom du serveur ou nom de l'arborescence** : les noms d'arborescence doivent se terminer par un point final (.).
- **Adresse Internet** : il peut s'agir d'un nom DNS ou d'une adresse IP. N'utilisez pas `localhost`.
- **Port du serveur** : facultatif, ajouté à l'adresse Internet à l'aide du signe deux-points (:).

Il n'est pas nécessaire d'inclure une entrée pour le serveur local dans le fichier, sauf si le serveur n'écoute pas sur un port NCP par défaut.

Pour configurer un fichier hosts.nds :

1. Créez ou ouvrez un fichier `hosts.nds`.
2. Ajoutez les informations suivantes :

   `partition_name.tree_name. host_name/ip-addr:port server_name dns-addr/ip-addr:port`

   Par exemple :

```
# This is an example of a hosts.nds file:
# Tree name Internet address/DNS Resolvable Name
  CORPORATE. myserver.mycompany.com
  novell.CORPORATE. 1.2.3.4:524

# Server name Internet address
  CORPSERVER myserver.mycompany.com:524
```

3 (Facultatif) Si vous décidez par la suite d'utiliser SLP pour résoudre le nom d'arborescence et garantir la disponibilité de l'arborescence du coffre-fort d'identité sur le réseau, ajoutez le texte suivant au fichier `hosts.nds` :

```
/usr/bin/slptool findattrs services:ndap.novell:///(svcname-ws==[treename or *])"
```

Par exemple, pour rechercher les services dont l'attribut `svcname-ws` correspond à la valeur `SAMPLE_TREE`, entrez la commande suivante :

```
/usr/bin/slptool findattrs services:ndap.novell:///(svcname-ws==SAMPLE_TREE)"
```

REMARQUE : effectuez cette opération après avoir installé SLP et le coffre-fort d'identité.

Si vous disposez d'un service dont l'attribut `svcname-ws` a pour valeur `SAMPLE_TREE`, vous obtenez un résultat similaire à `servicndap.novell:///SAMPLE_TREE`. Sinon, la recherche ne renvoie aucun résultat.

Présentation d'OpenSLP

OpenSLP est une mise en œuvre Open Source de la norme IETF Service Location Protocol version 2.0, documentée dans la RFC (Request for Comments) 2608 de l'IETF.

L'interface fournie par le code source OpenSLP est une mise en œuvre d'une autre norme de l'IETF concernant l'accès par programme à la fonctionnalité SLP, documentée dans la RFC 2614.

Pour comprendre parfaitement les travaux de SLP, il est important de lire ces documents et de les assimiler. Leur lecture peut s'avérer laborieuse, mais ils sont essentiels pour procéder à une configuration correcte de SLP sur un intranet.

Pour plus d'informations sur le projet OpenSLP, reportez-vous aux sites Web d'OpenSLP et de SourceForge. Le site Web d'OpenSLP propose plusieurs documents qui offrent de précieux conseils de configuration. La plupart de ces documents sont encore incomplets à la date de publication de la présente documentation.

Cette section inclut les rubriques suivantes sur l'utilisation de SLP et sa relation avec le coffre-fort d'identité :

- « Protocole SLP NetIQ » page 65
- « Agents Utilisateur » page 65
- « Agents Service » page 66
- « Agents Annuaire » page 66

Protocole SLP NetIQ

La version NetIQ de SLP prend certaines libertés vis-à-vis de la norme SLP afin de fournir un environnement d'annonce de service renforcé, mais au prix d'une certaine évolutivité.

Par exemple, pour améliorer l'évolutivité d'une structure d'annonce de service, vous pouvez limiter le nombre de paquets diffusés ou multidiffusés sur un sous-réseau. La norme SLP gère ce facteur en imposant des limitations aux agents Service et Utilisateur concernant les requêtes à l'agent Annuaire. Le premier agent Annuaire identifié qui dessert l'étendue souhaitée est celui qu'un agent de service (et par conséquent des agents Utilisateur locaux) utilisera pour toutes les requêtes futures sur cette étendue.

La mise en œuvre de NetIQ SLP permet d'analyser tous les agents Annuaire connus, à la recherche des informations de la requête. Un acheminement AR de 300 millisecondes étant considéré comme trop long, 10 serveurs peuvent être analysés en 3 à 5 secondes. Il n'est pas nécessaire d'effectuer cette opération si SLP est configuré correctement sur le réseau et que OpenSLP considère le réseau comme configuré correctement pour le trafic SLP. Les valeurs de timeout de réponse de OpenSLP sont supérieures à celles du fournisseur de services SLP de NetIQ et cela limite le nombre d'agents Annuaire au premier qui répond, que les informations de celui-ci soient ou non précises et complètes.

Agents Utilisateur

Un agent Utilisateur prend la forme physique d'une bibliothèque statique ou dynamique liée à une application. Il permet à l'application d'émettre des requêtes de services SLP. La fonction de l'agent Utilisateur est de fournir une interface par programmation aux clients pour leurs requêtes de services, et aux services pour leur permettre de publier leurs annonces. Un agent Utilisateur contacte un agent Annuaire pour interroger des services enregistrés d'une classe de service et d'une étendue spécifiées.

Les agents Utilisateur suivent un algorithme pour obtenir l'adresse d'un agent Annuaire auquel les requêtes seront envoyées. Une fois qu'ils ont obtenu l'adresse d'un agent Annuaire sur une étendue spécifiée, ils continuent à utiliser cette adresse pour cette étendue jusqu'à ce qu'elle ne réponde plus. Là, ils se procurent l'adresse d'un autre agent Annuaire pour l'étendue. Les agents Utilisateur localisent l'adresse d'un agent Annuaire sur une étendue spécifiée en :

1. vérifiant si l'identificateur de socket de la requête en cours est connecté à un agent Annuaire pour l'étendue indiquée ; s'il se trouve que la requête fait partie d'une requête en plusieurs parties, elle peut déjà contenir une connexion en cache ;
2. recherchant dans le cache de l'agent Annuaire connu un agent Annuaire correspondant à l'étendue indiquée ;
3. recherchant auprès de l'agent Service local un agent Annuaire de l'étendue spécifiée (et en ajoutant de nouvelles adresses au cache) ;
4. interrogeant DHCP pour obtenir des adresses d'agents Annuaire configurées pour le réseau et correspondant à l'étendue indiquée (et en ajoutant de nouvelles adresses au cache) ;
5. envoyant une requête d'identification d'agent Annuaire par multidiffusion sur un port connu (et en ajoutant de nouvelles adresses au cache).

L'étendue indiquée est celle « par défaut », sauf spécification contraire. Cela signifie que si aucune étendue n'est définie de façon statique dans le fichier de configuration SLP et qu'aucune étendue n'est indiquée dans la requête, l'étendue utilisée est le mot « default ». Notez également que le coffre-fort d'identité n'indique jamais d'étendue dans ses enregistrements. S'il existe une étendue configurée statiquement, celle-ci devient l'étendue par défaut pour les requêtes de l'agent Utilisateur local et les enregistrements de l'agent Service en l'absence d'une étendue spécifiée.

Agents Service

Les agents de service prennent la forme physique d'un processus distinct exécuté sur l'ordinateur hôte. Le fichier `slpd.exe` s'exécute en tant que service sur la machine locale. Des agents utilisateur interrogent l'agent de service local en envoyant des messages à l'adresse de bouclage sur un port connu.

La fonction de l'agent Service consiste à fournir des points de stockage et de maintenance persistants pour des services locaux s'étant enregistrés auprès de SLP. L'agent de service a pour tâche principale de gérer une base de données en mémoire des services locaux enregistrés. En fait, un service ne peut pas s'enregistrer auprès de SLP tant qu'un agent de service local n'est pas présent. Les clients peuvent identifier les services au moyen d'une seule bibliothèque d'agent Utilisateur, mais l'enregistrement nécessite obligatoirement un agent de service (SA), principalement parce que cet agent doit régulièrement vérifier l'existence de services enregistrés pour maintenir l'enregistrement des agents Annuaire à l'écoute.

Un agent de service localise et met en cache les agents Annuaire et la liste de l'étendue qu'ils prennent en charge en envoyant directement une requête d'identification d'agent Annuaire à des adresses d'agent Annuaire potentielles en :

1. vérifiant toutes les adresses d'agent Annuaire configurées statiquement (et en ajoutant de nouvelles au cache d'agent Annuaire connu de l'agent de service) ;
2. demandant la liste des agents Annuaire et des étendues à DHCP (et en en ajoutant de nouveaux au cache d'agent Annuaire connu de l'agent de service) ;
3. envoyant une requête d'identification d'agent Annuaire par multidiffusion sur un port connu (et en en ajoutant de nouvelles au cache d'agent Annuaire connu de l'agent de service) ;
4. recevant les paquets d'annonce régulièrement diffusés par les agents Annuaire (et en ajoutant les nouveaux au cache d'agent Annuaire connu de l'agent de service).

Le fait qu'un agent Utilisateur interroge toujours l'agent Service local en premier lieu revêt toute son importance, car la réponse de l'agent Service local détermine si l'agent Utilisateur passe ou non à l'étape suivante de la découverte (en l'occurrence, DHCP-- reportez-vous à l'Étape 3 et l'Étape 4 de la section « Agents Utilisateur » page 65).

Agents Annuaire

Le fonction de l'agent Annuaire consiste à fournir un cache persistant à long terme pour les services annoncés, ainsi qu'un point d'accès permettant aux agents Utilisateur de rechercher des services. En tant que cache, l'agent Annuaire reste à l'écoute de l'annonce de nouveaux services par les agents de service et met en cache ces notifications. Le cache d'un agent Annuaire se complète ou se remplit rapidement. Les agents Annuaire utilisent un algorithme d'expiration pour faire expirer les entrées de cache. Lorsqu'un agent Annuaire s'active, il lit le cache du stockage persistant (en général un disque dur), puis commence à faire expirer les entrées selon l'algorithme. Lorsqu'un nouvel agent Annuaire arrive ou lorsqu'un cache a été supprimé, l'agent Annuaire détecte cette condition et envoie une notification spéciale à tous les agents Service à l'écoute pour qu'ils vident leurs bases de données locales, de manière à ce que l'agent Annuaire puisse rapidement créer son cache.

En l'absence d'agents Annuaire, l'agent Utilisateur effectue une requête de multidiffusion générale à laquelle les agents de service peuvent répondre listant ainsi les services demandés de la même manière que les agents Annuaire créent leur cache. La liste des services renvoyée par une telle requête est incomplète et bien plus localisée que celle fournie par un agent Annuaire, notamment en présence d'un filtrage multidiffusion mis en œuvre par un grand nombre d'administrateurs réseaux, lesquels limitent les diffusions et les multidiffusions au sous-réseau local seulement.

En bref, tout s'articule autour de l'agent Annuaire trouvé par un agent Utilisateur dans une étendue donnée.

Configuration de SLP pour le coffre-fort d'identité

Les paramètres suivants du fichier `%systemroot%/slp.conf` contrôlent la découverte des agents Annuaire :

```
net.slp.useScopes = comma-delimited scope list
net.slp.DAAddresses = comma-delimited address list
net.slp.passiveDADetection = <"true" or "false">
net.slp.activeDADetection = <"true" or "false">
net.slp.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

useScopes

Ce paramètre indique à quelles étendues l'agent Service va s'annoncer et à quelles étendues les requêtes seront adressées en l'absence d'une étendue spécifique lors de l'enregistrement ou de la requête effectuée par le service ou l'application client. Comme le coffre-fort d'identité émet toujours ses annonces et ses requêtes sur l'étendue par défaut, cette liste sera considérée comme la liste d'étendues par défaut pour l'ensemble des enregistrements et des requêtes du coffre-fort d'identité.

DAAddresses

Ce paramètre représente une liste d'adresses IP décimales avec points, séparées par une virgule, d'agents Annuaire qui doivent être préférés à tous les autres. Si cette liste des agents Annuaire configurés ne prend pas en charge l'étendue d'un enregistrement ou d'une requête, les agents Service et Utilisateur font alors appel à la découverte multidiffusion des agents Annuaire, sauf si cette fonction a été désactivée.

passiveDADetection

Par défaut, ce paramètre est défini sur `True`. Les agents Annuaire annoncent régulièrement leur existence sur le sous-réseau au moyen d'un port connu si celui-ci est configuré à cet effet. Ils s'intitulent paquets DAAdvert. Si cette option est définie sur False, tous les paquets DAAdvert diffusés sont ignorés par l'agent Service.

activeDADetection

Par défaut, ce paramètre est défini sur `True`. Elle permet à l'agent de service de diffuser régulièrement une requête à tous les agents Annuaire pour qu'ils répondent au moyen d'un paquet DAAdvert dirigé. Un paquet dirigé n'est pas diffusé, mais envoyé directement à l'agent de service en réponse à ces requêtes. Si cette option est définie sur False, aucune requête régulière de découverte d'agents Annuaire n'est diffusée par l'agent Service.

DAActiveDirectoryInterval

Représente un paramètre à trois états. La valeur par défaut est `1`. Cela signifie que l'agent Service doit seulement envoyer une requête de découverte d'agents Annuaire lors de l'initialisation. Si vous définissez cette option sur la valeur 0, vous obtenez le même effet qu'en définissant l'option activeDADetection sur False. Toute autre valeur indique un nombre de secondes entre les diffusions de découverte.

Employées correctement, ces options assurent une utilisation appropriée de la bande passante du réseau pour l'annonce de services. En fait, les paramètres par défaut sont conçus pour optimiser l'évolutivité d'un réseau moyen.

7.2.3 Amélioration des performances du coffre-fort d'identité

eDirectory, l'infrastructure sous-jacente du coffre-fort d'identité, est une application qui consomme davantage d'E/S que de ressources processeur. Deux facteurs augmentent les performances du coffre-fort d'identité : une mémoire cache plus importante et des processeurs plus rapides. Pour obtenir des résultats optimaux, mettez en cache autant de paramètres de l'ensemble DIB (Directory Information Base, base de données des informations de l'Annuaire) que le permet le matériel.

Bien qu'eDirectory fonctionne correctement avec un seul processeur, vous pouvez envisager d'utiliser plusieurs processeurs. L'ajout de processeurs permet d'améliorer les performances dans des domaines tels que les connexions utilisateur. Le fait que plusieurs threads soient actifs sur plusieurs processeurs améliore également les performances.

Le tableau ci-dessous fournit des indications générales concernant les paramètres du serveur, en fonction du nombre d'objets de votre arborescence eDirectory.

Objets	Mémoire	Disque dur
100 000	384 Mo	144 Mo
1 million	4 Go	1,5 Go
10 millions	2 Go et plus	15 Go

Par exemple, une installation de base de eDirectory avec le schéma standard requiert environ 74 Mo d'espace disque pour chaque groupe de 50 000 utilisateurs. Cependant, si vous ajoutez un nouvel ensemble d'attributs ou si vous paramétrez tous les attributs existants, la taille de l'objet augmente. Ces ajouts affectent l'espace disque, le processeur et la mémoire nécessaires. Les exigences relatives aux processeurs dépendent également des services supplémentaires disponibles sur l'ordinateur, ainsi que du nombre d'authentifications, de lectures et d'écritures gérées par l'ordinateur. Certains processus, tels que le chiffrement et l'indexation, peuvent exiger d'importantes ressources processeur.

7.2.4 Utilisation d'adresses IPv6 sur le serveur du coffre-fort d'identité

Le coffre-fort d'identité prend en charge les adresses IPv4 et IPv6. Vous pouvez activer les adresses IPv6 lors de l'installation du coffre-fort d'identité. Si vous effectuez une mise à niveau à partir d'une version antérieure, vous devez activer manuellement les adresses IPv6.

Le coffre-fort d'identité prend également en charge les méthodes de transition de type « double pile IP », « tunnelage » et « pure IPv6 ». Seules les adresses IP globales sont prises en charge. Par exemple :

- `[::]`
- `[::1]`
- `[2015::12]`
- `[2015::12]:524`

Les adresses IPv6 doivent être spécifiées entre crochets `[ ]`. Pour utiliser un nom d'hôte au lieu d'une adresse IP, vous devez indiquer le nom dans le fichier `C:\Windows\System32\drivers\etc\hosts` et l'associer à l'adresse IPv6.

Pour utiliser des adresses IPv6 sur un serveur Windows, vous devez cocher la case **Activer IPv6** sous **Préférence IPv6** lors de l'installation. Cette option active les protocoles NCP, HTTP et HTTPS pour les adresses IPv6. Si vous n'activez pas les adresses IPv6 pendant la procédure d'installation et que vous décidez par la suite de les utiliser, vous devez réexécuter le programme d'installation. Pour plus d'informations, reportez-vous au Chapitre 7.3, « Installation du coffre-fort d'identité », page 71.

Vous pouvez accéder à iMonitor via des adresses IPv6 à l'aide du lien suivant :`http://[2015::3]:8028/nds`.

7.2.5 Utilisation du protocole LDAP pour communiquer avec le coffre-fort d'identité

Lors de l'installation du coffre-fort d'identité, vous devez spécifier les ports surveillés par le serveur LDAP pour qu'il puisse traiter les demandes LDAP. Dans le cadre de la configuration par défaut, les numéros de port pour texte clair et SSL/TLS sont définis sur 389 et 636.

Une liaison simple LDAP nécessite seulement un DN et un mot de passe. Le mot de passe se présente en texte clair. Si vous employez le port 389, l'ensemble du paquet est en texte clair. Dans la mesure où le port 389 autorise le texte clair, le serveur LDAP traite les demandes de lecture et d'écriture adressées à l'annuaire via ce port. Cette ouverture est adaptée aux environnements de confiance où aucune simulation n'a lieu et dans lesquels aucun utilisateur ne peut intercepter les paquets qui ne lui sont pas destinés. Par défaut, cette option est désactivée lors de l'installation.

La connexion via le port 636 est chiffrée. TLS (auparavant SSL) gère le chiffrement. La connexion au port 636 lance automatiquement une procédure de reconnaissance mutuelle. Si celle-ci échoue, la connexion est refusée.

REMARQUE : le programme d'installation sélectionne par défaut le port 636 pour les communications TLS/SSL. Cette configuration par défaut peut être problématique pour votre serveur LDAP. Si un service déjà chargé sur le serveur hôte (avant l'installation d'eDirectory) utilise le port 636, vous devez spécifier un autre port. Les installations antérieures à eDirectory 8.7 traitaient ce conflit comme une erreur fatale et déchargeaient `nldap`. Dans les versions ultérieures à 8.7.3, le programme d'installation charge `nldap`, place un message d'erreur dans le fichier `dstrace.log` et s'exécute sans le port sécurisé.

Lors de la procédure d'installation, vous pouvez configurer le coffre-fort d'identité pour interdire la transmission en clair de mots de passe et d'autres données. L'option **Exiger TLS en cas de liaison simple avec mot de passe** dissuade les utilisateurs d'envoyer des mots de passe lisibles. Si vous ne sélectionnez pas cette option, les utilisateurs ne savent pas que d'autres personnes peuvent voir leur mot de passe. Cette option, qui n'autorise pas la connexion, ne s'applique qu'au port non chiffré. Si vous établissez une connexion sécurisée avec le port 636 et disposez d'une liaison simple, la connexion est déjà codée. Personne ne peut voir les mots de passe, les paquets de données ou les demandes de liaison.

Prenons les scénarios suivants :

L'option Exiger TLS en cas de liaison simple avec mot de passe est activée

Olivia utilise un client qui demande un mot de passe. Une fois qu'elle a saisi le mot de passe, le client se connecte au serveur. Cependant, le serveur LDAP ne permet pas à la connexion d'établir la liaison avec le serveur via le port non codé. Tout le monde peut voir le mot de passe d'Olivia, mais cette dernière est dans l'impossibilité d'obtenir une connexion liée.

Le port 636 est déjà utilisé

Votre serveur exécute Active Directory. Active Directory s'exécute sur un programme LDAP qui utilise le port 636. Vous installez eDirectory. Le programme d'installation détecte alors que le port 636 est déjà utilisé et n'affecte pas de numéro de port au serveur LDAP NetIQ. Le serveur LDAP se charge et semble s'exécuter. Toutefois, comme le serveur LDAP ne peut pas dupliquer ni utiliser un port déjà ouvert, il ne traite pas les requêtes sur un port dupliqué.

Pour vérifier si le port 389 ou 636 est assigné au serveur LDAP NetIQ, exécutez l'utilitaire ICE. Si le champ *Vendor Version* (Version du fournisseur) n'indique pas NetIQ, vous devez reconfigurer le serveur LDAP pour eDirectory et sélectionner un port différent. Pour plus d'informations, reportez-vous à la section Verifying That the LDAP Server is Running (Vérification de l'exécution du serveur LDAP) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

Active Directory est en cours d'exécution

Lorsqu'Active Directory est en cours d'exécution et que le port 389 en texte clair est ouvert, vous pouvez exécuter la commande ICE sur ce port et demander la version du fournisseur. Le résultat affiché est **Microsoft***. Vous reconfigurez alors le serveur NetIQ LDAP en sélectionnant un autre port, afin que le serveur LDAP eDirectory puisse répondre aux requêtes LDAP.

iMonitor peut également signaler si le port 389 ou 636 est déjà ouvert. Si le serveur LDAP ne fonctionne pas, utilisez iMonitor pour identifier les détails. Pour plus d'informations, reportez-vous à la section Verifying That the LDAP Server is Running (Vérification de l'exécution du serveur LDAP) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

7.2.6 Installation manuelle de NICI sur les postes de travail disposant d'utilitaires de gestion

Vous devez installer NICI sur tous les postes de travail qui utilisent un utilitaire de gestion tel qu'iManager. Pour plus d'informations sur l'utilisation de NICI avec le coffre-fort d'identité, reportez-vous à la section « Conditions préalables à l'installation du coffre-fort d'identité » page 58.

Pour installer NICI, utilisez le fichier `NICI_wx64.msi`, qui se trouve par défaut dans le dossier `products\eDirectory\`*`type_processeur`*`\windows\`*`type_processeur`*`\nici`. Vous pouvez exécuter le fichier en tant que procédure guidée (assistant) ou qu'installation silencieuse.

7.2.7 Installation du logiciel NMAS Client

Vous devez installer le logiciel client NetIQ Modular Authentication Service (NMAS) sur tous les postes de travail clients sur lesquels vous souhaitez utiliser les méthodes de connexion NMAS. Les méthodes de connexion doivent être spécifiées lors de l'installation du coffre-fort d'identité.

1. Connectez-vous au poste de travail client avec un compte d'administrateur.
2. Exécutez le programme `nmasinstall.exe` à partir du répertoire d'installation (par défaut : `Win:\products\eDirectory\`*`type_processeur`*`\nmas\`).
3. Cliquez sur **NMAS Client Components** (Composants de NMAS Client).
4. (Facultatif) Sélectionnez l'option NICI pour installer le composant NICI.
5. Cliquez sur **OK**.
6. Une fois l'installation terminée, redémarrez le poste de travail client.

7.3 Installation du coffre-fort d'identité

Le programme d'installation peut vous guider lors de la configuration des paramètres du coffre-fort d'identité. Par défaut, le programme d'installation utilise automatiquement le mode assistant. Toutefois, vous pouvez aussi effectuer une installation silencieuse.

Cette section part du principe que vous souhaitez utiliser eDirectory comme structure de base pour le coffre-fort d'identité.

Lorsque vous lancez le programme d'installation, ce dernier vérifie si Novell International Cryptographic Infrastructure (NICI) et le client Novell pour Windows sont installés. Au besoin, le programme d'installation installe ou met à jour ces composants. Si vous installez le coffre-fort d'identité sur un ordinateur sur lequel le client Novell est déjà installé, eDirectory utilise le client existant. Vous pouvez installer le coffre-fort d'identité sans le client Novell.

Pour plus d'informations sur NICI, reportez-vous au manuel *Novell International Cryptographic Infrastructure Administration Guide* (Guide d'administration de Novell International Cryptographic Infrastructure 2.7). Pour plus d'informations sur le client, reportez-vous à la documentation relative au client Novell pour Windows.

Le programme d'installation peut installer les composants serveur pour NetIQ Module Authentication Service (NMAS). Au cours de l'installation, vous devez spécifier les méthodes de connexion à utiliser avec NMAS. Vous devez également installer le logiciel NMAS Client sur tous les postes de travail clients sur lesquels vous souhaitez utiliser les méthodes de connexion NMAS.

REMARQUE

- À partir d'eDirectory 8.8, vous pouvez utiliser des mots de passe sensibles à la casse pour tous les utilitaires.
- Les noms de vos conteneurs peut inclure un point (.). Pour plus d'informations sur l'utilisation de points dans les noms de conteneur, reportez-vous à la Section 7.1.2, « Conditions préalables et considérations relatives à l'installation du coffre-fort d'identité », page 58.

7.3.1 Utilisation de l'assistant pour l'installation du coffre-fort d'identité

1. Connectez-vous en tant qu'administrateur à l'ordinateur sur lequel vous souhaitez installer eDirectory.
2. Accédez au répertoire `\products\eDirectory\x64\`.
3. Exécutez le fichier `eDirectory_910_windows_x86_64.exe`.
4. Sous l'onglet **De base**, spécifiez les détails suivants :
   - Si vous sélectionnez **New Tree** (Nouvelle arborescence), spécifiez les détails suivants :
     - **Nom de l'arborescence :** spécifiez un nom d'arborescence pour le coffre-fort d'identité.
     - **Server FDN (FDN du serveur) :** spécifiez un FDN de serveur.

       REMARQUE : bien que le coffre-fort d'identité permette de définir le FDN de l'objet Serveur NCP jusqu'à 256 caractères, NetIQ recommande de limiter la variable à une valeur bien inférieure étant donné que le coffre-fort d'identité crée d'autres objets de longueur supérieure en fonction de la longueur de cet objet.

- **Tree Admin (Administrateur de l'arborescence) :** spécifiez un nom d'administrateur pour le coffre-fort d'identité.
- **Mot de passe de l'administrateur :** spécifiez le mot de passe de l'administrateur.

- Si vous sélectionnez **Existing Tree** (Arborescence existante), spécifiez les détails suivants :
  - **Adresse IP :** spécifiez l'adresse IP de l'arborescence existante pour le coffre-fort d'identité.
  - **Numéro de port :** spécifiez le numéro de port de l'arborescence existante. La valeur par défaut est 524.
  - **Server FDN (FDN du serveur) :** spécifiez un FDN de serveur.
  - **Tree Admin (Administrateur de l'arborescence) :** spécifiez le nom d'administrateur existant pour le coffre-fort d'identité.
  - **Mot de passe de l'administrateur :** spécifiez le mot de passe de l'administrateur.

5. (Conditionnel) Sous l'onglet **Avancé**, spécifiez les détails suivants :
   - Pour utiliser des adresses IPv6 sur le serveur du coffre-fort d'identité, sélectionnez **Activer IPv6**.

     REMARQUE : NetIQ recommande d'activer cette option. Pour activer l'adressage IPv6 après l'installation, vous devez réexécuter le programme d'installation.
   - Pour activer l'authentification EBA (Enhanced Background Authentication), sélectionnez **Enable EBA** (Activer EBA).
   - Spécifiez le texte clair HTTP et les ports sécurisés. Les valeurs par défaut sont 8028 et 8030 respectivement.
   - Spécifiez le texte clair LDAP et les ports sécurisés. Les valeurs par défaut sont 389 et 636 respectivement.
6. Dans le champ **Emplacement d'installation**, spécifiez l'emplacement auquel le coffre-fort d'identité est installé.
7. Dans le champ **DIB Location** Emplacement DIB), indiquez l'emplacement où se trouvent les fichiers DIB.
8. Cliquez sur **Installer** et effectuez l'installation.

7.3.2 Installation et configuration silencieuses du coffre-fort d'identité

Pour prendre en charge une installation ou une configuration silencieuse (sans surveillance) du coffre-fort d'identité, vous pouvez utiliser un fichier `response.ni` contenant des sections et des clés, semblable à un fichier `Windows.ini`.

REMARQUE : vous devez installer et configurer NetIQ SecreStore (`ss`). Pour plus d'informations, reportez-vous à la Section 7.4.1, « Ajout de SecretStore au schéma du coffre-fort d'identité », page 80.

Édition du fichier response.ni

Vous pouvez utiliser un éditeur de texte ASCII pour créer et éditer le fichier `response.ni`. Le fichier de réponses permet :

- d'effectuer une installation sans surveillance complète avec toutes les entrées utilisateur requises ;
- de définir la configuration par défaut des composants ;
- d'ignorer toutes les invites pendant l'installation.

NetIQ inclut un fichier `response.ni` dans le dossier `products\eDirectory\x64\windows\x64\NDSonNT` du kit d'installation. Ce fichier contient les valeurs par défaut des principaux paramètres. Vous devez modifier les valeurs de l'instance eDirectory dans la section NWI:NDS.

REMARQUE : lorsque vous modifiez le fichier `response.ni`, n'insérez pas d'espaces vides dans les paires clé=valeur.

AVERTISSEMENT : pour procéder à une installation sans surveillance, vous de devez spécifier les références de l'administrateur dans le fichier `response.ni`. Pour éviter toute compromission de ces références, il est recommandé de supprimer définitivement le fichier une fois l'installation ou la configuration terminée.

Les sections suivantes décrivent les sections et clés requises dans le fichier `response.ni` :

NWI:NDS

Upgrade Mode

Indique si le programme d'installation doit être exécuté en tant que mise à niveau. Les valeurs valides sont `False`, `True` et `Copy`.

Mode

Indique le type d'installation à effectuer :

- **full** permet à la fois d'installer et de configurer le coffre-fort d'identité. Spécifiez cette valeur lorsque vous souhaitez effectuer une nouvelle installation et configurer le coffre-fort d'identité ou mettre à niveau et configurer uniquement les fichiers requis.

- **install** permet d'installer une nouvelle version du coffre-fort d'identité ou de mettre à niveau les fichiers requis.
- **configure** permet de modifier les paramètres du coffre-fort d'identité. Si vous effectuez uniquement une mise à niveau des fichiers requis, le programme d'installation ne configure que les fichiers mis à niveau.

REMARQUE

- Si vous spécifiez *configure*, veillez à ne pas modifier la valeur `RestrictNodeRemove` de la clé `ConfigurationMode` dans la section [Initialization].
- Si vous spécifiez *full*, vous ne pouvez pas choisir l'option d'annulation de configuration et de désinstallation individuelles lors de la désinstallation du coffre-fort d'identité.

New Tree

Indique si cette installation concerne une nouvelle arborescence ou un serveur secondaire. Les valeurs valides sont `Yes` et `No`. Par exemple, si vous souhaitez installer une nouvelle arborescence, spécifiez `Yes`. Pour plus d'informations sur la spécification des valeurs pour une arborescence existante, reportez-vous à la section « Novell:ExistingTre1.0.0 » page 78.

Tree Name

S'il s'agit d'une nouvelle installation, spécifiez le nom de l'arborescence à installer. Pour installer un serveur secondaire, spécifiez l'arborescence à laquelle vous souhaitez ajouter le serveur.

Server Name

Indique le nom du serveur à installer dans le coffre-fort d'identité.

Server Container

Indique l'objet Conteneur de l'arborescence auquel l'objet Serveur sera ajouté. L'objet Serveur contient tous les détails de configuration propres au serveur du coffre-fort d'identité. Si vous installez une nouvelle version du coffre-fort d'identité, le programme d'installation crée ce conteneur avec l'objet Serveur.

Server Context

Indique le nom distinctif (DN) complet de l'objet Serveur (nom du serveur) et de l'objet Conteneur. Par exemple, si le nom du serveur du coffre-fort d'identité est EDIR-TEST-SERVER et que le nom du conteneur est Netiq, spécifiez `EDIR-TEST-SERVER.Netiq`.

Admin Context

Indique l'objet Conteneur de l'arborescence auquel l'objet Administrateur sera ajouté, par exemple, `Netiq`. Tout utilisateur ajouté à une arborescence possède un objet Utilisateur qui contient tous ses détails spécifiques. Si vous installez une nouvelle version du coffre-fort d'identité, le programme d'installation crée ce conteneur avec l'objet Serveur.

Admin Login Name

Indique le nom distinctif relatif (RDN) de l'objet Administrateur de l'arborescence qui dispose des droits complets, du moins sur le contexte auquel ce serveur est ajouté, par exemple, `Admin`. Le programme d'installation utilise ce compte pour effectuer toutes les opérations dans l'arborescence.

Admin Password

Indique le mot de passe de l'objet Administrateur, par exemple, `netiq123`. Si vous installez une nouvelle version du coffre-fort d'identité, le programme d'installation configure le mot de passe de l'objet Administrateur.

NDS Location

Indique le chemin au niveau du système local où vous souhaitez installer les fichiers binaires et les bibliothèques du coffre-fort d'identité. Lorsque vous configurez les composants du coffre-fort d'identité, ils se rapportent à cet emplacement d'installation pour les fichiers pertinents. Par défaut, le programme d'installation place les fichiers dans `C:\Novell\NDS`.

DataDir

Indique le chemin au niveau du système local où vous souhaitez installer les fichiers DIB. Par défaut, le programme d'installation place les fichiers dans `C:\Novell\NDS\DIBFiles`.

Vous pouvez spécifier un chemin différent si les fichiers de données DIB de votre environnement requièrent plus d'espace que n'en offre l'emplacement par défaut.

Installation Location

(Facultatif) Indique le chemin utilisé par le programme d'installation lors de la copie des fichiers à l'emplacement des NDS, par exemple, `[Novell:DST:1.0.0_Location]` ou `Path=fil//C:\Novell\NDS`. La valeur par défaut de ce paramètre est la même que celle de l'emplacement des NDS, à savoir `C:\Novell\NDS`. Le programme d'installation utilise ce chemin lors de la copie des fichiers aux emplacements des NDS et DataDir spécifiés.

System Location

(Facultatif) Indique le chemin du dossier système de l'ordinateur où vous souhaitez installer le serveur du coffre-fort d'identité, par exemple, `[Novell:SYS32_DST:1.0.0_Location]` ou `Path=fil/C:\Windows\system32`. Le programme d'installation requiert un accès au dossier système pour copier les DLL et accéder aux fichiers spécifiques du système pendant l'installation.

Require TLS

(Facultatif) Indique si le coffre-fort d'identité doit utiliser le protocole TLS (Transport Layer Security) lors de la réception de requêtes LDAP en texte clair.

LDAP TLS Port

(Facultatif) Indique le port sur lequel le coffre-fort d'identité doit être à l'écoute des requêtes LDAP en texte clair.

LDAP SSL Port

(Facultatif) Indique le port sur lequel le coffre-fort d'identité doit être à l'écoute des requêtes LDAP qui utilisent le protocole SSL (Secure Sockets Layer).

Install as Service

Indique au programme d'installation d'installer eDirectory en tant que service. Vous devez spécifier `Yes`.

Prompt

Indique si le programme d'installation doit vous demander de spécifier certaines informations, comme le nom de l'arborescence et le nom du serveur. Par exemple, dans le cadre d'une installation silencieuse ou sans surveillance, spécifiez `False`.

NWI:NMAS (méthodes NMAS)

Le coffre-fort d'identité prend en charge plusieurs méthodes NMAS, tant lors de l'installation que de la mise à niveau. Vous devez spécifier la méthode NMAS NDS dans le fichier `response.ni`. Si vous n'indiquez aucune méthode NMAS, par défaut, le programme d'installation installe la méthode NDS. Toutefois, si vous créez une liste explicite, vous devez inclure NDS.

Choices

Indique le nombre de méthodes NMAS à installer, par exemple, `5`.

Methods

Indique les types de méthodes NMAS à installer. Utilisez des virgules pour séparer les différents types, par exemple, `CertMutual,Challenge Response,DIGEST-MD5,NDS`.

Le programme d'installation recherche la chaîne exacte (sensible à la casse) pour choisir les méthodes NMAS à installer. Vous devez donc spécifier les valeurs exactement comme indiqué ci-dessous :

- `CertMutual`
- `Challenge Response` : méthode NMAS de réponse de vérification d'identité NetIQ.
- `DIGEST-MD5`
- `Enhanced Password`
- `Entrust`
- `GSSAPI` : mécanisme SASL GSSAPI pour eDirectory. L'authentification auprès du coffre-fort d'identité s'effectue via LDAP au moyen d'un ticket Kerberos.
- `NDS` : méthode de connexion par défaut. OBLIGATOIRE.
- `NDS Change Password`
- `Simple Password`
- `Universal Smart Card`
- `X509 Advanced Certificate`
- `X509 Certificate`

Lorsque vous spécifiez les méthodes NMAS dans le fichier de réponses, le coffre-fort d'identité affiche un message d'état lors de l'installation sans requérir la moindre intervention de l'utilisateur.

eDir:HTTP (ports)

Le coffre-fort d'identité écoute sur des ports HTTP préconfigurés pour un accès via le Web. Par exemple, iMonitor accède au coffre-fort d'identité par le biais d'interfaces Web. Certains ports doivent être spécifiés pour accéder aux applications adéquates. Les options suivantes vous permettent de configurer le coffre-fort d'identité pour utiliser des ports spécifiques :

Clear Text HTTP Port

Indique le numéro du port utilisé pour les opérations HTTP en texte clair.

SSL HTTP Port

Indique le numéro du port utilisé pour les opérations HTTP employant le protocole SSL.

Novell:Languages:1.0.0 (paramètres de langue)

Au cours de l'installation, vous pouvez spécifier les paramètres régionaux et la langue affichée pour le coffre-fort d'identité, à savoir anglais, français ou japonais. Ces valeurs sont mutuellement exclusives.

LangID4

Correspond à l'anglais, par exemple, `LangID4=true`.

LangID6

Correspond au français.

LangID9

Correspond au japonais.

REMARQUE

- Ne spécifiez pas la valeur `true` pour plusieurs langues.
- Vous pouvez également spécifier la langue dans laquelle le programme d'installation affiche les messages tout au long de la procédure d'installation. Pour plus d'informations, reportez-vous à la section « Initialization » page 77.

Initialization

La section `[Initialization]` du fichier `response.ni` inclut les paramètres de la procédure d'installation.

DisplayLanguage

Indique la langue dans laquelle s'affichent les messages au cours de la procédure d'installation, par exemple, `DisplayLanguage=en_US`.

InstallationMode

Indique la façon dont vous souhaitez exécuter la procédure d'installation. Par exemple, pour effectuer une installation silencieuse ou sans surveillance, spécifiez `silent`.

SummaryPrompt

Indique si le programme d'installation doit vous inviter à passer en revue un résumé des paramètres d'installation. Par exemple, dans le cadre d'une installation silencieuse ou sans surveillance, spécifiez `false`.

prompt

Indique si le programme d'installation doit vous demander de spécifier certaines informations. Par exemple, dans le cadre d'une installation silencieuse ou sans surveillance, spécifiez `false`.

NWI:SNMP

Des services SNMP sont configurés et s'exécutent sur la plupart des serveurs Windows. Lorsque vous installez le coffre-fort d'identité, vous devez arrêter les services SNMP, puis les redémarrer une fois le processus terminé. En cas d'installation manuelle, le programme vous invite à arrêter les services SNMP avant de poursuivre l'installation.

Pour arrêter les services SNMP sans que le programme vous y invite lors d'une installation silencieuse ou sans surveillance, spécifiez `Stop Service=yes` dans la section `[NWI:SNMP]` du fichier `response.ni`.

EDIR:SLP

Le coffre-fort d'identité utilise le protocole SLP (Service Location Protocol) pour identifier les autres serveurs ou arborescences dans le sous-réseau au cours de l'installation ou de la mise à niveau. Si des services SLP sont déjà installés sur votre serveur, vous pouvez les remplacer par la version fournie avec la version actuelle du coffre-fort d'identité ou utiliser vos propres services SLP.

Need to uninstall service

Indique si les éventuels services SLP déjà installés sur votre serveur doivent être désinstallés. La valeur par défaut est `true`.

Need to remove files

Indique si les fichiers des éventuels services SLP déjà installés sur votre serveur doivent être supprimés. La valeur par défaut est `true`.

Novell:ExistingTre1.0.0

Le programme d'installation fournit des options permettant d'installer sans surveillance un serveur primaire ou secondaire dans un réseau. Le programme d'installation utilise trois clés différentes pour déterminer s'il doit installer une nouvelle arborescence ou un serveur secondaire dans une arborescence existante.

REMARQUE : la clé `New Tree` se trouve dans la section `NWI:NDS`. Pour plus d'informations, reportez-vous à la rubrique « NWI:NDS » page 73.

ExistingTreeYes

Les valeurs valides sont `True` et `False`. Par exemple, si vous souhaitez installer une nouvelle arborescence, spécifiez `False`.

ExistingTreeNo

Les valeurs valides sont `True` et `False`. Par exemple, si vous souhaitez installer une nouvelle arborescence, spécifiez `True`.

Pour exécuter une installation silencieuse ou sans surveillance sans que le programme vous demande s'il convient d'installer un serveur primaire ou secondaire, spécifiez `prompt=false` dans la section `Existing Tree` du fichier `response.ni`.

Selected Nodes

Cette section du fichier `response.ni` liste les composants installés dans le coffre-fort d'identité, ainsi que des informations de la base de données de profils contenant davantage de détails sur les composants, notamment leur version, l'emplacement source et l'emplacement de copie cible. Ces détails de la base de données de profils sont compilés dans un fichier `.db` qui est fourni dans la version du coffre fort d'identité.

Pour exécuter une installation silencieuse ou sans surveillance sans invite pour des décisions telles que l'emplacement de copie cible ou les détails de la version, spécifiez `prompt=false` dans la section `[Selected Nodes]` du fichier `response.ni`.

Votre fichier de réponses doit inclure cette section. Utilisez les clés et les valeurs exactement telles que fournies dans le fichier `response.ni` d'exemple.

Novell:NOVELL_ROOT:1.0.0

Cette section du fichier `response.ni` contient les paramètres des affichages d'image et d'état au cours de l'installation. Par exemple, vous pouvez spécifier les paramètres définissant la manière dont le programme d'installation réagit dans certaines situations, comme en cas de conflits d'écriture ou de décisions concernant la copie de fichiers. Vous pouvez également indiquer si des images doivent s'afficher. La plupart des images contiennent des informations sur la version du coffre-fort d'identité installée, les composants installés, un écran d'accueil, des fichiers de licence, des options de personnalisation, un message d'état indiquant le composant en cours d'installation, la progression en pourcentage, etc. Il est possible que certaines applications visant à incorporer eDirectory ne veuillent pas afficher ces images.

Pour exécuter une installation silencieuse ou sans surveillance sans invite pour des décisions telles que l'emplacement de copie cible ou les détails de la version, spécifiez `prompt=false` dans cette section du fichier `response.ni`.

Votre fichier de réponses doit inclure cette section. Utilisez les clés et les valeurs fournies dans le fichier `response.ni` d'exemple.

Exécution d'une installation silencieuse ou sans surveillance

Avant de commencer, consultez les conditions préalables à l'exécution d'une installation silencieuse ou sans surveillance. Pour plus d'informations, reportez-vous à la Section 7.1.2, « Conditions préalables et considérations relatives à l'installation du coffre-fort d'identité », page 58. Créez également le fichier `response.ni` à utiliser comme modèle pour l'installation. Pour plus d'informations, reportez-vous à la section « Édition du fichier response.ni » page 73.

REMARQUE : pour que le système d'exploitation n'affiche pas de fenêtre d'état pour l'installation, la mise à niveau ou la configuration, utilisez l'option `nopleasewait` dans la commande.

---

1. Créez un fichier `response.ni` ou modifiez un fichier de réponses existant. Pour plus d'informations sur les valeurs du fichier de réponses, reportez-vous à la section « Édition du fichier response.ni » page 73.
2. Connectez-vous à l'aide d'un compte d'administrateur à l'ordinateur sur lequel vous souhaitez installer le coffre-fort d'identité.
3. Ouvrez une invite de commande avec l'option **Exécuter en tant qu'administrateur** activée.
4. Dans la ligne de commande, entrez la commande suivante :

   ```
   path_to_installation_files\windows\eDirectory\x64\NDSonNT>install.exe /silent
   /nopleasewait /template=Response file
   ```

   Par exemple :

   ```
   D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent /
   nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
   ```

Configuration en mode silencieux

1. Créez un fichier `response.ni` ou modifiez un fichier de réponses existant. Pour plus d'informations sur les valeurs du fichier de réponses, reportez-vous à la section « Édition du fichier response.ni » page 73.
2. Connectez-vous à l'aide d'un compte d'administrateur à l'ordinateur sur lequel vous souhaitez installer le coffre-fort d'identité.
3. Ouvrez une invite de commande avec l'option **Exécuter en tant qu'administrateur** activée.

4 Dans la ligne de commande, entrez la commande suivante :

```
Windows Drive\Program Files\Common Files\novell>install.exe /silent /
restrictnoderemove /nopleasewait /template=Response file
```

Par exemple :

```
c:\Program Files\Common Files\novell>install.exe /silent /restrictnoderemove /
nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
```

Installation silencieuse et configuration

Avant de commencer, consultez les conditions préalables à l'exécution d'une installation silencieuse ou sans surveillance. Pour plus d'informations, reportez-vous à la Section 7.1.2, « Conditions préalables et considérations relatives à l'installation du coffre-fort d'identité », page 58. Créez également le fichier `response.ni` à utiliser comme modèle pour l'installation.

1 Créez un fichier `response.ni` ou modifiez un fichier de réponses existant. Pour plus d'informations sur les valeurs du fichier de réponses, reportez-vous à la section « Édition du fichier response.ni » page 73.

2 Connectez-vous à l'aide d'un compte d'administrateur à l'ordinateur sur lequel vous souhaitez installer le coffre-fort d'identité.

3 Ouvrez une invite de commande avec l'option **Exécuter en tant qu'administrateur** activée.

4 Dans la ligne de commande, entrez la commande suivante :

```
Unzipped Location\windows\eDirectory\x64\NDSonNT>install.exe /silent /
nopleasewait /template=Response file
```

Par exemple :

```
D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent /
nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
```

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

Après avoir installé le coffre-fort d'identité, il se peut que vous deviez effectuer certaines tâches de configuration sur ce dernier.

7.4.1 Ajout de SecretStore au schéma du coffre-fort d'identité

Vous devez étendre le schéma du coffre-fort d'identité afin que la fonctionnalité SecretStore soit prise en charge. Les applications d'identité ont besoin de SecretStore pour se connecter au coffre-fort.

1 Pour étendre le schéma du coffre-fort d'identité, entrez la commande suivante :

```
ice -S SCH -f C:\NetIQ\eDirectory\sssv3.sch -D LDAP -s serverIP -d adminDN
```

Par exemple :

```
ice -S SCH -f C:\NetIQ\eDirectory\sssv3.sch -D LDAP -s 192.168.0.1 -d
cn=admin,o=administrators
```

2 Pour configurer SecretStore sur un serveur Windows, procédez comme suit :

2a Accédez au répertoire `C:\NetIQ\eDirectory`.

2b Saisissez la commande suivante :

```
ssscfg.exe -c
```

2c Spécifiez les paramètres de configuration de SecretStore, puis fermez l'utilitaire.

2d Exécutez `NDSCons.exe`.

2e Dans l'utilitaire, spécifiez `auto` pour le module `ssncp.dlm`.

2f Fermez l'utilitaire.

Pour plus d'informations, reportez-vous à la section SecretStore Configuration for eDirectory Server (Configuration de SecretStore pour le serveur eDirectory) du manuel *NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html) (Guide d'administration de NetIQ eDirectory).

7.4.2 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
```

7.4.3 Gestion des instances d'eDirectory

Vous pouvez créer, démarrer et arrêter les 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 DHost iConsole 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.

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

L'utilitaire DHost permet de créer une instance dans eDirectory.

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

L'utilitaire DHost permet de configurer et d'annuler la configuration d'une instance dans le coffre-fort d'identité.

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

Vous pouvez exécuter des utilitaires, tels que DSTrace, pour une instance.

1. Accédez au répertoire `C:\NetIQ\eDirectory`.
2. Exécutez le fichier `NDCCons.exe`.
3. Dans la console **NetIQ eDirectory Services**, accédez au fichier `dstrace.dlm`.
4. Cliquez sur **Démarrer**.

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

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

Pour démarrer une instance :

1. Accédez au répertoire `C:\NetIQ\eDirectory`.
2. Exécutez le fichier `NDCCons.exe`.
3. Accédez à une instance et cliquez sur **Démarrer**.

Pour arrêter une instance :

1. Accédez au répertoire `C:\NetIQ\eDirectory`.
2. Exécutez le fichier `NDCCons.exe`.
3. Accédez à une instance et cliquez sur **Arrêter**.

8 Planification de l'installation du moteur, des pilotes et des plug-ins

Cette section fournit les conditions préalables, les considérations et la configuration système nécessaires à l'installation du coffre-fort d'identité. Tout d'abord, consultez la liste de contrôle pour comprendre la procédure d'installation.

REMARQUE : ce programme d'installation peut également installer le chargeur distant. Pour plus d'informations, reportez-vous à la Section 10.2, « Installation du chargeur distant », page 105.

8.1 Liste de contrôle pour l'installation du moteur, des pilotes et des plug-ins 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 Chapitre 1, « Aperçu des composants Identity Manager », page 19.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.
❑	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, « Conditions préalables et considérations relatives à l'installation du moteur Identity Manager », page 85.
❑	4. Vérifiez la configuration matérielle et logicielle requise pour les ordinateurs qui hébergeront le moteur Identity Manager. Pour plus d'informations, reportez-vous à la section « Configuration système requise pour le serveur iManager » page 147.
❑	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 85.
❑	6. Apprenez-en davantage sur les options du programme d'installation. Pour plus d'informations, reportez-vous à la Section 8.2, « Présentation du programme d'installation », page 84.

	Éléments de la liste de contrôle
❑	7. (Conditionnel) Pour une procédure d'installation guidée (assistant) du moteur Identity Manager, reportez-vous à la Section 9, « Installation du moteur, des pilotes et des plug-ins d'iManager », page 89.
❑	8. (Facultatif) Pour installer les composants en utilisant une commande unique, reportez-vous à la Section 9.2, « Installation silencieuse », page 90.
❑	9. (Conditionnel) Pour installer le chargeur distant, reportez-vous à la Section 10.2, « Installation du chargeur distant », page 105.
❑	10. Démarrez l'instance de pilote dans le chargeur distant. Pour plus d'informations, reportez-vous au Chapitre 10.3, « Configuration des pilotes et du chargeur distant », page 110.
❑	11. Installez les autres composants Identity Manager, y compris les applications d'identité et Identity Reporting.

8.2 Présentation du programme d'installation

Pour plus de commodité, le programme d'installation contient plusieurs des composants constitutifs de l'infrastructure sous-jacente de votre solution Identity Manager. Vous pouvez choisir d'installer tous les composants sur le même serveur ou sur des serveurs distincts. Pour plus d'informations sur la configuration requise pour le serveur, reportez-vous à la section Planification de l'installation du moteur, des pilotes et des plug-ins pour chaque composant, au guide du pilote concerné, ainsi qu'aux dernières notes de version.

Le programme d'installation offre les options suivantes pour l'installation des composants :

Serveur Identity Manager

Installe le moteur Identity Manager, le schéma, l'agent d'audit NetIQ et XDAS (Distributed Audit services).

Serveur de système connecté (32 bits, 64 bits, .NET)

Installe le service du chargeur distant et les instances de pilote dans le chargeur. 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. Dans le programme d'installation, vous pouvez sélectionner les pilotes que vous souhaitez installer avec le chargeur distant sur le système connecté

Agent Fan-out

Installe l'agent Fan-out pour le pilote JDBC Fan-out. Ce dernier utilise l'agent Fan-out pour créer plusieurs instances de pilote JDBC Fan-out. L'agent Fan-out charge les instances de pilote JDBC en fonction de la configuration des objets de connexion dans le pilote Fan-out. 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).

Plug-ins iManager pour Identity Manager

Installe les plug-ins iManager qui vous permettent d'utiliser iManager pour gérer les pilotes Identity Manager qui présentent des valeurs de configuration globale.

Pilotes

Les pilotes Identity Manager synchronisent les informations d'identité entre plusieurs types d'annuaires, de bases de données et d'applications commerciales avec le coffre-fort d'identité. Vous pouvez configurer le pilote de manière à synchroniser les données dans une seule direction ou dans les deux sens.

Dans le programme d'installation, vous pouvez sélectionner les pilotes à installer avec les autres composants. Vous pouvez choisir d'installer des pilotes sur un serveur qui n'héberge pas le moteur Identity Manager. Dans ce cas, vous devez également installer le service de chargeur distant sur ce serveur.

8.3 Conditions préalables et considérations relatives à 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 85
- Section 8.3.2, « Considérations relatives à l'installation des pilotes avec le moteur Identity Manager », page 85

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 :

- Avant d'installer le moteur Identity Manager, vous devez installer le coffre-fort d'identité. Par ailleurs, le coffre-fort d'identité doit contenir une arborescence contenant au moins une unité organisationnelle, un utilisateur et un serveur iManager.
- Installez le moteur Identity Manager sur le même serveur qui héberge le coffre-fort d'identité. Le programme d'installation installe une version 32 ou 64 bits d'Identity Manager en fonction 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 10.1.6, « Conditions préalables et considérations relatives à l'installation du chargeur distant », page 101.

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 Section 30.6, « Activation d'Identity Manager », page 359.

8.4 Configuration système requise pour le moteur Identity Manager

Cette section décrit la configuration minimale requise pour le(s) serveur(s) sur le(s)quel(s) vous souhaitez installer le moteur Identity Manager. 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	◆ 300 Mo ◆ 150 Mo d'espace disque supplémentaire par tranche de 50 000 utilisateurs
Mémoire	◆ 2 Go pour le moteur Identity Manager ◆ 2 Go pour les pilotes Identity Manager
Système d'exploitation (certifié)	L'un des systèmes d'exploitation 64 bits suivants : ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 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.

Catégorie	Configuration requise
Système de virtualisation	◆ Hyper-V Server 2012 R2 ◆ VMware ESX 5.0 et versions ultérieures ◆ Virtualisation de Windows Server 2012 R2 avec Hyper-V (prise en charge) 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.
Logiciels supplémentaires	◆ NetIQ eDirectory 9.1 ◆ iManager 3.1

9 Installation du moteur, des pilotes et des plug-ins d'iManager

Cette section décrit la procédure d'installation pour le moteur Identity Manager, les pilotes, les plug-ins d'iManager et le chargeur distant. Vous pouvez installer ces programmes sur le même serveur ou sur des serveurs distincts. Par exemple, vous pouvez avoir besoin d'un pilote sur un système connecté, plutôt que sur le même serveur que le moteur Identity Manager. Dans ce cas, vous installez le chargeur distant sur ce système connecté.

NetIQ permet une installation guidée ou silencieuse.

9.1 Utilisation de l'assistant pour l'installation des composants

Le programme d'installation vous guide dans les paramètres de configuration du moteur Identity Manager. Par défaut, le programme d'installation utilise automatiquement le mode assistant.

Pour préparer l'installation, reportez-vous à la Section 8.1, « Liste de contrôle pour l'installation du moteur, des pilotes et des plug-ins Identity Manager », page 83. Reportez-vous également aux notes de version relatives à votre édition. Pour effectuer une installation sans surveillance, reportez-vous à la Section 9.2, « Installation silencieuse », page 90

REMARQUE : votre choix d'une installation en tant qu'administrateur ou non-administrateur doit correspondre à la méthode utilisée pour installer le coffre-fort d'identité.

9.1.1 Installation en tant qu'administrateur

Cette section décrit la procédure guidée appliquée en cas d'utilisation de l'assistant pour installer le moteur Identity Manager en tant qu'administrateur. Le programme d'installation se trouve à l'emplacement `\products\idm\windows\setup\idm_install.exe`.

Pour installer le moteur Identity Manager en tant qu'administrateur :

1. Connectez-vous en tant qu'administrateur sur l'ordinateur sur lequel installer le moteur Identity Manager.
2. À partir du répertoire qui contient les fichiers d'installation, recherchez le fichier `idm_install.exe` et exécutez-le.
3. Acceptez l'accord de licence, puis cliquez sur **Suivant**.
4. Dans la fenêtre Sélection composants, spécifiez les composants que vous souhaitez installer.

Pour plus d'informations sur les options, reportez-vous à la Section 8.2, « Présentation du programme d'installation », page 84.

5 (Facultatif) Pour sélectionner des pilotes spécifiques pour les différents composants, procédez comme suit :

5a Cliquez sur **Personnaliser les composants sélectionnés**, puis cliquez sur **Suivant**.

5b Développez le volet **Pilotes** sous le composant à installer.

5c Sélectionnez les pilotes à installer.

6 Cliquez sur **Suivant**.

7 Dans la fenêtre Avertissement d'activation, cliquez sur **OK**. Pour plus d'informations, reportez-vous à la Section 30.6, « Activation d'Identity Manager », page 359.

8 Pour l'authentification, spécifiez un compte utilisateur et un mot de passe associés à des droits suffisants dans eDirectory pour étendre le schéma. Indiquez le nom d'utilisateur au format LDAP. Par exemple, `cn=admin,o=company`.

9 Dans Résumé avant installation, vérifiez les paramètres.

10 Cliquez sur **Installer**.

11 Activez Identity Manager. Pour plus d'informations, reportez-vous à la Section 30.6, « Activation d'Identity Manager », page 359.

12 Pour créer et configurer les objets de pilote, consultez le guide consacré à ce pilote. Pour plus d'informations, reportez-vous au site Web de documentation des pilotes Identity Manager.

13 (Facultatif) Pour les emplacements d'installation par défaut, reportez-vous au journal d'installation, par exemple, `C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log`.

9.2 Installation silencieuse

Pour installer Identity Manager en mode silencieux, créez un fichier de propriétés contenant les paramètres nécessaires à l'installation. Le support d'Identity Manager inclut un exemple de fichier de propriétés dans `\products\idm\windows\setup\silent.properties`.

Pour effectuer une installation en mode silencieux :

1 Dans le répertoire d'installation, créez un fichier de propriétés ou modifiez le fichier exemple `silent.properties`.

2 Dans un éditeur de texte, spécifiez les paramètres suivants dans le fichier :

EDITION_INPUT_RESULTS

Spécifie l'édition du serveur Identity Manager. Par exemple, `Advanced Edition` ou `Standard Edition`. Le programme d'installation utilise ces informations pour configurer l'édition spécifiée d'Identity Manager.

EDIR_USER_NAME

Spécifie le nom distinctif LDAP du compte administrateur pour le coffre-fort d'identité. Par exemple, `c=admin,o=netiq`. Le programme d'installation utilise ce compte pour connecter le moteur Identity Manager au coffre-fort d'identité.

Vous devez peut-être ajouter ce paramètre au fichier exemple `silent.properties`.

EDIR_USER_PASSWORD

Spécifie le mot de passe du compte administrateur du coffre-fort d'identité. Par exemple, `netiq123`. Vous devez peut-être ajouter ce paramètre au fichier exemple `silent.properties`.

Si vous ne souhaitez pas inclure la valeur du mot de passe dans le fichier, laissez le champ vide. Le programme d'installation lit ensuite la valeur de la variable d'environnement `EDIR_USER_PASSWORD`. Vérifiez que vous disposez d'une variable d'environnement pour `EDIR_USER_PASSWORD`.

METADIRECTORY_SERVER_SELECTED

Indique si vous souhaitez installer le serveur et les pilotes Identity Manager.

CONNECTED_SYSTEM_SELECTED

Indique si vous souhaitez installer les pilotes et le service de chargeur distant 32 bits. Vous pouvez installer les versions 32 et 64 bits sur le même serveur.

FANOUTAGENT_SELECTED

Spécifie si vous souhaitez installer l'agent de dissémination pour le pilote JDBC.

X64_CONNECTED_SYSTEM_SELECTED

Indique si vous souhaitez installer les pilotes et le service de chargeur distant 64 bits. Vous pouvez installer les versions 32 et 64 bits sur le même serveur.

WEB_ADMIN_SELECTED

Applicable lorsque vous avez déjà installé iManager.

Indique si vous souhaitez installer les plug-ins iManager.

UTLITIES_SELECTED

Indique si vous souhaitez installer les utilitaires et les composants système pour le chargeur distant.

DOT_NET_REMOTELOADER_SELECTED

Indique si vous souhaitez installer le service de chargeur distant et les pilotes .NET sur le serveur Windows.

EDIR_NDS_CONF

Spécifie le chemin du fichier de configuration du coffre-fort d'identité.

Si vous disposez de plusieurs instances du coffre-fort d'identité, spécifiez la valeur appropriée de chacune.

EDIR_IP_ADDRESS

Spécifie l'adresse IP du coffre-fort d'identité.

Si vous disposez de plusieurs instances du coffre-fort d'identité, spécifiez l'adresse de chacune.

EDIR_NCP_PORT

Indique le numéro de port du coffre-fort d'identité.

Si vous disposez de plusieurs instances du coffre-fort d'identité, spécifiez le port de chacune.

3 Pour exécuter l'installation silencieuse, émettez la commande suivante à partir du répertoire du fichier de propriétés : `install.exe -i silent -f nom_fichier.properties`.

4 (Facultatif) Pour les emplacements d'installation par défaut, reportez-vous au journal d'installation, par exemple, `C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log`.

9.3 Installation sur un serveur hébergeant plusieurs instances de coffre-fort d'identité

Identity Manager prend en charge cette installation en tant qu'administrateur et en mode silencieux. Cette procédure nécessite la création d'un fichier `silent.properties` pour chaque instance de coffre-fort d'identité sur laquelle vous souhaitez installer Identity Manager.

Pour installer Identity Manager en mode silencieux, procédez comme suit :

1. Passez en revue les conditions préalables et la configuration système requise dans le Chapitre 8, « Planification de l'installation du moteur, des pilotes et des plug-ins », page 83.
2. Suivez les instructions de la Section 9.2, « Installation silencieuse », page 90.
   - **2a** Assurez-vous que le fichier silent.properties inclut les paramètres suivants :

     ```
     EDITION_INPUT_RESULTS=Advanced Edition
     EDIR_USER_NAME=cn=admin_name,o=organization_name
     EDIR_USER_PASSWORD=identity_vault_password
     METADIRECTORY_SERVER_SELECTED=true
     CONNECTED_SYSTEM_SELECTED=false
     X64_CONNECTED_SYSTEM_SELECTED=false
     WEB_ADMIN_SELECTED=false
     UTILITIES_SELECTED=false
     FANOUTAGENT_SELECTED=false
     EDIR_NCP_PORT=<ncp_port>
     EDIR_NDS_CONF=</path/to/edir/conf>
     EDIR_IP_ADDRESS=ip_address_for_identity_vault

     # For Customization use the following properties
     CUSTOM_SELECTED=true
     # engine custom list engine and drivers jdbc and delim
     CHOSEN_INSTALL_FEATURE_LIST_SERVER=ENGINE,JDBC,DELIM,additional_value
     ```

   - **2b** Vous pouvez inclure les valeurs supplémentaires suivantes pour personnaliser la liste de moteur :
     - Server_DRIVERS
     - AD
     - EBSHR
     - EBSTCA
     - EBSUM
     - DELIM
     - EDIR
     - BIEDIR
     - JDBC
     - JMS
     - LDAP
     - NXSET
     - NOTES
     - PS
     - REMEDY
     - SAPUMJ

- SAPHR
- SAPBL
- SAPPORTAL
- SOAP
- REST
- SFORCE
- SENTREST
- BLACK
- BANNER
- GOOGLE
- AR
- NPUM
- TSS
- RACF
- AFC2
- UAD
- RRSD

3 (Conditionnel) Pour vérifier si l'installation a réussi, recherchez les lignes ci-dessous dans le fichier journal d'installation, par exemple, `C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log`.

```
NDS schema extension complete.
exitValue=0
Schema extended
SCHEMA_EXTENDED=true
==== UpdateIDMConfigureStatus ==============================
stateFile: C:\IDM\Uninstall_Identity_Manager\idmconfigure_state.conf
INSTALL_SUCCESS: SUCCESS
enter loop:
==== Complete ==============================================
INSTALL_SUCCESS=SUCCESS
```

9.4 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 9.4.1, « Arrêt des pilotes », page 93
- Section 9.4.2, « Lancement des pilotes », page 94

9.4.1 Arrêt des pilotes

Avant de modifier les fichiers d'un pilote, vous devez arrêter les pilotes.

- « Utilisation de Designer pour arrêter les pilotes » page 94
- « Utilisation d'iManager pour arrêter les pilotes » page 94

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.

9.4.2 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 94
- « Utilisation d'iManager pour démarrer les pilotes » page 95

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.

10 Installation et gestion du chargeur distant

Cette section explique comment installer le chargeur distant, le chargeur distant .NET ou le chargeur distant Java et configurer les instances de pilote dans le chargeur.

Le programme d'installation du chargeur distant est livré avec le moteur Identity Manager. Les fichiers se trouvent dans le répertoire `\products\idm` du paquetage d'installation d'Identity Manager. Par défaut, le programme d'installation installe les composants à l'emplacement `C:\Netiq`.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous à la Section 10.1.1, « Liste de contrôle pour l'installation du chargeur distant », page 97.

10.1 Planification de l'installation du chargeur distant

Cette section fournit des informations pour préparer l'installation du chargeur distant .NET.

10.1.1 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 Chapitre 1, « Aperçu des composants Identity Manager », page 19.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.
❑	3. Vérifiez que le moteur Identity Manager a été installé. Pour plus d'informations, reportez-vous au Chapitre 9, « Installation du moteur, des pilotes et des plug-ins d'iManager », page 89.

	Éléments de la liste de contrôle
❑	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 10.1.6, « Conditions préalables et considérations relatives à l'installation du chargeur distant », page 101.
❑	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 10.1.7, « Configuration système requise pour le chargeur distant », page 103.
❑	6. (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 à la Section 10.3.1, « Création d'une connexion sécurisée au moteur Identity Manager », page 110.
❑	7. Déterminez si vous souhaitez installer une version 32 ou 64 bits du chargeur distant. Pour plus d'informations, reportez-vous à la Section 10.1.5, « Utilisation d'un chargeur distant 32 ou 64 bits sur le même ordinateur », page 100.
❑	8. Installez le chargeur distant : ◆ Pour vous guider dans la procédure d'installation, reportez-vous à la Section 10.2.1, « Installation du chargeur distant à l'aide de l'assistant », page 105. ◆ Pour effectuer une installation silencieuse, reportez-vous à la Section 10.2.5, « Installation du chargeur distant en mode silencieux », page 109.
❑	9. (Conditionnel) Pour installer le chargeur distant .NET, reportez-vous à la Section 10.2.4, « Installation du chargeur distant .NET », page 108.
❑	10. Passez en revue les paramètres de configuration d'une instance de pilote. Pour plus d'informations, reportez-vous à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.
❑	11. Pour configurer une instance de pilote sur le chargeur distant, reportez-vous à l'une des sections suivantes : ◆ Section 10.3.3, « Configuration du chargeur distant pour les instances de pilote », page 122 ◆ Section 10.3.4, « Configuration du chargeur distant Java pour les instances de pilote », page 125 ◆ Section 10.3.5, « Configuration du chargeur distant .NET pour les instances de pilote », page 126
❑	12. Préparez vos pilotes pour le chargeur distant. Pour plus d'informations, reportez-vous à la Section 10.3.6, « Configuration des pilotes Identity Manager pour fonctionner avec le chargeur distant », page 129.
❑	13. Démarrez l'instance de pilote dans le chargeur distant. Pour plus d'informations, reportez-vous à la Section 10.4.1, « Démarrage d'une instance de pilote dans le chargeur distant », page 141.
❑	14. (Conditionnel) Pour configurer l'authentification mutuelle entre le chargeur distant et le moteur Identity Manager, reportez-vous à la Section 10.3.7, « Configuration de l'authentification mutuelle avec le moteur Identity Manager », page 130.
❑	15. Vérifiez que le chargeur distant et le pilote communiquent avec le moteur Identity Manager et le système connecté. Pour plus d'informations, reportez-vous à la Section 10.3.8, « Vérification de la configuration », page 139.

	Éléments de la liste de contrôle
❑	16. Installez les autres composants Identity Manager, y compris les applications d'identité et Identity Reporting.

10.1.2 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 ni le moteur Identity Manager. Le chargeur distant .NET fonctionne sur les systèmes Windows uniquement.

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 leur plate-forme native.

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.

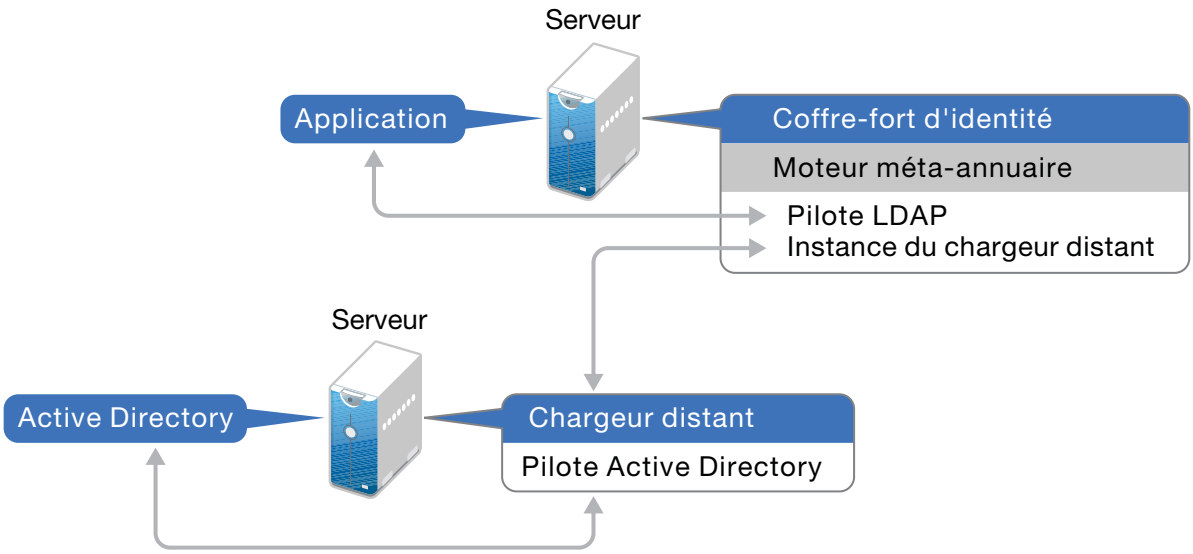
Pour plus d'informations, reportez-vous au Chapitre 10.3, « Configuration des pilotes et du chargeur distant », page 110.

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.

10.1.3 Présentation du chargeur distant Java

Le chargeur distant Java est une application Java compatible avec toute version de Java officiellement prise en charge.

Pour configurer le chargeur distant Java pour vos pilotes, reportez-vous à la Section 10.3.4, « Configuration du chargeur distant Java pour les instances de pilote », page 125.

10.1.4 Présentation du programme d'installation

Pour plus de commodité, le programme d'installation contient plusieurs des composants qui fournissent la structure sous-jacente de votre solution Identity Manager. Vous pouvez choisir d'installer tous les composants sur le même serveur ou sur des serveurs distincts. Outre le chargeur distant, vous pouvez sélectionner les pilotes à installer sur le système connecté. Le kit d'installation propose une option Chargeur distant .NET pour les systèmes d'exploitation Windows.

10.1.5 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.

10.1.6 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 :

- 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 10.1.7, « Configuration système requise pour le chargeur distant », page 103.
- (Conditionnel) Pour connecter Identity Manager à Active Directory, vous devez installer le chargeur distant et le pilote pour Active Directory sur un serveur membre ou un contrôleur de domaine. Il n'est pas nécessaire d'installer eDirectory et Identity Manager sur le même serveur que le système connecté. Le chargeur distant envoie tous les événements d'Active Directory au serveur Identity Manager. Le chargeur distant reçoit ensuite les informations du serveur Identity Manager et les transmet à l'application connectée.
- 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 eDirectory ni les autres pilotes.
  - eDirectory 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 :
  - Active Directory
  - 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

Pour plus d'informations sur le chargeur distant Identity Manager, consultez le document « The Many Faces of Remote Loader in Identity Manager » (Les multiples facettes du chargeur distant dans Identity Manager).

10.1.7 Configuration système requise pour le chargeur distant

Cette section décrit la configuration minimale requise pour les serveurs sur lesquels vous souhaitez installer le chargeur distant, ainsi que les chargeurs distants .Net et Java.

Chargeur distant 32 et 64 bits

Catégorie	Configuration requise
Processeur	Processeur 1 GHz
Mémoire	512 Mo
Système d'exploitation (certifié)	L'un des systèmes d'exploitation 64 bits suivants : ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 Pour un système d'exploitation 32 bits : ◆ Windows Server 2008 SP2 **IMPORTANT :** le client Lotus Notes est pris en charge uniquement sur les plates-formes de poste de travail. Un chargeur distant en cours d'exécution sous Windows XP, Windows 7 et 8 et SLED 32 bits est pris en charge uniquement pour l'intégration de pilote Lotus Notes. Dans les installations classiques d'Identity Manager, le chargeur distant est pris en charge uniquement sur les plates-formes de serveur. 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.
Système 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 ◆ Virtualisation de Windows Server 2012 R2 avec Hyper-V (prise en charge) 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.

Chargeur distant .NET

Le chargeur distant .NET est conçu pour une utilisation avec des serveurs Windows.

Catégorie	Configuration requise
Processeur	Processeur Pentium* III 600 MHz
Mémoire	512 Mo
Système d'exploitation (certifié)	L'un des systèmes d'exploitation 64 bits suivants : ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 Pour un système d'exploitation 32 bits : ◆ Windows Server 2008 SP2 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.
Système 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 ◆ Virtualisation de Windows Server 2012 R2 avec Hyper-V (prise en charge) 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.
.NET Framework	4.x

Chargeur distant Java

Le chargeur distant Java s'exécute quel que soit le système connecté pour autant qu'il dispose de sockets Java et JRE compatibles.

Catégorie	Configuration requise
Processeur	Pentium* III 600 MHz minimum
Mémoire	512 Mo pour le chargeur distant
JRE	Java 8u162, au minimum **REMARQUE :** le chargeur distant Java est compatible avec toute version de Java officiellement prise en charge.
Agent de plate-forme	PA v2011.1r6

10.2 Installation du chargeur distant

La console du chargeur distant utilise le fichier `rlconsole.exe` pour faire office d'interface avec le fichier `dirxml_remote.exe`, un exécutable qui permet au serveur du moteur Identity Manager de communiquer avec les pilotes Identity Manager en cours d'exécution.

10.2.1 Installation du chargeur distant à l'aide de l'assistant

Le programme d'installation vous guide pour configurer les paramètres du chargeur distant. Cette section décrit la procédure guidée appliquée en cas d'utilisation de l'assistant d'installation pour installer le chargeur distant. Le programme d'installation est disponible dans le répertoire `\products\idm\windows\setup\`.

Pour préparer l'installation, reportez-vous à la Section 10.1.1, « Liste de contrôle pour l'installation du chargeur distant », page 97. Reportez-vous également aux notes de version relatives à votre édition. Pour effectuer une installation sans surveillance, reportez-vous à la Section 9.2, « Installation silencieuse », page 90

REMARQUE : votre choix d'une installation en tant qu'administrateur ou non-administrateur doit correspondre à la méthode utilisée pour installer le coffre-fort d'identité.

Pour installer le chargeur distant :

1. Connectez-vous à l'ordinateur sur lequel vous souhaitez installer le chargeur distant.

   REMARQUE : vous pouvez installer le chargeur distant Java en tant que non-administrateur.

   ---

2. Accédez au répertoire `\products\idm\windows\setup\`.
3. Exécutez le programme `idm_install.exe`.
4. Acceptez l'accord de licence, puis cliquez sur **Suivant**.
5. Dans la fenêtre **Sélectionner les composants**, spécifiez les composants du chargeur distant que vous souhaitez installer.

   Pour plus d'informations sur les options, reportez-vous à la Section 8.2, « Présentation du programme d'installation », page 84.
6. (Facultatif) Pour sélectionner des pilotes spécifiques pour les différents composants, procédez comme suit :
   - **6a** Cliquez sur **Personnaliser les composants sélectionnés**, puis cliquez sur **Suivant**.
   - **6b** Développez le volet **Pilotes** sous le composant à installer.
   - **6c** Sélectionnez les pilotes à installer.
7. Cliquez sur **Suivant**.
8. Dans la fenêtre **Avertissement d'activation**, cliquez sur **OK**.

9 Pour l'authentification, spécifiez un compte utilisateur et un mot de passe associés à des droits suffisants dans eDirectory pour étendre le schéma. Indiquez le nom d'utilisateur au format LDAP. Par exemple, `cn=admin,o=company`.

10 Dans Résumé avant installation, vérifiez les paramètres.

11 Cliquez sur **Installer**.

12 Activez Identity Manager. Pour plus d'informations, reportez-vous à la Section 30.6, « Activation d'Identity Manager », page 359.

13 Configurez le chargeur distant pour établir une connexion avec les pilotes et Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 10.3, « Configuration des pilotes et du chargeur distant », page 110.

14 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.

15 (Facultatif) Pour les emplacements d'installation par défaut, reportez-vous aux fichiers journaux d'installation, par exemple, `C:\Users\Admin1\AppData\Local\Temp\1\i dmInstall.log`.

10.2.2 Installation du chargeur distant en mode silencieux

Pour installer le chargeur distant en mode silencieux, créez un fichier de propriétés contenant les paramètres nécessaires à l'installation. Le support d'Identity Manager inclut un exemple de fichier de propriétés. Par défaut, l'exemple de fichier de propriétés se trouve dans le répertoire `\products\idm\windows\setup\`.

Pour effectuer une installation en mode silencieux :

1 Connectez-vous à l'ordinateur sur lequel vous souhaitez installer le chargeur distant.

2 Accédez au répertoire `\products\idm\windows\setup\`.

3 Créez un fichier de propriétés ou modifiez le fichier exemple `silent.properties`.

4 Spécifiez les paramètres suivants dans le fichier :

CONNECTED_SYSTEM_SELECTED

Indique si vous souhaitez installer les pilotes et le service de chargeur distant 32 bits. Vous pouvez installer les versions 32 et 64 bits sur le même serveur.

X64_CONNECTED_SYSTEM_SELECTED

Indique si vous souhaitez installer les pilotes et le service de chargeur distant 64 bits. Vous pouvez installer les versions 32 et 64 bits sur le même serveur.

UTLITIES_SELECTED

Indique si vous souhaitez installer les utilitaires et les composants système pour le chargeur distant.

DOT_NET_REMOTELOADER_SELECTED

Indique si vous souhaitez installer les pilotes et le service de chargeur distant .NET.

5 Pour effectuer une installation silencieuse, exécutez la commande suivante à partir de l'invite de commande :

```
install.exe -i silent -f nom_fichier.properties
```

10.2.3 Installation du chargeur distant Java

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 le chargeur distant Java (dirxml_jremote) sur n'importe quelle plate-forme Windows exécutant un JRE compatible (1.8.0, au minimum) et des sockets Java.

1. Sur le serveur hébergeant le moteur Identity Manager, copiez les fichiers `.iso` ou `.jar` du module d'interface d'application dans l'emplacement par défaut. Par exemple, le répertoire `C:\NetIQ\idm\NDS\lib`.
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` du 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 dans `C:\NetIQ\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, utilisez 7-Zip ou un autre logiciel pris en charge pour dézipper les fichiers `.tar.gz`.
8. Définissez la variable d'environnement `CLASSPATH` sur tous les fichiers JAR présents dans le dossier `lib`. Si vous avez des fichiers JAR dépendants spécifiques d'un pilote, copiez-les dans le dossier `lib`, puis définissez aussi la variable d'environnement `CLASSPATH` sur ces fichiers JAR.

   Par exemple :

   ```
   CLASSPATH=E:\RL\JAVARL\lib\activation.jar;E:\RL\JAVARL\lib\commondrivershim.ja
   r;E:\RL\JAVARL\lib\delimitedtextshim.jar;E:\RL\JAVARL\lib\delimitedtextutil.ja
   r;E:\RL\JAVARL\lib\dirxml.jar;E:\RL\JAVARL\lib\dirxml_misc.jar;E:\RL\JAVARL\li
   b\dirxml_remote.jar;E:\RL\JAVARL\lib\jco3environment.jar;E:\RL\JAVARL\lib\mail
   .jar;E:\RL\JAVARL\lib\mapdb.jar;E:\RL\JAVARL\lib\nxsl.jar;E:\RL\JAVARL\lib\shi
   mwrapper.jar;E:\RL\JAVARL\lib\xds.jar;E:\RL\JAVARL\lib\xp.jar
   ```
9. Définissez la variable d'environnement `PATH` sur le dossier `bin` du JDK ou JRE pour le fichier `Java.exe`.
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.

   Ce fichier se trouve dans le fichier JAR `dirxml_jremote.tar.gz`. Pour plus d'informations, reportez-vous au Chapitre 10.3, « Configuration des pilotes et du chargeur distant », page 110.

12 Lancez le chargeur distant à l'aide des commandes suivantes :

   12a Pour spécifier un mot de passe de chargeur distant :

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config file name>
-sp <Remote Loader Password> <Object Driver Password>
```

   Exemples :

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt -sp novell novell
```

   12b Pour démarrer le chargeur distant :

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config file name>
```

   Exemples :

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt
```

   12c Pour arrêter le chargeur distant :

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config file name>
-unload
```

   Exemples :

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt -unload
```

10.2.4 Installation du chargeur distant .NET

Pour installer le chargeur distant .NET en tant qu'administrateur :

1 Connectez-vous en tant qu'administrateur sur l'ordinateur sur lequel vous souhaitez installer le chargeur distant .NET.

2 Pour accéder au programme d'installation, effectuez l'une des opérations suivantes :

   2a (Conditionnel) Si vous disposez du fichier image `.iso` du paquetage d'installation d'Identity Manager, accédez au répertoire contenant les fichiers d'installation du chargeur distant .NET, situé par défaut dans le répertoire `\products\idm\windows\setup\`.

   2b (Conditionnel) Si vous avez téléchargé les fichiers d'installation du chargeur distant .NET à partir du site Web de téléchargement NetIQ, procédez comme suit :

   - Accédez au fichier `.tgz` pour localiser l'image téléchargée.
   - Lancez l'extraction du contenu du fichier dans un dossier sur l'ordinateur local.

3 Exécutez le programme `idm_install.exe` depuis le répertoire d'installation.

4 Acceptez l'accord de licence, puis cliquez sur **Suivant**.

5 Dans la fenêtre Sélectionner les composants, spécifiez le chargeur distant .NET.

   Pour plus d'informations sur les options, reportez-vous à la Section 8.2, « Présentation du programme d'installation », page 84.

6 (Facultatif) Pour sélectionner des pilotes spécifiques pour les différents composants, procédez comme suit :

   6a Cliquez sur **Personnaliser les composants sélectionnés**, puis cliquez sur **Suivant**.

   6b Développez le volet **Pilotes** sous le composant à installer.

   6c Sélectionnez les pilotes à installer.

7 Cliquez sur **Suivant**.

8 Dans la fenêtre **Avertissement d'activation**, cliquez sur **OK**.

9 Sélectionnez le répertoire d'installation du chargeur distant .NET sur votre ordinateur.

10 Consultez la page Résumé, puis cliquez sur **Installer** pour effectuer l'installation.

10.2.5 Installation du chargeur distant en mode silencieux

Pour installer le chargeur distant en mode silencieux, créez un fichier de propriétés contenant les paramètres nécessaires à l'installation. Le support d'Identity Manager inclut un exemple de fichier de propriétés dans `\products\idm\windows\setup\silent.properties`.

Pour effectuer une installation en mode silencieux :

1 Dans le répertoire d'installation, créez un fichier de propriétés ou modifiez le fichier exemple `silent.properties`.

2 Dans un éditeur de texte, spécifiez les paramètres suivants dans le fichier :

CONNECTED_SYSTEM_SELECTED

Indique si vous souhaitez installer les pilotes et le service de chargeur distant 32 bits. Vous pouvez installer les versions 32 et 64 bits sur le même serveur.

X64_CONNECTED_SYSTEM_SELECTED

Indique si vous souhaitez installer les pilotes et le service de chargeur distant 64 bits. Vous pouvez installer les versions 32 et 64 bits sur le même serveur.

UTLITIES_SELECTED

Indique si vous souhaitez installer les utilitaires et les composants système pour le chargeur distant.

DOT_NET_REMOTELOADER_SELECTED

Indique si vous souhaitez installer le service de chargeur distant et les pilotes .NET sur le serveur Windows.

3 Pour exécuter l'installation silencieuse, émettez la commande suivante :

```
install.exe -i silent -f nom_fichier.properties
```

4 (Facultatif) Pour les emplacements d'installation par défaut, reportez-vous au fichier journal d'installation, par exemple, `C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log`.

10.3 Configuration des pilotes et du chargeur distant

Le chargeur distant peut héberger les modules d'interface d'application Identity Manager contenus dans les fichiers `.dll`, `.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 99.

10.3.1 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 section « Gestion des certificats de serveur auto-signés » page 111.
- **Pour un pilote Java**, vous devez créer un fichier Keystore. Pour plus d'informations, reportez-vous à la section « Création d'un fichier Keystore à l'aide de connexions SSL » page 112.
- **Pour un pilote .NET**, pointez vers un certificat codé en base64. Pour plus d'informations, reportez-vous à la section « Gestion des certificats de serveur auto-signés » page 111.

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.

REMARQUE : lorsque le chargeur distant est exécuté sur un serveur Windows 2012 R2 64 bits, le certificat doit être au format Base64. Si vous utilisez le format DER, le chargeur distant ne parvient pas à se connecter au moteur Identity Manager.

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 113
- « Création d'un fichier Keystore » page 113

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

Exécutez l'utilitaire Keytool situé par défaut dans le répertoire `c:\novell\remoteloader\jre\bin`.

10.3.2 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 ou dans la console du chargeur distant. 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 10.3.3, « Configuration du chargeur distant pour les instances de pilote », page 122.

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. L'exemple de fichier se trouve par défaut dans le répertoire `C:\novell\remoteloader\<architecture(64bit/32bit>\` ou `C:\Novell\remoteloader.NET`. Par exemple, le fichier de configuration peut contenir les lignes suivantes :

```
-commandport 8000
-connection "port=8090"
-trace 4
-tracefile ./trace8000.log
-class com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver
```

Utilisez les paramètres suivants :

-assembly

(Conditionnel) Lorsque vous utilisez un chargeur distant .NET, ce paramètre spécifie le chemin d'accès au fichier .dll du pilote. Assurez-vous que le fichier de configuration inclut ce paramètre. Par exemple :

```
-assembly C:\Novell\remoteloader.NET\DXMLMADDriver.dll
```

-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 121.

-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 C:\novell\remoteloader
```

Lorsque vous utilisez cette commande, le chargeur distant 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`).

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.

-module “*nom*” (-m “*nom*”)

(Conditionnel) Si vous utilisez un lecteur natif, spécifie le module qui contient le module d'interface d'application Identity Manager à héberger. Cette option indique à l'application d'utiliser un certificat `rootfile`. Par exemple, pour un pilote natif, saisissez un des éléments suivants :

```
-module "c:\Novell\RemoteLoader\ADDriver.dll"
-m "c:\Novell\RemoteLoader\ADDriver.dll"
```

REMARQUE

- Vous ne pouvez pas utiliser cette option si vous spécifiez une option `-class`.
- Si vous utilisez une `tabulation` comme séparateur dans l'option `-module`, 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`.

-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.

-service *valeur* (-serv *valeur*)

Indique si vous souhaitez configurer une instance en tant que service Win32. Les valeurs valides sont `install` et `uninstall` ainsi que les autres paramètres requis pour héberger un module d'interface d'application. Par exemple, vous devez inclure `-module` et pouvez également ajouter `-commandport` ainsi que les paramètres de connexion.

Cette commande installe ou désinstalle simplement l'instance en tant que service. Elle ne démarre pas le service.

Vous pouvez envoyer cette commande lorsque le chargeur distant est en cours d'exécution. Toutefois, vous ne pouvez pas utiliser cette commande avec le chargeur distant Java ou rdxml.

-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 c:\temp\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.

-window *valeur* (-w) *valeur*

Indique à l'application d'activer ou de désactiver la fenêtre de trace pour une instance de pilote. Les valeurs valides sont `on` et `off`. Par exemple :

```
-window on
```

Vous pouvez envoyer cette commande lorsque le chargeur distant est en cours d'exécution. Toutefois, vous ne pouvez pas utiliser cette commande avec le chargeur distant Java.

-wizard (-wiz)

Lance l'assistant de configuration du chargeur distant. Vous pouvez également lancer l'assistant en exécutant le fichier `dirxml_remote.exe` sans utiliser de paramètres de ligne de commande.

Si vous exécutez cette commande et spécifiez un fichier de configuration (option `-config`), l'assistant démarre avec les valeurs du fichier de configuration. Vous pouvez utiliser l'assistant pour changer la configuration sans modifier le fichier de configuration directement. Par exemple :

```
-wizard -config config.txt
```

Vous ne pouvez pas utiliser cette commande avec le chargeur distant Java.

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

Nom de la classe Java	Pilote
com.novell.idm.drivers.idprovider.IDProviderShim	Pilote du fournisseur d'ID
com.novell.nds.dirxml.driver.jdbc.JDBCDriverShim	Pilote JDBC
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

10.3.3 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, un fichier de configuration est requis pour l'application, tel que `LDAPShim.txt`. L'utilitaire de console du chargeur distant (la console) vous permet de gérer toutes les instances de pilotes Identity Manager qui s'exécutent sur le serveur Vous pouvez lancer, arrêter, ajouter, supprimer et modifier chaque instance d'un chargeur distant. Le programme d'installation du chargeur distant installe également la console.

Si vous effectuez une mise à niveau, la console détecte et importe les instances de pilote existantes. Pour pouvoir importer un pilote automatiquement, son fichier de configuration doit être enregistré dans le répertoire du chargeur distant situé par défaut à l'emplacement `c:\novell\remoteloader`. Vous pouvez ensuite utiliser la console pour gérer les pilotes distants.

Vous pouvez utiliser la ligne de commande ou la console du chargeur distant pour configurer ce dernier afin qu'il reconnaisse un pilote. Pour plus d'informations sur l'utilisation de la ligne de commande, reportez-vous à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.

Cette section fournit des instructions concernant les activités suivantes :

- « Création d'une instance de pilote dans le chargeur distant » page 123
- « Modification d'une instance de pilote existante dans le chargeur distant » page 125

Création d'une instance de pilote dans le chargeur distant

1 Ouvrez la console du chargeur distant.

REMARQUE : au cours de l'installation, si vous avez choisi de créer un raccourci pour la console, utilisez l'icône `Console du chargeur distant Identity Manager` sur le bureau. Dans le cas contraire, exécutez le fichier `rlconsole.exe` qui se trouve par défaut à l'emplacement `C:\novell\remoteloader\`*`nn`*`bit`.

---

2 Pour ajouter une instance de votre pilote sur ce serveur, cliquez sur **Ajouter**.

3 Dans le champ **Description**, indiquez un nom abrégé représentatif pour cette instance.

La console utilise cette information comme valeur par défaut pour le **fichier de configuration**.

4 Pour le champ **Pilote**, sélectionnez le nom de la classe Java.

REMARQUE : pour utiliser le pilote Active Directory, sélectionnez **ADDriver.dll**. Pour plus d'informations sur les noms de classe de chaque pilote, reportez-vous à la section « Présentation des noms du paramètre -class Java » page 121.

---

5 Pour le champ **Fichier de configuration**, indiquez le chemin du fichier dans lequel le chargeur distant stocke ses paramètres de configuration. La valeur par défaut est `C:\novell\remoteloader\`*`nn`*`bit\`*`Description`*`-config.txt`.

6 Indiquez les mots de passe du chargeur distant et de l'objet Pilote.

7 (Facultatif) Pour utiliser une connexion TLS/SSL entre le chargeur distant et le serveur du moteur Identity Manager, procédez comme suit :

7a Sélectionnez **Utiliser une connexion SSL**

REMARQUE : NetIQ recommande d'utiliser la même version de SSL sur le serveur du 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` (SSL3_GET_RECORD: numéro de version incorrect). 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.

7b Pour **Fichier de racine approuvée** (fichier au format base64), spécifiez le certificat auto-signé exporté à partir de l'autorité de certification organisationnelle de l'arborescence eDirectory. Pour plus d'informations, reportez-vous à la Section 10.3.1, « Création d'une connexion sécurisée au moteur Identity Manager », page 110 et à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.

8 (Facultatif) Pour configurer le fichier de trace pour le chargeur distant, procédez comme suit :

REMARQUE : NetIQ recommande de n'utiliser la fonctionnalité de trace que pour le dépannage des problèmes. L'activation de la trace réduit les performances du chargeur distant. Ne laissez pas la trace en production.

8a Pour le **niveau de trace**, entrez une valeur supérieure à zéro qui définit le niveau des messages d'information envoyés par le chargeur distant et le pilote que vous voulez afficher dans la fenêtre de trace. Les valeurs 1 à 4 sont prédéfinies par la console. Pour créer des types de messages personnalisés, spécifiez une valeur de 5 ou supérieure.

Le niveau de trace 3 est, qui permet un traitement général, est le paramètre le plus courant pour les documents XML et les messages du chargeur distant.

8b Pour le **fichier de trace**, indiquez le chemin d'accès au fichier dans lequel sont consignés les messages de trace. Par exemple, `C:\novell\remoteloader\64bit\Test-Delimited-Trace.log`.

Vous devez spécifier un fichier de trace par instance de pilote s'exécutant sur un ordinateur spécifique. Les messages de trace ne sont consignés dans le fichier de trace que si le niveau de trace indiqué est supérieur à zéro.

8c Dans le champ **Espace disque maximum autorisé pour tous les journaux de trace (Mo)**, spécifiez la valeur approximative maximale que peut occuper le fichier de trace de cette instance sur l'espace disque.

9 (Facultatif) Pour autoriser le chargeur distant à démarrer automatiquement lors du démarrage de l'ordinateur, sélectionnez **Établir un service de chargeur distant pour cette instance de pilote**.

REMARQUE : en cas d'échec de la connexion SSL en raison d'un timeout de reconnaissance mutuelle (`handshaketimeout`) lors de l'établissement de la connexion entre le chargeur distant et le moteur Identity Manager, mettez à jour la variable `handshaketimeout` en la définissant sur 10000, puis redémarrez le pilote et le chargeur distant.

10 (Facultatif) Pour modifier les paramètres de la configuration Java, procédez comme suit :

10a Sélectionnez **Avancé**.

10b Dans le champ **Chemin de classe**, spécifiez les chemins dans lesquels la machine virtuelle Java doit rechercher les fichiers de paquetage (`.jar`) et de classe (`.class`).

Ce paramètre équivaut à la commande `java -classpath`.

10c Pour le paramètre **Options JVM**, indiquez les options que vous souhaitez utiliser lors du démarrage de l'instance JVM du pilote.

10d Indiquez la taille des segments de mémoire initiale et maximale en Mo pour l'instance de la machine virtuelle Java.

10e Pour la communication Suite B, spécifiez `enforceSuiteB=true`. Cette communication est prise en charge uniquement avec le protocole TLS 1.2.

Pour plus d'informations, reportez-vous à la Section 10.3.1, « Création d'une connexion sécurisée au moteur Identity Manager », page 110 et à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.

10f Cliquez sur **OK**.

11 (Facultatif) Pour permettre au chargeur distant d'utiliser le protocole sécurisé lors de la connexion au moteur Identity Manager, spécifiez la version du protocole sécurisé dans le fichier de configuration du chargeur distant. Par exemple : `secureprotocol=TLSv1_2`

Pour plus d'informations, reportez-vous à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.

REMARQUE : si vous avez déjà configuré la version du protocole sécurisé sur le pilote, vous pouvez ignorer cette étape.

12 (Facultatif) Pour permettre au chargeur distant de communiquer en utilisant les protocoles spécifiés par Suite B, spécifiez `enforceSuiteB=true` dans le fichier de configuration du chargeur distant. Cette communication est prise en charge uniquement avec le protocole TLS 1.2.

Pour plus d'informations, reportez-vous à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.

REMARQUE : si vous avez déjà activé la communication Suite B sur le pilote, vous pouvez ignorer cette étape.

13 Cliquez sur **OK**.

Modification d'une instance de pilote existante dans le chargeur distant

1 Dans la console du chargeur distant, sélectionnez l'instance de pilote dans la colonne **Description**.

2 Cliquez sur **Arrêter**.

3 Entrez le mot de passe du chargeur distant, puis cliquez sur **OK**.

4 Cliquez sur **Éditer**.

5 Modifiez les informations de configuration. Pour plus d'informations sur chaque paramètre, reportez-vous à la section « Création d'une instance de pilote dans le chargeur distant » page 123.

6 Pour enregistrer les modifications, cliquez sur **OK**.

10.3.4 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.

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. L'exemple de fichier se trouve par défaut dans le répertoire `C:\novell\remoteloader\<architecture(64bit\32bit>\` ou `C:\Novell\remoteloader.NET`.

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
- -setpasswords
- Paramètres des fichiers de trace (facultatifs) :
  - -trace
  - -tracefile
  - -tracefilemax

REMARQUE : pour plus d'informations sur ces paramètres, reportez-vous à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.

---

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 `\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 <configFile> -service
```

Cette commande démarre le service de chargeur distant Java et ouvre une fenêtre de trace.

6 (Facultatif) Pour arrêter le service de pilote, accédez à Services, puis arrêtez le service.

10.3.5 Configuration du chargeur distant .NET pour les instances de pilote

Le chargeur distant peut héberger le module d'interface d'application Identity Manager contenu dans le fichier `.dll`. Pour que le chargeur distant s'exécute, un fichier de configuration est requis pour l'application, tel que `LDAPShim.txt`. L'utilitaire de console du chargeur distant (la console) vous

permet de gérer toutes les instances de pilotes Identity Manager qui s'exécutent sur le serveur Vous pouvez lancer, arrêter, ajouter, supprimer et modifier chaque instance d'un chargeur distant. Le programme d'installation du chargeur distant installe également la console.

Si vous effectuez une mise à niveau, la console détecte et importe les instances de pilote existantes. Pour pouvoir importer un pilote automatiquement, son fichier de configuration doit être enregistré dans le répertoire du chargeur distant situé par défaut à l'emplacement `c:\novell\remoteloader.net`. Vous pouvez ensuite utiliser la console pour gérer les pilotes distants.

Vous pouvez utiliser la ligne de commande ou la console du chargeur distant pour configurer ce dernier afin qu'il reconnaisse un pilote. Pour plus d'informations sur l'utilisation de la ligne de commande, reportez-vous à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.

Cette section fournit des instructions concernant les activités suivantes :

- « Création d'une instance de pilote dans le chargeur distant .NET » page 127
- « Modification d'une instance de pilote existante dans le chargeur distant .NET » page 129

Création d'une instance de pilote dans le chargeur distant .NET

1 Ouvrez la console du chargeur distant.

REMARQUE : au cours de l'installation, si vous avez choisi de créer un raccourci pour la console, utilisez l'icône `Console du chargeur distant Identity Manager` sur le bureau. Dans le cas contraire, exécutez le fichier `rlconsole.exe` qui se trouve par défaut à l'emplacement `C:\novell\remoteloader.net`.

---

2 Pour ajouter une instance de votre pilote sur ce serveur, cliquez sur **Ajouter**.

3 Dans le champ **Description**, indiquez un nom abrégé représentatif pour cette instance.

La console utilise cette information comme valeur par défaut pour le **fichier de configuration**.

4 Pour le champ **Pilote**, sélectionnez le fichier driver.dll approprié.

5 Pour le champ **Fichier de configuration**, indiquez le chemin du fichier dans lequel le chargeur distant stocke ses paramètres de configuration. La valeur par défaut est `C:\novell\remoteloader.net\`*`Description`*`-config.txt`.

6 Indiquez les mots de passe du chargeur distant et de l'objet Pilote.

7 (Facultatif) Pour utiliser une connexion TLS/SSL entre le chargeur distant et le serveur du moteur Identity Manager, procédez comme suit :

7a Sélectionnez **Utiliser une connexion SSL**

REMARQUE : NetIQ recommande d'utiliser la même version de SSL sur le serveur du 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` (SSL3_GET_RECORD: numéro de version incorrect). 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.

7b Pour **Fichier de racine approuvée** (fichier au format base64), spécifiez le certificat auto-signé exporté à partir de l'autorité de certification organisationnelle de l'arborescence eDirectory. Pour plus d'informations, reportez-vous à la Section 10.3.1, « Création d'une connexion sécurisée au moteur Identity Manager », page 110 et à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.

8 (Facultatif) Pour configurer le fichier de trace pour le chargeur distant, procédez comme suit :

REMARQUE : NetIQ recommande de n'utiliser la fonctionnalité de trace que pour le dépannage des problèmes. L'activation de la trace réduit les performances du chargeur distant. Ne laissez pas la trace en production.

8a Pour le **niveau de trace**, entrez une valeur supérieure à zéro qui définit le niveau des messages d'information envoyés par le chargeur distant et le pilote que vous voulez afficher dans la fenêtre de trace. Les valeurs 1 à 4 sont prédéfinies par la console. Pour créer des types de messages personnalisés, spécifiez une valeur de 5 ou supérieure.

Le niveau de trace 3 est, qui permet un traitement général, est le paramètre le plus courant pour les documents XML et les messages du chargeur distant.

8b Pour le **fichier de trace**, indiquez le chemin d'accès au fichier dans lequel sont consignés les messages de trace. Par exemple, `C:\novell\remoteloader.net\Test-Delimited-Trace.log`.

Vous devez spécifier un fichier de trace par instance de pilote s'exécutant sur un ordinateur spécifique. Les messages de trace ne sont consignés dans le fichier de trace que si le niveau de trace indiqué est supérieur à zéro.

8c Dans le champ **Espace disque maximum autorisé pour tous les journaux de trace (Mo)**, spécifiez la valeur approximative maximale que peut occuper le fichier de trace de cette instance sur l'espace disque.

9 (Facultatif) Pour autoriser le chargeur distant à démarrer automatiquement lors du démarrage de l'ordinateur, sélectionnez **Établir un service de chargeur distant pour cette instance de pilote**.

REMARQUE : en cas d'échec de la connexion SSL en raison d'un timeout de reconnaissance mutuelle (`handshaketimeout`) lors de l'établissement de la connexion entre le chargeur distant et le moteur Identity Manager, mettez à jour la variable `handshaketimeout` en la définissant sur 10000, puis redémarrez le pilote et le chargeur distant.

10 (Facultatif) Pour permettre au chargeur distant d'utiliser le protocole sécurisé lors de la connexion au moteur Identity Manager, spécifiez la version du protocole sécurisé dans le fichier de configuration du chargeur distant. Par exemple : `secureprotocol=TLSv1_2`

Pour plus d'informations, reportez-vous à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.

REMARQUE : si vous avez déjà configuré la version du protocole sécurisé sur le pilote, vous pouvez ignorer cette étape.

11 (Facultatif) Pour permettre au chargeur distant de communiquer en utilisant les protocoles spécifiés par Suite B, spécifiez `enforceSuiteB=true` dans le fichier de configuration du chargeur distant. Cette communication est prise en charge uniquement avec le protocole TLS 1.2.

Pour plus d'informations, reportez-vous à la Section 10.3.2, « Présentation des paramètres de configuration du chargeur distant », page 113.

REMARQUE : si vous avez déjà activé la communication Suite B sur le pilote, vous pouvez ignorer cette étape.

12 Cliquez sur **OK**.

Modification d'une instance de pilote existante dans le chargeur distant .NET

1. Dans la console du chargeur distant, sélectionnez l'instance de pilote dans la colonne **Description**.
2. Cliquez sur **Arrêter**.
3. Entrez le mot de passe du chargeur distant, puis cliquez sur **OK**.
4. Cliquez sur **Éditer**.
5. Modifiez les informations de configuration. Pour plus d'informations sur chaque paramètre, reportez-vous à la section « Création d'une instance de pilote dans le chargeur distant .NET » page 127.
6. Pour enregistrer les modifications, cliquez sur **OK**.

10.3.6 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 113.

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**.

10.3.7 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 130
- « Activation d'un pilote pour l'authentification mutuelle » page 133

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 130
- « Exportation d'un certificat tiers pour le chargeur distant » page 133

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

Vous devez créer un serveur KMO avant de créer un client KMO. Pour créer un KMO, procédez comme suit :

1. Connectez-vous à NetIQ iManager.
2. Dans le volet de gauche, sélectionnez **NetIQ Certificate Server > Créer un 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` pour le certificat de serveur et `clientkmo` pour le certificat client.
5. Sélectionnez **Personnalisée** comme méthode de création du certificat, puis cliquez sur **Suivant**.
6. Conservez la sélection par défaut **Autorité de certification organisationnelle**, puis cliquez sur **Suivant**.
7. (Conditionnel) Si vous créez un KMO client.
   - **7a** Sélectionnez **Activer l'utilisation de la clé étendue**.
   - **7b** Sélectionnez **Personnalisé**, puis sélectionnez **Authentification de l'utilisateur**.
   - **7c** Cliquez sur **Suivant**.

   REMARQUE : pour un KMO serveur, conservez les sélections par défaut et cliquez sur **Suivant**.

   ---
8. Spécifiez la **période de validité** du KMO.

   Vérifiez que l'heure système d'iManager est synchronisée avec vos composants Identity Manager et l'application connectée.
9. Passez en revue le résumé, cliquez sur **Terminer**, puis sur **Fermer**.
10. Répétez ces étapes pour créer un KMO client.

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 'C:\certs'`

Cette commande génère le fichier `serverkmo_server.ks` dans le répertoire `C:\certs`. Le mot de passe Keystore par défaut tout comme le mot de passe clé 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 10-1 *Exemples de différents types de pilotes*

Types de pilotes	Commande	Sortie
Pilote Java	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client java 'C:\certs'`	Fichier `clientkmo_client.ks` dans le répertoire `C:\certs` Le mot de passe par défaut du fichier Keystore est `dirxml`. Le **mot de passe de clé privée** par défaut est `dirxml`.
Pilote natif	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client native 'C:\certs'`	Fichiers `clientkmo_clientcert.pem`, `clientkmo_clientkey.pem` et `trustedcert.b64` dans le répertoire `C:\certs`. Le mot de passe clé par défaut est `dirxml`.
Pilote .NET	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client dotnet 'C:\certs'`	Fichiers `clientkmo_clientcert.pfx` et `trustedcert.b64` dans le répertoire `C:\certs.` Le mot de passe clé par défaut de `clientkmo_clientcert.pfx` 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`. Le pilote .NET utilise, quant à lui, le fichier au format `.pfx`. Vous ne devez donc pas convertir le fichier pour un pilote .NET.

Pilote natif

Procédez comme suit :

1. Récupérez la clé privée au format `.pem` à partir du fichier `.pfx`.

   Entrez une commande du type `openssl pkcs12 -in servercert.pfx -out serverkey.pem`
2. Récupérez la clé de certificat au format `.pem` à partir du fichier `.pfx`.

   Entrez une commande du type `openssl pkcs12 -in servercert.pfx -out servercert.pem`

Pilote Java

Créez un fichier Keystore Java à partir du fichier `.pfx`. Saisissez la commande suivante :

```
keytool -importkeystore -srckeystore servercert.pfx -srcstoretype pkcs12 -
destkeystore servercert.jks -deststoretype JKS
```

Cette commande vous invite à entrer le mot de passe Keystore source (`srckeystore passwd`) et le mot de passe Keystore cible (`dest keystorepasswd`). Entrez ces mots de passe de manière appropriée.

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 133
- « Ajout d'une nouvelle instance de pilote de chargeur distant » page 136
- « 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.

Designer

Avant de configurer un pilote à l'aide d'un KMO ou d'un Keystore dans Designer, assurez-vous d'avoir effectué la configuration du pilote de base comme suit :

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 le **nom d'hôte** au format `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`.

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**.

Pour modifier la configuration du pilote à l'aide de KMO ou du Keystore

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 Dans **Authentification**, sélectionnez **Activer l'authentification mutuelle** et spécifiez les paramètres suivants :

KMO

Spécifie le nom du KMO du serveur.

Autres paramètres

Spécifie le fichier racine (`rootfile`) et son chemin absolu.

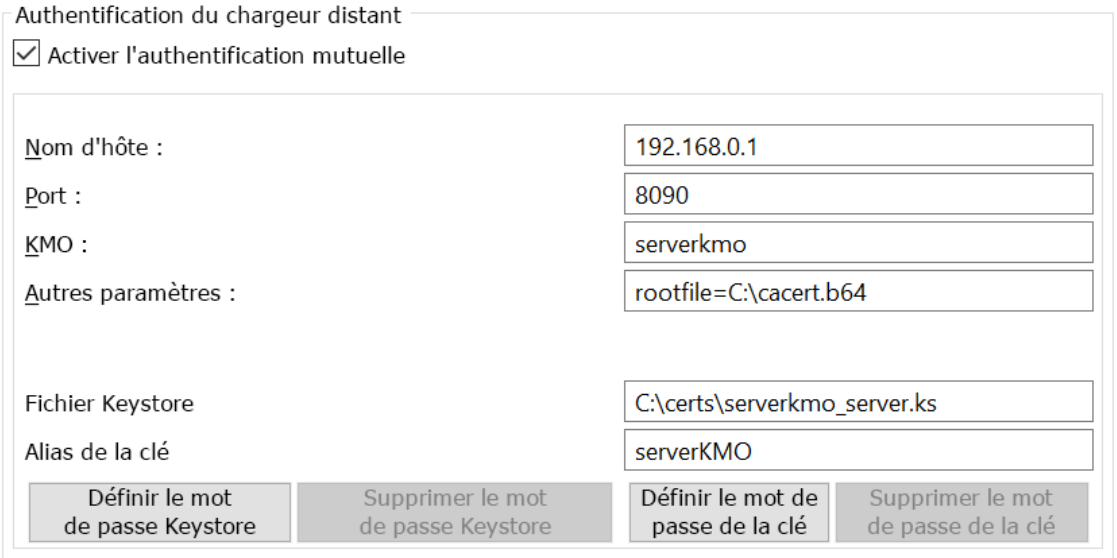
Fichier Keystore

Spécifie le chemin absolu du fichier Keystore.

Alias de la clé

Spécifie le nom du KMO du serveur.

Figure 10-1 *Exemple de configuration pour activer l'authentification mutuelle dans Designer*



5 **Définir le mot de passe Keystore**.

6 **Définir le mot de passe de la clé**.

REMARQUE : par défaut, le **mot de passe Keystore** et le **mot de passe de la clé** sont définis sur `dirxml`.

Vous pouvez également définir ces mots de passe à l'aide de la commande `dxcmd`.

```
dxcmd -user <administrative_user> -password <admin_password>
```

1. Sélectionnez `Actions du pilote`.
2. Sélectionnez le pilote pour lequel vous souhaitez définir les mot de passe Keystore et de la clé.
3. Sélectionnez `Opérations de mot de passe`.
4. Sélectionnez `Définir le mot de passe Keystore pour l'authentification mutuelle` et entrez le mot de passe Keystore.
5. Sélectionnez `Définir le mot de passe de la clé pour l'authentification mutuelle` et entrez le mot de passe de la clé.

---

iManager

Pour modifier la configuration dans iManager :

1 Lancez iManager.

2 Dans **Administration Identity Manager**, sélectionnez **Présentation d'Identity Manager**.

3 Dans **Présentation**, sélectionnez l'ensemble de pilotes Identity Manager.

4 Sélectionnez **Éditer les propriétés** pour le pilote que vous voulez configurer.

5 Dans **Configuration du pilote**, spécifiez les paramètres suivants :

5a Dans **Module pilote**, sélectionnez **Se connecter au chargeur distant**.

5b Dans les paramètres de connexion du chargeur distant, spécifiez les détails de connexion suivants :

```
KMO=<server_KMO_name>
rootfile=<absolute path to the file>
```

Exemples :

```
KMO=serverkmo
rootfile=C:\cacert.b64
```

5c Définissez le **Mot de passe de l'application**.

5d Sélectionnez **Activer l'authentification mutuelle**.

5e Pour utiliser la méthode Keystore, spécifiez les informations suivantes :

Alias de la clé

Spécifie le nom du KMO du serveur et définissez le mot de passe de la clé.

Par exemple, `serverKMO`

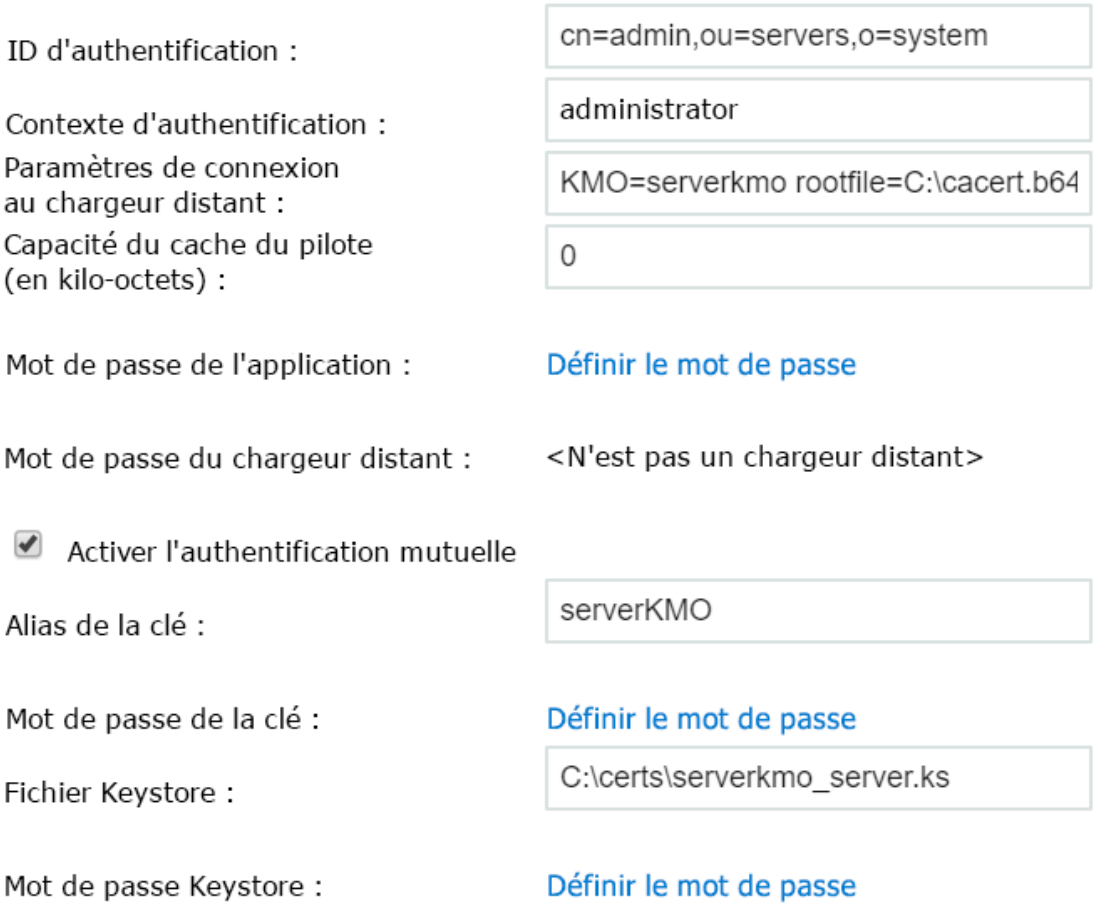
Fichier Keystore

Indique le chemin absolu du fichier Keystore et définit le mot de passe Keystore.

Par exemple : `C:\certs\serverkmo_server.ks`

5f Cliquez sur **Appliquer**, puis sur **OK**.

Figure 10-2 *Exemple de configuration pour activer l'authentification mutuelle dans iManager*



REMARQUE : lorsque vous activez l'authentification mutuelle, la configuration du **Mot de passe du chargeur distant** et du **Mot de passe de l'objet Pilote** ne sont pas nécessaires.

Ajout d'une nouvelle instance de pilote de chargeur distant

1. Cliquez avec le bouton droit sur l'application **Console du chargeur distant Identity Manager** et sélectionnez **Exécuter en tant qu'administrateur**.
2. Cliquez sur **Ajouter** pour ajouter une nouvelle instance du chargeur distant.
3. Spécifiez la **Description** et sélectionnez le type de pilote.
4. Spécifiez le **Port de connexion** qui permet de connecter le chargeur distant et le moteur Identity Manager.
5. Spécifiez le **Port de commande** pour votre instance de chargeur distant.
6. Sélectionnez **Authentification mutuelle** et spécifiez le type de pilote requis :
   - **Pilote Java :** recherchez le chemin du fichier Keystore qui contient le certificat. Le fichier Keystore doit contenir au moins une paire de clés publique/privée.

Fichier Keystore

Indique le chemin d'accès au fichier keystore Java que vous souhaitez utiliser pour l'authentification. Le fichier Keystore contient les clés de chiffrement et les certificats. Par exemple, le fichier `clientkmo_client.ks` créé par `dxcmd` dans le répertoire `C:\certs\` comme indiqué à la section « Exportation d'un certificat à partir d'eDirectory » page 130.

Alias de la clé

Spécifie le nom de la paire de clés publique/privée dans le fichier Keystore que vous souhaitez utiliser pour la génération de la clé symétrique. Par exemple : `clientkmo`.

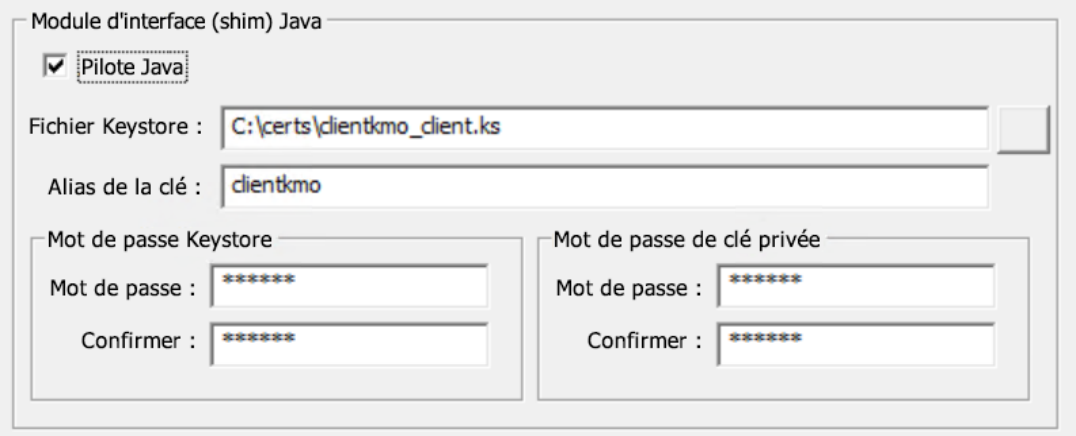
Mot de passe Keystore

Spécifie le mot de passe utilisé pour charger le fichier keystore

Mot de passe de la clé privée

Spécifie le mot de passe de la clé privée stockée dans le fichier Keystore. Identity Manager utilise cette clé pour chiffrer les communications SSL.

Figure 10-3 *Exemple d'ajout d'une instance de chargeur distant Java*



- **Pilote natif :** accédez au chemin du fichier de clé qui contient le certificat pour l'authentification. Le fichier de clé doit être au format Base 64.

  Fichier de clés

  Spécifie le chemin d'accès au fichier contenant la clé utilisée pour l'authentification. Par exemple, le fichier `clientkmo_clientkey.pem` dans le répertoire `C:\certs\` créé par `dxcmd`.

  Mot de passe de la clé

  Spécifie le mot de passe de la clé privée utilisée pour l'authentification.

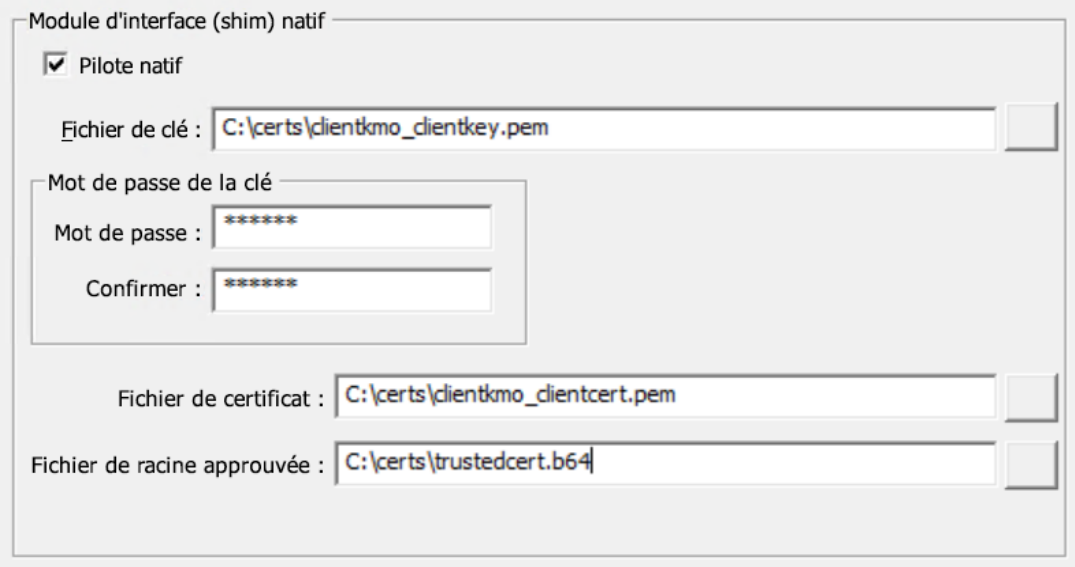
  Fichier de certificat

  Spécifie le fichier dans lequel les certificats sont stockés. Le fichier de certificat doit être au format Base 64. Par exemple, le fichier `clientkmo_clientcert.pem` créé par `dxcmd` dans le répertoire `C:\certs\` lors de l'étape « Exportation d'un certificat à partir d'eDirectory » page 130.

Fichier de racine approuvée

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 racine approuvée doit être au format Base 64. Par exemple, les fichiers `trustedcert.b64` dans le répertoire `C:\certs\` créé par `dxcmd` à la section « Exportation d'un certificat à partir d'eDirectory » page 130.

Figure 10-4 *Exemple d'ajout d'une instance de chargeur distant natif*



- **Pilote .NET :** accédez au chemin du fichier de clé qui contient le certificat pour l'authentification.

  Fichier de clés

  Spécifie le chemin d'accès au fichier contenant la clé utilisée pour l'authentification. Par exemple, le fichier `clientkmo_clientcert.pfx` créé par `dxcmd` dans le répertoire `C:\certs\` lors de l'étape « Exportation d'un certificat à partir d'eDirectory » page 130.

  Mot de passe de la clé

  Spécifie le mot de passe de la clé privée utilisée pour l'authentification.

  Fichier de racine approuvée

  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 racine approuvée doit être au format Base 64. Par exemple, le fichier `trustedcert.b64` créé par `dxcmd` dans le répertoire `C:\certs\` lors de l'étape « Exportation d'un certificat à partir d'eDirectory » page 130.

Figure 10-5 *Exemple d'ajout d'une instance de chargeur distant .NET*

Pour plus d'informations sur les fichiers de sortie générés pour ce pilote à l'aide de l'outil `dxcmd`, reportez-vous au Tableau 10-1, « Exemples de différents types de pilotes », page 132.

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 Keystore, 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.

1. Dans la console du chargeur distant, sélectionnez l'instance de pilote dans la colonne **Description**.
2. Cliquez sur **Arrêter**.
3. Entrez le mot de passe du chargeur distant, puis cliquez sur **OK**.
4. Cliquez sur **Éditer** et effectuez l'Étape 6 de la section « Ajout d'une nouvelle instance de pilote de chargeur distant » page 136.
5. Cliquez sur **OK**.

10.3.8 Vérification de la configuration

Pour plus d'informations à propos du démarrage et de l'arrêt du chargeur distant, reportez-vous au Chapitre 10.4, « Démarrage et arrêt du chargeur distant », page 140.

1. Démarrez le pilote à l'aide d'iManager.
2. Gérez le chargeur distant à l'aide de l'une des méthodes suivantes :

   Interface utilisateur du chargeur distant

   1. Cliquez avec le bouton droit sur la console **Chargeur distant Identity Manager** et sélectionnez **Exécuter en tant qu'administrateur**.
   2. Vous pouvez **démarrer**, **arrêter**, **ajouter**, **supprimer** et effectuer plusieurs opérations à l'aide de l'interface du chargeur distant.

REMARQUE : pour exécuter le chargeur distant en tant que service, sélectionnez **Establish a Remote Loader service for this driver instance** (Établir un service de chargeur distant pour cette instance de pilote). La désélection de cette option exécute le chargeur distant en tant qu'application.

Console du chargeur distant

Accédez à l'emplacement d'installation du chargeur distant et exécutez les commandes suivantes dans l'invite de commande :

1. Pour démarrer ou charger l'instance du chargeur distant :

   Pour le chargeur distant Java :

   ```
   dirxml_jremote -config <configuration_filename> -ksp
   <keystore_password> -kp <keypassword>

   dirxml_jremote -config <configuration_filename>
   ```

   Pour le chargeur distant natif :

   ```
   dirxml_remote -config <configuration_filename> -ksp <keystore_password>
   -kp <keypassword>

   dirxml_remote -config <configuration_filename>
   ```

   Pour le chargeur distant .NET :

   ```
   RemoteLoader.exe  -config <configuration_filename> -ksp
   <keystore_password> -kp <keypassword>

   RemoteLoader.exe  -config <configuration_filename>
   ```

2. Pour arrêter ou décharger l'instance du chargeur distant, ajoutez -u à la fin de la commande précédente. Par exemple

   Pour le chargeur distant Java :

   ```
   dirxml_jremote -config <configuration_filename> -u
   ```

   Pour le chargeur distant natif :

   ```
   dirxml_remote -config <configuration_filename> -u
   ```

   Pour le chargeur distant .NET :

   ```
   RemoteLoader.exe  -config <configuration_filename> -u
   ```

REMARQUE : pour exécuter l'instance du chargeur distant en tant que service, utilisez la commande suivante :

```
dirxml_remote -config config.txt -service install
```

10.4 Démarrage et arrêt du chargeur distant

Le chargeur distant est un service ou daemon nécessitant parfois un redémarrage. Ce chapitre explique comment arrêter et démarrer le chargeur distant.

10.4.1 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.

- « Démarrage automatique des instances de pilote » page 141
- « Utilisation de la console pour démarrer des instances de pilote » page 141

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 hôte.

1. Ouvrez la console du chargeur distant.

   Au cours de l'installation, si vous avez créé un raccourci pour la console du chargeur distant, utilisez l'icône `Console du chargeur distant Identity Manager` sur le bureau. Dans le cas contraire, exécutez le fichier `rlconsole.exe` qui se trouve par défaut à l'emplacement `C:\novell\remoteloader\`*`nn`*`bit`.
2. Sélectionnez une instance de pilote, puis cliquez sur **Éditer**.
3. Sélectionnez **Établir un service de chargeur distant pour cette instance du pilote**.
4. Enregistrez vos modifications, puis fermez la console.

Utilisation de la console pour démarrer des instances de pilote

1. Ouvrez la console du chargeur distant.

   Au cours de l'installation, si vous avez créé un raccourci pour la console du chargeur distant, utilisez l'icône `Console du chargeur distant Identity Manager` sur le bureau. Dans le cas contraire, exécutez le fichier `rlconsole.exe` qui se trouve par défaut à l'emplacement `C:\novell\remoteloader\`*`nn`*`bit`.
2. Sélectionnez une instance de pilote, puis cliquez sur **Démarrer**.

10.4.2 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. Pour plus d'informations sur les paramètres mentionnés dans cette section, reportez-vous à la « Présentation des paramètres de configuration du chargeur distant » page 113.

REMARQUE : lorsque vous arrêtez une instance de pilote, vous devez disposer de droits suffisants ou indiquer le mot de passe du chargeur distant. Par exemple, le chargeur distant s'exécute en tant que service Windows. 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

Utilisez la console du chargeur distant.

Au cours de l'installation, si vous avez créé un raccourci pour la console du chargeur distant, utilisez l'icône `Console du chargeur distant Identity Manager` sur le bureau. Dans le cas contraire, exécutez le fichier `rlconsole.exe` qui se trouve par défaut à l'emplacement `C:\novell\remoteloader\`*`nn`*`bit`.

Chargeur distant Java

Entrez la commande `dirxml_jremote -config` *`nom_fichier`* `-u`. Par exemple :

```
dirxml_jremote -config config.txt -u
```

11 Installation d'iManager

Cette section vous guide tout au long de la procédure d'installation des composants requis pour iManager. Les programmes d'installation permettent d'installer les composants suivants :

- iManager (version serveur)
- iManager Workstation (version cliente)
- Java
- Novell International Cryptographic Infrastructure (NICI)
- Tomcat

Les fichiers d'installation sont situés dans le répertoire `\products\iManager\installs\`*`plate-forme_serveur`*`\` dans le fichier image `.iso` du paquetage d'installation d'Identity Manager. Par défaut, le programme d'installation installe les composants à l'emplacement `C:\Novell`.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous au Chapitre 11.1, « Planification de l'installation d'iManager », page 143.

11.1 Planification de l'installation d'iManager

Cette section présente les conditions préalables, les considérations et la configuration système requise pour l'installation d'iManager. Tout d'abord, consultez la liste de contrôle pour comprendre la procédure d'installation.

11.1.1 Liste de contrôle pour l'installation d'iManager

Avant de commencer l'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 Chapitre 1, « Aperçu des composants Identity Manager », page 19.

	Éléments de la liste de contrôle
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.
❑	3. Découvrez la différence entre iManager et iManager Workstation. Pour plus d'informations, reportez-vous à la Section 11.1.2, « Présentation des versions serveur et client d'iManager », page 144.
❑	4. Pour vous assurer que les ordinateurs répondent aux conditions préalables pour l'installation du serveur et du poste de travail iManager, passez en revue les considérations suivantes : ◆ Pour le serveur iManager, reportez-vous à la section « Considérations relatives à l'installation du serveur iManager » page 146. ◆ Pour iManager Workstation, reportez-vous à la section « Considérations relatives à l'installation du poste de travail iManager » page 147
❑	5. Accédez aux fichiers d'installation d'iManager, situés par défaut dans le répertoire `\products\iManager\installs\`*`plate-forme_serveur`*`\` dans le fichier image `.iso` du paquetage d'installation Identity Manager. Sinon, téléchargez les fichiers d'installation à partir du site Web de téléchargement de NetIQ. Recherchez des produits iManager, sélectionnez la version d'iManager souhaitée, puis téléchargez le fichier `win.zip` dans un répertoire sur votre serveur. Par exemple, `iMan_31_win.zip`.
❑	6. (Facultatif) Pour en savoir plus sur la procédure d'installation des plug-ins, reportez-vous à la Section 11.1.3, « Présentation de l'installation des plug-ins d'iManager », page 145.
❑	7. (Facultatif) Pour passer en revue les opérations que vous pouvez effectuer après avoir installé iManager, reportez-vous au Chapitre 11.3, « Tâches postérieures à l'installation d'iManager », page 155.
❑	8. Pour installer iManager et iManager Workstation, reportez-vous aux sections suivantes : ◆ Pour l'installation de type interface graphique (GUI), reportez-vous à la Section 11.2.1, « Installation d'iManager et du poste de travail iManager », page 149. ◆ Pour effectuer une installation en mode silencieux, reportez-vous à la Section 11.2.2, « Installation d'iManager en mode silencieux », page 153

11.1.2 Présentation des versions serveur et client d'iManager

Vous devez installer iManager sur un serveur pouvant accéder à une arborescence eDirectory. Pour installer iManager sur un poste de travail au lieu d'un serveur, vous devez installer la version client d'iManager, à savoir **iManager Workstation**. Les instructions suivantes vous aideront à déterminer la version qui convient le mieux à votre environnement ou s'il est intéressant pour vos stratégies de gestion de eDirectory d'installer les deux versions :

- Si la gestion de eDirectory est toujours assurée par un seul administrateur à partir du même poste de travail client, vous pouvez utiliser et tirer parti d'iManager Workstation. iManager Workstation est totalement autonome et n'exige qu'une configuration minimale. Il lance et arrête automatiquement les ressources dont il a besoin au chargement ou au déchargement. iManager Workstation s'installe et s'exécute sur divers postes de travail clients Windows, n'a aucune dépendance vis-à-vis d'iManager version serveur et peut coexister avec n'importe quelle autre version d'iManager installée sur le réseau.

Les plug-ins d'iManager ne se synchronisent pas automatiquement entre les instances d'iManager. Si la gestion est assurée par plusieurs administrateurs et que vous utilisez des plug-ins personnalisés, iManager Workstation et ces plug-ins doivent être installés sur chaque poste client d'administration.

- Si la gestion de eDirectory s'effectue à partir de différents postes clients ou si elle est assurée par plusieurs administrateurs, installez iManager version serveur de sorte qu'il soit accessible à partir de n'importe quel poste de travail connecté. En outre, les plug-ins personnalisés ne doivent être installés qu'une seule fois pour chaque serveur iManager.

11.1.3 Présentation de l'installation des plug-ins d'iManager

Par défaut, les modules de plug-in ne sont pas répliqués entre les serveurs iManager. Vous devez installer les modules de plug-in souhaités sur chaque serveur iManager.

Dans le cas d'une nouvelle installation, le programme d'installation présélectionne les plug-ins « habituels ». Pour une mise à niveau, seuls les plug-ins à mettre à jour sont présélectionnés. Vous pouvez modifier les sélections par défaut et ajouter de nouveaux plug-ins à télécharger. Toutefois, pour une mise à niveau, NetIQ vous recommande de ne pas désélectionner les plug-ins présélectionnés. En règle générale, vous devez toujours mettre à niveau les plug-ins que vous avez installés avec une version antérieure d'iManager. En outre, les plug-ins plus récents risquent de ne pas être compatibles avec des versions antérieures d'iManager.

Les plug-ins de base d'iManager sont uniquement disponibles dans le cadre du téléchargement complet du logiciel iManager (par exemple, plug-ins administratifs eDirectory). À moins qu'il n'existe des mises à jour spécifiques pour ces plug-ins, vous ne pouvez les télécharger et les installer qu'avec le produit iManager complet.

Le programme d'installation utilise un fichier descripteur XML, `iman_mod_desc.xml`, pour identifier les plug-ins disponibles au téléchargement. L'URL par défaut du fichier descripteur est http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. En revanche, vous pouvez pointer le programme d'installation vers une autre URL réseau. Par exemple, vous pouvez installer iManager derrière un proxy ou un pare-feu qui empêche le programme d'installation d'accéder à l'URL par défaut.

IMPORTANT : vous devez utiliser la dernière version du kit SDK d'iManager pour recompiler tous les plug-ins personnalisés que vous souhaitez utiliser dans l'environnement que vous venez d'installer.

Pour plus d'informations sur le téléchargement et l'installation de plug-ins, reportez-vous à la procédure de l'une des sections suivantes :

- **Installation de type GUI** : Section 11.2.1, « Installation d'iManager et du poste de travail iManager », page 149
- **Installation en mode silencieux** : Section 11.2.2, « Installation d'iManager en mode silencieux », page 153

Pour plus d'informations sur la personnalisation de la procédure de téléchargement et d'installation de plug-ins, reportez-vous à la section Téléchargement et installation de plug-ins du *Guide d'installation de NetIQ iManager*.

11.1.4 Conditions préalables et considérations relatives à l'installation d'iManager

Cette section fournit des informations relatives à l'installation des versions d'iManager pour serveur et poste de travail.

Considérations générales relatives à l'installation d'iManager

Avant de procéder à l'installation d'iManager, passez en revue les considérations suivantes :

- Identity Manager 4.7 prend en charge eDirectory 9.1. Utilisez iManager 3.1. Pour plus d'informations, reportez-vous au Guide d'installation d'iManager 3.1.
- Si vous prévoyez que plus de 10 administrateurs travaillent régulièrement dans iManager simultanément, n'installez pas iManager sur le même serveur que d'autres composants Identity Manager.
- Si vous ne prévoyez qu'un seul administrateur, vous pouvez installer iManager sur le même serveur que le moteur Identity Manager.
- Si le programme d'installation du serveur iManager détecte une version précédemment installée d'iManager, vous avez la possibilité d'arrêter la procédure d'installation ou de supprimer les installations existantes d'iManager, de JRE et de Tomcat.
- Étant donné que iManager Workstation est un environnement indépendant, vous pouvez installer plusieurs versions sur le même poste de travail, y compris d'anciennes versions de Mobile iManager. Toutefois, vous ne devez pas essayer de les exécuter simultanément. Si vous devez utiliser différentes versions, exécutez-en une, fermez-la, puis exécutez l'autre version.
- vous ne pouvez pas exécuter iManager Workstation à partir d'un chemin qui comprend des espaces. Par exemple, `C:\NetIQ\iManager Workstation\working`.
- Vous devez disposer d'un accès administrateur pour les serveurs Windows.
- Pour créer une collection de services basés sur les rôles (RBS) dans l'arborescence eDirectory, vous devez disposer de droits équivalents à ceux d'un administrateur.
- Pour exécuter l'assistant de configuration des RBS dans iManager, vous devez disposer de droits équivalents à ceux d'un administrateur.
- Pour gérer la même arborescence eDirectory avec plusieurs versions d'iManager, vous devez mettre à jour vos collections RBS vers la dernière version d'iManager.

Considérations relatives à l'installation du serveur iManager

Si vous utilisez Microsoft IIS (Internet Information Services) ou un serveur HTTP Apache, vous devez intégrer iManager manuellement avec ces infrastructures de serveur Web. Par défaut, iManager utilise Tomcat.

Considérations relatives à l'installation du poste de travail iManager

Avant d'installer iManager Workstation sur des clients Windows, NetIQ recommande de passer en revue les considérations suivantes :

- Pour qu'Internet Explorer utilise un serveur proxy sur votre réseau local, vous devez spécifier **Ne pas utiliser de serveur proxy pour les adresses locales** sous **Outils** > **Options Internet** > **Connexions** > **Paramètres du réseau local**.
- Pour exécuter une version du client Novell antérieure à 4.9.1, le client NetIQ Modular Authentication Service (NMAS) doit être installé sur le poste de travail avant de démarrer iManager Workstation.
- Si vous exécutez iManager Workstation à partir d'un chemin qui comprend un répertoire dont le nom contient `temp` ou `tmp`, comme `c:\programs\temp\imanager`, les plug-ins d'iManager ne s'installent pas. Exécutez iManager Workstation partir de `C:\imanager` ou d'un répertoire qui ne soit pas temporaire.
- La première fois que vous exécutez iManager Workstation sur un poste de travail Windows, utilisez un compte faisant partie du groupe des administrateurs de ce poste.

11.1.5 Configuration système requise pour le serveur iManager

Cette section décrit la configuration minimale requise pour le(s) serveur(s) sur le(s)quel(s) vous souhaitez installer iManager. Pour plus d'informations sur la version serveur d'iManager, reportez-vous à la Section 11.1.2, « Présentation des versions serveur et client d'iManager », page 144.

Catégorie	Configuration requise
Processeur	1 GHz
Espace disque	200 Mo
Mémoire	512 Mo (1 024 Mo recommandés) 80 Mo pour les plug-ins iManager
Système d'exploitation (certifié)	L'un des systèmes d'exploitation suivants : ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 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. vous ne pouvez pas installer iManager sur une plate-forme Solaris. Toutefois, iManager peut toujours gérer et travailler avec des applications et ressources telles qu'eDirectory s'exécutant sur une plate-forme Solaris.
Système 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.

Catégorie	Configuration requise
Hot Fix de système d'exploitation	NetIQ vous recommande d'appliquer les derniers correctifs de système d'exploitation, en fonction de la mise à jour automatique du fabricant.
Navigateurs Web	Un des navigateurs suivants (versions minimales) : ◆ Google Chrome 61 ◆ Mozilla Firefox 51
Serveur d'applications	Tomcat 8.5.27 **REMARQUE :** vous pouvez intégrer manuellement une infrastructure de serveur Web IIS ou Apache existante avec iManager sur un serveur Windows.
Services Annuaire	NetIQ eDirectory 9.1 ou version ultérieure
Ports par défaut	8080, 8443 et 9009

11.1.6 Configuration système requise pour iManager Workstation (version client)

Cette section décrit la configuration minimale requise pour le(s) serveur(s) sur le(s)quel(s) vous souhaitez installer iManager Workstation. Pour plus d'informations sur la version client d'iManager, reportez-vous à la Section 11.1.2, « Présentation des versions serveur et client d'iManager », page 144

Catégorie	Configuration requise
Processeur	1 GHz
Espace disque	200 Mo
Mémoire	256 Mo (521 Mo recommandés)
Système d'exploitation (certifié)	L'un des systèmes d'exploitation suivants : ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 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.
Système 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.
Navigateurs Web	Un des navigateurs suivants (versions minimales) : ◆ Google Chrome 61 ◆ Mozilla Firefox 51

Catégorie	Configuration requise
Hot Fix de système d'exploitation	NetIQ vous recommande d'appliquer les derniers correctifs de système d'exploitation, en fonction de la mise à jour automatique du fabricant.
Serveur d'applications	Tomcat 8.5.27, fourni avec iManager Workstation
Java	JRE 1.8.0_162, fourni avec le poste de travail iManager
Ports par défaut	8080, 8443 et 9009

11.2 Installation de la version serveur d'iManager et d'iManager Workstation

Ce chapitre décrit la procédure d'installation d'iManager. Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise indiquée à la Section 11.1.4, « Conditions préalables et considérations relatives à l'installation d'iManager », page 146.

Pour passer en revue l'intégralité de la procédure d'installation, reportez-vous à la section « Planification de l'installation d'iManager » page 143.

- Section 11.2.1, « Installation d'iManager et du poste de travail iManager », page 149
- Section 11.2.2, « Installation d'iManager en mode silencieux », page 153

11.2.1 Installation d'iManager et du poste de travail iManager

Cette section présente les étapes nécessaires à l'installation d'iManager et d'iManager Workstation sur des serveurs et clients Windows. Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise :

- **iManager** : « Considérations relatives à l'installation du serveur iManager » page 146.
- **iManager Workstation** : « Considérations relatives à l'installation du poste de travail iManager » page 147.
- Reportez-vous également aux notes de version accompagnant la version du logiciel.

Installation du serveur iManager

La procédure suivante décrit l'installation de la version serveur d'iManager sur un serveur Windows à l'aide d'un assistant d'installation. Pour effectuer l'opération en mode silencieux sans surveillance, reportez-vous à la Section 11.2.2, « Installation d'iManager en mode silencieux », page 153.

Si le programme d'installation du serveur iManager détecte une version précédemment installée d'iManager, vous avez la possibilité d'arrêter la procédure d'installation ou de supprimer les installations existantes d'iManager, JRE et Tomcat. Lorsque le programme d'installation supprime la version précédemment installée d'iManager, il sauvegarde la structure de répertoires dans l'ancien répertoire *TOMCAT_HOME* afin de conserver tout contenu personnalisé créé précédemment.

Pour installer le serveur iManager :

1. Connectez-vous en tant qu'utilisateur disposant de privilèges d'administrateur sur l'ordinateur sur lequel vous souhaitez installer iManager.
2. (Conditionnel) Si vous disposez du fichier image `.iso` pour le paquetage d'installation d'Identity Manager, accédez aux fichiers d'installation d'iManager, situé par défaut dans le répertoire `\products\iManager\installs\win\`.
3. (Conditionnel) Si vous avez téléchargé les fichiers d'installation d'iManager sur le site Web de téléchargement de NetIQ, procédez comme suit :
   - **3a** Identifiez le fichier `win.zip`. Par exemple, `iMan_310_win_x86_64.zip`.
   - **3b** Extrayez le fichier `win.zip` dans un dossier de l'ordinateur local.
4. Exécutez `iManagerInstall.exe`.
5. (Facultatif) Pour afficher les données de débogage du programme d'installation, maintenez la touche `Ctrl` enfoncée juste après le lancement du programme d'installation jusqu'à ce qu'une fenêtre de console s'affiche. Pour plus d'informations sur le débogage, reportez-vous à la section Troubleshooting (Dépannage) du *NetIQ iManager Administration Guide* (guide d'administration de NetIQ iManager 2.7.7).
6. Dans la fenêtre de bienvenue d'iManager, sélectionnez une langue, puis cliquez sur **OK**.
7. Dans la fenêtre **Introduction**, cliquez sur **Next** (Suivant).
8. Acceptez l'accord de licence, puis cliquez sur **Suivant**.
9. (Conditionnel) Si votre serveur contient déjà une version de JVM, de Tomcat ou d'autres composants de support installés dans le cadre d'iManager, dans la fenêtre **Detection Summary** (Résumé de détection), procédez comme suit :
   - **9a** Sous **Install the following components** (Installer les composants suivants), assurez-vous que les versions indiquées des composants correspondent à celles que vous souhaitez installer.
   - **9b** (Facultatif) Si le programme d'installation ne répertorie pas les versions que vous voulez installer, sélectionnez les composants adéquats dans le dossier d'installation.
10. Cliquez sur **Next** (Suivant).
11. Dans la fenêtre **Get PORT Input** (Obtenir l'entrée PORT), indiquez les numéros de port sur lesquels le serveur Tomcat doit s'exécuter, puis cliquez sur **Next** (Suivant).

    Par défaut, les valeurs des ports HTTP et SSL sont respectivement 8080 et 8443. Toutefois, si un autre service ou serveur Tomcat utilise les ports par défaut, vous pouvez spécifier d'autres ports.
12. Indiquez l'algorithme de clé publique de certificat que le certificat TLS doit utiliser, puis cliquez sur **Suivant**. Par défaut, l'algorithme de clé publique est défini sur **RSA**.
    - **RSA :** le certificat utilise une paire de clés RSA 2048 bits. Si vous sélectionnez **RSA**, quatre niveaux de chiffrement sont autorisés. Par défaut, le niveau de chiffrement est défini sur **AUCUN**.
      - **AUCUN :** autorise tout type de chiffrement.
      - **FAIBLE :** autorise un chiffrement 56 ou 64 bits.
      - **MOYEN :** autorise un chiffrement de 128 bits.
      - **ÉLEVÉ :** autorise un chiffrement supérieur à 128 bits.
    - **ECDSA 256 :** le certificat utilise une paire de clés ECDSA avec une courbe secp256r1. Si vous sélectionnez **ECDSA 256**, un seul niveau de chiffrement est autorisé :
      - **SUITEB 128 UNIQUEMENT :** autorise un chiffrement de 128 bits.

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

13 (Facultatif) Pour utiliser des adresses IPv6 avec iManager, cliquez sur **Oui** dans la fenêtre **Activer IPv6**.

Vous pouvez activer les adresses IPv6 après l'installation d'iManager. Pour plus d'informations, reportez-vous à la Section 11.3.2, « Configuration d'iManager pour les adresses IPv6 après l'installation », page 158.

14 Cliquez sur **Next** (Suivant).

15 Dans la fenêtre **Sélectionner le dossier d'installation**, indiquez le dossier dans lequel stocker les fichiers d'installation, puis cliquez sur **Suivant**.

Le répertoire d'installation par défaut est `C:\Program Files\Novell`.

16 (Facultatif) Pour télécharger et installer des plug-ins dans le cadre de l'installation, procédez comme suit :

16a Dans la fenêtre **Sélectionner les plug-ins à télécharger et installer**, sélectionnez les plug-ins de votre choix.

16b (Facultatif) Pour télécharger des plug-ins à partir d'un autre emplacement réseau, spécifiez une autre **Network URL** (URL réseau).

Si vous utilisez une autre URL pour le téléchargement des plug-ins, vous devez vérifier son contenu et contrôler si le plug-in convient à votre utilisation. Par défaut, le programme d'installation télécharge les plug-ins à l'adresse http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. Pour plus d'informations, reportez-vous à la Section 11.1.3, « Présentation de l'installation des plug-ins d'iManager », page 145.

16c Cliquez sur **Next** (Suivant).

16d (Facultatif) Le programme d'installation peut afficher le message suivant :

```
No new or updated plug-ins found. All plug-ins are downloaded or updated or
the iManager download server is unavailable.
```

Si cette erreur s'affiche, une ou plusieurs des conditions suivantes sont réunies :

- Aucun plug-in mis à jour n'est disponible sur le site de téléchargement.
- Un problème est survenu avec votre connexion Internet. Vérifiez votre connexion, puis réessayez.
- La connexion au fichier descripteur (http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml) a échoué. Cette URL donne accès à un fichier descripteur XML contenant les plug-ins iManager disponibles.
- L'installation d'iManager s'effectue derrière un proxy qui n'autorise pas la connexion à l'URL ci-dessus.

16e (Facultatif) Pour installer des plug-ins à partir d'un répertoire local, dans la fenêtre Select Plug-ins to Install from Disk (Sélectionner les plug-ins à installer à partir du disque), spécifiez le chemin d'accès au répertoire contenant les fichiers de plug-in `.npm` appropriés.

Cette étape vous permet d'installer des plug-ins personnalisés ou téléchargés précédemment. Le chemin par défaut est `\emplacement_extraction\products\iManager\plugins`. Cependant, vous pouvez spécifier n'importe quel chemin d'accès valide.

16f Cliquez sur **Next** (Suivant).

17 (Facultatif) Dans la fenêtre **Get User and Tree Names** (Obtenir des noms d'utilisateur et d'arborescence), spécifiez un utilisateur autorisé ainsi que le nom de l'arborescence eDirectory gérée par cet utilisateur.

REMARQUE

- Si eDirectory utilise un autre port que le port par défaut 524, vous pouvez spécifier l'adresse IP ou le nom DNS du serveur eDirectory ainsi que le numéro de port. N'utilisez pas `localhost`. Par exemple, pour spécifier une adresse IPv6, entrez `https://[2001:db8::6]:1080/nps/servlet/webacc?taskId=fw.Startup&forceMaster=true`.
- NetIQ vous déconseille de ne pas renseigner ces paramètres. Si vous laissez ces champs vides, iManager permet à n'importe quel utilisateur d'installer des plug-ins et de modifier les paramètres du serveur iManager. Vous pouvez spécifier un utilisateur autorisé après avoir terminé la procédure d'installation. Pour plus d'informations, reportez-vous à la Section 11.3.3, « Spécification d'un utilisateur autorisé pour eDirectory », page 158.
- Le programme d'installation ne valide pas les références de l'utilisateur spécifiées dans eDirectory.

18 Cliquez sur **Next** (Suivant).

19 Lisez la page Résumé avant installation, puis cliquez sur **Installer**.

20 Une fois l'installation terminée, la fenêtre **Installation terminée** affiche les messages relatifs à la réussite de la procédure.

REMARQUE : même si l'installation a réussi, la fenêtre **Installation terminée** peut afficher le message d'erreur suivant :

```
The installation of iManager version is complete, but some errors occurred
during the install.
Please see the installation log Log file path for details. Press "Done" to quit
the installer.
```

21 (Conditionnel) Si le programme d'installation affiche le message d'erreur illustré à l'Étape 20, procédez comme suit :

21a Notez le chemin du fichier journal affiché dans le message d'erreur.

21b Dans la fenêtre **Installation terminée**, cliquez sur **Terminé** Terminé.

21c Ouvrez le fichier journal.

21d (Conditionnel) Si vous trouvez l'erreur suivante dans le fichier journal, vous pouvez ignorer le message d'erreur. L'installation s'est bien déroulée et iManager fonctionne correctement.

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class
com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The process
cannot access the file because it is being used by another process)
```

21e (Conditionnel) Si le fichier ne contient pas l'erreur indiquée à l'Étape 21d, NetIQ vous recommande de recommencer l'installation.

22 Cliquez sur **Terminer**.

23 Une fois l'initialisation d'iManager terminée, cliquez sur le premier lien de la page Getting Started (Mise en route), puis connectez-vous. Pour plus d'informations, reportez-vous à la section Accessing iManager (Accès à iManager) du manuel *NetIQ iManager Administration Guide* (Guide d'administration de NetIQ iManager 2.7.7).

Installation du poste de travail iManager

iManager Workstation est un environnement autonome. Vous pouvez installer plusieurs versions sur le même poste de travail (y compris les anciennes versions de Mobile iManager). Toutefois, vous ne devez pas essayer de les exécuter simultanément. Si vous devez utiliser différentes versions, exécutez-en une, fermez-la, puis exécutez l'autre version.

REMARQUE : vous ne pouvez pas exécuter iManager Workstation à partir d'un chemin qui comprend des espaces. Par exemple, `C:\NetIQ\iManager Workstation\working`.

Pour installer le poste de travail iManager :

1. (Conditionnel) Si vous disposez du fichier image `.iso` du paquetage d'installation Identity Manager, accédez aux fichiers d'installation d'iManager, situés par défaut dans le répertoire `\products\iManager\installs\win\`.
2. (Conditionnel) Si vous avez téléchargé les fichiers d'installation d'iManager sur le site Web de téléchargement de NetIQ, procédez comme suit :
   - **2a** Identifiez le fichier `win.zip`. Par exemple, `iMan_31_workstation_win.zip`.
   - **2b** Extrayez le fichier `win.zip` dans un dossier de l'ordinateur local.
3. À partir du dossier `imanager\bin`, exécutez le fichier `iManager.bat`.
4. Dans la fenêtre de connexion à iManager, indiquez les références d'un utilisateur autorisé ainsi que l'arborescence eDirectory gérée par cet utilisateur.

   Pour plus d'informations sur l'accès à iManager, reportez-vous à la section Accessing iManager (Accès à iManager) du *NetIQ iManager Administration Guide* (guide d'administration d'iManager 2.7.7).
5. (Facultatif) Pour activer les adresses IPv6, procédez comme suit :
   1. Ouvrez le fichier *<Rép_installation_utilisateur>*`\Tomcat\conf\catalina.properties`.
   2. Définissez les entrées de configuration suivantes dans le fichier `catalina.properties` :

      ```
      java.net.preferIPv4Stack=false
      ```

      ```
      java.net.preferIPv4Addresses=true
      ```
   3. Redémarrez le service Tomcat.

11.2.2 Installation d'iManager en mode silencieux

Une installation silencieuse (non interactive) n'affiche aucune interface utilisateur et ne pose aucune question à l'utilisateur. En revanche, InstallAnywhere utilise les informations contenues dans un fichier `install.properties` par défaut. Vous pouvez exécuter l'installation silencieuse avec le fichier par défaut ou modifier le fichier pour personnaliser la procédure d'installation.

Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise :

- **serveur iManager** : « Considérations relatives à l'installation du serveur iManager » page 146.
- **iManager Workstation** : « Considérations relatives à l'installation du poste de travail iManager » page 147.
- Reportez-vous également aux notes de version accompagnant la version du logiciel.

Modification du fichier de propriétés pour une installation en mode silencieux personnalisée

Pour mieux contrôler les modules installés, vous pouvez personnaliser la procédure d'installation en mode silencieux.

1 Ouvrez le fichier `install.properties`, situé par défaut dans le répertoire *`products`*`/iManager`, dans le fichier image `.iso` du paquetage d'installation Identity Manager pour chaque répertoire de l'environnement du système d'exploitation.

REMARQUE : si vous avez déjà installé la version la plus récente d'iManager sur un serveur, vous pouvez utiliser le fichier `installer.properties` généré par le programme d'installation. Le fichier, qui se trouve par défaut dans le répertoire `log`, contient les valeurs spécifiées lors de l'installation.

---

2 Dans le fichier de propriétés, ajoutez les valeurs et les paramètres suivants :

`$PLUGIN_INSTALL MODE$`

Indique la propriété qui contrôle si les plug-ins sont installés. Ajoutez l'une des valeurs suivantes :

- `DISK` : (valeur par défaut) indique au programme d'installation d'installer les plug-ins à partir du disque local.
- `NET` : indique au programme d'installation d'installer les plug-ins à partir du réseau.
- `BOTH` : indique au programme d'installation d'installer les plug-ins à partir du disque et du réseau.
- `SKIP` : n'installe pas les plug-ins.

`$PLUGIN_DIR$`

Indique un autre chemin d'accès pour les plug-ins situés sur le disque local. Le chemin d'accès par défaut est *`\répertoire_racine_programme_installation`*`\iManager\installs\`*`chemin_plate_forme`*`\plugin`.

Le programme d'installation installe tous les modules du répertoire de plug-ins, à l'exception des sous-répertoires.

`$PLUGIN_INSTALL_URL$`

Indique l'URL réseau permettant au programme d'installation de télécharger les plug-ins, par défaut http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. Si vous utilisez une autre URL, vous devez vérifier son contenu et contrôler si le plug-in est adapté à votre utilisation. Pour plus d'informations, reportez-vous à la Section 11.1.3, « Présentation de l'installation des plug-ins d'iManager », page 145.

`$LAUNCH_BROWSER$`

Spécifie si le programme d'installation lance le fichier `gettingstarted.html` une fois l'installation terminée.

`$USER_INSTALL_DIR$`

Indique le chemin où installer iManager.

`USER_INPUT_ENABLE_IPV6`

Indique si iManager doit utiliser des adresses IPv6. Par défaut, le programme d'installation définit cette valeur sur `Oui`.

3 Pour chaque module de plug-in à télécharger et installer, indiquez l'ID et la version du module du fichier `MANIFEST.MF`, situé dans le dossier `META-INF/` du fichier `.npm` (module de plug-in). Par exemple :

```
$PLUGIN_MODULE_ID_1$=eDirectoryBackupAndRestore

$PLUGIN_VERSION_1$=2.7.20050517

$PLUGIN_MODULE_ID_2$=ldap

$PLUGIN_VERSION_2$=2.7.20050517
```

REMARQUE

- Si vous n'en spécifiez aucun, le programme installe les modules les plus fréquemment installés, portant la mention « selected » dans les fichiers `iman_mod_desc.xml` sur le site Web de téléchargement.
- Si vous ne définissez aucune version d'un module, le programme d'installation installe n'importe quel module correspondant au nom `.npm`.

Exécution d'une installation d'iManager en mode silencieux

Vous pouvez effectuer une installation silencieuse d'iManager à l'aide des valeurs par défaut du fichier `install.properties`. Il est situé par défaut dans le répertoire `\products\iManager`, dans le fichier image `.iso` du paquetage d'installation Identity Manager pour chaque répertoire de l'environnement du système d'exploitation. Le répertoire `\products\iManager` doit également contenir le fichier exécutable de l'installation.

1 Dans une fenêtre de la console, accédez au répertoire qui contient le fichier `install.properties` téléchargé.

2 Sur la ligne de commande, entrez la commande suivante :

```
iManagerInstall.exe -i silent
```

11.3 Tâches postérieures à l'installation d'iManager

Après avoir installé iManager, vous pouvez modifier les paramètres de configuration, comme l'activation des adresses IPv6 ou la modification de l'utilisateur autorisé pour une arborescence eDirectory. En outre, NetIQ recommande de remplacer les certificats auto-signés créés lors de la procédure d'installation.

- Section 11.3.1, « Remplacement des certificats auto-signés temporaires pour iManager », page 155
- Section 11.3.2, « Configuration d'iManager pour les adresses IPv6 après l'installation », page 158
- Section 11.3.3, « Spécification d'un utilisateur autorisé pour eDirectory », page 158

11.3.1 Remplacement des certificats auto-signés temporaires pour iManager

Les installations d'iManager en mode autonome incluent un certificat auto-signé temporaire destiné à être utilisé par Tomcat. Ce certificat expire après un an. NetIQ fournit ce certificat pour vous aider à rendre votre système opérationnel afin de pouvoir utiliser iManager immédiatement en toute sécurité

après l'installation du produit. NetIQ et OpenSSL déconseillent l'utilisation de certificats auto-signés sauf à des fins de test. Nous vous conseillons de remplacer le certificat temporaire par un certificat sûr.

Tomcat stocke le certificat auto-signé dans un keystore qui utilise le format de fichier Tomcat (JKS). Normalement, vous devriez importer une clé privée pour remplacer le certificat. Toutefois, le `keytool` que vous utilisez pour modifier ce keystore Tomcat ne peut pas importer les clés privées. Cet outil n'utilise que les clés générées automatiquement.

Cette section explique comment générer une paire clé publique/clé privée dans eDirectory à l'aide du serveur de certificats NetIQ et remplacer le certificat temporaire. Si vous utilisez eDirectory, vous pouvez faire appel au serveur de certificats NetIQ pour générer, suivre, stocker et révoquer des certificats en toute sécurité sans autre investissement.

Remplacement des certificats auto-signés d'iManager

Cette section décrit comment créer une paire de clés dans eDirectory et exporter les clés publiques, privées et de racine des autorités de certification (CA) via un fichier `PKCS#12`. Cela inclut la modification du fichier de configuration `server.xml` de Tomcat afin d'utiliser la directive PKCS12 et de faire pointer la configuration vers un fichier P12 proprement dit plutôt que d'utiliser le keystore JKS par défaut.

Ce processus utilise les fichiers suivants :

- `C:\Program Files\Novell\Tomcat\conf\ssl\.keystore`, qui contient la paire de clés temporaire
- `C:\Program Files\Novell\jre\lib\security\cacerts`, qui contient les certificats root approuvés
- `C:\Program Files\Novell\Tomcat\conf\server.xml`, utilisé pour configurer l'utilisation de certificats par Tomcat

Pour remplacer les certificats auto-signés :

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, 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 (`.pfx`).

3 Pour convertir le fichier `.pfx` en fichier `.pem`, procédez comme suit :

REMARQUE : OpenSSL n'est pas installé par défaut. Toutefois, vous pouvez télécharger une version à partir du site Web OpenSSL.

3a Entrez une commande, par exemple `openssl pkcs12 -in newtomcert.pfx -out newtomcert.pem`.

3b Spécifiez le même mot de passe pour le certificat que celui spécifié à l'Étape 2.

3c Spécifiez un mot de passe pour le nouveau fichier `.pem`.

Si vous le souhaitez, vous pouvez utiliser le même mot de passe.

4 Pour convertir le fichier `.pem` en fichier `.p12`, procédez comme suit :

4a Entrez une commande, par exemple `openssl pkcs12 -export -in newtomcert.pem -out newtomcert.p12 -name "New Tomcat"`.

4b Spécifiez le même mot de passe pour le certificat que celui spécifié à l'Étape 3.

4c Spécifiez un mot de passe pour le nouveau fichier `.p12`.

Si vous le souhaitez, vous pouvez utiliser le même mot de passe.

5 Copiez le fichier `.p12` à l'emplacement du certificat de Tomcat, par défaut `C:\Program Files\Novell\Tomcat\conf\ssl\`.

6 Arrêtez le service Tomcat à l'aide du script de démarrage `services.msc`.

7 Pour vous assurer que Tomcat utilise le fichier de certificat `.p12` qui vient d'être créé, ajoutez les variables `keystoreType`, `keystoreFile` et `keystorePass` au fichier `server.xml` de Tomcat. Par exemple :

```
<Connector className="org.apache.coyote.http11.Http11AprProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"
 keystoreFile="C:\Program Files\Novell\Tomcat\conf\ssl\newtomcert.p12"
keystorePass="password" />
```

Ou

```
<Connector className="org.apache.coyote.http11.Http11NioProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"
 keystoreFile="C:\Program Files\Novell\Tomcat\conf\ssl\newtomcert.p12"
keystorePass="password" />
```

Lorsque vous définissez le type de keystore sur `PKCS12`, vous devez spécifier le chemin d'accès complet au fichier de certificat, étant donné que Tomcat n'utilise plus par défaut le chemin du répertoire privé de Tomcat.

8 Démarrez le service Tomcat à l'aide du script de démarrage `services.msc`.

11.3.2 Configuration d'iManager pour les adresses IPv6 après l'installation

Une fois iManager installé, vous pouvez le configurer de manière à ce qu'il utilise les adresses IPv6.

1. Ouvrez le fichier `catalina.properties` dans le répertoire d'installation, situé par défaut dans *`répertoire_installation`*`\Tomcat\conf`.
2. Définissez les entrées de configuration suivantes dans le fichier de propriétés :

   ```
   java.net.preferIPv4Stack=false
   ```

   ```
   java.net.preferIPv4Addresses=true
   ```

3. Relancez Tomcat.

11.3.3 Spécification d'un utilisateur autorisé pour eDirectory

Une fois iManager installé, vous pouvez modifier les références de l'utilisateur autorisé ainsi que le nom de l'arborescence eDirectory gérée par cet utilisateur. Pour plus d'informations, reportez-vous à la section iManager Authorized Users and Groups (Groupes et utilisateurs autorisés par iManager) du *NetIQ iManager Administration Guide* (Guide d'administration de NetIQ iManager 2.7.7).

1 Connectez-vous à iManager.

2 Dans la vue Configurer, cliquez sur **iManager Server**(Serveur iManager) > **Configure iManager** (Configurer iManager) > **Security** (Sécurité).

3 Mettez à jour les références de l'utilisateur et le nom de l'arborescence.

IV Installation des applications d'identité

Cette section vous guide tout au long de la procédure d'installation de l'infrastructure et des composants requis pour les applications d'identité :

- Administration des applications d'identité
- Tableau de bord des applications d'identité
- Pilote de service de rôle et de ressource
- Application utilisateur
- Pilote d'application utilisateur

Par défaut, le programme d'installation installe ces composants à l'emplacement `C:\NetIQ\idm\apps`.

Les applications d'identité nécessitent l'accès à d'autres composants Identity Manager pendant et après l'installation. NetIQ vous recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous au Chapitre 15.1, « Planification de l'installation des applications d'identité », page 189.

12 Installation de PostgreSQL et de Tomcat pour Identity Manager

Dans cette section, vous allez installer les programmes de serveur d'applications et de base de données suivants, qui sont utilisés par la plupart des composants Identity Manager :

- Apache Tomcat
- PostgreSQL

Les fichiers d'installation sont situés dans le répertoire `\products\CommonApplication\` du paquetage d'installation d'Identity Manager. Par défaut, le programme d'installation installe les applications à l'emplacement `C:\NetIQ\idm\apps`.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous à la Section 12.1.1, « Liste de contrôle pour l'installation de Tomcat et de PostgreSQL », page 162.

12.1 Planification de l'installation de PostgreSQL et de Tomcat

À partir d'Identity Manager 4.6, NetIQ prend uniquement en charge Apache Tomcat en tant que serveur d'applications. Si votre société fournit une version prise en charge de Tomcat, vous pouvez l'utiliser avec Identity Manager.

De même, pour plus de facilité, NetIQ fournit Tomcat et PostgreSQL dans le même programme d'installation. Ce programme d'installation vous permet d'installer ces applications sans les télécharger séparément. NetIQ ne fournit pas de mises à jour pour ces composants et ne gère pas non plus l'administration, la configuration ou le paramétrage des informations, à l'exception de ce qui est décrit dans la documentation de NetIQ Identity Manager.

12.1.1 Liste de contrôle pour l'installation de Tomcat et de PostgreSQL

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 aux sections suivantes : ◆ Section 4.4, « Utilisation de la gestion des mots de passe en self-service dans Identity Manager », page 32 ◆ Section 4.5, « Utilisation de l'accès Single Sign-on dans Identity Manager », page 34
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3.4, « Configuration recommandée pour le serveur », page 43.
❑	3. Déterminez si vous devez installer NetIQ Sentinel avant d'installer Tomcat ou PostgreSQL. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41. **REMARQUE :** l'installation de Sentinel est prise en charge uniquement sur un serveur Linux. Pour installer Sentinel, vous devez disposer d'un serveur Linux dans votre environnement.
❑	4. Consultez les considérations relatives à l'installation des applications afin de vérifier que les ordinateurs respectent la configuration requise : ◆ Section 12.1.4, « Conditions préalables à l'installation de Tomcat », page 163 ◆ Section 12.1.3, « Conditions préalables à l'installation de PostgreSQL », page 163
❑	5. Installez les applications : ◆ Pour effectuer une installation guidée, reportez-vous à la Section 12.2.1, « Utilisation de l'assistant pour l'installation de PostgreSQL et de Tomcat », page 164. ◆ Pour effectuer une installation silencieuse, reportez-vous à la Section 12.2.2, « Installation en mode silencieux de Tomcat et PostgreSQL pour Identity Manager », page 167.
❑	6. Installez le reste des composants Identity Manager.

12.1.2 Présentation de la procédure d'installation de PostgreSQL et de Tomcat

Vous pouvez choisir d'installer une application ou les deux. Par exemple, vous n'avez peut-être pas besoin de PostgreSQL parce que vous avez déjà une version prise en charge de l'application sur le serveur. Les considérations suivantes valent pour les installations individuelles :

PostgreSQL

La procédure d'installation installe la base de données des applications d'identité et crée un administrateur nommé `idmadmin` qui devient le propriétaire de la base de données. Cependant, l'installation ne crée pas le schéma dans la base de données des applications d'identité. Les informations du schéma sont ajoutées lors de l'installation des applications d'identité.

si vous avez déjà une version prise en charge de PostgreSQL en cours d'exécution sur le serveur, le programme d'installation vous demande d'insérer le mot de passe de l'utilisateur `postgres` par défaut. Le programme crée ensuite l'utilisateur `idmadmin` et lui assigne le même mot de passe que pour `postgres`.

À la fin du processus, le programme d'installation démarre l'instance de base de données. L'instance doit être en cours d'exécution lorsque vous installez d'autres composants Identity Manager qui utilisent la base de données, tels que l'application utilisateur.

Vous n'êtes pas obligé d'utiliser PostgreSQL pour la base de données des applications d'identité.

Tomcat

La procédure d'installation crée le service IDM Apps Tomcat Service. Pour prendre en charge le serveur d'applications Tomcat, le programme d'installation installe également Apache ActiveMQ et Oracle JRE. Ces éléments aident Tomcat à envoyer des notifications par message électronique.

Le programme d'installation ne démarre pas Tomcat une fois l'opération terminée. Tomcat doit être arrêté avant d'installer d'autres composants Identity Manager, tels qu'Identity Reporting.

12.1.3 Conditions préalables à l'installation de PostgreSQL

Passez en revue les considérations suivantes avant d'envisager l'installation de PostgreSQL :

- Vous pouvez installer la version de PostgreSQL fournie avec Identity Manager dans un environnement qui exécute une ancienne version du programme de base de données. Pour que la nouvelle installation ne remplace pas la version précédente, indiquez un autre répertoire pour les fichiers.
- Les applications d'identité imposent certaines conditions préalables à la base de données qu'elles utilisent, telle que PostgreSQL. Pour plus d'informations, reportez-vous à la section « Conditions préalables à l'installation de la base de données pour les applications d'identité » page 196.
- Vous ne pouvez pas installer plusieurs versions de PostgreSQL, car le compte de service pour PostgreSQL ne gère pas les deux instances. Désinstallez l'ancienne version avant d'installer cette version de PostgreSQL.

12.1.4 Conditions préalables à l'installation de Tomcat

Passez en revue les considérations suivantes avant d'envisager l'installation de Tomcat :

- Vous pouvez installer Tomcat et PostgreSQL sur le même serveur ou sur des serveurs distincts.
- La procédure d'installation installe les versions prises en charge d'Oracle JRE et d'Apache ActiveMQ.
- Elle installe également les fichiers requis pour le service Apache Log4j qui permet d'auditer les événements Tomcat.
- Vous pouvez utiliser votre propre programme d'installation Tomcat au lieu de celui fourni dans le kit d'installation d'Identity Manager. Toutefois, pour utiliser le service Apache Log4j avec votre version de Tomcat, vérifiez que les fichiers appropriés sont installés. Pour plus d'informations, reportez-vous à la Section 13.1.4, « Utilisation du service Apache Log4j pour consigner les événements de connexion », page 171. Cette exigence vaut pour l'utilisation de Tomcat pour OSP, les applications d'identité et Identity Reporting.
- Pour garantir l'envoi de notifications par message électronique avec ActiveMQ, installez MQServer.

- Les applications d'identité imposent certaines conditions préalables au serveur d'applications Tomcat sur lequel elles s'exécutent. Pour plus d'informations, reportez-vous à la section « Conditions préalables et considérations relatives au serveur d'applications » page 194.
- La procédure d'installation définit l'emplacement du JRE dans le fichier `setenv.bat`, situé par défaut dans le répertoire `c:\NetIQ\idm\apps\tomcat\bin`. Lorsque vous installez les applications d'identité et Identity Reporting sur Tomcat, la procédure met à jour les entrées `JAVA_OPTs` ou `CATALINA_OPTS` dans le fichier `setenv.bat`.

12.1.5 Configuration système requise pour PostgreSQL

Pour PostgreSQL, la configuration matérielle requise est identique à celle des applications d'identité. Pour plus d'informations, reportez-vous à la section « Configuration système requise pour les applications d'identité » page 197. Reportez-vous également aux notes de version pour la dernière version d'Identity Manager et à la documentation pour PostgreSQL.

12.1.6 Configuration système requise pour Tomcat

Pour Tomcat, la configuration matérielle requise est identique à celle des applications d'identité. Pour plus d'informations, reportez-vous à la Section 15.1.4, « Configuration système requise pour les applications d'identité », page 197. Reportez-vous également aux notes de version pour la dernière version d'Identity Manager et à la documentation pour Apache.

12.2 Installation de PostgreSQL et de Tomcat

Cette section vous guide dans la procédure d'installation de Tomcat et de PostgreSQL.

- Section 12.2.1, « Utilisation de l'assistant pour l'installation de PostgreSQL et de Tomcat », page 164
- Section 12.2.2, « Installation en mode silencieux de Tomcat et PostgreSQL pour Identity Manager », page 167

12.2.1 Utilisation de l'assistant pour l'installation de PostgreSQL et de Tomcat

La procédure suivante décrit comment installer Tomcat et PostgreSQL sur une plate-forme Windows à l'aide d'un processus guidé. Pour effectuer une installation sans surveillance en mode silencieux, reportez-vous à la Section 12.2.2, « Installation en mode silencieux de Tomcat et PostgreSQL pour Identity Manager », page 167.

Pour préparer l'installation, passez en revue les considérations et la configuration système requise reprises dans les sections suivantes :

- Section 12.1.4, « Conditions préalables à l'installation de Tomcat », page 163
- Section 12.1.3, « Conditions préalables à l'installation de PostgreSQL », page 163
- Les notes de version accompagnant le logiciel

REMARQUE : que vous installiez PostgreSQL ou utilisiez une version existante de PostgreSQL, vous devez spécifier des mots de passe pour la base de données. Toutefois, ce programme d'installation ne prend pas en charge les mots de passe incluant le caractère " ou $. Si vous souhaitez utiliser ces caractères spéciaux, modifiez le mot de passe une fois la procédure d'installation terminée.

Pour effectuer une installation guidée :

1. Connectez-vous en tant qu'administrateur à l'ordinateur sur lequel vous souhaitez installer les applications.
2. Assurez-vous que le chemin d'installation prévu n'inclut pas de répertoires avec l'un des noms suivants :
   - tomcat
   - postgres
   - activemq
   - jre

   REMARQUE : lors de l'installation de l'édition standard, vous devez installer ActiveMQ. Dans le cas contraire, la page Création de rapports ne se charge pas après vous être connecté à Identity Reporting. Vous pouvez également copier le fichier `activemq-all-5.15.2 jar` dans le répertoire `C:\NetIQ\idm\apps\tomcat\lib` après avoir terminé l'installation de PostgreSQL. Redémarrez ensuite Tomcat.
3. (Conditionnel) Si vous disposez du fichier image `.iso` pour le paquetage d'installation d'Identity Manager, accédez au répertoire `\products\CommonApplication\postgre_tomcat_install` contenant les fichiers d'installation.
4. (Conditionnel) Si vous avez téléchargé les fichiers d'installation à partir du site Web de téléchargement NetIQ, procédez comme suit :
   - **4a** Accédez au fichier `win.zip` de l'image téléchargée.
   - **4b** Extrayez le contenu du fichier dans un répertoire de l'ordinateur local.
5. À partir du répertoire qui contient les fichiers d'installation, exécutez le fichier `TomcatPostgreSQL.exe`.
6. Dans le programme d'installation, indiquez la langue que vous souhaitez utiliser pour l'installation, puis cliquez sur **OK**.
7. Consultez les informations d'introduction, puis cliquez sur **Suivant**.
8. Acceptez l'accord de licence, puis cliquez sur **Suivant**.
9. Indiquez si vous souhaitez ou non installer Tomcat, PostgreSQL ou les deux.
10. Pour terminer le processus guidé, indiquez des valeurs pour les paramètres suivants :
    - **Dossier parent Tomcat**

      S'applique uniquement lors de l'installation de Tomcat.

      Indique le répertoire dans lequel vous voulez installer les fichiers Tomcat.
    - **Détails de Tomcat**

      S'applique uniquement lors de l'installation de Tomcat.

      Représente les ports nécessaires pour Tomcat.

      Port d'arrêt Tomcat

      Indique le port que vous souhaitez utiliser pour arrêter correctement toutes les applications Web et Tomcat. La valeur par défaut est 8005.

Port http Tomcat

Indique le port que le serveur Tomcat doit utiliser pour la communication avec des ordinateurs client. La valeur par défaut est 8080. Pour utiliser SSL, la valeur par défaut est 8443.

Port de redirection Tomcat

(Conditionnel) Si vous n'utilisez pas de protocoles TLS/SSL, indique le port vers lequel le serveur d'applications redirige les requêtes qui nécessitent un transport SSL. La valeur par défaut est 8443.

Port ajp Tomcat

(Facultatif) Indique le port que le serveur d'applications doit utiliser pour communiquer avec un connecteur Web qui utilise le protocole AJP au lieu de `http`. La valeur par défaut est 8009.

Utilisez ce paramètre lorsque vous voulez que le serveur d'applications gère le contenu statique se trouvant dans l'application Web et/ou utilise le traitement SSL du serveur d'applications.

- **Dossier parent PostgreSQL**

  S'applique uniquement lors de l'installation de PostgreSQL.

  Représente le répertoire dans lequel vous voulez installer les fichiers PostgreSQL.

- **Détails de PostgreSQL**

  S'applique uniquement lors de l'installation de PostgreSQL.

  Représente les paramètres de la base de données PostgreSQL des applications d'identité.

REMARQUE : si vous avez déjà une version prise en charge de PostgreSQL en cours d'exécution sur le serveur, le programme d'installation vous demande d'insérer le mot de passe de l'utilisateur `postgres` par défaut. Le programme crée ensuite l'utilisateur `idmadmin` et lui assigne le même mot de passe que pour `postgres`.

Ce programme d'installation ne prend pas en charge les mots de passe incluant le caractère " ou $.

Nom de la base de données

Indique le nom de la base de données. La valeur par défaut est `idmuserappdb`.

Administrateur de la base de données

Indique le compte `idmadmin`, qui est un administrateur de base de données pouvant créer des tables de base de données, des vues, et d'autres artefacts.

Ce compte n'est pas le même que celui de l'utilisateur par défaut postgres.

Mot de passe de l'administrateur

Indique le mot de passe de l'administrateur de la base de données et de l'utilisateur par défaut `postgres`.

Ce programme d'installation ne prend pas en charge les mots de passe incluant le caractère " ou $.

Port PostgreSQL

Indique le port du serveur qui héberge la base de données Postgres La valeur par défaut est 5432.

11. Vérifiez le résumé avant installation.
12. Démarrez la procédure d'installation.
13. Lorsque la procédure d'installation est terminée, cliquez sur *Terminé*.

12.2.2 Installation en mode silencieux de Tomcat et PostgreSQL pour Identity Manager

Une installation silencieuse (non interactive) n'affiche aucune interface utilisateur et ne pose aucune question à l'utilisateur. À la place, InstallAnywhere utilise les informations contenues dans un fichier par défaut `silent.properties`. Vous pouvez exécuter l'installation silencieuse avec le fichier par défaut ou modifier le fichier pour personnaliser la procédure d'installation. Pour effectuer une installation guidée, reportez-vous à la Section 12.2.1, « Utilisation de l'assistant pour l'installation de PostgreSQL et de Tomcat », page 164.

Pour préparer l'installation, passez en revue les considérations et la configuration système requise reprises dans les sections suivantes :

- Section 12.1.4, « Conditions préalables à l'installation de Tomcat », page 163
- Section 12.1.3, « Conditions préalables à l'installation de PostgreSQL », page 163
- « Sauvegarde des mots de passe pour une installation en mode silencieux » page 167
- Les notes de version accompagnant le logiciel

Sauvegarde des mots de passe pour une installation en mode silencieux

Si vous ne souhaitez pas indiquer les mots de passe dans le fichier `postgresq_tomcat-silent.properties` utilisé pour l'installation, vous pouvez aussi les définir dans l'environnement à la place. Dans ce cas, le programme d'installation en mode silencieux lit les mots de passe à partir de l'environnement et non à partir du fichier `postgresq_tomcat-silent.properties`, ce qui permet d'accroître la sécurité.

Vous devez spécifier les mots de passe suivants pour l'installation :

- NETIQ_DB_PASSWORD
- NETIQ_DB_PASSWORD_CONFIRM

Utilisez la commande `set`. Par exemple :

```
set NETIQ_DB_PASSWORD_CONFIRM=myPassWord
```

Le programme d'installation ne prend pas en charge les mots de passe incluant le caractère `"` ou `$`. Si vous souhaitez utiliser ces caractères spéciaux, modifiez le mot de passe après l'installation de PostgreSQL.

Installation en mode silencieux de Tomcat et PostgreSQL

1. Connectez-vous à l'ordinateur sur lequel vous souhaitez installer les applications.
2. (Conditionnel) Si vous disposez du fichier image `.iso` pour le paquetage d'installation d'Identity Manager, accédez au répertoire `\products\CommonApplication\postgre_tomcat_install` contenant les fichiers d'installation.
3. (Conditionnel) Si vous avez téléchargé les fichiers d'installation à partir du site Web de téléchargement NetIQ, procédez comme suit :
   - **3a** Accédez au fichier `win.zip` de l'image téléchargée.
   - **3b** Extrayez le contenu du fichier dans un répertoire de l'ordinateur local.

4 Pour spécifier les paramètres d'installation, procédez comme suit :

4a Assurez-vous que le fichier `postgresq_tomcat-silent.properties` se trouve dans le même répertoire que le fichier d'exécution de l'installation.

4b Dans un éditeur de texte, ouvrez le fichier `postgresq_tomcat-silent.properties`.

4c Spécifiez les valeurs des différents paramètres. Pour obtenir une description de ces paramètres, reportez-vous à l'Étape 10 page 165.

4d Enregistrez et fermez le fichier.

5 Pour lancer la procédure d'installation, entrez la commande suivante :

```
install -i silent -f postgresq_tomcat-silent.properties
```

REMARQUE : si le fichier `postgresq_tomcat-silent.properties` ne se trouve pas dans le même répertoire que le script d'installation, vous devez indiquer le chemin complet du fichier. Le script décompresse les fichiers requis dans un répertoire temporaire et lance l'installation en mode silencieux.

---

13 Installation du composant Single Sign-on

Cette section explique comment installer One SSO Provider (OSP) afin de garantir un accès Single Sign-on aux applications d'identité et à Identity Reporting.

Les fichiers d'installation sont situés dans le répertoire `products\CommonApplication\osp_install` du paquetage d'installation d'Identity Manager. Par défaut, le programme d'installation installe les composants à l'emplacement `C:\NetIQ\idm\apps\osp`.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer.

13.1 Planification de l'installation du composant Single Sign-on pour Identity Manager

Cette section décrit les éléments à prendre en compte, ainsi que les conditions préalables et la configuration système requises pour l'installation de One SSO Provider (OSP).

- Section 13.1.1, « Liste de contrôle pour le composant Single Sign-on », page 169
- Section 13.1.2, « Conditions préalables à l'installation d'OSP », page 170
- Section 13.1.3, « Configuration système requise pour OSP », page 170
- Section 13.1.4, « Utilisation du service Apache Log4j pour consigner les événements de connexion », page 171

13.1.1 Liste de contrôle pour le composant Single Sign-on

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 à la Section 4.5, « Utilisation de l'accès Single Sign-on dans Identity Manager », page 34.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.
❑	3. Assurez-vous que Tomcat est installé. Pour plus d'informations, reportez-vous au Chapitre 12.2, « Installation de PostgreSQL et de Tomcat », page 164.
❑	4. (Conditionnel) Afin d'utiliser le service Apache Log4j pour enregistrer des événements dans Tomcat, vérifiez que vous disposez des fichiers appropriés. Pour plus d'informations, reportez-vous à la Section 13.1.4, « Utilisation du service Apache Log4j pour consigner les événements de connexion », page 171.

	Éléments de la liste de contrôle
❑	5. Installez OSP: ◆ Pour vous guider dans la procédure d'installation, reportez-vous à la Section 13.2.1, « Installation de One SSO Provider à l'aide de l'assistant », page 171. ◆ Pour effectuer une installation silencieuse, reportez-vous à la Section 13.2.2, « Installation de One SSO Provider en mode silencieux », page 174.
❑	6. Installez Self Service Password Reset (SSPR) pour gérer les mots de passe utilisateur des applications d'identité. Pour plus d'informations, reportez-vous à la Section 14.2, « Installation du composant de gestion des mots de passe pour Identity Manager », page 179.
❑	7. Installez et configurez les applications d'identité pour utiliser l'accès Single Sign-on. Pour plus d'informations, reportez-vous à la Section 15.5, « Installation des applications d'identité », page 208.

13.1.2 Conditions préalables à l'installation d'OSP

Les composants suivants d'Identity Manager nécessitent OSP pour l'authentification des utilisateurs :

- Applications d'identité
- Identity Reporting

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

- Pour exécuter OSP, vous pouvez utiliser votre propre programme d'installation Tomcat au lieu de celui fourni dans le kit d'installation d'Identity Manager. Toutefois, afin d'utiliser le service Apache Log4j avec votre version de Tomcat, assurez-vous d'avoir installé les fichiers appropriés. Pour plus d'informations, reportez-vous à la Section 13.1.4, « Utilisation du service Apache Log4j pour consigner les événements de connexion », page 171.
- OSP nécessite des certificats approuvés pour garantir que les applications d'identité et la création de rapports puissent communiquer avec le serveur d'authentification. La procédure d'installation crée automatiquement un certificat pour TLS/SSL dans le fichier `osp.jks`. Grâce au processus, vous pouvez également créer le certificat de racine approuvée pour une assertion SAML auprès d'eDirectory.

  REMARQUE : ces certificats expirent deux ans après leur date de création. Vous devez créer de nouveaux certificats lorsque les originaux expirent. Pour plus d'informations, reportez-vous à la « Serveur d'authentification » page 248 et à la Partie VIII, « Configuration de l'accès Single Sign-on dans Identity Manager », page 317.

13.1.3 Configuration système requise pour OSP

OSP requiert un serveur d'applications Apache Tomcat. La version de Tomcat doit être la même que celle requise pour les applications d'identité.

Toutes les autres exigences de serveur sont les mêmes que celles requises pour les applications d'identité. Pour plus d'informations, reportez-vous à la Section 15.1.3, « Conditions requises et considérations relatives à l'installation des applications d'identité », page 192 et aux notes de version les plus récentes pour cette version.

13.1.4 Utilisation du service Apache Log4j pour consigner les événements de connexion

Pour enregistrer des événements qui se produisent dans Tomcat, vous pouvez utiliser le service Apache Log4j ou java.util.logging. Le programme d'installation de Tomcat dans le kit d'installation d'Identity Manager contient les fichiers dont vous avez besoin pour Log4j. Toutefois, si vous installez votre propre version de Tomcat, vous avez besoin des fichiers suivants pour utiliser le service de consignation Apache :

- `log4j-1.2.16.jar`
- `tomcat-juli-adapters.jar`
- `tomcat-juli.jar`

Pour ajouter ces fichiers à votre installation Tomcat, procédez comme suit :

1. Téléchargez les fichiers « JULI » pour Tomcat v8.5.x à partir du site Web Apache :
   - `tomcat-juli.jar`
   - `tomcat-juli-adapters.jar`
2. Téléchargez le fichier `log4j-1.2.16.jar` à partir du site Web Apache.
3. Placez les fichiers suivants dans le répertoire `$TOMCAT_HOME\lib` :
   - `log4j-1.2.16.jar`
   - `tomcat-juli-adapters.jar`
4. Placez le fichier `tomcat-juli.jar` dans le répertoire `$TOMCAT_HOME/bin`.
5. Indiquez une valeur pour `-Dlog4j.configuration` dans `CATALINA_OPTS` ou créez un fichier `log4j.properties` dans le répertoire `$TOMCAT_HOME\lib`.

13.2 Installation du composant Single Sign-on pour Identity Manager

13.2.1 Installation de One SSO Provider à l'aide de l'assistant

La procédure suivante décrit comment installer OSP sur une plate-forme Windows à l'aide d'un assistant d'installation. Pour effectuer une installation silencieuse sans surveillance, reportez-vous à la Section 13.2.2, « Installation de One SSO Provider en mode silencieux », page 174. Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise répertoriées à la Section 13.1.1, « Liste de contrôle pour le composant Single Sign-on », page 169.

1. Connectez-vous en tant qu'administrateur au serveur sur lequel vous souhaitez installer OSP.
2. Arrêtez le serveur Tomcat.
3. (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'OSP, situés par défaut dans le répertoire `products\CommonApplication\osp_install`.

4 (Conditionnel) Si vous avez téléchargé les fichiers d'installation d'OSP, procédez comme suit :

4a Accédez au fichier `win.zip` de l'image téléchargée.

4b Extrayez le contenu du fichier dans un répertoire de l'ordinateur local.

5 À partir du répertoire qui contient les fichiers d'installation, exécutez le fichier `osp-install-win.exe`.

6 Lisez et acceptez l'accord de licence, puis cliquez sur **Suivant**.

7 Indiquez un chemin d'accès pour les fichiers installés.

8 Terminez la procédure guidée en utilisant les paramètres suivants :

- **Détails de Tomcat**

  Représente le répertoire privé du serveur Tomcat. Par exemple : `C:\NetIQ\idm\apps\tomcat\`. La procédure d'installation ajoute à ce dossier certains fichiers pour OSP.

- **Répertoire privé Java Tomcat**

  Représente le répertoire privé pour Java sur le serveur Tomcat. Par exemple : `C:\netiq\idm\jre`. La procédure d'installation ajoute au répertoire certains fichiers pour OSP.

- **Adresse de l'application**

  Représente les paramètres de l'URL permettant aux utilisateurs de se connecter à OSP sur le serveur Tomcat. Par exemple : `https:monserveur.masociété.com:8543`.

  Protocole

  Indique si vous souhaitez utiliser *http* ou *https*. Afin d'utiliser SSL (Secure Sockets Layer) pour les communications, indiquez `https`.

  Nom d'hôte

  Indique le nom DNS ou l'adresse IP du serveur sur lequel vous installez OSP. N'utilisez pas `localhost`.

  Port

  Indique le port que le serveur doit utiliser pour la communication avec des ordinateurs clients.

- **Personnalisation de l'écran de connexion**

  Indique le nom personnalisé que vous voulez afficher sur l'écran de connexion utilisateur. La valeur par défaut est **Identity Access** (Accès à Identity).

  REMARQUE : seule la valeur `Jeu de caractères standard Latin1` est prise en charge.

- **Détails de l'authentification**

  Représente la configuration requise pour se connecter au serveur d'authentification contenant la liste des utilisateurs qui peuvent se connecter à l'application. Pour plus d'informations sur le serveur d'authentification, reportez-vous à la Section 4.5.1, « Présentation de l'authentification avec One SSO Provider », page 35.

  Hôte LDAP

  Indique le nom DNS ou l'adresse IP du serveur d'authentification LDAP. N'utilisez pas `localhost`.

  Port LDAP

  Indique le port que le serveur d'authentification LDAP doit utiliser pour la communication avec Identity Manager. Par exemple, indiquez `389` pour un port non sécurisé ou `636` pour les connexions SSL.

Utiliser SSL

Indique si vous souhaitez utiliser le protocole Secure Sockets Layer pour les connexions entre le coffre-fort d'identité et le serveur d'authentification.

Fichier (cacerts) du Truststore JRE

Ne s'applique que si vous souhaitez utiliser SSL pour les connexions LDAP.

Indique le chemin d'accès au certificat. Par exemple : `C:\NetIQ\idm\apps\jre\lib\security\cacerts`.

Mot de passe du Truststore JRE

Ne s'applique que si vous souhaitez utiliser SSL pour les connexions LDAP.

Indique le mot de passe du fichier `cacerts`.

DN administrateur

S'applique uniquement lors de l'installation d'un nouveau serveur d'authentification.

Indique le DN pour un compte administrateur du serveur d'authentification LDAP. Par exemple : `cn=admin,ou=sa,o=system`.

Mot de passe de l'administrateur

S'applique uniquement lors de l'installation d'un nouveau serveur d'authentification.

Indique le mot de passe pour le compte administrateur du serveur d'authentification LDAP.

Conteneur des utilisateurs

S'applique uniquement lors de l'installation d'un nouveau serveur d'authentification.

Indique le conteneur du serveur d'authentification LDAP dans lequel vous enregistrez les comptes utilisateur qui peuvent se connecter à Access Review. Par exemple : `o=data`.

Conteneur des administrateurs

S'applique uniquement lors de l'installation d'un nouveau serveur d'authentification.

Indique le conteneur du serveur d'authentification LDAP dans lequel vous enregistrez les comptes administrateur. Par exemple : `ou=sa,o=system`.

Coffre-fort d'identité

Spécifie votre coffre-fort d'identité.

Mot de passe Keystore

S'applique uniquement lors de l'installation d'un nouveau serveur d'authentification.

Indique le mot de passe que vous souhaitez créer pour le nouveau fichier Keystore du serveur d'authentification LDAP.

Le mot de passe doit contenir au moins six caractères.

- **Détails de l'audit (OSP)**

Représente les paramètres d'audit des événements OSP qui se produisent sur le serveur d'authentification.

(Conditionnel) *Activer l'audit pour OSP*

Indique si vous souhaitez envoyer les événements OSP vers un serveur d'audit.

Si vous sélectionnez ce paramètre, indiquez également l'emplacement de mise en cache des journaux d'audit.

Dossier de mise en cache des journaux d'audit

Ne s'applique que lorsque vous activez l'audit pour OSP.

Indique l'emplacement du répertoire de mise en cache que vous souhaitez utiliser pour l'audit. Par exemple, `C:\NetIQ\idm\naudit\jcache`.

Préciser un certificat existant / Générer un certificat

Indique si vous souhaitez utiliser un certificat existant pour le serveur NAudit ou en créer un nouveau.

Entrez une clé publique

Ne s'applique que si vous souhaitez utiliser un certificat existant.

Répertorie le certificat de clé publique personnalisé que le service NAudit doit utiliser pour authentifier les messages d'audit.

Entrez une clé RSA

Ne s'applique que si vous souhaitez utiliser un certificat existant.

Indique le chemin d'accès au fichier de clé privée personnalisé que le service NAudit doit utiliser pour authentifier les messages d'audit.

9 Pour installer SSPR, passez à la Partie 14, « Installation du composant de gestion des mots de passe », page 177.

Pour plus d'informations sur la configuration de la gestion des mots de passe oubliés, reportez-vous à la Section 15.7.8, « Configuration de la gestion des mots de passe oubliés », page 229.

13.2.2 Installation de One SSO Provider en mode silencieux

Une installation silencieuse (non interactive) n'affiche aucune interface utilisateur et ne pose aucune question à l'utilisateur.

1 Connectez-vous en tant qu'administrateur à l'ordinateur sur lequel vous souhaitez installer les composants.

2 Arrêtez Tomcat.

3 (Conditionnel) Si vous disposez du fichier image `.iso` du paquetage d'installation d'Identity Manager, accédez au répertoire contenant les fichiers d'installation d'OSP, situés par défaut dans le répertoire `osp_`.

4 (Conditionnel) Si vous avez téléchargé les fichiers d'installation à partir du site Web de téléchargement NetIQ, procédez comme suit :

4a Accédez au fichier `.zip` de l'image téléchargée.

4b Lancez l'extraction du contenu du fichier dans un dossier sur l'ordinateur local.

5 Copiez le fichier `osp.configure.properties` à l'emplacement auquel vous avez un accès en écriture et éditez ce fichier.

Pour plus d'informations sur les paramètres d'installation, reportez-vous à l'Étape 7 et à l'Étape 8 page 172.

6 Pour exécuter l'installation silencieuse, émettez la commande suivante :

```
osp-install-win.exe -i silent -f chemin_fichier_silent.properties
```

Dans cette commande, indiquez le chemin absolu du fichier. Par exemple :

```
osp-install-win.exe -i silent -f c:\NetIQ\idm\apps\osp\osp.silent.properties
```

7 Installez SSPR. Pour plus d'informations, reportez-vous à la Partie 14, « Installation du composant de gestion des mots de passe », page 177.

13.2.3 Configuration de l'accès Single Sign-on

Vous devez effectuer certaines opérations pour configurer l'accès Single Sign-on immédiatement après l'installation d'OSP. Toutefois, le processus de configuration final implique d'installer au préalable les applications d'identité. Pour plus d'informations, reportez-vous à la Partie VIII, « Configuration de l'accès Single Sign-on dans Identity Manager », page 317.

REMARQUE : lors de la configuration du fournisseur d'authentification unique One en mode silencieux, veillez à avoir spécifié correctement les dossiers d'installation, Java, Tomcat et Keystore SSL dans le fichier `osp.silent.properties`. Exemples :

Dossier d'installation : `USER_INSTALL_DIR=C:\NetIQ\idm\apps\osp`

Dossier Tomcat : `NETIQ_TOMCAT_HOME=C:\NetIQ\idm\apps\tomcat`

Windows : `NETIQ_TOMCAT_HOME=C:\NetIQ\idm\apps\tomcat`

Dossier Java : `NETIQ_JAVA_HOME=C:\NetIQ\idm\apps\jre`

Dossier Keystore SSL : `USER_INSTALL_DIR=C:\NetIQ\idm\apps\jre\lib\security\cacerts`

---

14 Installation du composant de gestion des mots de passe

Cette section explique comment installer Self Service Password Reset (SSPR), un composant qui permet de configurer Identity Manager de manière à ce que les utilisateurs puissent réinitialiser leur mot de passe.

SSPR s'intègre aux applications d'identité, à Identity Reporting et à OSP afin que les utilisateurs devant modifier leur mot de passe soient dirigés vers les pages Web appropriées sans effectuer d'autres opérations. Une fois que les utilisateurs ont réalisé leurs activités en self-service, SSPR les redirige vers l'application qu'ils essayaient d'atteindre à l'origine.

REMARQUE : Identity Manager 4.6 et versions ultérieures utilisent SSPR comme principal outil de gestion des mots de passe.

Identity Manager ne nécessite pas obligatoirement SSPR. Vous pouvez utiliser une autre méthode de réinitialisation des mots de passe utilisateur. Toutefois, vous devrez peut-être modifier certains paramètres de configuration pour Identity Manager. Pour plus d'informations, reportez-vous à la Section 15.7.8, « Configuration de la gestion des mots de passe oubliés », page 229.

Les fichiers d'installation sont situés dans le répertoire `\products\CommonApplication\sspr_install`. Par défaut, le programme d'installation installe les composants SSPR à l'emplacement `C:\NetIQ\idm\apps\sspr`.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer.

14.1 Planification de l'installation du composant de gestion des mots de passe pour Identity Manager

Cette section décrit les éléments à prendre en compte, ainsi que les conditions préalables et la configuration système requises pour l'installation de Self Service Password Reset (SSPR).

14.1.1 Liste de contrôle pour l'installation des composants de gestion des mots de passe

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 à la Section 4.4, « Utilisation de la gestion des mots de passe en self-service dans Identity Manager », page 32.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.
❑	3. Assurez-vous que Tomcat est installé. Pour plus d'informations, reportez-vous au Chapitre 12.2, « Installation de PostgreSQL et de Tomcat », page 164.
❑	4. (Conditionnel) Afin d'utiliser le service Apache Log4j pour enregistrer des événements dans Tomcat, vérifiez que vous disposez des fichiers appropriés. Pour plus d'informations, reportez-vous à la Section 13.1.4, « Utilisation du service Apache Log4j pour consigner les événements de connexion », page 171.
❑	5. Installez SSPR : ◆ Pour vous guider dans la procédure d'installation, reportez-vous à la Section 14.2.1, « Installation de Self Service Password Request à l'aide de l'assistant », page 180. ◆ Pour effectuer une installation silencieuse, reportez-vous à la Section 14.2.2, « Installation de Self Service Password Reset en mode silencieux », page 183.
❑	6. Installez et configurez les applications d'identité pour utiliser l'accès Single Sign-on et la gestion des mots de passe. Pour plus d'informations, reportez-vous au Chapitre 15.5, « Installation des applications d'identité », page 208.

14.1.2 Conditions préalables à l'installation du module de réinitialisation de mot de passe en self-service

L'installation du module NetIQ de réinitialisation de mot de passe en self-service (SSPR, Self Service Password Reset) doit respecter la configuration serveur requise pour les applications d'identité, dont les considérations suivantes :

- SSPR nécessite un protocole de communication TSL/SSL.
- SSPR requière une version prise en charge du serveur d'applications Tomcat. Pour plus d'informations, reportez-vous à la Section 12.1.4, « Conditions préalables à l'installation de Tomcat », page 163 et aux notes de version les plus récentes pour cette version.
- NetIQ recommande de consulter les conditions préalables et la configuration requise stipulées dans le manuel *NetIQ Self Service Password Reset Administration Guide* (Guide d'administration du module NetIQ de réinitialisation de mot de passe en self-service).

14.1.3 Configuration système requise pour le module SSPR

SSPR requiert un serveur d'applications Apache Tomcat. La version de Tomcat doit être la même que celle requise pour les applications d'identité.

Toutes les autres exigences de serveur sont les mêmes que celles requises pour les applications d'identité. Pour plus d'informations, reportez-vous à la Section 15.1.3, « Conditions requises et considérations relatives à l'installation des applications d'identité », page 192 et aux notes de version les plus récentes pour cette version.

14.1.4 Utilisation du service Apache Log4j Apache pour consigner les événements de mot de passe

Pour enregistrer des événements qui se produisent dans Tomcat, vous pouvez utiliser le service Apache Log4j ou java.util.logging. Le programme d'installation de Tomcat dans le kit d'installation d'Identity Manager contient les fichiers dont vous avez besoin pour Log4j. Toutefois, si vous installez votre propre version de Tomcat, vous avez besoin des fichiers suivants pour utiliser le service de consignation Apache :

- `log4j-1.2.16.jar`
- `tomcat-juli-adapters.jar`
- `tomcat-juli.jar`

Pour ajouter ces fichiers à votre installation Tomcat, procédez comme suit :

1. Téléchargez les fichiers « JULI » pour Tomcat v8.5.x à partir du site Web Apache :
   - `tomcat-juli.jar`
   - `tomcat-juli-adapters.jar`
2. Téléchargez le fichier `log4j-1.2.16.jar` à partir du site Web Apache.
3. Placez les fichiers suivants dans le répertoire `$TOMCAT_HOME\lib` :
   - `log4j-1.2.16.jar`
   - `tomcat-juli-adapters.jar`
4. Placez le fichier `tomcat-juli.jar` dans le répertoire `$TOMCAT_HOME/bin`.
5. Indiquez une valeur pour `-Dlog4j.configuration` dans `CATALINA_OPTS` ou créez un fichier `log4j.properties` dans le répertoire `$TOMCAT_HOME\lib`.

14.2 Installation du composant de gestion des mots de passe pour Identity Manager

Cette section décrit la procédure d'installation de SSPR. Vous pouvez installer ce programme sur le même serveur qu'OSP ou sur un autre serveur.

REMARQUE : si vous utilisez la méthode de mot de passe oublié existante, il n'est pas nécessaire d'installer SSPR. Pour plus d'informations, reportez-vous à la Section 4.4.2, « Présentation du fournisseur hérité pour la gestion des mots de passe », page 33.

14.2.1 Installation de Self Service Password Request à l'aide de l'assistant

La procédure suivante décrit comment installer SSPR sur une plate-forme Windows à l'aide d'un assistant d'installation. Pour effectuer une installation silencieuse sans surveillance, reportez-vous à la Section 14.2.2, « Installation de Self Service Password Reset en mode silencieux », page 183. Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise répertoriées à la Section 14.1.1, « Liste de contrôle pour l'installation des composants de gestion des mots de passe », page 178.

1. Connectez-vous en tant qu'administrateur au serveur sur lequel vous souhaitez installer SSPR.
2. Arrêtez le serveur Tomcat.
3. (Conditionnel) Si vous avez le fichier image `.iso` pour le paquetage d'installation d'Identity Manager, accédez au répertoire contenant les fichiers d'installation de SSPR, situés par défaut dans le répertoire `products\CommonApplication\sspr_install`.
4. (Conditionnel) Si vous avez téléchargé les fichiers d'installation de SSPR, procédez comme suit :
   - **4a** Accédez au fichier `win.zip` de l'image téléchargée.
   - **4b** Extrayez le contenu du fichier dans un répertoire de l'ordinateur local.
5. À partir du répertoire qui contient les fichiers d'installation, exécutez le fichier `sspr-install-win.exe`.
6. Lisez et acceptez l'accord de licence, puis cliquez sur **Suivant**.
7. Indiquez un chemin d'accès pour les fichiers installés.
8. Terminez la procédure guidée en utilisant les paramètres suivants :
   - **Détails de Tomcat**

     Représente le répertoire privé du serveur Tomcat. Par exemple : `C:\NetIQ\idm\apps\tomcat`. La procédure d'installation ajoute à ce dossier certains fichiers pour SSPR.
   - **Connexion Tomcat**

     Représente les paramètres de l'URL permettant aux utilisateurs de se connecter à SSPR sur le serveur Tomcat. Par exemple : `https:monserveur.masociété.com:8080`.

     REMARQUE : vous devez également sélectionner **Se connecter à un serveur d'authentification externe** et indiquer des valeurs pour le serveur externe si les considérations suivantes s'appliquent :
     - Vous installez SSPR.
     - OSP s'exécute sur une autre instance du serveur d'applications pris en charge que SSPR.

     Protocole

     Indique si vous souhaitez utiliser *http* ou *https*. Afin d'utiliser SSL (Secure Sockets Layer) pour les communications, indiquez `https`.

Nom d'hôte

Indique le nom DNS ou l'adresse IP du serveur sur lequel vous installez SSPR. N'utilisez pas `localhost`.

Port

Indique le port que le serveur doit utiliser pour la communication avec des ordinateurs clients.

Se connecter à un serveur d'authentification externe

Indique si une autre instance de Tomcat héberge le serveur d'authentification (OSP). Le serveur d'authentification contient la liste des utilisateurs qui peuvent se connecter à SSPR.

Si vous sélectionnez ce paramètre, vous devez aussi indiquer des valeurs pour les champs **Protocole**, **Nom d'hôte** et **Port** du serveur d'authentification.

- **Répertoire privé Java Tomcat**

  Représente le répertoire privé pour Java sur le serveur Tomcat. Par exemple : `C:\netiq\idm\jre`. La procédure d'installation ajoute au répertoire certains fichiers pour OSP.

- **Détails de l'authentification**

  Représente la configuration requise pour se connecter au serveur d'authentification contenant la liste des utilisateurs qui peuvent se connecter à l'application. Pour plus d'informations sur le serveur d'authentification, reportez-vous à la Section 4.5.1, « Présentation de l'authentification avec One SSO Provider », page 35.

  Hôte LDAP

  Indique le nom DNS ou l'adresse IP du serveur d'authentification LDAP. N'utilisez pas `localhost`.

  Port LDAP

  Indique le port que le serveur d'authentification LDAP doit utiliser pour la communication avec Identity Manager. Par exemple, indiquez `389` pour un port non sécurisé ou `636` pour les connexions SSL.

  Utiliser SSL

  Indique si vous souhaitez utiliser le protocole Secure Sockets Layer pour les connexions entre le coffre-fort d'identité et le serveur d'authentification.

  Fichier (cacerts) du Truststore JRE

  Ne s'applique que si vous souhaitez utiliser SSL pour les connexions LDAP.

  Indique le chemin d'accès au certificat. Par exemple : `C:\NetIQ\idm\apps\jre\lib\security\cacerts`.

  Mot de passe du Truststore JRE

  Ne s'applique que si vous souhaitez utiliser SSL pour les connexions LDAP.

  Indique le mot de passe du fichier `cacerts`.

  DN administrateur

  S'applique uniquement lors de l'installation d'un nouveau serveur d'authentification.

  Indique le DN pour un compte administrateur du serveur d'authentification LDAP. Par exemple : `cn=admin,ou=sa,o=system`.

Mot de passe de l'administrateur

S'applique uniquement lors de l'installation d'un nouveau serveur d'authentification.

Indique le mot de passe pour le compte administrateur du serveur d'authentification LDAP.

Conteneur des utilisateurs

S'applique uniquement lors de l'installation d'un nouveau serveur d'authentification.

Indique le conteneur du serveur d'authentification LDAP dans lequel vous enregistrez les comptes utilisateur qui peuvent se connecter à Access Review. Par exemple : `o=data`.

Conteneur des administrateurs

S'applique uniquement lors de l'installation d'un nouveau serveur d'authentification.

Indique le conteneur du serveur d'authentification LDAP dans lequel vous enregistrez les comptes administrateur pour Access Review. Par exemple : `ou=sa,o=system`.

Mot de passe Keystore

S'applique uniquement lors de l'installation d'un nouveau serveur d'authentification.

Indique le mot de passe que vous souhaitez créer pour le nouveau fichier Keystore du serveur d'authentification LDAP.

Le mot de passe doit contenir au moins six caractères.

- **Détails relatifs à l'application SSPR**

  Représente les paramètres requis pour configurer SSPR.

  Mot de passe de configuration

  Indique le mot de passe que vous souhaitez créer pour un administrateur afin qu'il l'utilise pour configurer SSPR.

  Par défaut, SSPR ne dispose pas d'un mot de passe de configuration. Sans le mot de passe, tout utilisateur qui peut se connecter à SSPR peut également modifier les paramètres de configuration.

  SSPR redirect URL

  Indique l'URL absolue vers laquelle le client est redirigé lorsque des opérations telles que des changements de mot de passe ou des questions de vérification d'identité sont terminées dans SSPR. Par exemple, redirigez le client vers le tableau de bord.

  Utilisez le format suivant : `protocol//serveur:port/chemin`. Par exemple, `http://idm_userapp_server_ip:port_no/idmdash/#/landing`.

- **Détails du serveur d'authentification**

  Représente le mot de passe que le service SSPR doit utiliser lors de la connexion au client OSP sur le serveur. Également appelé le secret client.

  Pour modifier ce mot de passe après l'installation, utilisez l'utilitaire de configuration RBPM.

- **Détails de l'audit (SSPR)**

  Représente les paramètres d'audit des événements SSPR qui se produisent sur le serveur d'authentification.

  (Conditionnel) *Activer l'audit pour SSPR*

  Indique si vous souhaitez envoyer les événements SSPR vers un serveur d'audit.

  Si vous sélectionnez ce paramètre, indiquez également les paramètres pour le serveur Syslog.

Nom d'hôte Syslog

Ne s'applique que lorsque vous activez l'audit pour SSPR.

Indique le DNS ou l'adresse IP du serveur qui héberge le serveur Syslog. N'utilisez pas `localhost`.

Port Syslog

Ne s'applique que lorsque vous activez l'audit pour SSPR.

Indique le port du serveur qui héberge le serveur Syslog.

9 Pour configurer les applications d'identité et le module Identity Reporting afin qu'ils utilisent SSPR, passez au Chapitre 15, « Installation des applications d'identité », page 189.

10 Dans l'utilitaire de mise à jour de configuration, mettez à jour les paramètres des clients SSO. Pour plus d'informations, reportez-vous à la documentation, « Self Service Password Reset » page 255.

Pour plus d'informations sur la configuration de la gestion des mots de passe oubliés, reportez-vous à la Section 15.7.8, « Configuration de la gestion des mots de passe oubliés », page 229.

14.2.2 Installation de Self Service Password Reset en mode silencieux

Une installation silencieuse (non interactive) n'affiche aucune interface utilisateur et ne pose aucune question à l'utilisateur.

1 Connectez-vous en tant qu'administrateur à l'ordinateur sur lequel vous souhaitez installer les composants.

2 Arrêtez Tomcat.

3 (Conditionnel) Si vous disposez du fichier image `.iso` du paquetage d'installation d'Identity Manager, accédez au répertoire contenant les fichiers d'installation de SSPR, situés par défaut dans le répertoire `sspr`.

4 (Conditionnel) Si vous avez téléchargé les fichiers d'installation à partir du site Web de téléchargement NetIQ, procédez comme suit :

4a Accédez au fichier `.zip` de l'image téléchargée.

4b Lancez l'extraction du contenu du fichier dans un dossier sur l'ordinateur local.

5 Modifiez le fichier d'installation de SSPR `sspr-silent.properties`, situé par défaut dans le même répertoire que les scripts d'installation.

Pour plus d'informations sur les paramètres d'installation, reportez-vous à l'Étape 7 page 180 et à l'Étape 8 page 180.

6 Pour exécuter l'installation silencieuse, émettez la commande suivante :

```
sspr-install-win.exe -i silent -f path_to_silent.properties_file
```

7 Dans l'utilitaire de mise à jour de configuration, mettez à jour les paramètres des clients SSO. Pour plus d'informations, reportez-vous à la documentation, « Self Service Password Reset » page 255.

14.2.3 Tâches de post-installation

Installation garantie sans erreur

Après avoir installé SSPR, vous pouvez modifier les paramètres de configuration, notamment modifier une autorisation d'un administrateur du DN de groupe LDAP pour le profil par défaut ou modifier l'URL de transfert. En outre, NetIQ vous recommande de vérifier les URL créées pendant la procédure d'installation et de les modifier au besoin.

1. Pour ouvrir la page de connexion SSPR, entrez l'URL suivante dans votre navigateur :

   `protocol://server:port/web-context`

   Exemples :

   `http://192.168.0.1:8080/sspr/`

2. Dans l'angle supérieur droit de la page de connexion SSPR, sélectionnez **Éditeur de configuration** dans la liste.
3. Spécifiez le mot de passe de configuration et cliquez sur **Se connecter**.
4. Dans la vue arborescence, sélectionnez **Paramètres par défaut** et vérifiez que l'option **Intégration NetIQ IDM/OAuth** est sélectionnée dans la liste **Paramètres par défaut du fournisseur LDAP**.
5. À partir de la vue arborescence, cliquez sur **LDAP > Répertoires LDAP > valeur par défaut > Connexion > Certificats LDAP**, puis cliquez sur **Importer à partir du serveur** pour importer les certificats.

   (Conditionnel) Cliquez sur **Tester le profil LDAP** sur la même page pour vous assurer que tous les serveurs LDAP configurés sont accessibles.
6. À partir de la vue arborescence, cliquez sur **Modules > Authentifié > Administration** et assurez-vous que les autorisations d'administrateur sont assignées au DN de groupe LDAP du profil par défaut.

   Si vous effectuez une nouvelle installation de SSPR, la liste sera vide. Vous devez créer un groupe dans iManager et ajouter l'utilisateur `admin` au groupe.
7. À partir de la vue arborescence, cliquez sur **Paramètres > Application > Application**, puis vérifiez que l'**URL de réacheminement** est définie sur `http://<Serveur:Port>/idmdash/#/landing`.

   Par exemple, `http:/192.168.0.1:8080/idmdash/#/landing`.
8. À partir de la vue arborescence, cliquez sur **Paramètres > Interface utilisateur > Apparence** et modifiez le **thème de l'interface** sur **Micro Focus (mdefault)** si ce n'est pas déjà fait.
9. À partir de la vue arborescence, accédez à **Paramètres > Client Single Sign On (SSO) > OAuth** et vérifiez que les valeurs sont correctement spécifiées pour les paramètres suivants :

   OAuth Login URL (URL de connexion à OAuth)

   Spécifie l'URL pour la connexion au serveur OAuth. Lorsque l'utilisateur se connecte, cette URL permet de rediriger les utilisateurs pour une authentification avec OSP.

   Par exemple : `http://192.168.0.1:8080/osp/a/idm/auth/oauth2/grant`

   OAuth Code Resolve Service URL (URL du service de résolution de codes OAuth)

   Spécifie l'URL du service de résolution de codes OAuth. SSPR utilise cette URL de service Web pour résoudre l'artefact renvoyé par le serveur d'identités OAuth.

   Par exemple : `http://192.168.0.1:8080/osp/a/idm/auth/oauth2/authcoderesolve`

OAuth Profile Service URL (URL du service de profil OAuth)

Spécifie l'URL du service Web fourni par Identity Manager pour renvoyer les données d'attribut de l'utilisateur.

Par exemple : `http://192.168.0.1:8080/osp/a/idm/auth/oauth2/getattributes`

OAUTH Web Service Server Certificate (Certificat de serveur du service Web OAUTH)

(Conditionnel) Si HTTPS est activé, importez le certificat du serveur du service Web OAuth.

OAuth Client ID (ID client OAuth)

Spécifie l'ID du client OAuth. Par exemple, `sspr`.

OAuth Shared Secret (Secret partagé OAuth)

Spécifie un mot de passe pour le secret partagé OAuth. Ce mot de passe est partagé par les applications OSP et SSPR.

OAuth User Name/DN Login Attribute (Nom d'utilisateur OAuth/Attribut de connexion DN)

Spécifie l'attribut de l'utilisateur utilisé par SSPR pour demander au serveur OAuth d'authentifier l'utilisateur localement. Par exemple : `nom`.

10 Cliquez sur dans le coin supérieur droit de la page pour enregistrer votre configuration.

11 Dans l'angle supérieur droit de la page de connexion SSPR, sélectionnez **Gestionnaire de configuration** dans la liste.

12 Cliquez sur **Restreindre la configuration**.

Assignation de la stratégie de mot de passe universel à un conteneur d'utilisateurs

Pour assigner la stratégie de mot de passe universel à un conteneurs d'utilisateurs :

1 Connectez-vous à iManager.

2 Sélectionnez **Rôles et tâches > Stratégies de mot de passe**, puis sélectionnez la stratégie de mot de passe.

3 Pour sélectionner un utilisateur disposant de droits d'administrateur, procédez comme suit :

3a Cliquez sur **Mot de passe universel > les Options de configuration > Récupération du mot de passe universel**.

3b Sélectionnez **Autoriser l'administrateur à récupérer les mots de passe** ou **Autoriser ce qui suit pour récupérer les mots de passe**, puis cliquez sur **OK**.

Par exemple, `cn=admin,ou=sa,o=system`

4 Cliquez sur **Assignations de stratégies** et assignez `Conteneur` au conteneur dans lequel se trouve l'utilisateur.

Par exemple, `o=data` ou administrateur.

Octroi de droits aux attributs pwmResponseSet

Les utilisateurs disposant de droits authentifiés effectuent des opérations en fonction des autorisations associées à la connexion de l'utilisateur. Les utilisateurs authentifiés ont besoin des droits suivants pour leur propre entrée utilisateur :

- Droits Parcourir pour [droits d'entrée]
- Droits Lire, Comparer et Écrire pour pwmResponseSet

Pour accorder des droits à l'attribut pwmResponseSet, procédez comme suit :

1. Connectez-vous à iManager.
2. Cliquez sur  .
3. Cliquez sur **Serveur iManager** > **Configurer iManager**.
4. Cliquez sur **Divers** > **Activer [ceci]**.
5. Cliquez sur  .
6. À partir de la vue **Arborescence**, sélectionnez le conteneur de niveau supérieur de tous les utilisateurs dans l'annuaire.
7. Cochez la case **niveau actuel**, puis cliquez sur **Opérations** > **Modifier les ayants droit**.
8. Cliquez sur **[Ceci]** dans la liste, puis cliquez sur **Ajouter un ayant droit**.
9. Cliquez sur **Appliquer**.
10. Cliquez sur **Droits assignés** pour **[Cet]** ayant droit.
11. Cliquez sur **Ajouter une propriété**, puis cochez la case **Afficher toutes les propriétés dans le schéma**.
12. Sélectionnez **pwdResponseSet** dans la liste.

    Assurez-vous que les options Écrire, Comparer, Lire et Hérité sont sélectionnées.
13. Cliquez sur **Terminé**.

14.2.4 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.

Configuration de SSPR pour la prise en charge de la mise en grappe

Pour configurer le module SSPR déjà installé sur un ordinateur distinct, procédez comme suit :

1. Passez en revue les conditions préalables et la configuration système requise décrites dans la Section 14.1.1, « Liste de contrôle pour l'installation des composants de gestion des mots de passe », page 178.
2. Suivez les instructions de la Section 14.2.1, « Installation de Self Service Password Request à l'aide de l'assistant », page 180 et veillez à effectuer les opérations suivantes au cours de la procédure d'installation :
    a. Sur la page de connexion au serveur d'applications, sélectionnez **Se connecter à un serveur d'authentification externe** et spécifiez le nom DNS du serveur sur lequel est installé l'équilibreur de charge.
    b. Sur la page des détails d'authentification, spécifiez l'adresse IP et le port du serveur du moteur Identity Manager. Le mot de passe pour les certificats d'autorité de certification est « changeit ».
    c. À l'issue de l'installation de SSPR, mettez à jour les paramètres SSL. Pour plus d'informations, reportez-vous à la Section 29.8, « Mise à jour des paramètres SSL pour SSPR », page 353.

3 Pour mettre à jour les informations SSPR sur le premier noeud de la grappe, lancez l'utilitaire de configuration à partir de `C:\NetIQ\idm\apps\UserApplication\configupdate.bat`.

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).

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 15.7.8, « Configuration de la gestion des mots de passe oubliés », page 229.

2 Pour modifier le lien Modifier mon mot de passe, reportez-vous à la section « Mise à jour des liens SSPR dans le tableau de bord pour un environnement distribué ou de grappe » page 234.

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 :

```
C:NetIQ\idm\apps\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 : `C:NetIQ\idm\apps\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 :

```
C:NetIQ\idm\apps\jre\bin\keytool -list -v -keystore osp.jks -storepass changeit
```

6 Effectuez une sauvegarde du fichier `osp.jks` d'origine situé sous `C:\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 `C:\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.bat` 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.bat` sur tous les noeuds.

9b Ajoutez la propriété « -Dcom.novell.afw.wf.Engine-id=Engine » dans le fichier `setenv.bat` 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. Pour plus d'informations, reportez-vous à l'Étape 10 page 221.

11 Activez l'index des autorisations pour la mise en grappe. Pour plus d'informations, reportez-vous à la Section 15.4.2, « Activation de l'index des autorisations pour la mise en grappe », page 205.

12 Activez la grappe Tomcat. Pour plus d'informations, reportez-vous à l'étape 9 de la Section 15.4.3, « Préparation de votre serveur d'applications pour les applications d'identité », page 205.

13 Redémarrez Tomcat sur tous les noeuds.

14 Configurez le pilote d'application utilisateur pour la mise en grappe. Pour plus d'informations, reportez-vous à la Section 15.6.2, « Configuration du pilote d'application utilisateur pour la mise en grappe », page 222.

15 Installation des applications d'identité

Cette section vous guide tout au long de la procédure d'installation de l'infrastructure et des composants requis pour les applications d'identité :

- Administration des applications d'identité
- Tableau de bord des applications d'identité
- Pilote de service de rôle et de ressource
- Application utilisateur
- Pilote d'application utilisateur

Par défaut, le programme d'installation installe ces composants à l'emplacement `C:\NetIQ\idm\apps`.

Les applications d'identité nécessitent l'accès à d'autres composants Identity Manager pendant et après l'installation. NetIQ vous recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous au Chapitre 15.1, « Planification de l'installation des applications d'identité », page 189.

15.1 Planification de l'installation des applications d'identité

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

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

L'installation n'inclut pas les deux pilotes requis pour les applications d'identité : le pilote d'application utilisateur et le pilote de services de rôle et de ressource.

REMARQUE : Identity Reporting peut techniquement être considéré comme une application d'identité car ce composant utilise également SSPR et OSP. En outre, vous pouvez modifier les paramètres à l'aide de l'utilitaire de configuration de RBPM. Toutefois, Identity Reporting dispose de son propre programme d'installation, peut être installé sur un serveur distinct et utilise une autre base de données. Pour plus d'informations, reportez-vous à la Section 16.5, « Configuration système requise pour Identity Reporting », page 262.

15.1.1 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 à la Section 4.3.1, « Application utilisateur et module de provisioning basé sur les rôles », page 29.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3.4, « Configuration recommandée pour le serveur », page 43.
❑	3. Déterminez si vous devez installer Sentinel avant d'installer les applications d'identité. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.
❑	4. Vérifiez que le moteur Identity Manager est installé. Pour plus d'informations sur l'installation du moteur, reportez-vous au Chapitre 8, « Planification de l'installation du moteur, des pilotes et des plug-ins », page 83.
❑	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 15.1.3, « Conditions requises et considérations relatives à l'installation des applications d'identité », page 192.
❑	6. 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 « Configuration système requise pour les applications d'identité » page 197.
❑	7. Vérifiez qu'eDirectory est exécuté sur les ports LDAP 389 et 636 par défaut pour éviter l'apparition d'un message d'erreur de schéma non valide. Vous pouvez étendre manuellement le schéma eDirectory après l'installation. Pour plus d'informations, reportez-vous à la Section 15.2.1, « Ajout du schéma d'application utilisateur à votre serveur d'audit en tant qu'application de consignation », page 199.
❑	8. Créez un compte d'administrateur de l'application utilisateur dans le coffre-fort d'identité d'eDirectory. Pour plus d'informations, reportez-vous à la Section 15.2.2, « Assignation de droits aux comptes de l'administrateur du coffre-fort d'identité et de l'administrateur de l'application utilisateur », page 200.
❑	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 section « Conditions préalables à l'installation de la base de données pour les applications d'identité » page 196. ◆ Pour installer la base de données, reportez-vous au Chapitre 15.3, « Configuration de la base de données des applications d'identité », page 201.
❑	10. Préparez un serveur d'applications sur l'ordinateur local ou dans une grappe. ◆ Pour connaître la configuration requise, reportez-vous à la section « Conditions préalables et considérations relatives au serveur d'applications » page 194. ◆ Pour préparer la grappe, reportez-vous au Chapitre 15.4, « Préparation de votre environnement pour les applications d'identité », page 204. ◆ Pour installer un serveur d'applications, reportez-vous à la Section 15.4.3, « Préparation de votre serveur d'applications pour les applications d'identité », page 205.

	Éléments de la liste de contrôle
❑	11. (Conditionnel) Afin d'utiliser le service Apache Log4j pour enregistrer des événements dans Tomcat, vérifiez que vous disposez des fichiers appropriés. Pour plus d'informations, reportez-vous à la Section 13.1.4, « Utilisation du service Apache Log4j pour consigner les événements de connexion », page 171.
❑	12. Vérifiez le contenu du kit d'installation des applications d'identité pour déterminer quels fichiers sont nécessaires dans votre environnement. Pour plus d'informations, reportez-vous à la Section 15.1.2, « Présentation du programme d'installation pour les applications d'identité », page 191.
❑	13. Créez et déployez le pilote d'application utilisateur ainsi que le pilote de rôles et de ressource. Pour plus d'informations, reportez-vous au Chapitre 15.6, « Création et déploiement des pilotes pour les applications d'identité », page 221.
❑	14. Installez les applications d'identité. Pour plus d'informations, reportez-vous au Chapitre 15.5, « Installation des applications d'identité », page 208.
❑	15. Pour effectuer les tâches finales de la procédure d'installation, reportez-vous au Chapitre 15.7, « Fin de l'installation des applications d'identité », page 223.
❑	16. Assurez-vous d'avoir configuré correctement les applications d'identité et les paramètres d'authentification unique. Pour plus d'informations, reportez-vous au Chapitre 28, « Vérification de l'accès Single Sign-on pour les applications d'identité », page 339.
❑	17. (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).

15.1.2 Présentation du programme d'installation pour les applications d'identité

Les fichiers d'installation des applications d'identité se trouvent dans le répertoire `\products\UserApplication\` du paquetage d'installation.

Le programme d'installation (`IdmUserApp.exe`) effectue les opérations suivantes :

- Désigne une version existante d'un serveur d'applications à utiliser.
- Désigne une version existante d'une base de données à utiliser. La base de données stocke les informations de configuration et les données de l'application d'identité.
- Configure le fichier de certificats de JDK pour que l'application d'identité (exécutée sous Tomcat) puisse communiquer en toute sécurité avec le coffre-fort d'identité et le pilote d'application utilisateur.
- Configure et déploie le fichier WAR (Web Application Archive) Java de l'application utilisateur sur Tomcat.
- Permet d'activer la consignation via les clients d'audit Sentinel (selon vos besoins).
- Permet d'importer une clé principale existante pour restaurer une installation particulière des applications d'identité et pour prendre en charge les grappes.

15.1.3 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 :
  - Designer
  - Coffre-fort d'identité
  - Moteur Identity Manager
  - Chargeur distant
  - One SSO Provider

  Pour plus d'informations sur les versions et les correctifs requis pour ces composants, reportez-vous aux dernières notes de version.
- Vérifiez que le coffre-fort d'identité inclut les pilotes d'application utilisateur et de service de rôles et de ressources créés et déployés. Pour plus d'informations, reportez-vous au Chapitre 15.6, « Création et déploiement des pilotes pour les applications d'identité », page 221.
- Installez les éléments suivants avant d'installer les applications d'identité :
  - Un serveur d'applications sur l'ordinateur local. Pour plus d'informations, reportez-vous à la section « Conditions préalables et considérations relatives au serveur d'applications » page 194.
  - Une base de données sur l'ordinateur local ou un serveur connecté. Pour plus d'informations, reportez-vous à la section « Conditions préalables à l'installation de la base de données pour les applications d'identité » page 196.
- (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).

- Installez le pilote d'application utilisateur avant de créer celui des rôles et des ressources. Le pilote de rôles et de ressource fait référence au conteneur du coffre-fort de rôle (`RoleConfig.Appconfig`) dans le pilote d'application utilisateur.
- 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.
- Définissez la variable d'environnement `JAVA_HOME` de façon à ce qu'elle pointe vers le JDK à utiliser avec les applications d'identité. Pour remplacer `JAVA_HOME`, spécifiez manuellement le chemin d'accès lors de l'installation.
- Par défaut, le processus d'installation place les fichiers du programme dans le répertoire `C:\NetIQ\idm`.

  Si vous envisagez d'installer l'application utilisateur à un emplacement par défaut, le nouveau répertoire doit exister et être accessible en écriture.
- 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.
- (Conditionnel) Si vous prévoyez d'utiliser une gestion des mots de passe externe, votre environnement doit respecter la configuration suivante :
  - Activez le protocole SSL (Secure Sockets Layer) pour les instances Tomcat sur lesquelles vous déployez les applications d'identité et le fichier `IDMPwdMgt.war`.
  - Veillez à ce que le port SSL soit ouvert dans votre pare-feu.

  Pour plus d'informations sur l'activation de SSL pour Tomcat, reportez-vous à la Section 29.8, « Mise à jour des paramètres SSL pour SSPR », page 353.

  Pour plus d'informations sur le fichier `IDMPwdMgt.war`, reportez-vous à la Section 15.7.8, « Configuration de la gestion des mots de passe oubliés », page 229.
- (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 3.6.1, 4.0 ou des versions ultérieures. 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. Pour plus d'informations, reportez-vous à la Section 11.1.3, « Présentation de l'installation des plug-ins d'iManager », page 145.

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 section « Divers » page 244.
- Activez les cookies dans tous les navigateurs. Les applications ne fonctionnent pas si les cookies sont désactivés.

- Les utilisateurs ne peuvent pas accéder aux applications d'identité en tant qu'invité ou utilisateur anonyme sans être connectés aux applications d'identité. Ils sont invités à se connecter à l'interface utilisateur. Pour plus d'informations, reportez-vous à la Partie VIII, « Configuration de l'accès Single Sign-on dans Identity Manager », page 317.
- Pour qu'Identity Manager applique le mot de passe universel, configurez le coffre-fort d'identité de façon à ce qu'il utilise la connexion NMAS comme processus de connexion initiale d'un utilisateur. Ajoutez `NDSD_TRY_NMASLOGIN_FIRST` avec la valeur de chaîne `true` à la clé de registre HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment.
- (Conditionnel) Pour exécuter les rapports, les composants Identity Reporting doivent être installés dans votre environnement. Pour plus d'informations, reportez-vous au Administrator Guide to NetIQ Identity Reporting (Guide de l'administrateur de NetIQ Identity Reporting).
- 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. 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).

Conditions préalables et considérations relatives au serveur d'applications

Les applications d'identité nécessitent que Tomcat soit installé en tenant compte des aspects suivants :

- Tomcat doit fonctionner avec JDK (Java Development Kit) ou JRE (Java Runtime Environment). Pour plus d'informations sur les versions compatibles, reportez-vous à la section « Configuration système requise pour les applications d'identité » page 197.
- Définissez la variable d'environnement `JAVA_HOME` de façon à ce qu'elle pointe vers le JDK à utiliser avec l'application utilisateur. Pour remplacer `JAVA_HOME`, spécifiez manuellement le chemin d'accès lors de l'installation.
- (Facultatif) Vous pouvez utiliser votre propre programme d'installation Tomcat, plutôt que celui fourni dans le kit d'installation d'Identity Manager. Toutefois, afin d'utiliser le service Apache Log4j avec votre version de Tomcat, assurez-vous d'avoir installé les fichiers appropriés. Pour plus d'informations, reportez-vous à la Section 13.1.4, « Utilisation du service Apache Log4j pour consigner les événements de connexion », page 171.
- (Conditionnel) Pour protéger les documents portant une signature numérique, vous devez installer les applications d'identité sur un serveur d'applications Tomcat et utiliser Novell Identity Audit. Les documents comportant une signature numérique ne sont pas stockés avec les données de workflow dans la base de données de l'application utilisateur. Ils sont enregistrés

dans la base de données de consignation. Vous devez également activer la fonction de consignation pour conserver ces documents. Pour plus d'informations, reportez-vous à la section Setting Up Logging in the Identity Applications (Configuration de la consignation dans les 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).

- (Conditionnel) Si vous consignez une grande quantité de données utilisateur dans votre environnement ou si votre répertoire de serveur contient un grand nombre d'objets, vous pouvez choisir plusieurs applications serveur avec un déploiement des applications d'identité. Pour plus d'informations sur la configuration permettant d'obtenir des performances optimales, reportez-vous à la section Tuning the Performance of the Applications (Optimisation des performances 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).
- (Conditionnel) Si vous utilisez un serveur d'applications Tomcat, ne démarrez pas le serveur avant d'avoir terminé la procédure d'installation.
- (Conditionnel) Pour utiliser une gestion des mots de passe externe, vous devez procéder comme suit pour activer le protocole SSL (Secure Sockets Layer) :
  - Activez SSL pour les instances de Tomcat sur lesquelles déployer les applications d'identité et le fichier `IDMPwdMgt.war`.
  - Veillez à ce que le port SSL soit ouvert dans votre pare-feu.

  Pour plus d'informations sur le fichier `IDMPwdMgt.war`, reportez-vous à la section Configuration de la gestion des mots de passe oubliés et au *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (Guide de l'administrateur des applications d'identité de NetIQ Identity Manager).
- La procédure d'installation ne modifie pas les entrées `JAVA_HOME` ou `JRE_HOME` sur un serveur Tomcat. Par défaut, le programme d'installation simplifiée de Tomcat place le fichier `setenv.bat` dans le répertoire `C:\NetIQ\idm\apps\tomcat\bin\`. L'installation configure également l'emplacement JRE dans le fichier.

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.

Pour plus d'informations sur la configuration des applications d'identité dans un environnement de grappe, reportez-vous au Chapitre 15.4, « Préparation de votre environnement pour les applications d'identité », page 204.

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 section « Configuration du jeu de caractères » page 203 ou à la Section 15.3.1, « Configuration d'une base de données Oracle », page 202.
- 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.

15.1.4 Configuration système requise pour les applications d'identité

Cette section présente la configuration minimale requise pour installer les applications d'identité.

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	4 Go

Catégorie	Configuration requise
Système d'exploitation (certifié)	L'un des systèmes d'exploitation 64 bits suivants : ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 Pour un système d'exploitation 32 bits : ◆ Windows Server 2008 SP2 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.
Système 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	◆ 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 ◆ Orcale 12c ◆ MsSQL 2016, 2014 **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.
Navigateur Web	Un des navigateurs suivants (versions minimales) : ◆ Google Chrome 61 ◆ Mozilla Firefox 51 **REMARQUE :** les cookies du navigateur doivent être activés.
Serveur d'applications	Apache Tomcat 8.5.27
Java	JRE 1.8.0_162
Port	8180

15.2 Préparation du coffre-fort d'identité pour les applications d'identité

Cette section vous permet de vous préparer à l'installation des applications. Les applications sont exécutées sur un cadre appelé RBPM (module de provisioning basé sur les rôles). Lorsque vous installez le moteur Identity Manager, le processus d'installation installe automatiquement `netiq-DXMLuad-4.7.0-0.noarch` qui installe le pilote de l'application utilisateur ainsi que celui du service de rôles et de ressources, et qui étend le schéma eDirectory pour qu'il interagisse avec RBPM.

Les fichiers d'installation sont situés dans le répertoire `products\UserApplication\` au sein du fichier image `.iso` pour le paquetage d'installation d'Identity Manager.

- Section 15.2.1, « Ajout du schéma d'application utilisateur à votre serveur d'audit en tant qu'application de consignation », page 199
- Section 15.2.2, « Assignation de droits aux comptes de l'administrateur du coffre-fort d'identité et de l'administrateur de l'application utilisateur », page 200

15.2.1 Ajout du schéma d'application utilisateur à votre serveur d'audit en tant qu'application de consignation

Si votre serveur d'audit utilise l'application utilisateur en tant qu'application de consignation, vous devez copier le fichier `dirxml.lsc` sur le serveur. Cette section s'applique uniquement à Novell Identity Audit.

1. Recherchez le fichier `dirxml.lsc`.

   Ce fichier est situé dans le répertoire d'installation de l'application utilisateur Identity Manager à l'issue de l'installation, par exemple `C:\NetIQ\idm\apps\UserApplication`.
2. Utilisez un navigateur Web pour accéder à iManager, le plug-in Novell Identity Audit étant installé, et connectez-vous en tant qu'administrateur.
3. Accédez à **Roles and Tasks > Auditing and Logging** (Rôles et tâches > Audit et consignation) et sélectionnez **Logging Server Options** (Options du serveur de consignation).
4. Accédez au conteneur Services de consignation de votre arborescence et sélectionnez le serveur de consignation sécurisé Audit approprié, puis cliquez sur **OK**.
5. Sous l'onglet **Log Applications** (Applications de consignation), sélectionnez le nom du conteneur approprié et cliquez sur le lien **New Log Application** (Nouvelle application de consignation).
6. Dans la boîte de dialogue New Log Application (Nouvelle application de consignation), procédez comme suit :
   - **6a** Sous Log Application Name (Nom de l'application de consignation), spécifiez un nom pertinent pour votre environnement.
   - **6b** Sous Import LSC File (Importer le fichier LSC), recherchez le fichier `dirxml.lsc`.
   - **6c** Cliquez sur **OK**.
7. Cliquez sur **OK** pour achever la configuration du serveur Audit.
8. Vérifiez que l'option Log Application (Applications de consignation) est définie sur **ON** (ACTIF). (Le cercle situé sous l'état doit être vert.)
9. Redémarrez le serveur Audit pour activer les nouveaux paramètres de l'application de consignation.

15.2.2 Assignation de droits aux comptes de l'administrateur du coffre-fort d'identité et de l'administrateur de l'application utilisateur

L'administrateur du coffre-fort d'identité est un utilisateur qui dispose de droits lui permettant de configurer le coffre-fort d'identité. Il s'agit d'un rôle logique qui peut être partagé avec d'autres types d'administrateur.

L'administrateur du coffre-fort d'identité doit disposer des droits suivants :

- Droits Superviseur sur le pilote de l'application utilisateur et tous les objets qu'il contient. Pour ce faire, définissez les droits au niveau du conteneur du pilote et faites en sorte qu'ils puissent être hérités.
- Droits Entrée Superviseur pour tous les utilisateurs configurés dans la définition d'entité utilisateur de la couche d'abstraction de l'annuaire. Celle-ci doit inclure les droits d'attribut Écrire pour la classe d'objet et tous les attributs associés aux classes auxiliaires `DirXML-EntitlementRecipient`, `srvprvEntityAux` et `srvprvUserAux`.
- Droits Superviseur sur l'objet Conteneur `cn=DefaultNotificationCollection`, `cn=Security`. Cet objet conserve les paramètres de serveur de messagerie utilisés pour les messages électroniques de provisioning automatisé. Il peut contenir les références SecretStore pour l'authentification auprès du serveur de messagerie.
- Droits Superviseur sur l'objet Conteneur `cn=Authorized Login Methods`, `cn=Security`. Lors de l'installation de l'application utilisateur, l'objet Assertion SAML est créé dans ce conteneur.
- Vérifiez que vous disposez des droits Superviseur sur le conteneur `cn=Security` avant d'installer l'application utilisateur. Lors de l'installation de l'application utilisateur, le conteneur `cn=RBPMTrustedRootContainer` est créé sous le conteneur `cn=Security`.

  Vous pouvez également créer manuellement le conteneur `cn=RBPMTrustedRootContainer`, `cn=Security` (créez un objet appelé `Trusted Root Container` (Conteneur de racine approuvée) avec la classe d'objet `NDSPKI:Trusted Root` à l'intérieur du conteneur `Security`), puis assignez les droits de superviseur sur le conteneur.

Vous devez créer manuellement un compte d'administrateur de l'application utilisateur dans le coffre-fort d'identité pour installer correctement le module de provisioning basé sur les rôles. Le compte administrateur de l'application utilisateur doit être un ayant droit du conteneur maître et doit disposer de droits de superviseur sur le conteneur.

Lorsque vous créez le compte administrateur de l'application utilisateur, vous devez assigner une stratégie de mot de passe de ce compte utilisateur. Pour plus d'informations, consultez la section « Creating Password Policies » (Création de stratégies de mot de passe) du manuel *Password Management Administration Guide* (Guide d'administration pour la gestion des mots de passe).

Pour créer les autorisations du compte d'administrateur de l'application utilisateur, exécutez les commandes suivantes dans un fichier LDIF (LDAP Data Interchange Format) :

```
dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 1#subtree#[Root]#[Entry Rights]
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#description
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#directReports
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#mail
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#manager
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#photo
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvQueryList
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvUserPrefs
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#telephoneNumber
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#title

dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 17#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[Entry Rights]
ACL: 35#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[All Attributes Rights]
```

15.3 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 Section 15.1.4, « Configuration système requise pour les applications d'identité », page 197. Pour plus d'informations sur les considérations concernant la base de données de l'application utilisateur, reportez-vous à la section « Conditions préalables à l'installation de la base de données pour les applications d'identité » page 196.

REMARQUE : si vous effectuez une migration vers une nouvelle version du module RBPM et des applications d'identité, vous devez utiliser la même base de données que celle employée pour l'installation précédente. Autrement dit, l'installation à partir de laquelle vous effectuez la migration.

15.3.1 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 section « Configuration système requise pour les applications d'identité » page 197.

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
```

REMARQUE : il est recommandé d'utiliser la version JAR de JDBC`ojdbc6.jar`.

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.

15.3.2 Configuration d'une base de données PostgreSQL

Pour votre confort, NetIQ fournit un programme d'installation pour PostgreSQL, qui prend totalement en charge les services et applications de la structure d'Identity Manager. Le programme d'installation vous guide tout au long du processus de configuration. Pour plus d'informations, reportez-vous au Chapitre 12.2, « Installation de PostgreSQL et de Tomcat », page 164.

15.3.3 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 section « Configuration système requise pour les applications d'identité » page 197.

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 d'une version prise en charge 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 de fichier JAR du pilote JDBC `sqljdbc4.jar` avec Microsoft SQL Server 2014 et `sqljdbc42.jar` avec Microsoft SQL Server 2016.

15.4 Préparation de votre environnement pour les applications d'identité

Les applications d'identité gagnent en disponibilité lorsque vous les exécutez dans une grappe. De plus, elles prennent en charge la réplication de session HTTP et le basculement de session. Cela signifie que 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.

Cette section fournit les instructions de préparation de votre environnement, y compris un environnement de cluster, afin qu'il fonctionne avec les applications d'identité. Vous devez effectuer les étapes décrites dans ce chapitre en combinaison avec les instructions de la Section 15.5.2, « Utilisation de la procédure guidée pour installer les applications d'identité », page 209.

Pour plus d'informations sur la configuration requise pour un environnement de grappe, reportez-vous à la Section 15.1.3, « Conditions requises et considérations relatives à l'installation des applications d'identité », page 192 et à la Section 15.1.4, « Configuration système requise pour les applications d'identité », page 197.

15.4.1 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 : `C:\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 = C:\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.

15.4.2 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**.

15.4.3 Préparation de votre serveur d'applications pour les applications d'identité

Vous devez préparer l'instance Tomcat qui va exécuter les applications d'identité. Pour votre confort, NetIQ fournit Apache Tomcat dans le kit d'installation. Pour plus d'informations sur l'utilisation des applications dans un environnement de grappe, reportez-vous également à la Section 15.4.4, « Préparation d'une grappe pour les applications d'identité », page 206.

Le fichier `.iso` pour l'installation d'Identity Manager inclut un programme d'installation de Tomcat (et, le cas échéant, de PostgreSQL). Pour plus d'informations, reportez-vous au Chapitre 12.2, « Installation de PostgreSQL et de Tomcat », page 164.

Vous pouvez utiliser votre propre programme d'installation Tomcat au lieu de celui fourni par commodité dans le paquetage d'installation. Toutefois, si vous choisissez cette option, vous devez effectuer des étapes supplémentaires pour que Tomcat fonctionne correctement avec les applications d'identité.

Avant de démarrer la procédure d'installation, assurez-vous que les versions des composants que vous installez sont prises en charge par cette version des applications d'identité. Pour plus d'informations, reportez-vous à la Section 15.1.3, « Conditions requises et considérations relatives à l'installation des applications d'identité », page 192.

1. Installez Apache Tomcat en tant que service sur votre serveur.

   Pour plus d'informations, reportez-vous à la configuration de tomcat.

2. Installez les composants suivants sur le même serveur que celui sur lequel vous avez installé Tomcat.
   - **JRE (Java Runtime Environment) :** pour plus d'informations, reportez-vous au document Java Platform Installation Guide (Guide d'installation de la plate-forme Java).
   - **Apache ActiveMQ :** pour plus d'informations, consultez le site ActiveMQ.
   - **PostgreSQL :** pour plus d'informations, reportez-vous aux manuels de PostgreSQL.
3. Copiez le fichier `activemq-all-5.15.2 jar` dans le dossier *`C:\NetIQ\idm\apps\activemq`*.
4. Copiez les fichiers suivants dans le dossier *`C:\NetIQ\idm\apps\tomcat\bin`* pour la consignation.
   - `log4j.jar`
   - `log4j.properties`
   - `tomcat-juli-adapters.jar`
5. Définissez les propriétés suivantes dans le fichier `setenv.bat`.

   ```
   JAVA_HOME
   JRE_HOME
   PATH (set Java path)
   JAVA_OPTS="-Xms1024m -Xmx1024m"
   ```

6. Copiez le fichier `postgresql 9.4.1212jdbc42.jar` dans le dossier `C:\NetIQ\idm\apps\tomcat\bin`.
7. (Conditionnel) Dans un environnement de grappe, ouvrez le fichier `server.xml`, situé par défaut dans le répertoire `\TOMCAT_INSTALLED_HOME\conf\` , sur le premier noeud de la grappe et supprimez les marques de commentaire de cette ligne :

   ```
   <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
   ```

   Effectuez cette opération pour tous les noeuds de la grappe.

   Pour une configuration avancée de mise en grappe Tomcat, suivez les étapes de la Documentation Tomcat d'Apache.

15.4.4 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 207
- « Configuration des propriétés système pour les ID de moteur de workflow » page 207
- « Utilisation de la même clé principale pour chaque application utilisateur dans la grappe » page 207

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 15.1.3, « Conditions requises et considérations relatives à l'installation des applications d'identité », page 192.

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 la création de la clé principale, reportez-vous à la section **Sécurité - Clé principale** à l'Étape 6 page 209. 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.

15.5 Installation des applications d'identité

Ce chapitre fournit des instructions d'installation et de configuration d'un serveur d'applications pour l'application utilisateur et RBPM. Vous devez disposer de la version de l'environnement Java correspondant à votre serveur d'applications.

Pour plus d'informations sur la configuration requise pour Tomcat et Java, reportez-vous à la Section 15.1.4, « Configuration système requise pour les applications d'identité », page 197.

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

Utilisez la liste de contrôle suivante pour vous guider tout au long de la procédure d'installation des applications d'identité.

	Éléments de la liste de contrôle
❑	1. (Conditionnel) Passez en revue les considérations relatives à l'installation des applications d'identité sous Tomcat dans un environnement de grappe. Pour plus d'informations, reportez-vous à la section « Présentation des groupes de grappes dans les environnements Tomcat » page 207.
❑	2. Installez une version prise en charge de votre serveur d'applications et du kit de développement Java ou de l'environnement d'exécution. Pour plus d'informations, reportez-vous à la Section 15.1.4, « Configuration système requise pour les applications d'identité », page 197.
❑	3. Vérifiez que les paramètres de Tomcat sont corrects. Pour plus d'informations, reportez-vous à la Section 15.4.3, « Préparation de votre serveur d'applications pour les applications d'identité », page 205.
❑	4. Configurez un fichier de source de données et un fournisseur JDBC pour la base de données.
❑	5. Installez les applications d'identité. Pour plus d'informations, reportez-vous à la Section 15.5.2, « Utilisation de la procédure guidée pour installer les applications d'identité », page 209.
❑	6. Configurez Tomcat pour les applications d'identité. Pour plus d'informations, reportez-vous à la Section 15.5.3, « Étapes postérieures à l'installation », page 215.
❑	7. Déployez et démarrez les applications d'identité Pour plus d'informations, reportez-vous à la section « Démarrage des applications d'identité » page 219.

15.5.2 Utilisation de la procédure guidée pour installer les applications d'identité

La procédure suivante décrit comment installer les applications d'identité à l'aide d'un assistant d'installation.

Pour préparer l'installation, passez en revue les opérations énumérées à la Section 15.5.1, « Liste de contrôle de l'installation des applications d'identité », page 208. Reportez-vous également aux notes de version accompagnant le logiciel.

REMARQUE

- Le programme d'installation n'enregistre pas les valeurs que vous entrez dans les fenêtres de l'assistant. Si vous cliquez sur **Précédent** pour revenir à une fenêtre précédente, vous devez les réinsérer.
- Le programme d'installation crée le compte utilisateur *novlua* et définit les autorisations de cet utilisateur dans Tomcat. Par exemple, le script `services.msc` utilise ce compte utilisateur pour exécuter Tomcat.

Avec la procédure d'installation guidée :

1. Connectez-vous en tant qu'administrateur sur l'ordinateur où vous souhaitez installer les applications d'identité.
2. Arrêtez Tomcat.
3. (Conditionnel) Si vous disposez du fichier image `.iso` pour le paquetage d'installation d'Identity Manager, accédez au répertoire contenant les fichiers d'installation, situés par défaut dans le répertoire `products\UserApplication\`.
4. (Conditionnel) Si vous avez téléchargé les fichiers d'installation, procédez comme suit :
   - **4a** Accédez au fichier `win.zip` de l'image téléchargée.
   - **4b** Extrayez le contenu du fichier dans un répertoire de l'ordinateur local.
5. À partir du répertoire qui contient les fichiers d'installation, exécutez le fichier `IdmUserApp.exe`.
6. Terminez la procédure guidée en utilisant les paramètres suivants :
   - **Plate-forme du serveur d'applications**

     Représente Tomcat pour l'exécution des applications d'identité. Tomcat doit déjà être installé.
   - **Dossier d'installation**

     Représente le chemin d'un répertoire où le programme d'installation crée les fichiers de l'application.
   - **Plate-forme de la base de données**

     Représente la plate-forme de la base de données de l'application utilisateur. La base de données doit déjà être installée. Toutefois, il n'est pas nécessaire de créer le schéma de base de données pendant l'installation.

     Pour votre confort, NetIQ fournit PostgreSQL.
   - **Hôte et port de la base de données**

     Représente les paramètres pour le serveur qui héberge la base de données de l'application utilisateur.

REMARQUE : dans un environnement de grappe, vous devez spécifier les mêmes paramètres de base de données pour chaque membre de la grappe.

Hôte

Indique le nom ou l'adresse IP du serveur.

Port

Indique le port que le serveur doit utiliser pour la communication avec l'application utilisateur.

- **Nom d'utilisateur et mot de passe de la base de données**

Représente les paramètres pour l'exécution de la base de données de l'application utilisateur.

REMARQUE

- Si vous avez installé une base de données PostgreSQL dans le cadre de l'installation de cette version d'Identity Manager, la procédure d'installation a déjà créé la base de données et son administrateur. Par défaut, la base de données installée est `idmuserappdb` et l'utilisateur est `idmadmin`. Spécifier les mêmes valeurs que celles utilisées pour l'installation de PostgreSQL.
- Dans un environnement de grappe, vous devez spécifier le même nom de base de données, le même nom d'utilisateur et le même mot de passe pour chaque membre de la grappe.

Nom ou SID de la base de données

Spécifie le nom de la base de données en fonction de la plate-forme de base de données. Par défaut, le nom de la base de données est `idmuserappdb`.

- Pour une base de données PostgreSQL ou SQL Server, indiquez le nom.
- Pour une base de données Oracle, indiquez l'identificateur de sécurité (SID) que vous avez créé avec l'instance de base de données.

Nom d'utilisateur de la base de données

Indique le nom d'un compte qui permet à l'application utilisateur d'accéder à des données et de les modifier dans les bases de données.

Mot de passe de la base de données

Indique le mot de passe pour le nom d'utilisateur spécifié.

Fichier JAR du pilote de base de données

Spécifie le fichier JAR pour la plate-forme de base de données.

Le fournisseur de la base de données fournit le fichier JAR du pilote, qui représente le fichier JAR du client léger pour le serveur de base de données. Par exemple, pour PostgreSQL, vous pouvez spécifier `postgresql-9.4-1212.jdbc42.jar`, situé par défaut dans le dossier `C:\NetIQ\idm\apps\Postgres`.

NetIQ ne prend pas en charge les fichiers JAR de pilote fournis par d'autres fournisseurs.

- **Administrateur de la base de données**

Facultatif

Représente le nom et le mot de passe de l'administrateur de la base de données.

Ce champ reprend automatiquement le même compte utilisateur et le même mot de passe que ceux spécifiés sous Nom d'utilisateur et mot de passe de la base de données. Pour utiliser ce compte, n'apportez pas de modification.

Administrateur de la base de données

(Facultatif) Spécifie le compte d'un administrateur de la base de données qui peut créer des tables de base de données, des vues, et d'autres artéfacts.

Mot de passe

(Facultatif) Entrez le mot de passe de l'administrateur de la base de données.

- **Créer des tables de base de données**

  Indique si vous voulez configurer votre nouvelle base de données ou la base existante dans le cadre du processus d'installation, ou ultérieurement.

  Création des tables maintenant

  Le programme d'installation crée les tables de base de données dans le cadre de la procédure d'installation.

  Créer des tables au démarrage de l'application

  Le programme d'installation conserve des instructions pour créer les tables lorsque l'application utilisateur est lancée pour la première fois.

  Écrire SQL dans un fichier

  Génère un script SQL que l'administrateur de la base de données peut exécuter pour créer la base de données. Si vous choisissez cette option, vous devez également spécifier un nom pour le **Fichier de schéma**. Ce paramètre est défini dans le fichier de configuration **Fichier de sortie SQL**.

  Vous pouvez sélectionner cette option si vous ne disposez pas des autorisations permettant de créer ou de modifier une base de données dans votre environnement. Pour plus d'informations sur la création de tableaux avec le fichier, reportez-vous à la Section 15.7.2, « Création manuelle du schéma de base de données », page 224.

- **Nouvelle base de données ou base de données existante**

  Indique si vous souhaitez utiliser des bases de données vides existantes ou créer de nouvelles tables dans la base de données existante. Tenez compte des considérations suivantes :

  - Nouvelle base de données

    Si vous utilisez une nouvelle base de données, cliquez sur **Nouvelle base de données.** Avant de sélectionner cette option, assurez-vous qu'une base de données existe.

  - Base de données existante

    Si la base de données existe et comporte des tables d'application utilisateur provenant d'une installation précédente, sélectionnez **Base de données existante.**

    Si la base de données existante s'exécute sur une plate-forme Oracle, vous devez préparer Oracle avant de mettre à jour le schéma.

  Après avoir sélectionné le type de base de données, vous devez spécifier à quel moment les tables de base de données doivent être créées. L'écran Créer des tables de base de données vous permet de créer les tables au moment de l'installation ou au démarrage de l'application. Vous pouvez également créer, lors de l'installation, un fichier de schéma que l'administrateur de la base de données utilisera ultérieurement pour créer les tables.

  Si vous souhaitez générer un fichier de schéma, sélectionnez le bouton Écrire SQL dans un fichier et indiquez un nom pour le fichier dans le champ Fichier de sortie du schéma.

- **Tester la connexion à la base de données**

  Indique si vous souhaitez que le programme d'installation se connecte à la base de données pour créer des tables directement ou pour créer le fichier `.sql`.

Le programme d'installation tente la connexion lorsque vous cliquez sur **Suivant** ou appuyez sur **Entrée**.

REMARQUE : vous pouvez poursuivre l'installation même si la connexion à la base de données échoue. Toutefois, une fois l'installation terminée, vous devrez créer manuellement les tables et la connexion avec la base de données. Pour plus d'informations, reportez-vous à la section « Création manuelle du fichier SQL pour générer le schéma de base de données » page 225.

- **Installation de Java**

  Représente le chemin d'accès au fichier JRE pour lancer le programme d'installation. Par exemple : `C:\NetIQ\idm\jre`.

- Configuration ***Application_Server***

  Représente le chemin des fichiers d'installation de Tomcat. Par exemple : `C:\NetIQ\idm\jre`. La procédure d'installation ajoute des fichiers à ce dossier.

- **Configuration d'IDM**

  Représente les paramètres du contexte de l'application d'identité utilisé dans les URL et pour le moteur de workflow.

  Contexte de l'application

  Indique un nom qui correspond à la configuration de Tomcat, au fichier WAR de l'application et au nom inclus dans le contexte de l'URL.

  Le script d'installation crée une configuration de serveur, puis nomme la configuration en fonction du nom que vous avez créé lors de l'installation de Tomcat. Exemple : `IDMProv`.

  IMPORTANT : NetIQ vous recommande de noter le **Contexte de l'application** spécifié. Vous utiliserez ce nom dans l'URL lorsque vous démarrez les applications d'identité à partir d'un navigateur.

- **Sélectionner le type de consignation de l'audit**

  Indique si vous souhaitez activer CEF ou Sentinel Log Management for IGA. Sélectionnez **Oui** ou **Non**.

- **Consignation d'audit**

  S'applique uniquement si vous spécifiez Oui pour l'option Sélectionner le type de consignation de l'audit.

  Indique le type de consignation que vous souhaitez activer.

  Pour plus d'informations sur la configuration de la consignation, reportez-vous au manuel *User Application: Administration Guide* (Guide d'administration de l'application utilisateur).

  Sentinel Log Management for IGA

  Active la consignation via un client Novell ou NetIQ pour l'application utilisateur.

  REMARQUE : si vous choisissez cette option, vous devez également spécifier le nom d'hôte ou l'adresse IP du serveur client et le chemin d'accès au cache du journal.

  CEF

  Permet à l'application utilisateur de consigner des événements par le biais de CEF.

  REMARQUE : si vous choisissez cette option, vous devez également spécifier le nom d'hôte ou l'adresse IP du serveur et du port Syslog.

- **Sécurité - Clé principale**

Indique si vous souhaitez importer une clé principale existante. L'application utilisateur emploie la clé principale pour accéder aux données codées. Sélectionnez **Oui** ou **Non**.

Vous pouvez importer la clé principale dans les situations suivantes :

- Après l'installation de la première instance des applications d'identité dans une grappe. Chaque instance de l'application utilisateur dans une grappe doit utiliser la même clé principale. Pour plus d'informations, reportez-vous à la section « Utilisation de la même clé principale pour chaque application utilisateur dans la grappe » page 207.
- Si vous déplacez votre installation d'un système provisoire à un système de production et que vous souhaitez conserver l'accès à la base de données utilisée avec le système provisoire.
- Si vous restaurez votre application utilisateur et que vous souhaitez accéder aux données codées stockées par votre version antérieure de l'application utilisateur.

Oui

Indique que vous souhaitez importer une clé principale existante.

Non

Indique que vous souhaitez que le programme d'installation crée la clé.

Par défaut, la procédure d'installation inscrit la clé principale codée dans le fichier `master-key.txt`, situé dans le répertoire d'installation.

- **Importer la clé principale**

  S'applique uniquement si vous spécifiez Oui pour l'option Sécurité - Clé principale

  Permet d'indiquer la clé principale que vous souhaitez utiliser. Vous pouvez copier la clé principale du fichier `master-key.txt`.

- **Connexion au serveur d'applications**

  Représente les paramètres de l'URL dont les utilisateurs ont besoin pour se connecter aux applications d'identité sous Tomcat. Par exemple, `https:myserver.mycompany.com:8080`.

REMARQUE : si OSP s'exécute sur une autre instance du serveur d'applications Tomcat, vous devez également sélectionner **Se connecter à un serveur d'authentification externe** et spécifier des valeurs pour le serveur OSP.

Protocole

Indique si vous souhaitez utiliser *http* ou *https*. Afin d'utiliser SSL (Secure Sockets Layer) pour les communications, indiquez `https`.

Nom d'hôte

Indique le nom DNS ou l'adresse IP du serveur qui héberge OSP. N'utilisez pas `localhost`.

Port

Indique le port que le serveur doit utiliser pour la communication avec des ordinateurs clients.

Se connecter à un serveur d'authentification externe

Indique si une autre instance de Tomcat héberge le serveur d'authentification (OSP). Le serveur d'authentification contient la liste des utilisateurs qui peuvent se connecter à SSPR.

Si vous sélectionnez cette option, indiquez également les valeurs pour le **Protocole**, le **Nom d'hôte** et le **Port**.

- **Détails du serveur d'authentification**

  Spécifie le mot de passe que vous souhaitez que les applications d'identité utilisent lors de la connexion au serveur d'authentification. Cette information est également appelée le secret du client. La procédure d'installation crée ce mot de passe.

7 Configurez les paramètres des applications d'identité dans la fenêtre de mise à jour de la configuration.

7a Recherchez les **DN de coffre-fort d'identité**.

7b Cliquez sur **OK**.

REMARQUE

- Assurez-vous que les pilotes d'application utilisateur et de service de rôles et de ressources sont déjà créés et déployés dans le coffre-fort d'identité. Pour plus d'informations, reportez-vous à la section « Considérations relatives à l'installation des applications d'identité » page 192.
- Si vous cliquez sur **Annuler**, le programme d'installation vous ramène à la fenêtre de connexion au serveur d'applications.
- Après l'installation de l'application utilisateur, vous pouvez modifier la plupart des paramètres dans le fichier `configureupdate.bat`. Pour plus d'informations sur la spécification des valeurs pour les paramètres, reportez-vous au Chapitre 15.8, « Configuration des paramètres pour les applications d'identité », page 235.

---

8 (Conditionnel) Dans une installation de type GUI, pour configurer immédiatement les applications d'identité, procédez comme suit dans la fenêtre Configurer IDM :

8a Cliquez sur **Oui**, puis sur **Suivant**.

8b Dans configuration du module de provisioning basé sur les rôles, cliquez sur **Aff. options avancées**.

8c Modifiez les paramètres à votre convenance.

REMARQUE

- Pour plus d'informations sur la spécification des valeurs, reportez-vous au Chapitre 15.8, « Configuration des paramètres pour les applications d'identité », page 235.
- Dans les environnements de production, toutes les assignations d'administrateur sont limitées par les licences. NetIQ recueille des données de surveillance dans la base de données d'audit afin de vérifier que les environnements de production sont conformes. Par ailleurs, NetIQ recommande de n'octroyer les autorisations de l'administrateur de la sécurité qu'à un seul utilisateur.

8d Cliquez sur **OK**.

9 Cliquez sur **Suivant**.

10 Dans la fenêtre Résumé avant installation, cliquez sur **Installer**.

11 (Facultatif) Consultez les fichiers journaux de l'installation. Pour les résultats de l'installation de base, reportez-vous au fichier journal `user_application_install_log.log` dans le répertoire `C:\NetIQ\idm\apps\UserApplication\logs\`.

Pour plus d'informations sur la configuration des applications d'identité, reportez-vous au fichier `NetIQ-Custom-Install.log` dans le répertoire `C:\NetIQ\idm\apps\UserApplication`.

12 (Facultatif) Si vous utilisez un WAR de gestion des mots de passe externe, copiez-le manuellement dans le répertoire d'installation et dans le répertoire de déploiement du serveur d'applications distant qui exécute la fonction WAR de mot de passe externe.

13 Passez aux tâches post-installation décrites au Chapitre 15.7, « Fin de l'installation des applications d'identité », page 223.

15.5.3 Étapes postérieures à l'installation

Cette section fournit des informations sur la mise à jour de votre environnement Tomcat après l'installation des applications d'identité.

Si vous avez utilisé le programme d'installation de Tomcat fourni pour votre confort, les programmes d'installation d'Identity Manager configurent Tomcat pour vous. Si vous avez installé votre propre programme Tomcat, tenez compte des points suivants :

- Vous pouvez modifier le service Tomcat pour optimiser les performances. Pour plus d'informations, reportez-vous à l'article *So You Want High Performance*.
- Vous pouvez ajouter la prise en charge des événements de consignation. Pour plus d'informations, reportez-vous à la Section 13.1.4, « Utilisation du service Apache Log4j pour consigner les événements de connexion », page 171.

Configuration du pilote d'application utilisateur pour la mise en grappe

Pour plus d'informations, reportez-vous à la Section 15.6.2, « Configuration du pilote d'application utilisateur pour la mise en grappe », page 222.

Transmission de la propriété preferIPv4Stack à la JVM

Les applications d'identité utilisent JGroups pour l'implémentation du caching. Dans certaines configurations, JGroups requiert que la propriété preferIPv4Stack soit définie sur true pour garantir le bon fonctionnement de la liaison mcast_addr.

Sans cette option, l'erreur suivante peut se produire :

```
[10/1/09 16:11:22:147 EDT] 0000000d UDP           W org.jgroups.util.Util
createMulticastSocket could not bind to /228.8.8.8 (IPv4 address); make sure
your mcast_addr is of the same type as the IP stack (IPv4 or IPv6).
```

L'erreur suivante peut également s'afficher :

```
[3/21/12 10:04:32:470 EDT] 00000024 UDP      E org.jgroups.protocols.TP down
failed sending message to null (131 bytes)
        java.lang.Exception: dest=/228.8.8.8:45654 (134 bytes)
    at org.jgroups.protocols.UDP._send(UDP.java:353)
```

Le paramètre `java.net.preferIPv4Stack=true` est une propriété système qui peut être configurée de la même façon que les autres propriétés système telles que `extend.local.config.dir`.

Vérification de l'état de santé du serveur

La plupart des équilibreurs de charge incluent une fonctionnalité de vérification de l'état de santé qui permet de déterminer si un serveur HTTP est opérationnel et à l'écoute. L'application utilisateur inclut une URL qui peut être utilisée pour configurer des vérifications de l'état de santé du serveur HTTP sur votre équilibreur de charge. Cette URL est la suivante :

```
http://<IP_noeud>:port/IDMProv/jsps/healthcheck.jsp
```

Surveillance des statistiques d'état de santé

L'API REST permet de récupérer des informations sur l'état de santé de l'application utilisateur. L'`API` peut accéder au système pour collecter des informations à propos des threads en cours d'exécution, de la consommation de mémoire, du cache et de la grappe, et renvoie ces informations à l'aide de l'opération `GET`.

- **Informations sur la mémoire (mémoire système et JVM) :** lit les informations relatives à la mémoire, notamment la mémoire système et la mémoire consommée par la machine virtuelle Java (JVM).

  Par exemple :

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/memoryinfo
  ```

- **Informations sur les threads :** lit les informations relatives aux threads consommant énormément de ressources processeur et renvoie la liste des principaux threads à l'origine d'une utilisation intensive du processeur.

  Par exemple :

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo
  ```

  Pour accéder à la trace de pile des threads dans la JVM, définissez le paramètre de pile sur **True**.

  Par exemple :

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo?stack=true
  ```

  Pour spécifier le nombre de threads dans la JVM, définissez la valeur du paramètre **thread-count**.

  Exemples :

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo?thread-count=1
  ```

- **Informations sur le cache :** lit les informations relatives au cache pour l'application utilisateur.

  Par exemple :

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/cacheinfo
  ```

- **Informations sur la grappe :** lit les informations relatives à la grappe.

  Par exemple :

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/clusterinfo
  ```

REMARQUE : pour pouvoir afficher les statistiques d'état de santé de l'application utilisateur à l'aide de l'API REST, vous devez être administrateur de la sécurité.

Création d'index composés

Après l'installation ou la mise à niveau des applications d'identité, créez manuellement les index composés pour chaque attribut que vous souhaitez utiliser pour trier les utilisateurs dans le tableau de bord Identity Manager. Vous pouvez créer des index composés à l'aide de l'utilitaire `ndsindex` qui se trouve au même emplacement que l'installation d'eDirectory. Vous pouvez spécifier plusieurs attributs séparés par le signe `$` pour l'indexation des composés. Les attributs de base suivants sont requis pour l'indexation des composés :

- Nom, prénom
- Prénom, nom
- CN, nom
- Title,Surname (Titre, Nom)
- Telephone Number,Surname (Numéro de téléphone, Nom)
- Internet Email Address,Surname (Adresse de messagerie Internet, Nom)
- L,Surname (L, Nom)
- OU,Surname (OU, Nom)

La commande suivante vous aide à créer des index composés à l'aide de l'utilitaire `ndsindex` :

```
ndsindex add [-h <hostname>] [-p <port>] -D <admin DN> -W|[-w <password>] -s
<eDirectory Server DN> [<indexName1>, <indexName2>.....]
```

Par exemple, pour trier les utilisateurs en fonction de leur **Titre**, exécutez la commande suivante :

```
ndsindex add -h <hostname> -p <ldap port> -D <admin DN> -w <admin passwd> -s
<eDirectory Server DN> Title-SN;Title$Surname;value
```

Vous pouvez également créer des index composés à l'aide de l'utilitaire d'exportation de conversion.

Ces opérations nécessitent l'utilisation d'un fichier LDIF. Une fois le fichier LDIF importé, lancez l'indexation en déclenchant le contrôleur de connectivité (limber). Sans cela, l'indexation a lieu lors du déclenchement automatique du contrôleur de connectivité.

Exemple de fichier LDIF pour créer des index composés afin de trier les utilisateurs sur l'attribut **Titre** :

```
dn: cn=osg-nw5-7, o=Novell

changetype: modify

add: indexDefinition

indexDefinition: 0$sntitleindex$0$0$0$1$Title$surname
```

Pour plus d'informations sur les fichiers LDIF, reportez-vous à la section Fichiers LDIF dans le *Guide d'administration de NetIQ eDirectory*.

Configuration de l'application d'identité pour rejeter une renégociation SSL lancée par le client

Par défaut, le programme d'installation des applications d'identité configure une connexion non sécurisée (http). Dans certaines circonstances, une connexion non sécurisée peut exposer Identity Manager à une attaque par déni de service causée par la renégociation SSL client lancée par le client avec le serveur d'applications d'identité. Pour éviter ce problème, ajoutez le drapeau suivant pour l'entrée `CATALINA_OPTS` dans le fichier `<répertoire-installation-tomcat>\bin\setenv.bat`.

```
"-Djdk.tls.rejectClientInitiatedRenegotiation=true"
```

15.5.4 Désactivation du paramètre Prevent HTML Framing (Empêcher le tramage HTML) pour l'intégration d'Identity Manager à SSPR

Cette section traite de la configuration requise d'Identity Manager pour l'intégrer à un environnement SSPR 4.2 n'ayant pas été déployé par Identity Manager 4.5. SSPR fournit une option configurable, **Prevent HTML Framing** (Empêcher le tramage HTML), qui permet aux utilisateurs d'afficher SSPR dans une trame imbriquée pour toute application qui contient le code source HTML iframe. Si vous sélectionnez cette option, SSPR n'est pas inclus dans l'iframe spécifié pour l'application. Pour désactiver cette option pour Identity Manager, procédez comme suit :

1. Accédez à http://*<IP/nom DNS>:<port>/sspr.* Ce lien vous permet d'accéder au portail SSPR.
2. Connectez-vous en tant qu'administrateur SSPR.
3. Cliquez sur **Configuration Editor** (Éditeur de configuration) en haut de la page et indiquez le mot de passe de configuration OSP.
4. Cliquez sur **Settings > Security** (Paramètres > Sécurité) > **Always Show Advanced Settings** (Afficher les paramètres avancés) et procédez comme suit :
   - **4a** Recherchez **Prevent HTML Framing** (Empêcher le tramage HTML), désactivez l'option **Enabled** (Activé) et cliquez sur **Save** (Enregistrer) pour enregistrer le paramètre.
   - **4b** Dans la fenêtre de confirmation, cliquez sur **OK**.

15.5.5 Vérification des propriétés de l'utilisateur

Pour permettre à vos utilisateurs d'utiliser les applications d'identité, vous devez vous assurer que des propriétés de l'utilisateur avec des droits nécessaires sont ajoutées au conteneur qui comprend tous vos utilisateurs système. Vous pouvez vérifier ces propriétés à l'aide d'iManager. Effectuez les étapes suivantes dans iManager pour vérifier ces paramètres :

1. Connectez-vous à iManager en tant qu'administrateur à l'aide de l'adresse IP de votre coffre-fort d'identité en tant qu'arborescence.
2. Dans le tableau de bord **Arborescence**, sélectionnez l'arborescence dans laquelle vos applications d'identité sont configurées.
3. Cliquez sur **Droits assignés** pour le conteneur qui comprend l'ensemble des utilisateurs système.
4. Vérifiez que les propriétés suivantes possèdent les droits nécessaires dans la liste :
   - Description
   - Internet EMail Address

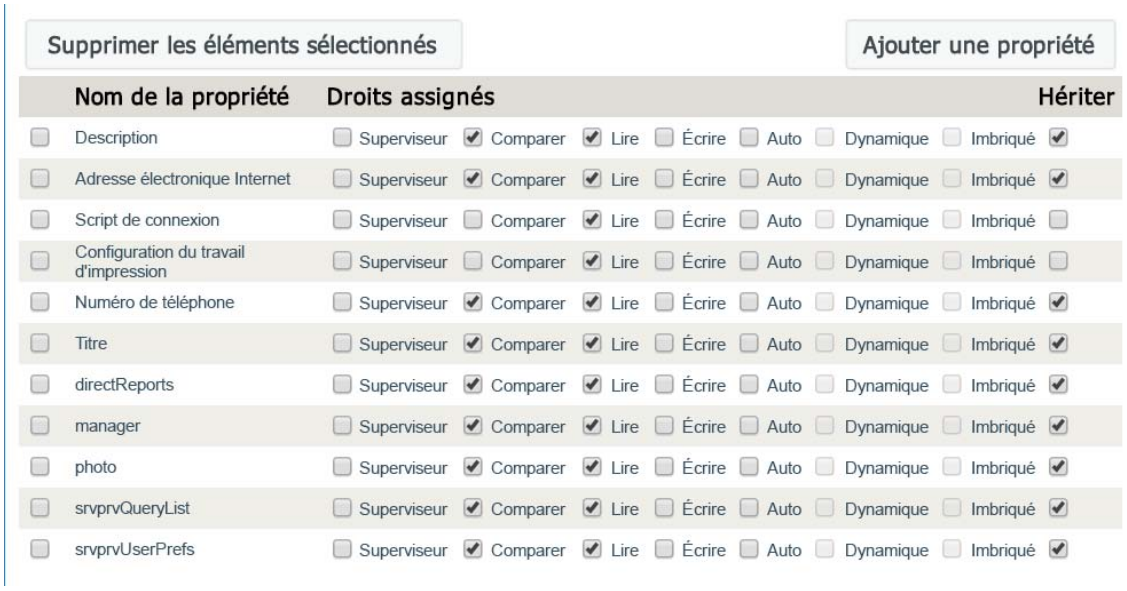
- Script de connexion
- Configuration des travaux d'impression
- Numéro de téléphone
- Titre
- directReports
- gestionnaire
- photo
- srvprvQueryList
- srvprvUserPrefs

Si certaines propriétés sont manquantes, cliquez sur **Ajouter une propriété**.

4a Sélectionnez la propriété requise dans la liste, puis cliquez sur **Terminé**.

4b Sélectionnez les droits nécessaires pour la propriété, puis cliquez sur **Terminé**.

Figure 15-1 *Ajout de propriétés au conteneur des utilisateurs*



15.5.6 Démarrage des applications d'identité

Cette section fournit des instructions pour démarrer les applications d'identité et se connecter pour la première fois à un serveur d'applications. Dans un environnement de grappe, entamez la procédure sur le nœud principal. Les applications d'identité doivent être installées et prêtes pour le déploiement. Pour plus d'informations sur les tâches post-installation, reportez-vous au Chapitre 15.7, « Fin de l'installation des applications d'identité », page 223.

Le script de démarrage `services.msc` vous permet de démarrer le service Tomcat. Vous pouvez également utiliser ce fichier pour arrêter ou redémarrer le service Tomcat.

Si votre navigateur n'affiche pas la page de l'application utilisateur après avoir suivi cette procédure, vérifiez que la console du terminal n'affiche pas de message d'erreur et reportez-vous au Chapitre 37, « Dépannage », page 423.

Pour démarrer les applications d'identité :

1. Démarrez la base de données des applications d'identité. Pour plus d'informations, reportez-vous à la documentation relative à votre base de données.
2. Pour que l'application utilisateur génère des rapports, ajoutez le drapeau `Djava.awt.headless=true` au script de démarrage pour Tomcat. Exemple :

   ```
   JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -
   Dsun.jnu.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:MaxPermSize=512m
   ```

   REMARQUE : vous ne devez pas effectuer cette étape si vous utilisez un système Windows X11.
3. Démarrez Tomcat à partir de l'emplacement où vous avez installé les applications d'identité.

   REMARQUE : dans une grappe, démarrez le noeud principal uniquement.
4. Dans la ligne de commande, faites du répertoire d'installation votre répertoire de travail.
5. Exécutez le script de démarrage.
6. Pour activer la communication avec le pilote de l'application utilisateur, procédez comme suit :
   - **6a** Connectez-vous à iManager.
   - **6b** Sous **Rôles et tâches > Identity Manager** dans le volet de navigation gauche, cliquez sur **Présentation d'Identity Manager**.
   - **6c** Dans la vue de contenu, spécifiez l'ensemble de pilotes qui contient le pilote de l'application utilisateur, puis cliquez sur **Rechercher**.
   - **6d** Dans le graphique qui présente l'ensemble de pilotes et les pilotes associés, cliquez sur l'icône rouge et blanc pour le pilote de l'application utilisateur.
   - **6e** Cliquez sur **Démarrer le pilote**.

     Au démarrage, le pilote tente une « reconnaissance mutuelle » avec l'application utilisateur. Si votre serveur d'applications n'est pas en cours d'exécution ou si le WAR n'a pas été correctement déployé, le pilote renvoie une erreur. Dans le cas contraire, le statut du pilote change et passe au symbole du yin et du yang, indiquant que le pilote est démarré.
7. Pour démarrer le pilote de service de rôle et de ressources, répétez la procédure de l'Étape 6.
8. Pour lancer et se connecter à l'application utilisateur, entrez l'URL suivante dans votre navigateur Web :

   `http://`*`hostname`*`:`*`port/ApplicationName`*

   hostname

   Représente le nom du serveur d'applications (Tomcat). Exemple : `monserveur.domaine.com`

   port

   Indique le numéro de port du serveur d'applications. Exemple : `8180`.

   ApplicationName

   Représente le nom que vous avez spécifié au cours de l'installation de l'application lorsque vous avez fourni les informations de configuration du serveur d'applications. Exemple : `IDMProv`.
9. Dans l'angle supérieur droit de la page de renvoi de l'application utilisateur, cliquez sur **Login**.

10 (Conditionnel) Pour activer l'application utilisateur dans un groupe de grappes, procédez comme suit :

10a Cliquez sur **Administration**.

10b Dans le portail de configuration de l'application, cliquez sur **Mise en cache**.

10c Dans la fenêtre Gestion de la mise en cache, sélectionnez **Vrai** pour **Grappe activée**

10d Cliquez sur **Enregistrer**.

10e Redémarrez le serveur.

10f (Conditionnel) Pour utiliser des paramètres locaux, répétez cette procédure pour chaque serveur de la grappe.

15.6 Création et déploiement des pilotes pour les applications d'identité

La procédure d'installation de RBPM ajoute les fichiers nécessaires à la création des pilotes pour les applications d'identité. La prise en charge de la configuration du pilote vous permet d'effectuer les tâches suivantes :

- Associer un pilote d'application utilisateur unique à un pilote de service de rôles et de ressources.
- Associer une application utilisateur unique à un pilote d'application utilisateur.

Avant toute tentative de configuration des pilotes, assurez-vous que vous disposez bien de tous les paquetages nécessaires dans le catalogue de paquetages de Designer. Lors de la création d'un nouveau projet Identity Manager, l'interface utilisateur vous invite automatiquement à importer plusieurs paquetages dans le nouveau projet.

- Section 15.6.1, « Création du pilote d'application utilisateur », page 221
- Section 15.6.2, « Configuration du pilote d'application utilisateur pour la mise en grappe », page 222
- Section 15.6.3, « Création du pilote du service de rôles et de ressources », page 222
- Section 15.6.4, « Déploiement des pilotes de l'application utilisateur », page 223

15.6.1 Création du pilote d'application utilisateur

Le pilote d'application utilisateur fait non seulement office de composant d'exécution, mais également de wrapper de stockage pour les objets d'annuaire (comprenant les artéfacts d'exécution de l'application utilisateur). Il est chargé de stocker les données de configuration d'un environnement spécifiques à l'application. En outre, le pilote avertit la couche d'abstraction d'annuaire lorsque des valeurs de données importantes changent dans le coffre-fort d'identité. Cette notification provoque la mise à jour du cache de la couche d'abstraction de l'annuaire.

1 Ouvrez votre projet dans Designer.

2 Dans la vue **Modélisateur > Provisioning**, sélectionnez **Application utilisateur** dans la palette.

3 Faites glisser l'icône de l'**application utilisateur** dans la vue **Modélisateur**.

4 Dans l'assistant de configuration des pilotes, sélectionnez le paquetage **Data Collection Service Base**, puis cliquez sur **Suivant**.

5 À l'invite permettant d'installer plusieurs paquetages supplémentaires, cliquez sur **OK**.

6 (Facultatif) Spécifiez le nom de ce pilote.

Cliquez sur **Suivant**.

7. Dans la fenêtre de paramètres de connexion, indiquez l'ID et le mot de passe de l'administrateur de l'application utilisateur.
8. Indiquez l'hôte et le port pour le serveur de l'application utilisateur.
9. Indiquez le contexte d'application du serveur de l'application utilisateur.
10. (Facultatif) Pour autoriser l'administrateur du provisioning à démarrer des workflows au nom d'une personne pour laquelle il a été désigné proxy, définissez le paramètre **Autoriser le remplacement de l'initiateur** sur **Oui**.
11. Dans la fenêtre **Confirmer les tâches d'installation**, cliquez sur **Terminer**.

15.6.2 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**.

15.6.3 Création du pilote du service de rôles et de ressources

L'application utilisateur fait appel au pilote du service de rôles et de ressources pour gérer les processus de traitement d'interface dorsale applicables aux ressources. Par exemple, il gère toutes les requêtes de ressource, lance les workflows pour ces dernières et initie également leur processus de provisioning.

1. Ouvrez votre projet dans Designer.
2. Dans la vue **Modélisateur > Provisioning**, sélectionnez **Service de rôle** dans la palette.
3. Faites glisser l'icône du **service de rôle** dans la vue **Modélisateur**.
4. Dans l'assistant de configuration des pilotes, sélectionnez le paquetage **Role and Resource Service Base**, puis cliquez sur **Suivant**.
5. (Conditionnel) S'il s'agit du premier pilote vous installez dans Designer, cliquez sur **OK** pour installer le paquetage **Common Settings Advanced Edition**.
   - **5a** Indiquez l'URL du serveur de l'application utilisateur.
   - **5b** Spécifiez le DN eDirectory de l'administration de l'application utilisateur.

5c Indiquez le DN LDAP du compte de service de provisioning de l'application utilisateur. Il peut s'agir du même compte que l'administrateur de votre application utilisateur ou d'un autre compte.

Si une requête de provisioning de rôle ou de ressource est initiée par ce compte de service, les approbations ou les workflows de provisioning associés à ce rôle ou cette ressource sont contournés.

6 (Facultatif) Spécifiez le nom de ce pilote.

7 Cliquez sur **Suivant**.

8 Dans la fenêtre Connexion workflow/application utilisateur, indiquez le DN du conteneur de base du groupe d'utilisateurs et le pilote de l'application utilisateur que vous venez de créer.

Puisque le pilote n'a pas encore été déployé, la fonction de navigation n'affiche pas le pilote de l'application utilisateur que vous venez de configurer. Vous devez peut-être saisir le DN du pilote.

9 Spécifiez l'URL de l'application utilisateur.

10 Indiquez le DN LDAP du compte administrateur de l'application utilisateur.

Le compte administrateur de l'application utilisateur s'authentifie auprès de l'application utilisateur afin de lancer le workflow d'approbation. Pour plus d'informations, reportez-vous à la Section 15.2.2, « Assignation de droits aux comptes de l'administrateur du coffre-fort d'identité et de l'administrateur de l'application utilisateur », page 200.

11 Saisissez le mot de passe de l'administrateur de l'application utilisateur.

12 Cliquez sur **Suivant**.

13 Dans la fenêtre Confirmer les tâches d'installation, cliquez sur **Terminer**.

15.6.4 Déploiement des pilotes de l'application utilisateur

Les pilotes de l'application utilisateur et du service de rôles et de ressources ne seront utilisables qu'une fois déployés.

REMARQUE : lorsque vous répliquez un environnement eDirectory, vous devez vous assurer que les répliques contiennent bien l'objet Serveur NCP pour Identity Manager. Identity Manager est limité aux répliques locales d'un serveur. Pour cette raison, le pilote de service de rôles et de ressources risque de ne pas démarrer correctement si l'objet Serveur est manquant sur un serveur secondaire.

Pour déployer les pilotes :

1 Ouvrez votre projet dans Designer.

2 Dans la vue **Modélisateur** ou **Aperçu**, sélectionnez l'ensemble de pilotes.

3 Cliquez sur **En direct > Déployer**.

15.7 Fin de l'installation des applications d'identité

Cette section fournit des instructions concernant les opérations à exécuter éventuellement après l'installation de l'application d'identité et de son infrastructure :

- Section 15.7.1, « Vérification de l'état de santé du serveur dans un environnement de grappe », page 224
- Section 15.7.2, « Création manuelle du schéma de base de données », page 224

15.7.1 Vérification de l'état de santé du serveur dans un environnement de grappe

Pour plus d'informations, reportez-vous à la section « Vérification de l'état de santé du serveur » page 216

15.7.2 Création manuelle du schéma de base de données

Lorsque vous installez les applications d'identité, vous pouvez repousser la connexion à la base de données ou créer des tables dans la base de données. Si vous ne disposez pas d'autorisations pour la base de données, vous pouvez être amené à sélectionner cette option. Le programme d'installation crée un fichier SQL que vous pouvez utiliser pour créer le schéma de base de données. Une fois l'installation terminée, vous avez également la possibilité de recréer les tables de la base de données sans toutefois devoir réinstaller. Pour ce faire, supprimez la base de données des applications d'identité et créez-en une nouvelle portant le même nom.

Utilisation du fichier SQL pour générer le schéma de base de données

Cette section présume que le programme d'installation a créé un fichier SQL que vous pouvez exécuter pour créer le schéma de base de données. Si vous ne disposez pas du fichier SQL, reportez-vous à la section « Création manuelle du fichier SQL pour générer le schéma de base de données » page 225.

REMARQUE : n'utilisez pas SQL*Plus pour exécuter le fichier SQL. La longueur des lignes du fichier dépasse 4 000 caractères.

---

1. Arrêtez le serveur d'applications
2. Connectez-vous au serveur de base de données.
3. Supprimez la base de données utilisée par les applications d'identité.
4. Créez une nouvelle base de données portant le même nom que celle supprimée à l'Étape 3.
5. Accédez au script SQL créé par la procédure d'installation, situé par défaut dans le répertoire/*chemin_installation*/userapp/sql.
6. Faites en sorte que l'administrateur de la base de données exécute le script SQL pour créer et configurer la base de données de l'application utilisateur.
7. Relancez Tomcat.

Création manuelle du fichier SQL pour générer le schéma de base de données

Vous pouvez recréer les tables de base de données après l'installation, sans qu'il soit nécessaire de réinstaller et sans avoir le fichier SQL. Cette section vous aide à créer le schéma de base de données dans le cas où vous n'avez pas le fichier SQL.

1. Arrêtez Tomcat.
2. Connectez-vous au serveur qui héberge votre base de données des applications d'identité.
3. Supprimez la base de données existante.
4. Créez une nouvelle base de données portant le même nom que celle que vous avez supprimée à l'Étape 3.
5. Dans un éditeur de texte, ouvrez le fichier `NetIQ-Custom-Install.log`. Il est situé par défaut à la racine du répertoire d'installation des applications d'identité. Exemple :

   ```
   C:\NetIQ\idm\apps\UserApplication
   ```

6. Recherchez et copiez la commande ci-dessous à partir du fichier `NetIQ-Custom-Install.log`.

   ```
   C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m  -Dwar.context.name=IDMProv -
   Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -
   Duser.container="o=data" -jar C:\NetIQ\idm\jre\liquibase.jar --
   databaseClass=liquibase.database.core.PostgresDatabase --
   driver=org.postgresql.Driver --
   classpath=C:\NetIQ\idm\apps\postgresql\postgresql-9.4.1212jdbc42.jar
   C:\NetIQ\idm\apps\UserApplication\IDMProv.war --
   changeLogFile=DatabaseChangeLog.xml  --url="jdbc:postgresql://localhost:5432/
   idmuserappdb" --contexts="prov,newdb" --logLevel=info --
   logFile=C:\NetIQ\idm\apps\UserApplication\db.out --username=******** --
   password=******** update
   ```

7. Connectez-vous au serveur sur lequel vous avez installé la base de données des applications d'identité.
8. Dans un terminal, collez la chaîne de commande que vous avez copiée.

   REMARQUE : la commande doit être `updateSQL`. Si seule la mention `update` est indiquée, remplacez la commande par `updateSQL`.

   ---

9. Dans la commande, remplacez les astérisques (*) qui représentent le nom d'utilisateur et mot de passe d'accès à la base de données par les valeurs réelles requises pour l'authentification. En outre, vérifiez que le nom du fichier SQL n'est pas déjà utilisé.
10. Exécutez la commande.
11. (Facultatif) Si le processus génère un fichier SQL au lieu d'alimenter la base de données, indiquez à votre administrateur de base de données le fichier à importer sur le serveur de la base de données. Pour plus d'informations, reportez-vous à la section « Utilisation du fichier SQL pour générer le schéma de base de données » page 224.
12. Une fois que l'administrateur de la base de données a importé le fichier SQL, démarrez Tomcat.

15.7.3 Importation manuelle des applications d'identité et des certificats Identity Reporting dans le coffre-fort d'identité.

- Si vous avez des certificats personnalisés pour les applications d'identité et le composant Identity Reporting, importez ces certificats dans le coffre-fort d'identité à l'emplacement `C:\NetIQ\eDirectory\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 <User Application certificate alias> -
  srckeystore  <backup cacert> -srcstorepass changeit -destkeystore
  C:\NetIQ\eDirectory\jre\lib\security\cacerts
  ```

- 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`.

15.7.4 Enregistrement de la clé principale

NetIQ recommande de copier la clé principale codée et de l'enregistrer en lieu sûr immédiatement après l'installation. Si cette installation est sur le premier membre d'une grappe, utilisez cette clé principale codée lors de l'installation des applications d'identité sur d'autres membres de la grappe.

AVERTISSEMENT : conservez toujours une copie de la clé maîtresse codée. Vous avez besoin de la clé principale codée pour accéder à nouveau aux données codées en cas de perte de la clé principale. Par exemple, vous aurez peut-être besoin de la clé après une panne matérielle.

15.7.5 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*.

15.7.6 Modification du nom de contexte par défaut pour l'application utilisateur

Au lieu d'utiliser le nom de contexte par défaut, vous pouvez créer un contexte selon vos besoins organisationnels. Vous pouvez modifier le nom du contexte en effectuant les opérations suivantes :

1. Arrêtez le service Tomcat à l'aide du fichier `services.msc`.
2. Accédez au répertoire de l'application utilisateur situé à l'emplacement `C:\NetIQ\idm\apps\UserApplication`.

3 Lancez l'utilitaire configupdate en mode GUI.

Assurez-vous que l'option `use_console` est définie sur `false` dans le fichier `configupdate.bat.properties`.

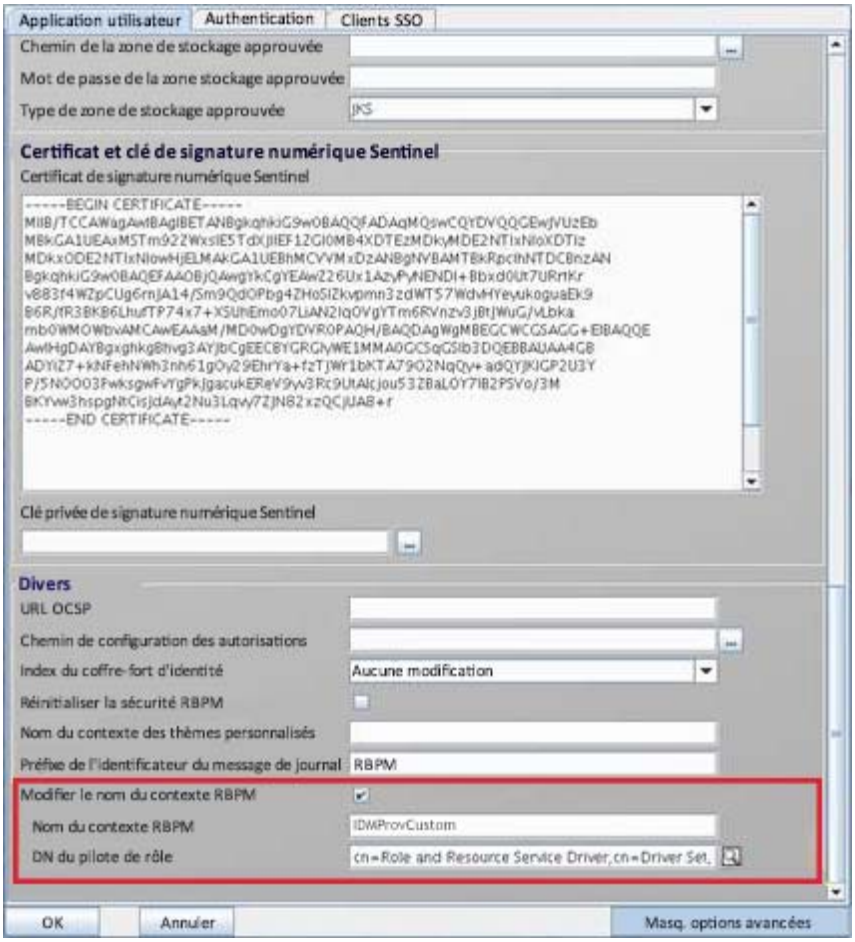
4 Sous l'onglet **Application utilisateur**, cliquez sur **Aff. options avancées** et effectuez les opérations suivantes :

4a Sélectionnez **Modifier le nom du contexte RBPM**.

4b Spécifiez le nom de contexte personnalisé dans **Nom du contexte RBPM**. Par exemple : `IDMProvCustom`.

4c Recherchez et le DN du pilote de rôles et sélectionnez-le. Par exemple : `cn=Role and Resource Service Driver,cn=Driver Set,o=system`.

4d Cliquez sur **OK**.



5 Vérifiez que le fichier WAR a été renommé.

- Accédez au dossier `Tomcat webapps`, puis vérifiez si l'entrée `IDMProvCustom.war` a été mise à jour.
- Accédez au fichier de propriétés `ism-configuration` situé dans `\TOMCAT_INSTALLED_HOME\conf` et vérifiez si l'entrée `portal.context` indique le nouveau nom de contexte.

6 Mettez à jour votre base de données avec le nouveau nom de contexte à l'aide du fichier `update-context.bat` situé dans `C:\NetIQ\idm\apps\UserApplication`.

Émettez la commande suivante pour exécuter le fichier `update-context.bat`.

```
ua:C:\NetIQ\idm\apps\UserApplication # vi update-context.bat
```

Vous devez voir les entrées suivantes sur votre écran :

```
# copy and paste or execute this script before changing context name

# Substitute your new context where indicated

#

C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m  -Dwar.context.name=[New Context
Here] -Ddriver.dn=[UA Driver DN] -jar
C:\NetIQ\idm\apps\UserApplication\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase  --
driver=org.postgresql.Driver  --classpath=
C:\NetIQ\idm\apps\postgres\postgresql-9.4.1212.jdbc42.jar:
C:\NetIQ\idm\apps\tomcat\webapps\IDMProv.war --
changeLogFile=UpdateProducerId.xml   --url="jdbc:postgresql://localhost:5432/
idmuserappdb?compatible=true" --contexts="prov,updatedb" --logLevel=debug --
username=******** --password=******** update
```

Par exemple, exécutez le script suivant si vous utilisez une base de données PostgreSQL :

```
C:\NetIQ\idm\apps\jre\bin\java -Xms256m -Xmx256m  -
Dwar.context.name=IDMProvCustom  -Ddriver.dn= cn=Role and Resource Service
Driver,cn=driverset1,o=system -jar
C:\NetIQ\idm\apps\UserApplication\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase  --
driver=org.postgresql.Driver  --classpath=
C:\NetIQ\idm\apps\postgres\postgresql-9.4.1212.jdbc42.jar:
C:\NetIQ\idm\apps\tomcat\webapps\IDMProv.war --
changeLogFile=UpdateProducerId.xml   --url="jdbc:postgresql://<Database
Server:5432/idmuserappdb?compatible=true" --contexts="prov,updatedb" --
logLevel=debug --username=dbadmin --password=******** update
```

où

`-Dwar.context.name=IDMProvCustom` indique le nouveau contexte.

`-Ddriver.dn ="cn=User Application Driver,cn=driverset1,o=system"` spécifie le DN du pilote de l'application utilisateur.

`--username=dbadmin` spécifie le nom de l'administrateur de base de données qui peut créer des tables de base de données, des vues et d'autres artefacts.

IMPORTANT : ne modifiez pas les détails du pilote de base de données dans le script pour les autres bases de données prises en charge.

---

7 Assurez-vous que les tables de base de données contiennent le nouveau nom de contexte.

Nom des tables	Colonne à vérifier
PORTALPRODUCERS	`producerid`
PORTALPRODUCERREGISTRY	`producerid`
PORTALREGISTRY	`producerid`
PORTALPORTLETSETTINGS	`producerid`
PORTALPORTLETHANDLES	`producerid`
PROFILEGROUPPREFERENCES	`ElementID`

Par exemple, exécutez la commande SQL suivante pour vérifier le nouveau nom de contexte dans la table `PORTALPRODUCERS` :

```
Select * from PORTALPRODUCERS;
```

La commande doit renvoyer uniquement le nouveau nom de contexte.

8 Démarrez le service Tomcat à l'aide du fichier `services.msc`.

15.7.7 Reconfiguration du fichier WAR des applications d'identité

Pour mettre à jour le fichier WAR des applications d'identité, exécutez l'utilitaire de configuration de RBPM.

1 Exécutez l'utilitaire dans le répertoire d'installation à l'aide de la commande `configupdate.bat`.

Pour plus d'informations sur les paramètres de l'utilitaire, reportez-vous au Chapitre 15.8, « Configuration des paramètres pour les applications d'identité », page 235.

2 Déployez le nouveau fichier WAR sur votre serveur d'applications.

Dans le cas d'un serveur Tomcat unique, les modifications sont appliquées au fichier WAR déployé.

15.7.8 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.

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 :

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 15.8.1, « Exécution de l'utilitaire de configuration des applications d'identité », page 235.
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.

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. Pour plus d'informations sur la configuration du mot de passe, reportez-vous au Chapitre 14.2, « Installation du composant de gestion des mots de passe pour Identity Manager », page 179.

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 231.
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.

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.

Utilisation du fournisseur hérité pour la gestion des mots de passe oubliés

Au lieu de SSPR, vous pouvez utiliser le fournisseur hérité d'Identity Manager pour la gestion des mots de passe oubliés. Si vous choisissez ce fournisseur, vous n'avez pas besoin d'installer SSPR. Toutefois, vous devez réassigner les autorisations des utilisateurs pour accéder aux pages partagées pour la gestion des mots de passe. Cette section présente la procédure nécessaire pour effectuer ces opérations :

- « Configuration du fournisseur hérité pour la gestion des mots de passe oubliés » page 232
- « Nouvelle assignation d'autorisations pour les pages de gestion des mots de passe » page 232

Pour plus d'informations sur le fournisseur hérité, reportez-vous à la Section 4.4.2, « Présentation du fournisseur hérité pour la gestion des mots de passe », page 33. Pour plus d'informations sur les autorisations et pages partagées, reportez-vous à la section « Page Administration » (Administration de pages) du *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager - Guide de l'administrateur des applications d'identité).

Configuration du fournisseur hérité pour la gestion des mots de passe oubliés

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 15.8.1, « Exécution de l'utilitaire de configuration des applications d'identité », page 235.
3. Dans l'utilitaire, accédez à **Authentification > Gestion des mots de passe**.
4. Pour **Fournisseur de gestion des mots de passe**, spécifiez **Application utilisateur (héritée)**.
5. Pour **Mot de passe oublié**, spécifiez **Interne**.
6. Accédez à **Clients SSO > Réinitialisation de mot de passe en self-service**.
7. Pour **URL de redirection OSP**, le paramètre doit être vide.
8. Enregistrez les modifications, puis fermez l'utilitaire.

Nouvelle assignation d'autorisations pour les pages de gestion des mots de passe

Les paramètres pour les applications d'identité sont définis par défaut sur SSPR au cours de l'installation. Vous devez assigner ou réassigner les autorisations concernant les utilisateurs, groupes ou conteneurs auxquels vous souhaitez accorder l'accès aux pages partagées de gestion des mots de passe. Lorsque vous assignez à des utilisateurs l'autorisation `Afficher` pour une page de conteneur ou une page partagée, les utilisateurs peuvent accéder à cette page et la visualiser dans une liste de pages disponibles.

1. Vérifiez qu'Identity Manager utilise le fournisseur hérité. Pour plus d'informations, reportez-vous à la section « Configuration du fournisseur hérité pour la gestion des mots de passe oubliés » page 232.
2. Connectez-vous à l'application utilisateur en tant qu'administrateur. Par exemple, connectez-vous en tant que `uaadmin`.
3. Accédez à **Administration > Admin. des pages**.
4. Dans le volet **Pages partagées**, accédez à **Gestion des mots de passe**.
5. Sélectionnez la page pour laquelle vous souhaitez définir des autorisations. Par exemple, Modifier le mot de passe ou Réponse de vérification d'identité de mot de passe.
6. Dans le volet de droite, cliquez sur **Assigner des autorisations**.
7. Dans **Afficher**, sélectionnez les utilisateurs, les groupes ou les conteneurs à assigner à la page.
8. (Facultatif) Pour que seul un administrateur de l'application puisse accéder à la page spécifiée, sélectionnez **Autorisation d'affichage accordée à l'administrateur uniquement**.
9. Cliquez sur **Enregistrer**.
10. Répétez la procédure de l'Étape 5 à l'Étape 9 pour chaque page à configurer.
11. Sélectionnez l'icône **Accueil** pour revenir au tableau de bord.
12. Accédez à **Applications**, puis sélectionnez ⚙.
13. Sur la page **Gérer les applications**, remplacez le lien vers SSPR par le lien pour UserApp PwdMgt.

Pour plus d'informations, reportez-vous à la section « Mise à jour des liens SSPR dans le tableau de bord pour un environnement distribué ou de grappe » page 234 et à l'*Aide relative aux applications d'identité*.

14 Déconnectez-vous, puis redémarrez Tomcat.

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 :

- « Spécification d'un fichier WAR externe de gestion des mots de passe oubliés » page 233
- « Test de la configuration du fichier externe pour les mots de passe oubliés » page 234
- « Configuration de la communication SSL entre serveurs d'applications » page 234

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 15.8.1, « Exécution de l'utilitaire de configuration des applications d'identité », page 235.

   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 234.

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.

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**.

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.

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.

15.8 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.bat`) est situé par défaut dans un sous-répertoire d'installation des applications d'identité (`C:\NetIQ\idm\apps\UserApplication`).

REMARQUE : 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.

15.8.1 Exécution de l'utilitaire de configuration des applications d'identité

1. Ouvrez le fichier `configupdate.properties` dans un éditeur de texte et vérifiez que les options suivantes sont configurées :

   ```
   edit_admin="true"
   ```

   ```
   use_console="false"
   ```

2. À l'invite de commande, exécutez l'utilitaire de configuration (`configupdate.bat`).

   REMARQUE : vous devrez peut-être attendre quelques minutes pour que l'utilitaire démarre.

15.8.2 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.bat`.
- 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.bat`.

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.bat`.
- 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.bat`.
- 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.bat`.

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 : `C:\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 renseigner 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.

15.8.3 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 247
- « Valeurs de conservation du rapport » page 247
- « Modifier le paramètre local » page 248
- « Configuration du rôle » page 248

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 : `C:\NetIQ\idm\apps\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**

15.8.4 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 248
- « Configuration de l'authentification » page 249
- « Méthode d'authentification » page 250
- « Gestion des mots de passe » page 250
- « Clé et certificat de signature numérique de Sentinel » page 251

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.

15.8.5 Paramètres des clients SSO

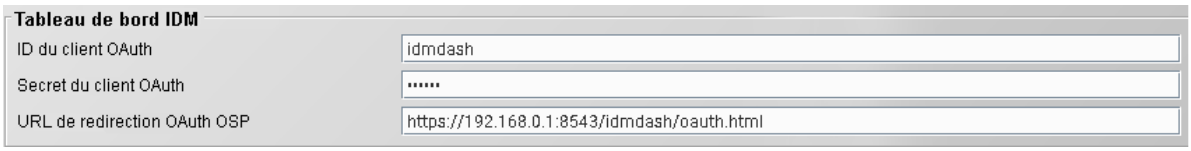
Lors de la configuration des applications d'identité, cet onglet permet de définir les valeurs pour la gestion d'un accès Single Sign-On aux applications.

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 15-2 *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 réacheminement 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

Indique le nom à utiliser pour 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

Indique le mot de passe du client Single Sign-on pour l'administrateur Identity Manager.

URL de redirection OAuth OSP

Requis

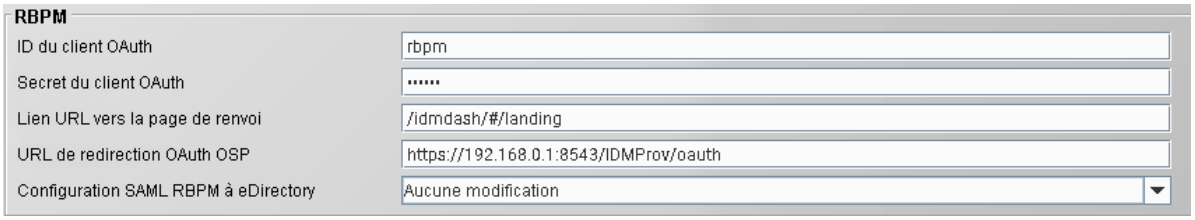
Indique l'URL absolue vers laquelle le serveur d'authentification redirige un client de navigateur une fois l'authentification terminée.

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 15-3 *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

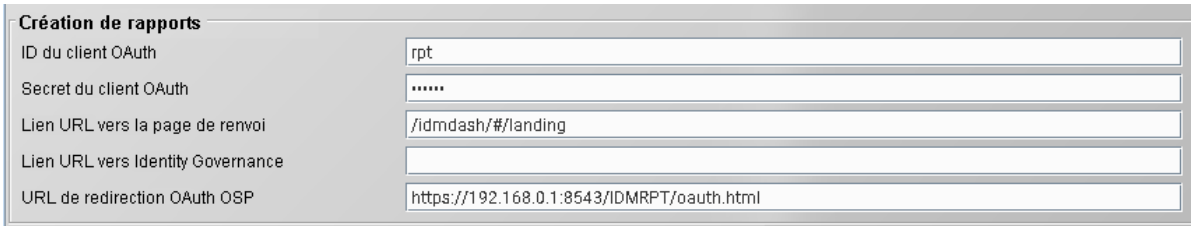
Requis

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 15-4 *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`. Par 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`. Par 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

Indique le nom à 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

Indique 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

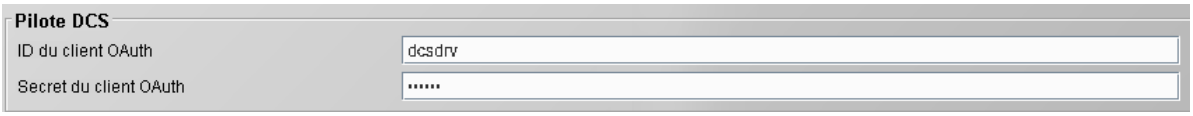
Indique l'URL absolue vers laquelle le serveur d'authentification redirige un client de navigateur une fois l'authentification terminée.

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 15-5



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`.

15.8.6 Paramètres de l'audit CEF

Cette section définit les valeurs pour gérer les paramètres de l'audit CEF.

Envoyer des événements d'audit

Indique si vous souhaitez utiliser CEF pour auditer les événements dans les applications d'identité.

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 du cache.

V Installation d'Identity Reporting

Cette section vous explique les différentes étapes à effectuer pour installer les composants qui vous permettront de générer des rapports. Cette procédure d'installation inclut tous les composants nécessaires à l'application :

- Module NetIQ Identity Reporting
- Pilote Identity Manager MSGW (Managed System Gateway)
- Pilote Identity Manager DCS (Data Collection Service)

Les fichiers d'installation sont situés dans le répertoire `\products\Reporting` au sein du fichier image `.iso` pour le paquetage d'installation d'Identity Manager. Par défaut, le programme d'installation installe les composants à l'emplacement `C:\NetIQ\idm\apps\IDMReporting`.

Pour plus de commodité, le kit d'installation d'Identity Manager inclut Sentinel Log Management for IGA (Sentinel) que vous pouvez utiliser comme service d'audit intégré. Pour plus d'informations, reportez-vous à la section Installation de Sentinel Log Management for Identity Governance and Administration du Guide d'installation de NetIQ Identity Manager pour Linux.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous au Chapitre 16, « Planification de l'installation du module Identity Reporting », page 259.

16 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.

16.1 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 à la Section 3.3.4, « Identity Reporting », page 25.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.
❑	3. Prenez en compte les considérations relatives à l'installation d'Identity Reporting. Pour plus d'informations, reportez-vous à la Section 16.3, « Conditions préalables à l'installation des composants du module Identity Reporting », page 261.
❑	4. Vérifiez les configurations matérielle et logicielle requises pour les ordinateurs qui hébergeront Identity Reporting. Pour plus d'informations, reportez-vous à la Section 16.5, « Configuration système requise pour Identity Reporting », page 262.
❑	5. Vérifiez l'installation des applications d'identité. Pour plus d'informations, reportez-vous au Chapitre 15.1, « Planification de l'installation des applications d'identité », page 189.
❑	6. Pour auditer les événements, installez Sentinel sur un serveur Linux. Pour plus d'informations, reportez-vous à la section Installation de Sentinel Log Management for Identity Governance and Administration du Guide d'installation de NetIQ Identity Manager pour Linux.
❑	7. Assurez-vous que le serveur sur lequel vous voulez installer Identity Reporting est un serveur d'applications, tel que Tomcat. Pour plus d'informations, reportez-vous au Chapitre 12.2, « Installation de PostgreSQL et de Tomcat », page 164.

	Éléments de la liste de contrôle
❑	8. (Conditionnel) Afin d'utiliser le service Apache Log4j pour enregistrer des événements dans Tomcat, vérifiez que vous disposez des fichiers appropriés. Pour plus d'informations, reportez-vous à la Section 13.1.4, « Utilisation du service Apache Log4j pour consigner les événements de connexion », page 171.
❑	9. Installation d'Identity Reporting : ◆ Pour une installation guidée, reportez-vous à la Section 17.1, « Installation d'Identity Reporting avec l'assistant », page 265. ◆ Pour une installation silencieuse, reportez-vous à la Section 17.2, « Installation silencieuse d'Identity Reporting », page 270.
❑	10. Terminez la configuration d'Identity Reporting. Pour plus d'informations, reportez-vous au Chapitre 18, « Configuration d'Identity Reporting », page 275.
❑	11. Configurez les pilotes MSG (Managed System Gateway) et DCS (Data Collection Service). Pour plus d'informations, reportez-vous à la Section 19.1, « Configuration des pilotes pour Identity Reporting », page 277.
❑	12. Déployez, puis lancez les pilotes. Pour plus d'informations, reportez-vous à la Section 19.2, « Déploiement et démarrage des pilotes pour Identity Reporting », page 283.
❑	13. Configurez l'environnement pour les pilotes. Pour plus d'informations, reportez-vous à la Section 19.3, « Configuration de l'environnement d'exécution », page 288.
❑	14. Configurez Identity Manager et eDirectory pour envoyer des données vers les pilotes. Pour plus d'informations, reportez-vous à la Section 19.4, « Configuration des drapeaux d'audit pour les pilotes », page 298.

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

Vous pouvez installer Sentinel, Identity Reporting et les pilotes de création de rapports sur le même serveur. Toutefois, en raison de la charge de travail, NetIQ recommande d'installer Sentinel et les composants de création de rapports 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 :

- Invitation à choisir une plate-forme de serveur d'applications
- Déploiement dans Tomcat du fichier WAR client (DCS et Reporting), lequel contient les composants de l'interface utilisateur permettant de créer des rapports
- Déploiement du fichier WAR core (DCS et Reporting), lequel contient les principaux services REST requis pour la création de rapports
- Déploiement du fichier WAR d'API, lequel contient la documentation des services REST requis pour la création de rapports

- Déploiement du fichier WAR d'API, lequel contient le service de collecte de données d'Identity Manager requis pour la création de rapports
- 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
- Création de comptes utilisateur pour Identity Reporting (**idmrptsrv** et **idmrptuser**)
- Création des comptes utilisateur permettant d'interagir avec Sentinel (**appuser** et **rptuser**)

16.3 Conditions préalables à l'installation des composants du module 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 de l'application utilisateur
  - Sentinel installé sur un ordinateur Linux distinct.
  - Pilote pour le service de collecte de données (DCS, Data Collection Service)
  - Pilote pour le service de la passerelle système gérée (MSGW, Managed System Gateway)

  Pour plus d'informations sur les versions et les correctifs requis pour ces composants, reportez-vous aux dernières notes de version. Pour plus d'informations sur l'installation des pilotes, reportez-vous au Chapitre 19, « Gestion des pilotes pour Reporting », page 277.
- N'installez pas Identity Reporting sur un serveur appartenant à un environnement de grappes.
- Si vous souhaitez utiliser une base de données autre que la base de données locale, vous devez en créer une sur un autre serveur, puis spécifier les détails au cours de l'installation d'Identity Reporting.
- (Facultatif) Pour générer des rapports à partir d'une base de données Oracle 12c, vous devez installer le fichier JDBC approprié. Pour plus d'informations, reportez-vous à la Section 18.1, « Génération de rapports à partir d'une base de données Oracle », page 275.
- (Facultatif) Vous pouvez utiliser votre propre programme d'installation Tomcat, plutôt que celui fourni dans le kit d'installation d'Identity Manager. Toutefois, afin d'utiliser le service Apache Log4j avec votre version de Tomcat, assurez-vous d'avoir installé les fichiers appropriés. Pour plus d'informations, reportez-vous à la Section 13.1.4, « Utilisation du service Apache Log4j pour consigner les événements de connexion », page 171.
- 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.bat` pour Tomcat.

  Par défaut, le programme d'installation simplifiée de Tomcat place le fichier `setenv.bat` dans le répertoire `C:\NetIQ\idm\apps\tomcat\bin`. Le programme d'installation configure également l'emplacement JRE dans le fichier.

16.4 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**

16.5 Configuration système requise pour Identity Reporting

Cette section décrit la configuration minimale requise pour le(s) serveur(s) sur le(s)quel(s) vous souhaitez installer les composants Identity Reporting.

Catégorie	Configuration requise
Processeur	Processeur 1 GHz

Catégorie	Configuration requise
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 : ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 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.
Système 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 ◆ Virtualisation de Windows Server 2012 R2 avec Hyper-V (prise en charge) 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 2014, 2016
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)

Catégorie	Configuration requise
Navigateur Web	Un des navigateurs suivants (versions minimales) : **Desktop** ◆ Apple Safari 9 ◆ Apple Safari 5.1.7 pour Windows ◆ Google Chrome 61 ◆ Microsoft Internet Explorer 11 ◆ Mozilla Firefox 51 **iPad** ◆ Apple Safari 9 ◆ Google Chrome 61 **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

17 Installation d'Identity Reporting

Cette section décrit la procédure d'installation d'Identity Reporting.

17.1 Installation d'Identity Reporting avec l'assistant

La procédure suivante décrit comment installer Identity Reporting à l'aide d'un assistant d'installation. Pour effectuer une installation en mode silencieux sans surveillance, reportez-vous à la Section 17.2, « Installation silencieuse d'Identity Reporting », page 270.

Pour préparer l'installation, vérifiez les conditions préalables et les exigences système répertoriées à la Section 16.5, « Configuration système requise pour Identity Reporting », page 262. Reportez-vous également aux notes de version relatives à votre édition.

1. Connectez-vous à l'ordinateur sur lequel vous voulez installer Identity Reporting.
2. Arrêtez Tomcat.
3. (Conditionnel) Si vous utilisez le fichier image `.iso` du paquetage d'installation d'Identity Manager, accédez au répertoire contenant les fichiers d'installation d'Identity Reporting. Ceux-ci sont situés par défaut dans le répertoire `\products\Reporting`.
4. (Facultatif) Si vous avez téléchargé les fichiers d'installation d'Identity Reporting à partir du site Web de téléchargement NetIQ, procédez de la manière suivante :
   - **4a** Accédez au fichier `.tgz` pour localiser l'image téléchargée.
   - **4b** Lancez l'extraction du contenu du fichier dans un dossier sur l'ordinateur local.
5. À partir du répertoire qui contient les fichiers d'installation, exécutez le fichier `rpt-install-win.exe`.
6. Dans le programme d'installation, indiquez la langue que vous souhaitez utiliser pour l'installation, puis cliquez sur **OK**.
7. Lisez attentivement le texte d'introduction, puis cliquez sur **Suivant**.
8. Acceptez l'accord de licence, puis cliquez sur **Suivant**.
9. Terminez la procédure guidée, à l'aide des paramètres suivants :
   - **Dossier d'installation**

     Spécifie le chemin d'un répertoire dans lequel le programme d'installation crée les fichiers d'application, notamment les fichiers journaux d'installation, les scripts du programme auxiliaire et les scripts de configuration.
   - **Reporting Setup** (Installation de Reporting)

     Représente l'environnement et ses paramètres, auxquels vous souhaitez ajouter Identity Reporting. Pour **Identity Manager**, spécifiez les valeurs suivantes :

Serveur du coffre-fort d'identité

Indique le nom d'hôte au serveur eDirectory.

Port LDAP sécurisé

Spécifie le port à utiliser pour établir une connexion LDAP au serveur eDirectory via le protocole SSL. Le numéro de port par défaut est 636.

Page d'accueil du provisioning

Spécifie l'emplacement d'origine du provisioning d'Identity Manager. Il peut s'agir de l'URL complète du serveur d'applications ou d'un chemin relatif pour l'URL.

- **Détails du serveur d'applications**

Représente le serveur Tomcat sur lequel vous souhaitez exécuter Identity Reporting. Le serveur d'applications doit être préalablement installé.

Secondaire

Indique si l'installation actuelle se trouve sur un noeud secondaire d'une grappe.

Dossier racine de Tomcat

Indique le chemin d'accès à l'instance de Tomcat. Par exemple : `C:\NetIQ\idm\apps\tomcat`.

Dossier de la base JRE Java

Indique l'emplacement du dossier de base du JRE Java.

Ce chemin contient le fichier de l'utilitaire de mise à jour de configuration et est utilisé pour lancer cet utilitaire après l'installation d'Identity Reporting.

- **Adresse de l'application**

Représente les paramètres du serveur qui héberge Identity Reporting.

Protocole

Permet d'indiquer si vous voulez utiliser *http* ou *https*. Pour utiliser SSL pour les communications, entrez `https`.

Nom d'hôte

Spécifie le nom DNS ou l'adresse IP du serveur Tomcat. N'utilisez pas `localhost`.

Port

Indique le port que Tomcat doit utiliser pour communiquer avec l'application Identity Reporting.

Se connecter à un serveur d'authentification externe

Indique si une autre instance de Tomcat héberge le serveur d'authentification (OSP). Le serveur d'authentification dispose de la liste des utilisateurs qui peuvent se connecter à Identity Reporting.

Si vous sélectionnez cette option, indiquez les valeurs correspondantes dans les champs **Protocole**, **Nom d'hôte** et **Port** pour le serveur d'authentification.

- **Détails du serveur d'authentification**

Spécifie le mot de passe du service Identity Reporting.

Identity Manager utilise ce mot de passe pour se connecter au client OSP sur le serveur d'authentification.

- **Détails de la base de données**

Représente les paramètres de la base de données de création de rapports, lesquels vous permettent notamment d'indiquer si vous souhaitez que la procédure d'installation crée la base de données ou génère un fichier SQL permettant de créer la base de données ultérieurement.

Nom de la base de données

Spécifiez le nom de la base de données en fonction de vos besoins :

- Dans le cas d'une nouvelle installation, spécifiez le nom de votre base de données de création de rapports. Par exemple, `idmrptdb` ou `SIEM`.
- Si vous effectuez une migration à partir d'EAS, spécifiez le nom de la base de données EAS, par exemple, `SIEM`.

Hôte de la base de données

Spécifiez l'hôte de la base de données en fonction de vos besoins :

- Dans le cas d'une nouvelle installation, spécifiez le nom DNS ou l'adresse IP du serveur sur lequel la base de données doit être créée.
- Si vous effectuez une migration à partir d'EAS, spécifiez le nom DNS ou l'adresse IP du serveur qui héberge votre base de données `SIEM`.

Type de base de données

Sélectionnez la base de données que vous souhaitez utiliser.

Si vous sélectionnez **Oracle**, spécifiez les détails suivants :

- **Fichier JAR du pilote JDBC**

  Permet d'indiquer le chemin d'accès au fichier JAR du pilote JDBC Oracle. Par exemple : `C:\oracle\ojdbc7.jar`.

  Pour plus d'informations, reportez-vous à la Section 18.1, « Génération de rapports à partir d'une base de données Oracle », page 275.

- **Nom de classe du pilote JDBC**

  Permet d'indiquer la classe du pilote JDBC.

- **Type de pilote JDBC**

  Permet d'indiquer le type de pilote JDBC.

Si vous sélectionnez **PostgresSQL**, cliquez sur **Suivant**.

***Share password* (Mot de passe partagé)**

Permet de spécifier un mot de passe unique pour tous les utilisateurs d'Identity Reporting qui se connectent à la base de données.

Spécifier le mot de passe pour chaque utilisateur

Permet de spécifier un mot de passe unique pour chaque utilisateur d'Identity Reporting qui se connecte à la base de données. Vous devez spécifier un mot de passe pour `idm_rpt_data_password`, `idm_rpt_cfg_password` et `idmrptuserpassword`.

Port de base de données

Permet de spécifier le port de connexion à la base de données. Le port par défaut est 5432.

***Configure database now or at startup* (Configurer la base de données maintenant ou au démarrage)**

Indique que vous disposez des paramètres de connexion à la base de données afin que le programme d'installation puisse la créer immédiatement ou au démarrage du module de création de rapports. Vous devez également spécifier les valeurs suivantes :

- **ID utilisateur du DBA**

  Spécifie le nom du compte d'administration du serveur de base de données SIEM. Par exemple, *postgres.*

- **Mot de passe du DBA**

  Permet d'indiquer le mot de passe du compte administrateur pour la base de données.

- **Tester la connexion à la base de données :** Permet d'indiquer si vous souhaitez que le programme d'installation teste les valeurs spécifiées pour la base de données.

  Le programme d'installation tente une connexion lorsque vous cliquez sur **Suivant** ou appuyez sur **Entrée**.

  REMARQUE : vous pouvez poursuivre l'installation même si la connexion à la base de données échoue. Toutefois, une fois l'installation terminée, vous devrez créer manuellement les tables et la connexion avec la base de données. Pour plus d'informations, reportez-vous à la Section 17.3, « Génération manuelle du schéma de base de données », page 271.

***Generate SQL for later* (Générer SQL pour plus tard)**

Indique au programme d'installation de générer un fichier SQL que votre administrateur de base de données utilisera pour créer la base de données une fois la procédure d'installation terminée. Pour créer la base de données après l'installation, reportez-vous à la Section 17.3, « Génération manuelle du schéma de base de données », page 271.

- **Langue par défaut**

  Spécifie la langue qu'Identity Reporting doit utiliser pour les recherches.

- **Références du coffre-fort d'identité**

  Représente les paramètres utilisés par Identity Reporting pour se connecter au coffre-fort d'identité.

  Administrateur du coffre-fort d'identité

  Spécifie le nom distinctif de l'administrateur LDAP. Par exemple, `cn=admin`. Cet utilisateur doit déjà exister dans le coffre-fort d'identité.

  Mot de passe de l'administrateur du coffre-fort d'identité

  Spécifie le mot de passe de l'administrateur du coffre-fort d'identité.

  Chemin du fichier Keystore

  Indique le chemin d'accès complet au fichier (`cacerts`) de votre keystore du JRE utilisé par Tomcat.

  Mot de passe Keystore

  Spécifie le mot de passe pour le fichier keystore.

  DN du conteneur du rôle d'administrateur de création de rapports

  Spécifiez le DN du conteneur dans lequel figure le rôle Administrateur de rapports.

  DN de l'administrateur de création de rapports

  Spécifie un compte utilisateur existant dans le coffre-fort d'identité qui possède les droits nécessaires pour exécuter des tâches d'administration pour Identity Reporting.

- **Pilote d'application utilisateur**

  Représente le nom de votre pilote d'application, de l'ensemble de pilotes et du conteneur d'ensembles de pilotes.

  Pilote d'application utilisateur

  Permet d'indiquer le nom du pilote d'application utilisateur.

Nom de l'ensemble de pilotes

Indique le nom de l'ensemble de pilotes.

Conteneur de l'ensemble de pilotes

Indique le nom du conteneur de l'ensemble de pilotes.

- **Email Delivery** (Envoi par message électronique)

  Il s'agit des paramètres relatifs au serveur SMTP qui envoie les notifications de rapport. Pour modifier ces paramètres une fois l'installation terminée, utilisez l'utilitaire de configuration RBPM.

  Adresse électronique par défaut

  Permet de spécifier l'adresse électronique à partir de laquelle Identity Reporting envoie les 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. N'utilisez pas `localhost`.

  Port du serveur SMTP

  Permet d'indiquer le numéro de port du serveur SMTP. Le numéro de port par défaut est 465.

  Utiliser SSL pour SMTP

  Permet d'indiquer si vous voulez utiliser le protocole SSL pour les communications avec le serveur SMTP.

  Exiger l'authentification du serveur

  Permet d'indiquer si vous voulez demander une authentification pour les communications avec le serveur SMTP. Vous devez également spécifier les valeurs suivantes :

  - ***Nom d'utilisateur SMTP***

    Permet d'indiquer le nom d'un compte de connexion au serveur SMTP.

  - ***Mot de passe SMTP***

    Permet de spécifier le mot de passe d'un compte de connexion au serveur SMTP.

- **Détails du rapport**

  Paramètres relatifs aux définitions de rapport et aux rapports terminés.

  Conserver les rapports terminés pendant

  Permet d'indiquer pendant combien de temps les rapports sont conservés dans Identity Reporting avant d'être supprimés.

  Par exemple, pour six mois, tapez `6` puis sélectionnez **Mois**.

  Emplacement des définitions de rapport

  Permet d'indiquer où vous voulez stocker les définitions de rapport.

  Par exemple : `C:\NetIQ\idm\apps\IdentityReporting`.

10 Dans la fenêtre Résumé avant installation, cliquez sur **Installer**.

17.2 Installation silencieuse d'Identity Reporting

Une installation silencieuse (non interactive) n'affiche aucune interface utilisateur et ne pose aucune question à l'utilisateur. Au lieu de cela, le système utilise les informations contenues dans un fichier `.properties`. Vous pouvez lancer l'installation silencieuse en utilisant le fichier fourni par défaut ou modifier ce fichier afin de personnaliser la procédure d'installation. Pour effectuer une installation guidée, reportez-vous à la section « Installation d'Identity Reporting avec l'assistant » page 265.

Pour préparer l'installation, vérifiez les conditions préalables et les exigences système répertoriées à la Section 16.5, « Configuration système requise pour Identity Reporting », page 262. Reportez-vous également aux notes de version relatives à votre édition.

1 (Facultatif) Pour ne pas avoir à spécifier dans le fichier `.properties` les mots de passe des comptes administrateur en vue d'une installation silencieuse, utilisez la commande `set` ou `export`. Par exemple : `set NOVL_ADMIN_PWD=`*`mon_mot_de_passe`*

   La procédure d'installation silencieuse lit les mots de passe à partir de l'environnement (plutôt qu'à partir du fichier `.properties`).

   Indiquez les mots de passe suivants :

   NOVL_DB_RPT_USER_PASSWORD

   Permet d'indiquer le mot de passe de l'administrateur de la base de données SIEM.

   NOVL_IDM_SRV_PWD

   Permet d'indiquer le mot de passe du propriétaire des objets et schémas de la base de données pour la création de rapports.

   NOVL_IDM_USER_PWD

   Permet d'indiquer le mot de passe de l'utilisateur idmrptuser, lequel dispose d'un accès en lecture seule aux données des rapports.

   NOVL_ADMIN_PWD

   (Facultatif) Pour autoriser les recherches sur le sous-conteneur lors de la connexion, vous devez indiquer le mot de passe du compte administrateur LDAP.

   NOVL_SMTP_PASSWORD

   (Facultatif) Pour utiliser l'authentification pour les communications électroniques, vous indiquez le mot de passe de l'utilisateur SMTP par défaut.

2 Pour spécifier les paramètres d'installation, procédez comme suit :

   2a Vérifiez que le fichier `.properties` figure dans le même répertoire que le fichier d'exécution de l'installation.

   Par commodité, NetIQ fournit deux fichiers `.properties`. Par défaut, ils figurent dans le répertoire `products\Reporting` de l'image `.iso` :

   - Le fichier `rpt_installonly.properties` vous permet d'utiliser les paramètres d'installation par défaut.
   - Vous utilisez le fichier `rpt_configonly.properties` pour personnaliser les paramètres d'installation.

   2b Dans un éditeur de texte, ouvrez le fichier `.properties`.

   2c Spécifiez les valeurs des différents paramètres. Pour obtenir une description de ces paramètres, reportez-vous à l'Étape 9 page 265.

   REMARQUE : le fichier `.properties` permettant d'installer l'édition Standard n'inclut que les paramètres requis pour cette version.

   2d Enregistrez et fermez le fichier.

3 Pour lancer la procédure d'installation, entrez la commande suivante :

```
rpt-install.exe -i silent -f path_to_properties_file
```

REMARQUE : si le fichier `.properties` se trouve dans un autre répertoire que celui du script d'installation, vous devez indiquer son chemin complet. Le script décompresse les fichiers requis dans un répertoire temporaire et lance l'installation en mode silencieux.

17.3 Génération manuelle du schéma de base de données

Une fois l'installation terminée, vous avez la possibilité de recréer les tables de la base de données sans toutefois devoir réinstaller. Cette section vous aide à créer le schéma de la base de données.

1 Arrêtez Tomcat à l'aide du fichier `services.msc`.

2 (Conditionnel) Créez une nouvelle base de données.

Si votre base de données est en cours d'exécution sur un serveur distinct, vous devez vous connecter à ce serveur de base de données. Pour une base de données PostgreSQL installée à distance, vérifiez que le serveur de base de données est en cours d'exécution. Pour vous connecter à une base de données PostgreSQL à distance, reportez-vous à la Section 17.4, « Connexion à une base de données PostgreSQL distante », page 272. Si vous vous connectez à une base de données Oracle, vérifiez que vous avez créé une instance de base de données Oracle dans ce serveur de base de données. Pour plus d'informations, reportez-vous à la documentation Oracle.

3 Ajoutez les rôles requis pour la base de données à l'aide des fichiers SQL suivants à partir de l'emplacement `C:\NetIQ\idm\apps\IdentityReporting\sql`.

- **PostgreSQL :** `create_dcs_roles_and_schemas.sql` et `create_rpt_roles_and_schemas.sql`
- **Oracle :** `create_dcs_roles_and_schemas-orcale.sql` et `create_rpt_roles_and_schemas-orcale.sql`

4 Pour créer des rôles IDM_RPT_DATA, IDM_RPT_CFG et IDMRPTUSER, effectuez les opérations suivantes :

- **PostgreSQL :** 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>');
```

- **Oracle :** 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;
```

5 Ajoutez la fonction get_formatted_user_dn au schéma IDM_RPT_DATA.

5a Connectez-vous à la base de données tant qu'administrateur de la base de données.

5b Ajoutez la fonction get_formatted dn à partir de `C:\NetIQ\idm\apps\IdentityReporting\sql`.

Recherchez les fichiers `get_formatted_user_dn.sql` pour PostgreSQL et `get_formatted_user_dn-oracle.SQL` pour Oracle.

6 Effacez les contrôle de cohérence de la base de données pour les fichiers `.sql` suivants situés à l'emplacement `C:\NetIQ\idm\apps\IdentityReporting\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`

6a Ajoutez la ligne suivante au début de chaque fichier SQL :

```
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;
```

6b Exécutez chaque fichier SQL avec l'utilisateur correspondant.

7 Validez les modifications apportées à la base de données.

8 Démarrez Tomcat à l'aide du fichier `services.msc`.

17.4 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 `C:\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 `C:\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.

18 Configuration d'Identity Reporting

Après avoir installé Identity Reporting, vous pouvez modifier la plupart des propriétés d'installation en exécutant le fichier `configupdate.bat`.

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.

18.1 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. Toutefois, vous devez, pour ce faire, ajouter un fichier JDBC Oracle à la bibliothèque de votre serveur d'applications.

1. Téléchargez le fichier `ojdbc7.jar` depuis le site Web d'Oracle.
2. Copiez le fichier à l'emplacement approprié pour le serveur Tomcat (répertoire `common/lib` dans *`tomcat_lib`*).

Pour plus d'informations sur les bases de données Oracle prises en charge, reportez-vous à la Section 16.5, « Configuration système requise pour Identity Reporting », page 262.

18.2 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, le fichier `WAR rptdoc` est automatiquement déployé lors de l'installation d'Identity Reporting.

Dans un environnement de production ou de test, supprimez manuellement les fichiers et dossiers `WAR rptdoc` de votre environnement Tomcat.

18.3 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 `C:\NetIQ\idm\apps\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 `C:\NetIQ\idm\apps\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.

19 Gestion des pilotes pour Reporting

Identity Reporting requiert les pilotes suivants :

- Pilote Identity Manager MSGW (Managed System Gateway)
- Pilote Identity Manager DCS (Data Collection Service)

Vous pouvez utiliser les outils de gestion des paquetages fournis avec Designer pour installer et configurer les pilotes. Cette procédure implique les opérations suivantes :

19.1 Configuration des pilotes pour Identity Reporting

Cette section vous aide à installer et à configurer le pilote de la passerelle système gérée (MSGW) et celui du service de collecte de données (DCS) pour Identity Reporting.

REMARQUE : dans cette section, on part de l'hypothèse que vous avez déjà installé et configuré les pilotes de l'application utilisateur ainsi que ceux des rôles et ressources pour RBPM. Pour plus d'informations, reportez-vous au Chapitre 15.6, « Création et déploiement des pilotes pour les applications d'identité », page 221.

19.1.1 Installation des paquetages de pilotes pour Identity Reporting

Avant de configurer les pilotes, vous devez disposer de tous les paquetages nécessaires dans le catalogue de paquetages. Lors de la création d'un projet Identity Manager dans Designer, vous êtes automatiquement invité à importer plusieurs paquetages dans le nouveau projet. Vous n'avez pas à importer les paquetages au cours de l'installation, mais vous devez procéder ensuite à leur installation pour qu'Identity Reporting puisse s'exécuter correctement.

1. Ouvrez votre projet dans Designer.
2. Sélectionnez **Catalogue de paquetages > Importer le paquetage**.

3 Dans la boîte de dialogue Sélectionner le paquetage, cliquez sur **Sélectionner tout**, puis cliquez sur **OK**.

   Designer ajoute plusieurs nouveaux dossiers de paquetage sous le **catalogue de paquetages**. Ces dossiers correspondent aux objets de la palette située à droite de la vue Modélisateur dans Designer.

4 Cliquez sur **Enregistrer**.

19.1.2 Configuration du pilote de la passerelle système gérée (MSG, Managed System Gateway)

1 Ouvrez votre projet dans Designer.

2 Dans la palette de la vue **Modélisateur**, sélectionnez **Service > Passerelle système gérée**.

3 Faites glisser l'icône correspondant à **Passerelle système gérée** dans la vue **Modélisateur**.

4 Dans l'Assistant de configuration des pilotes, sélectionnez le paquetage **Managed System Gateway Base**, puis cliquez sur **Suivant**.

5 Dans la fenêtre Sélectionner les fonctions obligatoires, choisissez les fonctions requises, puis cliquez sur **Suivant**.

6 (Facultatif) Si l'application vous demande un autre paquetage appelé **Advanced Java Class**, sélectionnez-le, puis cliquez sur **OK**.

7 (Facultatif) Spécifiez le nom que vous souhaitez utiliser pour le pilote.

8 Cliquez sur **Suivant**.

9 Pour les paramètres de connexion, indiquez les valeurs utilisées par Identity Reporting pour les requêtes de données envoyées au pilote.

   Lorsque vous spécifiez plusieurs adresses IP, vous continuez à utiliser le même numéro de port pour écouter toutes les interfaces. Par exemple, si vous spécifiez `192.168.0.1,127.0.0.1` pour l'adresse et `9000` pour le port, le pilote utilise les paramètres suivants :

   ```
   192.168.0.1:9000
   127.0.0.1:9000
   ```

10 (Facultatif) Pour activer le suivi des noeuds d'extrémité, sélectionnez **vrai**, puis spécifiez un emplacement pour le fichier de trace.

11 Cliquez sur **Suivant**.

12 (Facultatif) Pour connecter le pilote à un chargeur distant, effectuez les étapes suivantes :

   12a Dans la fenêtre relative au chargeur distant, sélectionnez **oui**.

   12b Définissez les paramètres du chargeur distant que vous souhaitez utiliser.

13 Cliquez sur **Suivant**.

14 Vérifiez les informations affichées dans la fenêtre Confirmer les tâches d'installation, puis cliquez sur **Terminer**.

15 (Facultatif) Pour configurer des paramètres supplémentaires pour le pilote, effectuez les étapes suivantes dans la vue Modélisateur :

   15a Cliquez avec le bouton droit de la souris sur la ligne reliant le pilote de la passerelle système gérée à l'ensemble de pilotes, puis cliquez sur **Propriétés**.

   15b Dans la boîte de dialogue Propriétés, sélectionnez **Configuration du pilote > Option de démarrage**.

   15c Sélectionnez **Manuel** pour l'option de démarrage, puis cliquez sur **Appliquer**.

15d Cliquez sur l'onglet **Paramètres du pilote**.

15e (Facultatif) Dans l'onglet **Options de pilote**, modifiez les paramètres du pilote, les connexions et le suivi des noeuds d'extrémité.

Il est possible que vous deviez sélectionner **afficher** sous **Paramètres de connexion** et **Paramètres du pilote** pour voir les paramètres.

15f (Facultatif) Pour que le pilote envoie régulièrement des messages d'état sur le canal Éditeur, cliquez sur l'onglet **Options de l'éditeur**, puis indiquez une valeur en minutes dans **Intervalle de pulsation**.

En l'absence de trafic sur le canal Éditeur dans l'intervalle spécifié, le pilote envoie une nouvelle pulsation.

15g Cliquez sur **Appliquer**.

16 (Facultatif) Pour définir les valeurs de configuration globale du serveur, effectuez les étapes suivantes :

16a Dans le volet de navigation, sélectionnez **GCV**.

16b Indiquez les valeurs de configuration globale, comme suit :

Query Managed Systems across driversets (Requête sur les systèmes gérés de tous les ensembles de pilotes)

Permet de définir le champ d'action du pilote de la passerelle système gérée. Si la valeur est **vrai**, le pilote renvoie les informations concernant les systèmes gérés à tous les ensembles de pilotes. Dans le cas contraire, l'envoi est limité à l'ensemble de pilotes local.

Add end-point request data to queries (Ajouter des données de requête sur le noeud d'extrémité)

Permet de spécifier si les données de requête du noeud d'extrémité doivent être ajoutées aux requêtes envoyées par le pilote. Cet ajout est réalisé sous la forme d'un noeud `operation-data`.

End-point request data node name (Nom du noeud de données de requête sur le noeud d'extrémité)

Permet de préciser le nom du noeud `operation-data` pour les requêtes. Les attributs du noeud indiquent les détails relatifs à la requête.

16c Cliquez sur **Appliquer**.

17 (Facultatif) Pour consulter les paquetages installés, cliquez sur **Paquetages** dans le volet de navigation.

Vous ne devez pas modifier les paramètres **Opération**, à moins que vous souhaitiez procéder à la désinstallation d'un paquetage en particulier.

18 Cliquez sur **OK**.

19 Vous devez activer le canal Abonné pour qu'Identity Reporting puisse fonctionner correctement.

19.1.3 Configuration du pilote pour le service de collecte de données (DCS, Data Collection Service)

1 Ouvrez votre projet dans Designer.

2 Dans la palette de la vue **Modélisateur**, sélectionnez **Service > Service de collecte de données**.

3 Faites glisser l'icône correspondant au **Service de collecte de données** jusqu'à la vue **Modélisateur**.

4 Dans l'Assistant de configuration des pilotes, sélectionnez le paquetage **Data Collection Service Base**, puis cliquez sur **Suivant**.

5 Dans la fenêtre Sélectionner les fonctions obligatoires, choisissez les fonctions requises, puis cliquez sur **Suivant**.

6 Sélectionnez les fonctions facultatives à appliquer, puis cliquez sur **Suivant**.

7 (Facultatif) Si l'application vous invite à indiquer un autre paquetage appelé **LDAP Library**, effectuez les étapes suivantes :

7a Sélectionnez le paquetage, puis cliquez sur **OK**.

7b (Facultatif) Pour configurer un profil de connexion globale pour tous les pilotes, sélectionnez **Oui** sur la page d'installation de la bibliothèque LDAP.

8 Cliquez sur **Suivant**.

9 (Facultatif) Spécifiez le nom que vous souhaitez utiliser pour le pilote.

10 Cliquez sur **Suivant**.

11 Pour les paramètres de connexion, indiquez les valeurs utilisées par Identity Reporting pour les requêtes de données envoyées au pilote.

Par exemple, indiquez le nom d'utilisateur et le mot de passe de l'administrateur de Reporting aux fins de l'authentification.

Lorsque vous spécifiez plusieurs adresses IP, vous continuez à utiliser le même numéro de port pour écouter toutes les interfaces. Par exemple, si vous spécifiez `192.168.0.1,127.0.0.1` pour l'adresse et `9000` pour le port, le pilote utilise les paramètres suivants :

```
192.168.0.1:9000
127.0.0.1:9000
```

12 Cliquez sur **Suivant**.

13 Dans **Identity Vault Registration** (Enregistrement du coffre-fort d'identité), indiquez les paramètres du coffre-fort d'identité.

vous devez spécifier une adresse IP. Ne spécifiez pas l'adresse de l'hôte local pour enregistrer le coffre-fort d'identité.

14 (Facultatif) Pour enregistrer le pilote de la passerelle système gérée, effectuez les étapes suivantes :

14a Dans **Managed System Gateway Registration** (Enregistrement de la passerelle système gérée), cliquez sur **oui**.

14b Spécifiez le DN du pilote, ainsi que le nom d'utilisateur et le mot de passe de l'administrateur LDAP.

REMARQUE : le pilote de la passerelle système gérée que vous venez de configurer n'a pas encore été déployé. Il n'est donc pas indiqué lorsque vous utilisez la fonction Parcourir. Il vous faudra alors saisir le DN du pilote.

---

15 Cliquez sur **Suivant**.

16 (Facultatif) Pour connecter le pilote à un chargeur distant, effectuez les étapes suivantes :

16a Dans la fenêtre relative au chargeur distant, sélectionnez **oui**.

16b Définissez les paramètres du chargeur distant que vous souhaitez utiliser.

17 Cliquez sur **Suivant**.

18 Dans **Scoping Configuration** (Étendue de la configuration), précisez le rôle du pilote du service de collecte de données.

19 Vérifiez les informations figurant dans la fenêtre Confirmer les tâches d'installation, puis cliquez sur **Terminer**.

20 (Facultatif) Pour configurer des paramètres supplémentaires pour le pilote, effectuez les étapes suivantes dans la vue Modélisateur :

20a Cliquez avec le bouton droit de la souris sur la ligne reliant le pilote du service de collecte de donnée à l'ensemble de pilotes, puis cliquez sur **Propriétés**.

20b Dans la boîte de dialogue Propriétés, sélectionnez **Configuration du pilote > Option de démarrage**.

20c Sélectionnez **Manuel** pour l'option de démarrage, puis cliquez sur **Appliquer**.

20d Cliquez sur l'onglet **Paramètres du pilote**.

Dans les environnements où le pilote reçoit un grand nombre d'événements, NetIQ recommande de ne pas définir plus de 5 lots par fichier. Si vous définissez ce paramètre sur une valeur supérieure à 5, le pilote ne peut pas traiter efficacement les événements.

20e (Facultatif) Dans l'onglet **Options de pilote**, modifiez les paramètres du pilote, les connexions et l'enregistrement.

Dans un environnement de test, il peut être judicieux d'indiquer des chiffres bas afin de vérifier que les événements sont traités correctement. Cependant, dans un environnement de production, il est généralement souhaitable d'utiliser des chiffres plus élevés afin que le système ne traite pas inutilement des événements.

Adresse IP

Permet d'indiquer l'adresse IP du serveur qui héberge Identity Reporting.

Port

Permet de spécifier le numéro du port utilisé par Identity Reporting pour les connexions REST.

Protocole

Permet d'indiquer le protocole d'accès à Identity Reporting. Si vous sélectionnez HTTPS, vous devez également indiquer si vous voulez approuver le certificat du serveur.

Nom

Permet d'indiquer le nom permettant de faire référence à votre coffre-fort d'identité dans Identity Reporting.

Description

Permet de décrire brièvement le coffre-fort d'identité.

Adresse

Permet d'indiquer l'adresse IP du coffre-fort d'identité.

Par exemple, `192.168.0.1`

REMARQUE : vous devez spécifier une adresse IP. Ne spécifiez pas une adresse de « localhost » pour enregistrer le coffre-fort d'identité.

Register Managed System Gateway (Enregistrer la passerelle système gérée)

Permet d'indiquer si vous voulez enregistrer le pilote de la passerelle système gérée.

DN du pilote de passerelle système gérée (LDAP)

Permet d'indiquer le DN du pilote de la passerelle système gérée dans un format utilisant des barres obliques.

Managed System Gateway Driver Configuration Mode (Mode de configuration du pilote de passerelle système gérée)

Permet d'indiquer si le pilote est configuré en local ou à distance.

DN utilisateur (LDAP)

Indique le DN LDAP du compte utilisateur permettant l'authentification auprès du pilote de la passerelle système gérée. Ce DN doit figurer dans le coffre-fort d'identité.

Mot de passe

Permet d'indiquer le mot de passe de l'utilisateur.

Time interval between submitting events (Intervalle de temps entre la soumission d'événements)

La durée maximum, en minutes, durant laquelle un événement peut rester dans la couche de persistance avant d'être soumis au DCS (et à la base de données d'Identity Reporting).

20f (Facultatif) Pour collecter des données à partir des applications d'identité, spécifiez les valeurs correspondantes sous **SSO Service Support** (Support du service SSO). Pour plus d'informations, reportez-vous à la Section 19.1.4, « Configuration d'Identity Reporting pour collecter des données à partir des applications d'identité », page 282.

20g Cliquez sur **Appliquer**.

21 Pour configurer des DN, procédez de la manière suivante :

21a Dans le menu de navigation, sélectionnez **Valeurs de contrôle du moteur**.

21b Pour le paramètre **Forme qualifiée des valeurs de l'attribut de syntaxe DN**, sélectionnez **Vrai**.

21c Cliquez sur **Appliquer**.

22 (Facultatif) Pour définir les valeurs de configuration globale du serveur, effectuez les étapes suivantes :

22a Dans le volet de navigation, sélectionnez **GCV**.

22b Pour **Show override options** (Afficher les options de remplacement), sélectionnez **Afficher**.

22c Modifiez les paramètres afin de remplacer les valeurs de configuration globale.

22d Cliquez sur **Appliquer**.

23 Cliquez sur **OK**.

19.1.4 Configuration d'Identity Reporting pour collecter des données à partir des applications d'identité

Pour qu'Identity Reporting collecte des données à partir des applications d'identité, vous devez configurer le pilote DCS afin qu'il prenne en charge le processus d'authentification unique Single Sign-on.

1 Ouvrez votre projet dans Designer.

2 Dans la vue **Mode plan**, cliquez avec le bouton droit de la souris sur le pilote du service de collecte de données, puis cliquez sur **Propriétés**.

3 Sélectionnez **Configuration du pilote > Paramètres du pilote**.

4 Sélectionnez **Show connection parameters > show** (Afficher les paramètres de connexion > Afficher).

5 Sélectionnez **SSO Service Support > Yes** (Support du service SSO > Oui).

6 Spécifiez les paramètres de la fonctionnalité d'authentification unique Single Sign-on :

SSO Service Address (Adresse du service SSO)

Requis

Permet d'indiquer l'URL relative du serveur d'authentification qui émet les jetons pour OSP. Par exemple, `10.10.10.48`.

Cette valeur doit correspondre à la valeur que vous avez spécifiée dans l'utilitaire de configuration RBPM pour **OSP server host identifier** (Identifiant d'hôte du serveur OSP). Pour plus d'informations, reportez-vous à la section « Serveur d'authentification » page 248.

SSO Service Port (Port du service SSO)

Requis

Permet de spécifier le port du serveur d'authentification. La valeur par défaut est 8180.

Cette valeur doit correspondre à la valeur que vous avez spécifiée dans l'utilitaire de configuration RBPM pour **OSP server TCP port** (Port TCP du serveur OSP). Pour plus d'informations, reportez-vous à la section « Serveur d'authentification » page 248.

SSO Service Client ID (ID du client du service SSO)

Requis

Permet d'indiquer le nom servant à identifier le client SSO pour le pilote DCS auprès du serveur d'authentification. La valeur par défaut est `dcsdrv`.

Cette valeur doit correspondre à la valeur que vous avez spécifiée dans l'utilitaire de configuration RBPM pour **OSP client ID** (ID du client OSP). Pour plus d'informations, reportez-vous à la section « Création de rapports » page 254.

SSO Service Client Secret (Secret du client du service SSO)

Requis

Permet d'indiquer le mot de passe du client SSO pour le pilote DCS.

Cette valeur doit correspondre à la valeur que vous avez spécifiée dans l'utilitaire de configuration RBPM pour **OSP client secret** (Secret du client OSP). Pour plus d'informations, reportez-vous à la section « Création de rapports » page 254.

Protocole

Permet d'indiquer si le client du service utilise le protocole `http` (non sécurisé) ou `https` (sécurisé) lorsqu'il communique avec le serveur d'authentification.

7 Cliquez sur **Appliquer**, puis sur **OK**.

8 (Facultatif) Si vous avez modifié ces paramètres après le déploiement de pilote, vous devez redéployer et redémarrer le pilote. Pour plus d'informations, reportez-vous à la Section 19.2, « Déploiement et démarrage des pilotes pour Identity Reporting », page 283.

9 Répétez cette procédure pour chaque pilote DCS de votre environnement.

19.2 Déploiement et démarrage des pilotes pour Identity Reporting

Identity Reporting requiert les pilotes suivants :

- Pilote Identity Manager MSGW (Managed System Gateway)
- Pilote Identity Manager DCS (Data Collection Service)

Cette procédure implique les opérations suivantes :

- Section 19.2.1, « Déploiement des pilotes », page 284
- Section 19.2.2, « Vérification de l'exécution des systèmes gérés », page 284
- Section 19.2.3, « Lancement des pilotes pour Identity Reporting », page 287

Pour plus d'informations sur l'installation et la configuration de ces pilotes, reportez-vous à la Section 19.1, « Configuration des pilotes pour Identity Reporting », page 277.

19.2.1 Déploiement des pilotes

Vous devez déployer deux pilotes pour Identity Reporting.

1. Ouvrez votre projet dans Designer.
2. Dans la vue **Modélisateur** ou **Mode plan**, cliquez avec le bouton droit de la souris sur l'ensemble de pilotes à déployer.
3. Sélectionnez **En direct** > **Déploiement**.
4. Spécifiez les références du coffre-fort d'identité pour le pilote sélectionné.

19.2.2 Vérification de l'exécution des systèmes gérés

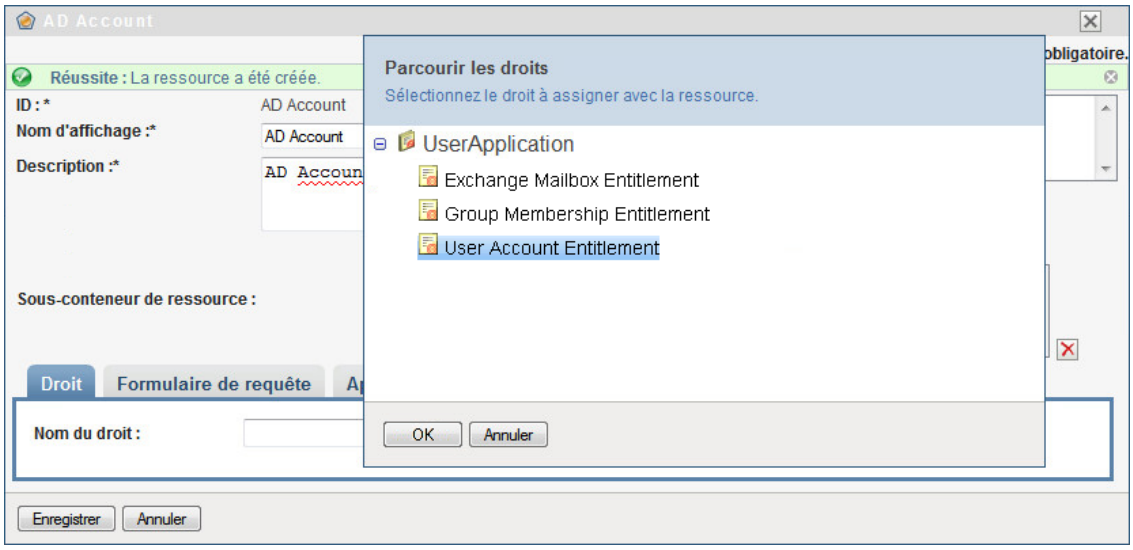
Avant de démarrer le pilote de la passerelle système gérée (MSGW) et celui du service de collecte de données (DCS), vous devez vérifier que les systèmes gérés sous-jacents sont correctement configurés. En procédant ainsi, vous isolez les problèmes relatifs à votre environnement et qui n'ont aucun lien avec la configuration des pilotes d'Identity Reporting.

Ainsi, pour diagnostiquer votre environnement Active Directory, vous pouvez tester un droit Active Directory en assignant une ressource dans l'application utilisateur.

REMARQUE : pour plus d'informations sur le pilote Active Directory, consultez le manuel *NetIQ Identity Manager Driver for Active Directory Implementation Guide* (Guide d'implémentation du pilote NetIQ Identity Manager pour Active Directory).

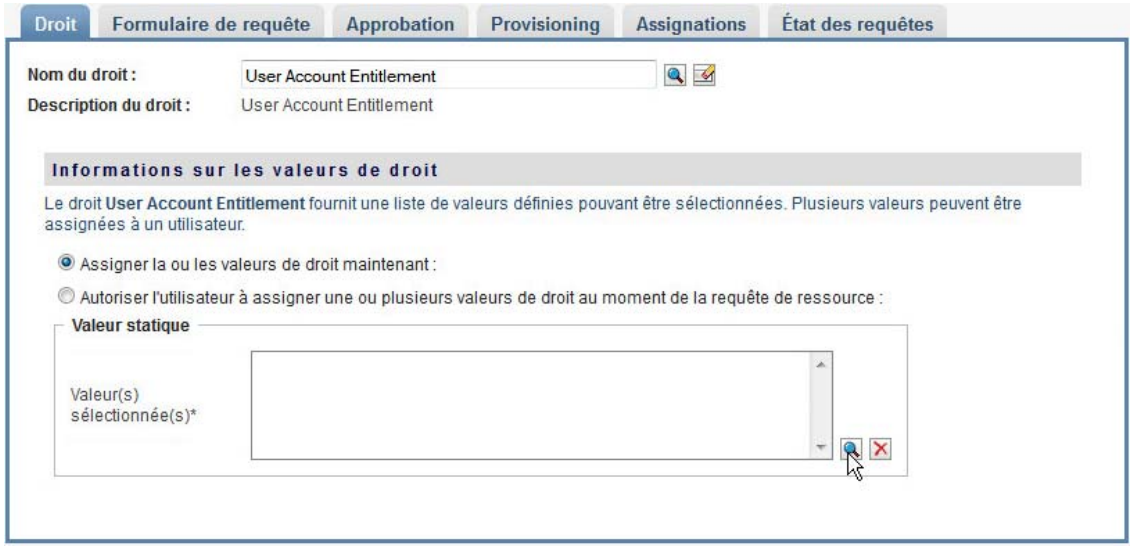
Pour vérifier qu'Active Directory est correctement configuré, vous pouvez notamment procéder comme suit :

1. Assurez-vous que l'application utilisateur et Identity Reporting s'exécutent sur le même serveur.
2. Dans iManager, assurez-vous que le pilote de l'application utilisateur et celui du service des rôles et ressources sont en cours d'exécution, puis vérifiez que le pilote du système géré est aussi en cours d'exécution.
3. Pour vérifier que l'application utilisateur peut récupérer des informations à partir d'Active Directory, vous devez vous y connecter en tant qu'administrateur.
4. Dans le catalogue de ressources, créez de nouvelles ressources pour les comptes Active Directory :
5. Liez la ressource à un droit au sein du pilote Active Directory. Par exemple, **User Account Entitlement** (Droit du compte utilisateur).



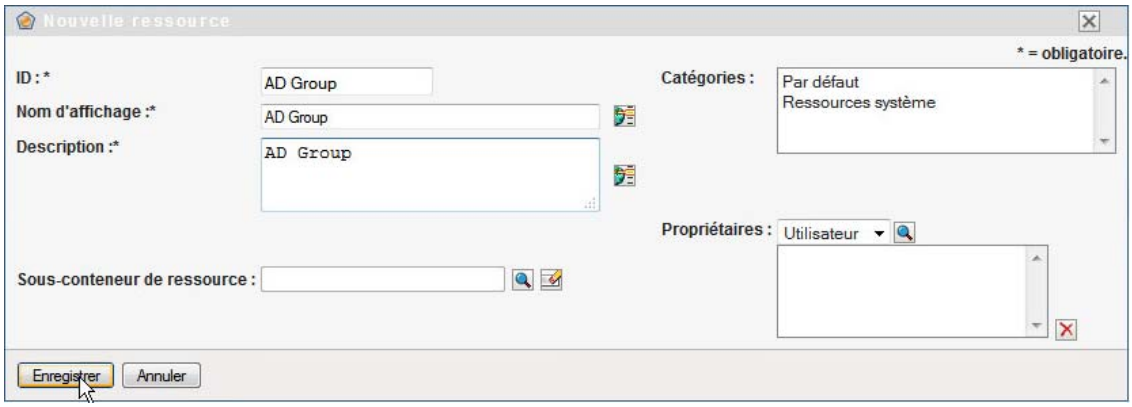
L'application utilisateur peut récupérer ce droit à partir du pilote.

6 Étant donné que cette ressource particulière est relative aux comptes, configurez la ressource afin d'y assigner une valeur de compte.



7 Sélectionnez la valeur Compte, puis cliquez sur **Ajouter**.

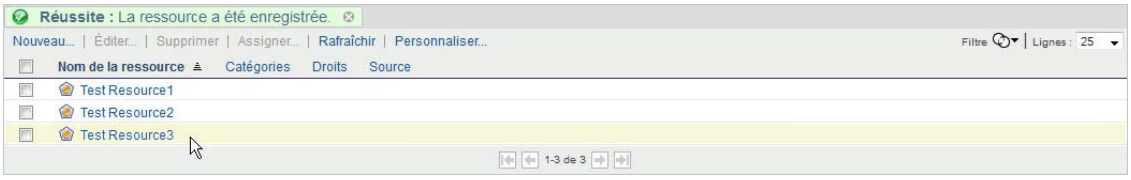
8 Créez une autre ressource afin d'y assigner des groupes.



9 Liez la ressource à un droit approprié pour les groupes. Dans le cas de cette ressource, vous assignez **Group Membership Entitlement** (Droit d'appartenance au groupe).

10 Configurez la ressource de sorte que l'utilisateur attribue la valeur relative au droit au moment de la requête et qu'il puisse sélectionner plusieurs valeurs pour une même requête d'assignation.

11 Vérifiez que les droits ont été correctement créés.



À ce stade, vous pouvez constater que l'architecture sous-jacente du système géré (dans ce cas, Active Directory) fonctionne correctement. Cela vous aidera à résoudre par la suite d'éventuels problèmes.

19.2.3 Lancement des pilotes pour Identity Reporting

Cette section vous explique comment démarrer le pilote de la passerelle système gérée (MSGW) et celui du service de collecte de données (DCS).

1. Ouvrez iManager.
2. Cliquez avec le bouton droit de la souris sur le pilote de la passerelle système gérée, puis cliquez sur **Démarrer le pilote**.
3. Cliquez avec le bouton droit de la souris sur le pilote du service de collecte de données, puis cliquez sur **Démarrer le pilote**.
4. Une fois que les pilotes sont démarrés, vérifiez que la console du serveur affiche de nouvelles informations. Exemple :

```
21:22:56,399 INFO  [LogEvent] [DCS_Driver_Registration_Add] DCS Driver DN
TREE\novell\TestDrivers\Data Collection Service Driver; DCS-Report Driver
d44571a5708446bad65832481bb401d
```

5. Connectez-vous à Identity Reporting en tant qu'administrateur d'Identity Reporting.
6. Dans le volet de navigation situé à gauche, cliquez sur **Présentation**.
7. Vérifiez que la section **Configuration** indique qu'un coffre-fort d'identité a été configuré.
8. Dans le volet de navigation, cliquez sur **Coffres-forts d'identité**.
9. Vérifiez que la page Coffre-fort d'identité affiche les détails relatifs au pilote du service de collecte de données et à celui de la passerelle système gérée. L'état du pilote de la passerelle système gérée doit indiquer que le pilote a été initialisé.

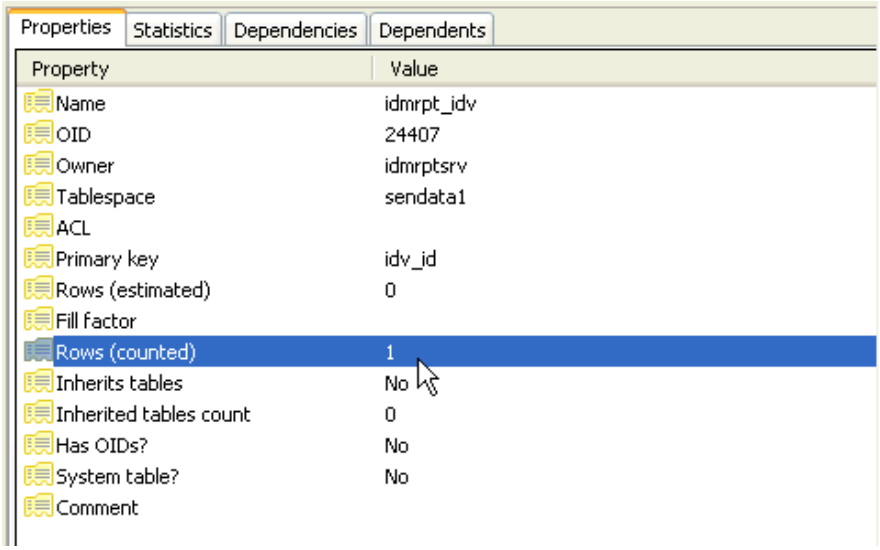
   À ce stade, vous pouvez consulter les informations contenues dans l'entrepôt d'informations d'identité afin d'en savoir plus sur la richesse des données stockées concernant le coffre-fort d'identité, ainsi que les systèmes gérés de votre entreprise.
10. Pour consulter les informations figurant dans l'entrepôt d'informations d'identité, utilisez un outil d'administration de base de données, tel que PGAdmin pour PostgreSQL, afin d'examiner le contenu de la base de données SIEM. Lorsque vous consultez la base de données SIEM, vous devez voir les schémas suivants :

    idm_rpt_cfg

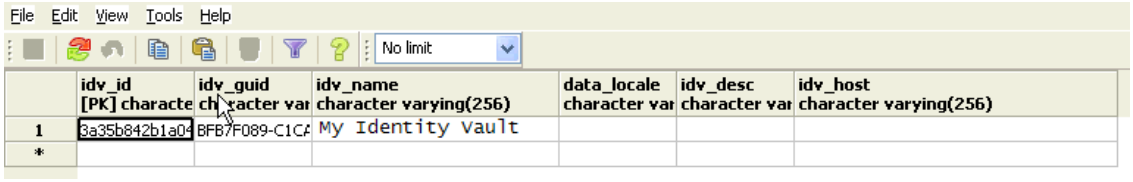
    Contient les données de configuration d'Identity Reporting, notamment les définitions et planifications de rapports. Le programme d'installation d'Identity Reporting ajoute ce schéma à la base de données.

    idm_rpt_data

    Contient des informations collectées par le pilote de la passerelle système gérée et celui du service de collecte de données. Le programme d'installation d'Identity Reporting ajoute ce schéma à la base de données.
11. Pour consulter les données collectées par les pilotes, développez **idm_rpt_data > Tables > idmrpt_idv**.
12. Vérifiez qu'une seule ligne a été ajoutée à cette table pour le nouveau pilote du service de collecte de données :



13 Vérifiez que les données de cette table indiquent le nom du coffre-fort d'identité :



Si vous voyez une nouvelle ligne inscrite dans cette table, cela signifie que le pilote a bien été enregistré.

19.3 Configuration de l'environnement d'exécution

Cette section fournit des instructions 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 19.3.1, « Configuration du pilote du service de collecte de données (DSC) afin de collecter des données à partir des applications d'identité », page 289
- Section 19.3.2, « Migration du pilote du service de collecte de données », page 290
- Section 19.3.3, « Prise en charge des attributs et objets personnalisés », page 292
- Section 19.3.4, « Prise en charge de plusieurs ensembles de pilotes », page 295
- Section 19.3.5, « Configuration des pilotes pour une exécution en mode distant avec SSL », page 296

Si vous rencontrez des problèmes avec un ou plusieurs pilotes et que vous ne savez pas comment les résoudre, reportez-vous à la section Troubleshooting (Dépannage) du manuel Administrator Guide to NetIQ Identity Reporting (Guide d'administration de NetIQ Identity Reporting).

19.3.1 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 votre projet n'inclut pas encore le pilote du service de collecte de données, importez-le dans votre projet. Pour plus d'informations, reportez-vous au Chapitre 15.6, « Création et déploiement des pilotes pour les applications d'identité », page 221.
4. (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 :
   - **4a** Téléchargez la dernière version du fichier de correctif pour le pilote DCS.
   - **4b** Lancez l'extraction du fichier de correctif dans un répertoire sur votre serveur.
   - **4c** 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
     change this
     ```

   - **4d** Redémarrez eDirectory.
   - **4e** 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 16.3, « Conditions préalables à l'installation des composants du module Identity Reporting », page 261.
   - **4f** Redéployez et redémarrez le pilote DCS dans Designer.
5. Dans la vue **Mode plan**, cliquez avec le bouton droit de la souris sur le pilote DCS, puis sélectionnez **Propriétés**.
6. Cliquez sur **Configuration du pilote**.
7. Cliquez sur l'onglet **Paramètres du pilote**.
8. Cliquez sur **Show connection parameters** (Afficher les paramètres de connexion), puis sélectionnez **show** (Afficher).
9. Cliquez sur **SSO Service Support** (Support du service SSO), puis sélectionnez **Oui**.
10. Indiquez l'adresse IP et le port du module Identity Reporting.
11. Indiquez un mot de passe pour le client du service SSO. Le mot de passe par défaut est `driver`.
12. Cliquez sur **Appliquer**, puis sur **OK**.

13 Dans la vue **Modélisateur**, cliquez avec le bouton droit de la souris sur le pilote DCS, puis sélectionnez **Pilote > Déployer**.

14 Cliquez sur **Déployer**.

15 Si vous êtes invité à redémarrer le pilote DCS, cliquez sur **Oui**.

16 Cliquez sur **OK**.

19.3.2 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**.

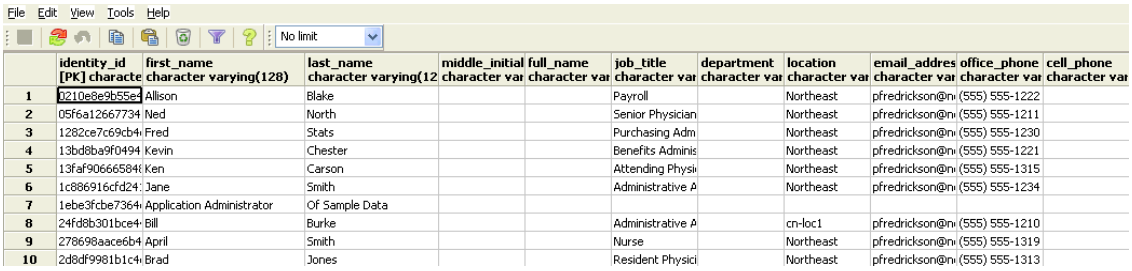
3 Sélectionnez les arborescences contenant des données pertinentes, puis cliquez sur **Démarrer**.

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 :

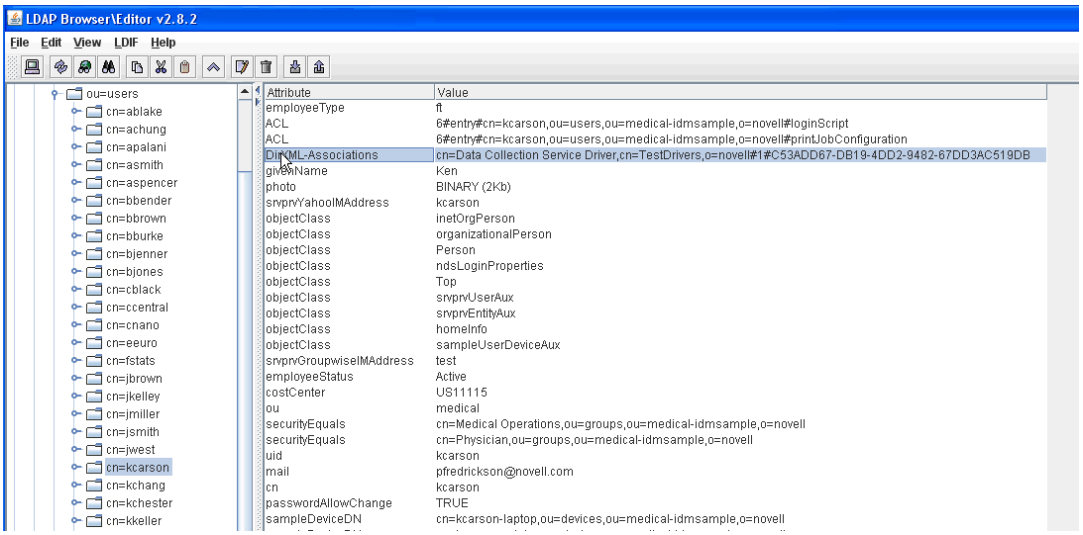

File Edit View Tools Help

No limit

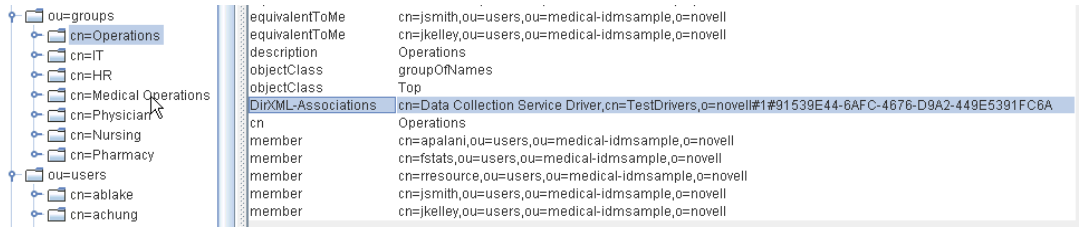
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	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.

19.3.3 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 292
- « Inclusion d'un nom et d'une description dans la base de données » page 293
- « Ajout d'attributs étendus à des types d'objets connus » page 294

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.

19.3.4 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 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. Pour configurer le pilote du service de collecte de données sur ce serveur, reportez-vous à la Section 19.1.3, « Configuration du pilote pour le service de collecte de données (DCS, Data Collection Service) », page 279.
- **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.

19.3.5 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 296 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 297.

   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 296.

   5e Enregistrez les modifications et redémarrez le pilote.

19.4 Configuration des drapeaux d'audit pour les pilotes

Cette section décrit les paramètres d'audit recommandés pour le pilote de la passerelle système gérée et celui du service de collecte de données.

19.4.1 Définition des drapeaux d'audit dans Identity Manager

NetIQ vous recommande de définir des drapeaux d'audit pour les pilotes dans Identity Manager. Ces drapeaux concernent Novell Audit (pas XDAS).

Pour définir les drapeaux dans iManager, sélectionnez **Driver Set Properties (Propriétés de l'ensemble de pilotes) > Niveau de consignation > Consigner des événements spécifiques**.

Catégorie	Drapeaux recommandés
Événements du moteur méta-annuaire	◆ Avertissements du moteur méta-annuaire
Événements d'état	◆ Réussite **REMARQUE :** le rapport **Événements d'assignations de ressources corrélés par utilisateur** requiert le drapeau Réussite. Afin de pouvoir exécuter ce rapport ou des versions personnalisées de celui-ci, vous devez activer le drapeau Réussite. ◆ Erreur ◆ Fatal
Événements de l'opération	◆ Modifier ◆ Ajouter une association ◆ Vérifier le mot de passe ◆ Ajouter valeur ◆ Ajouter ◆ Renommer ◆ Retirer l'association ◆ Vérifier le mot de passe de l'objet ◆ Effacer l'attribut ◆ Supprimer la valeur ◆ Obtenir le mot de passe nommé ◆ Retirer ◆ Déplacer ◆ Modifier le mot de passe ◆ Ajouter une valeur (lors d'une modification) ◆ Réinitialiser les attributs

Catégorie	Drapeaux recommandés
Événements de transformation	◆ Réinitialisation du mot de passe ◆ Requête de l'agent utilisateur ◆ Sync mot de passe
Événements de provisioning de référence	◆ Définir la référence SSO ◆ Effacer la référence SSO ◆ Définir la phrase secrète SSO

19.4.2 Configuration des drapeaux d'audit dans eDirectory

NetIQ vous recommande de définir des drapeaux d'audit pour les pilotes dans eDirectory. Ces drapeaux concernent Novell Audit (pas XDAS).

Pour définir les drapeaux dans iManager, sélectionnez **Audit eDirectory > Configuration de l'audit > Novell Audit**.

Catégorie	Drapeaux recommandés
Global	◆ Ne pas envoyer d'événement répliqué
Métadonnées	◆ (*Sélectionnez tous les drapeaux)*
Objets	◆ Ajouter une propriété ◆ Autoriser la connexion ◆ Modifier le mot de passe ◆ Changer les équivalents de sécurité ◆ Créer ◆ Supprimer ◆ Supprimer la propriété ◆ Connexion ◆ Logout ◆ Modifier RDN ◆ Déplacer (Source) ◆ Déplacer (Destination) ◆ Retirer ◆ Renommer ◆ Restauration ◆ Rechercher ◆ Vérifier le mot de passe
Attributs	◆ *(Sélectionnez tous les drapeaux)*

Catégorie	Drapeaux recommandés
Agent	◆ DS rechargé ◆ Agent local ouvert ◆ Agent local fermé ◆ NLM chargé
Divers	◆ Generate CA Keys (Générer les clés de l'autorité de certification) ◆ Clé publique recertifiée
LDAP	◆ Liaison LDAP ◆ Liaison de réponse LDAP ◆ Modification LDAP ◆ Modification de réponse LDAP ◆ Modification de mot de passe LDAP ◆ Annulation de la liaison LDAP ◆ Suppression LDAP ◆ Suppression de réponse LDAP ◆ Modification de DN LDAP ◆ Modification de réponse DN LDAP ◆ Recherche LDAP ◆ Recherche de réponse LDAP ◆ Ajout LDAP ◆ Ajout de réponse LDAP

VI Installation de Designer

Cette section vous guide dans la procédure d'installation de Designer pour Identity Manager. Par défaut, le programme d'installation installe les composants à l'emplacement `C:\NetIQ`.

IMPORTANT : assurez-vous que le nom du répertoire contenant le programme d'installation de Designer ne comporte aucun espace, faute de quoi NICI ne sera pas installé durant l'installation de Designer. Par exemple, votre nom de répertoire ne peut pas être `Installation Designer`. Par contre, ce peut être `InstallationDesigner`.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous au Chapitre 20, « Planification de l'installation de Designer », page 303.

20 Planification de l'installation de Designer

Cette section présente les conditions préalables, les considérations et la configuration système requise pour installer Designer. Tout d'abord, consultez la liste de contrôle pour comprendre la procédure d'installation.

20.1 Liste de contrôle pour l'installation de Designer

Avant de commencer l'installation, NetIQ recommande de passer en revue les étapes suivantes:

	Éléments de la liste de contrôle
❑	1. Passez en revue les informations relatives à l'architecture du produit pour en savoir plus sur les interactions entre les composants Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 1, « Aperçu des composants Identity Manager », page 19.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.
❑	3. 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 20.2, « Conditions préalables à l'installation de Designer », page 304.
❑	4. 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 20.3, « Configuration système requise pour Designer », page 304.
❑	5. Pour installer Designer, reportez-vous à l'une des sections suivantes : ◆ « Exécution du fichier exécutable » page 307 ◆ « Installation en mode silencieux » page 307
❑	6. Installez les autres composants Identity Manager.
❑	7. (Facultatif) Pour démarrer un projet dans votre solution Identity Manager, reportez-vous au *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer for Identity Manager).

20.2 Conditions préalables à l'installation de Designer

Cette section présente les considérations et la configuration système requise pour l'installation de Designer.

Avant d'installer ou de mettre à niveau Designer, passez en revue les considérations suivantes :

- Avant d'installer Designer, vous devez installer la version 32 bits du paquetage Novell International Cryptographic Infrastructure (NICI).
- Vous ne pouvez pas utiliser d'espaces de travail Designer 2.1*x* pour Designer 3.0 ou des versions ultérieures étant donné que les anciennes versions des espaces de travail ne sont pas compatibles avec les versions plus récentes de Designer. Designer stocke les projets et les informations de configuration dans des **espaces de travail**. Par exemple, sous **Windows 10 et Windows 7**, les espaces de travail de Designer 4.x sont installés par défaut dans le répertoire `%UserProfile%\designer_workspace`.

20.3 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
Système d'exploitation (certifié)	Un des systèmes d'exploitation 64 bits suivants (minimum requis) : **Serveurs** ◆ Windows Server 2016 ◆ Windows Server 2012 R2 **Bureaux** ◆ Windows 10 ◆ Windows 8
Système 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.

Catégorie	Configuration requise
Système de virtualisation	◆ Hyper-V Server 2012 R2 ◆ VMware ESX 5.0 et versions ultérieures ◆ Virtualisation de Windows Server 2012 R2 avec Hyper-V (prise en charge) 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.
Navigateur Web	Un des navigateurs suivants (versions minimales) : ◆ Internet Explorer 11 ◆ Chrome 61 ◆ Firefox 51

21 Installation de Designer

Vous pouvez installer Identity Manager Designer à l'aide d'un fichier exécutable, d'un fichier binaire ou en mode texte, en fonction de l'ordinateur cible. Vous pouvez également effectuer une installation silencieuse. Utilisez le programme d'installation situé par défaut dans le répertoire `\products\Designer\` :

Plusieurs composants Identity Manager nécessitent des paquetages dans Designer. Lors de l'installation de Designer, le programme d'installation ajoute automatiquement plusieurs paquetages au nouveau projet.

21.1 Exécution du fichier exécutable

1. Connectez-vous à l'aide d'un compte d'administrateur à l'ordinateur sur lequel vous souhaitez installer Designer.
2. Téléchargez le fichier `Identity_Manager_4.7_Windows_Designer.zip` à partir du site Web de téléchargement de NetIQ.
3. Extrayez le fichier `Identity_Manager_4.7_Windows_Designer.zip`.
4. Exécutez le fichier `install.exe`.
5. Suivez les étapes de l'assistant jusqu'à la fin de la procédure d'installation.

21.2 Installation en mode silencieux

Vous pouvez utiliser des scripts pour effectuer une installation silencieuse de Designer sans intervention de l'utilisateur. L'option `-i silent` utilise les valeurs par défaut des paramètres pour l'installation, sauf si vous modifiez le fichier `designerInstaller.properties`.

1. Connectez-vous à l'aide d'un compte d'administrateur à l'ordinateur sur lequel vous souhaitez installer Designer.
2. Accédez au répertoire contenant les fichiers d'installation.
3. (Facultatif) Pour configurer le répertoire d'installation et la langue de Designer, procédez comme suit.
   - **3a** Ouvrez le fichier `designerInstaller.properties`, situé par défaut dans le répertoire *`Chemin_fichier_Designer_extrait`*`\products\Designer`.
   - **3b** Dans le fichier properties, modifiez les valeurs des paramètres suivants :

     USER_INSTALL_DIR

     Indique le chemin d'accès à l'emplacement où vous souhaitez installer Designer. Par exemple :

```
USER_INSTALL_DIR=C:\designer
```

Si vous spécifiez un chemin qui ne se termine pas par le répertoire `designer`, le programme d'installation de Designer ajoute automatiquement un répertoire `designer`.

SELECTED_DESIGNER_LOCALE

Spécifie l'une des langues suivantes que vous souhaitez utiliser dans Designer après l'installation :

- `zh_CN` : chinois simplifié
- `zh_TW` : chinois traditionnel
- `nl` : néerlandais
- `en` : anglais
- `fr` : français
- `de` : allemand
- `it` : italien
- `ja` : japonais
- `pt_BR` : portugais du Brésil
- `es` : espagnol

3c Enregistrez, puis fermez le fichier properties.

4 Exécutez la commande suivante :

```
install -i silent -f Path\designerInstaller.properties
```

21.3 Modification d'un chemin d'installation qui contient un espace

Vous pouvez installer Designer à un emplacement dont les noms de répertoires contiennent des espaces. Toutefois, après avoir installé Designer, vous devez modifier les fichiers `StartDesigner.bat` et `Designer.ini` pour garantir le bon fonctionnement de Designer. Remplacez manuellement l'espace par un caractère d'échappement (« \ »). Par exemple :

Remplacez

```
C:\designer installation
```

par

```
C:\designer\ installation
```

VII 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.

Les fichiers d'installation sont situés dans le répertoire `\products\Analyzer` au sein du fichier image `.iso` pour le paquetage d'installation d'Identity Manager. Par défaut, le programme d'installation installe les composants à l'emplacement `C:\NetIQ\Analyzer`.

NetIQ recommande de passer en revue la procédure d'installation avant de commencer. Pour plus d'informations, reportez-vous à la Section 22.1, « Liste de contrôle pour l'installation d'Analyzer », page 311.

22 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.

22.1 Liste de contrôle pour l'installation d'Analyzer

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 Chapitre 1, « Aperçu des composants Identity Manager », page 19.
❑	2. Choisissez les serveurs que vous souhaitez utiliser pour vos composants Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.3, « Configuration de serveur et scénarios d'installation recommandés », page 41.
❑	3. Assurez-vous que votre environnement remplit les conditions nécessaires pour héberger Analyzer. Pour plus d'informations, reportez-vous à la Section 22.2, « Configuration système requise pour l'installation d'Analyzer », page 312.
❑	4. Pour installer Analyzer, reportez-vous aux sections suivantes : ◆ Pour utiliser l'assistant d'installation, reportez-vous à la Section 23.1, « Utilisation de l'assistant pour installer Analyzer », page 313. ◆ Pour effectuer une installation en mode silencieux, reportez-vous à la Section 23.2, « Installation d'Analyzer en mode silencieux », page 314
❑	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 23.3, « Installation d'un client Audit pour Analyzer », page 314.
❑	6. Pour activer Analyzer, reportez-vous à la section « Activation d'Analyzer » page 361.
❑	7. (Facultatif) Pour mettre à niveau Analyzer, reportez-vous à la Section 32.7, « Mise à niveau d'Analyzer », page 394.

22.2 Configuration système requise pour l'installation d'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	512 Mo (4 Go recommandé)
Résolution vidéo	1024*768 (1280*1025 recommandés)
Système d'exploitation (certifié)	L'un des systèmes d'exploitation 64 bits suivants : ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 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.
Système 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.

23 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.

23.1 Utilisation de l'assistant pour installer Analyzer

La procédure suivante décrit comment installer Analyzer à l'aide d'un assistant d'installation. Pour effectuer une installation sans surveillance en mode silencieux, reportez-vous à la Section 23.2, « Installation d'Analyzer en mode silencieux », page 314.

Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise reprises à la Section 22.1, « Liste de contrôle pour l'installation d'Analyzer », page 311.

1. Connectez-vous 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, par défaut dans le répertoire `\products\Analyzer`.
3. (Conditionnel) Si vous avez téléchargé les fichiers d'installation d'Analyzer, procédez comme suit :
   - **3a** Accédez au fichier `win.zip` de l'image téléchargée.
   - **3b** Lancez l'extraction du contenu du fichier dans un dossier sur l'ordinateur local.
4. À partir du répertoire `\products\Analyzer`, exécutez le programme d'installation `install.exe` :
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. (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.
9. Pour activer Analyzer, reportez-vous à la section « Activation d'Analyzer » page 361.

23.2 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 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, 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 `win.zip` de l'image téléchargée.
   - **3b** Lancez l'extraction du 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 `analzerInstaller.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 silencieuse, émettez la commande suivante :

   ```
   install.exe -i silent -f analyzerInstaller.properties
   ```
6. Pour activer Analyzer, reportez-vous à la section « Activation d'Analyzer » page 361.

23.3 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 Windows 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 (fichier `.msi`) pour le client XDAS :

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.

VIII 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. Pour plus d'informations sur OSP, reportez-vous à la Section 4.5, « Utilisation de l'accès Single Sign-on dans Identity Manager », page 34.

24 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. Comprenez comment Identity Manager utilise OSP pour l'accès Single Sign-on. Pour plus d'informations, reportez-vous à la Section 4.5, « Utilisation de l'accès Single Sign-on dans Identity Manager », page 34.
❑	2. Installez OSP. Pour plus d'informations, reportez-vous à la Partie 14, « Installation du composant de gestion des mots de passe », page 177.
❑	3. Installez les applications d'identité. Pour plus d'informations, reportez-vous à la Partie IV, « Installation des applications d'identité », page 159.
❑	4. (Facultatif) Installez Identity Reporting. Pour plus d'informations, reportez-vous à la Partie V, « Installation d'Identity Reporting », page 257.
❑	5. Configurez les applications d'identité pour l'accès Single Sign-on à l'aide d'OSP. Pour plus d'informations, reportez-vous au Chapitre 25, « Utilisation d'OSP pour l'accès Single Sign-on dans Identity Manager », page 321.
❑	6. Installez le système d'authentification que vous souhaitez utiliser avec Identity Manager. Par exemple : Access Manager ou Kerberos.
❑	7. (Conditionnel) Configurez Access Manager et OSP. Pour plus d'informations, reportez-vous au Chapitre 26, « Utilisation de l'authentification SAML avec NetIQ Access Manager pour Single Sign-on », page 325.
❑	8. Vérifiez les paramètres Single Sign-on. Pour plus d'informations, reportez-vous au Chapitre 28, « Vérification de l'accès Single Sign-on pour les applications d'identité », page 339.

25 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.

25.1 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 Section 15.7.5, « Configuration du coffre-fort d'identité pour les applications d'identité », page 226. 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.

25.2 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 15.8.1, « Exécution de l'utilitaire de configuration des applications d'identité », page 235.
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. Pour plus d'informations, reportez-vous au Chapitre 14.2, « Installation du composant de gestion des mots de passe pour Identity Manager », page 179.
- 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. Pour plus d'informations, reportez-vous au Chapitre 14.2, « Installation du composant de gestion des mots de passe pour Identity Manager », page 179.

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. Pour plus d'informations, reportez-vous au Chapitre 14.2, « Installation du composant de gestion des mots de passe pour Identity Manager », page 179.
- 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.

25.3 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. Le chemin par défaut du fichier Keystore de SSPR est `C:\[Java_Home]\lib\security\cacerts`.

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).

26 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).

26.1 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.

26.2 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.

26.2.1 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 26.2.2, « Installation du certificat Access Manager dans le Truststore Identity Manager », page 327.

26.2.2 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 : `C:\NetIQ\idm\apps\jre\bin\keytool -importcert -trustcacerts -alias <cert_NAM> -keystore C:\NetIQ\idm\apps\jre\bin\security\cacerts -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 26.2.3, « Installation du certificat du serveur SSL dans le Truststore Access Manager », page 327.

26.2.3 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 26.4.2, « Création d'un ensemble d'attributs pour SAML », page 329.

26.3 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 15.8.1, « Exécution de l'utilitaire de configuration des applications d'identité », page 235.
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.

26.4 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 26.4.1, « Copie des métadonnées pour Identity Manager », page 328
- Section 26.4.2, « Création d'un ensemble d'attributs pour SAML », page 329
- Section 26.4.3, « Ajout d'Identity Manager en tant que fournisseur de service approuvé », page 329

26.4.1 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 selon la procédure mentionnée à la section « Ajout d'Identity Manager en tant que fournisseur de service approuvé » page 329.

26.4.2 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).

26.4.3 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 328.

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 329. 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).

26.5 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 `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp`.

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).

27 Utilisation de Kerberos pour Single Sign-on

Vous pouvez utiliser Kerberos comme une méthode d'authentification pour les applications d'identité qui permet Single Sign-on (SSO). Cela permet aussi aux utilisateurs d'utiliser l'authentification Windows intégrée pour se connecter aux applications. Cette section explique comment configurer Active Directory afin d'utiliser Kerberos pour se connecter aux applications d'identité :

27.1 Configuration du compte utilisateur Kerberos dans Active Directory

Utilisez les outils d'administration Active Directory pour configurer Active Directory pour l'authentification Kerberos. Vous devez créer un nouveau compte utilisateur Active Directory pour les applications d'identité et Identity Reporting. Le nom du compte utilisateur doit utiliser le nom DNS du serveur qui héberge les applications d'identité et Identity Reporting.

REMARQUE : pour les références de domaine ou de domaine Kerberos, utilisez le format en majuscules. Par exemple : `@MYCOMPANY.COM`.

---

1. En tant qu'administrateur dans Active Directory, utilisez MMC (Microsoft Management Console) pour créer un nouveau compte utilisateur avec le nom DNS du serveur hébergeant les applications d'identité.

   Par exemple, si le nom DNS du serveur d'applications d'identité est `rbpm.mycompany.com`, utilisez les informations suivantes pour créer l'utilisateur :

   First name (Prénom) : rbpm

   User login name (Nom de connexion de l'utilisateur) : HTTP/rbpm.mycompany.com

   Pre-windows logon name (Nom de connexion pré-Windows) : rbpm

   Set password (Définir le mot de passe) : spécifiez le mot de passe approprié. Par exemple : `Passw0rd`.

   Password never expires (Le mot de passe n'expire jamais) : sélectionnez cette option.

   User must change password at next logon (L'utilisateur doit changer de mot de passe à la prochaine connexion) : ne sélectionnez pas cette option.

2. Associez le nouvel utilisateur avec le SPN (Service Principal Name).

   2a Sur le serveur Active Directory, ouvrez un shell de commande.

   2b À l'invite, saisissez la commande suivante :

   ```
   setspn -A HTTP/DNS_Identity_Applications_server@WINDOWS-DOMAIN userID
   ```

   Par exemple :

```
setspn -A HTTP/rbpm.mycompany.com@MYCOMPANY.COM rbpm
```

2c Vérifiez setspn en entrant `setspn -L userID`.

3 Pour générer le fichier `keytab`, utilisez l'utilitaire `ktpass` :

3a Dans la ligne de commande, entrez ce qui suit :

```
ktpass /out filename.keytab /princ servicePrincipalName /mapuser
userPrincipalName /mapop set /pass password /crypto ALL /ptype
KRB5_NT_PRINCIPAL
```

Par exemple :

```
ktpass /out rbpm.keytab /princ HTTP/rbpm.mycompany.com@MYCOMPANY.COM /mapuser
rbpm  /mapop set /pass Passw0rd /crypto All /ptype KRB5_NT_PRINCIPAL
```

IMPORTANT : pour les références de domaine ou de domaine Kerberos, utilisez le format en majuscules. Par exemple : `@MYCOMPANY.COM`.

3b Copiez le fichier `rbpm.keytab` sur votre serveur d'applications d'identité.

4 En tant qu'administrateur dans Active Directory, créez un compte utilisateur final avec MCC pour préparer la fonctionnalité SSO.

Le nom du compte utilisateur final doit correspondre à une valeur d'attribut d'un utilisateur eDirectory pour permettre la prise en charge de Single Sign-on. Créez un utilisateur avec un nom comme `cnano`, mémorisez le mot de passe et veillez à ce que l'option **User must change password at next logon** (L'utilisateur doit changer de mot de passe à la prochaine connexion) ne soit pas sélectionnée.

5 (Facultatif) Si vous avez installé Identity Reporting sur un serveur distinct, répétez ces étapes pour le composant de création de rapports.

6 Configurez le serveur des applications d'identité pour accepter la configuration Kerberos. Pour plus d'informations, reportez-vous à la Section 27.2, « Configuration du serveur d'applications d'identité », page 334.

27.2 Configuration du serveur d'applications d'identité

Vous devez configurer votre serveur d'applications d'identité pour utiliser le fichier keytab Kerberos et le compte utilisateur que vous avez créé dans Active Directory. Avant de poursuivre, assurez-vous que vous avez terminé la Section 27.1, « Configuration du compte utilisateur Kerberos dans Active Directory », page 333.

REMARQUE : pour les références de domaine ou de domaine Kerberos, utilisez le format en majuscules. Par exemple : `@MYCOMPANY.COM`.

---

1 Pour définir vos paramètres de système d'exploitation pour la configuration Kerberos, procédez comme suit :

1a Ouvrez le fichier `krb5` à partir d'un éditeur de texte sur le serveur qui héberge les applications d'identité.

1b Ajoutez les informations suivantes au fichier `krb5` :

```
[libdefaults]
    default_realm = WINDOWS-DOMAIN
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    WINDOWS-DOMAIN = {
         kdc = FQDN Active Directory Server
         admin_server = FQDN Active  Directory Server
    }
[domain_realm]
    .your.domain = WINDOWS-DOMAIN
    your.domain = WINDOWS-DOMAIN
```

Par exemple :

```
[libdefaults]
    default_realm = MYCOMPANY.COM
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    MYCOMPANY.COM = {
         kdc = myadserver.mycompany.com
         admin_server = myadserver.mycompany.com
    }
[domain_realm]
    .mycompany.com = MYCOMPANY.COM
    mycompany.com = MYCOMPANY.COM
```

1c Enregistrez les modifications et fermez le fichier `krb5`.

2 (Conditionnel) Pour définir les informations de configuration Kerberos pour Tomcat, procédez comme suit :

2a Sur le serveur d'applications Tomcat, créez un exemple de fichier `Kerberos_login.config` incluant le contenu ci-dessous :

REMARQUE : l'utilisateur novlua a besoin d'autorisations pour créer le fichier `Kerberos_login.config`.

```
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
    debug="true"
    refreshKrb5Config="true"
    useTicketCache="true"
ticketCache="c:\NetIQ\idm\apps\tomcat\kerberos\spnegoTicket.cache"
    doNotPrompt="true"
        principal="HTTP/DNS_Identity_Applications_server@WINDOWS-DOMAIN
"
    useKeyTab="true"
        keyTab="/absolute_path/filename.keytab"
    storeKey="true";
    };
```

Par exemple, sur un serveur Windows :

```
keyTab="c:\\NetIQ\\idm\\apps\\tomcat\kerberos\\rbpm.keytab"
```

2b Dans le fichier, spécifiez des valeurs pour les paramètres `principal` et `keyTab`. Par exemple :

```
principal="HTTP/rbpm.mycompany.com@MYCOMPANY.COM"
keyTab="/home/usr/rbpm.keytab"
```

- La valeur du paramètre `principal` doit correspondre à celle que vous avez spécifiée pour Kerberos. Pour plus d'informations, reportez-vous à l'Étape 3 page 334.
- Spécifiez le chemin d'accès absolu au fichier `keytab` sur votre serveur d'applications d'identité. Le fichier ne doit pas forcément se trouver dans le répertoire par défaut des applications d'identité.

2c Faites référence au fichier `Kerberos_login.config` dans le fichier JVM `java.security` avec la ligne suivante :

```
login.config.url.1=file:c:\NetIQ\idm\apps\tomcat\kerberos\Kerberos_login.config
```

3 Pour spécifier la méthode d'authentification dans l'utilitaire de configuration de RBPM, procédez comme suit :

3a Ouvrez l'utilitaire `Configupdate`.

3b Cliquez sur l'onglet **Authentification**.

3c Faites défiler jusqu'à la section **Méthode d'authentification**.

3d Dans le champ **Méthode**, sélectionnez **Kerberos**.

3e Dans le champ **Nom d'attribut de mappage**, indiquez `cn`.

REMARQUE : pour plus d'informations sur l'utilitaire de configuration de RBPM, reportez-vous au Chapitre 15.8, « Configuration des paramètres pour les applications d'identité », page 235.

---

4 (Facultatif) Si vous avez installé Identity Reporting sur un serveur distinct, répétez ces étapes pour le composant de création de rapports.

5 Configurez les navigateurs employés par les utilisateurs finaux pour accéder aux applications d'identité. Pour plus d'informations, reportez-vous à la Section 27.3, « Configuration des navigateurs des utilisateurs finaux pour l'authentification Windows intégrée », page 336.

27.3 Configuration des navigateurs des utilisateurs finaux pour l'authentification Windows intégrée

Les navigateurs employés par vos utilisateurs finaux pour accéder aux applications d'identité et à Identity Reporting doivent également être configurés pour l'authentification Windows intégrée. Cette section explique comment configurer l'ordinateur d'un utilisateur final pour prendre en charge l'accès SSO à l'aide de l'authentification Windows intégrée.

REMARQUE : vous devez effectuer cette procédure pour l'ordinateur de chaque utilisateur final à qui vous souhaitez fournir un accès SSO aux applications d'identité et à Identity Reporting.

---

1 Connectez-vous à l'ordinateur des utilisateurs nécessitant un accès SSO.

2 Ouvrez le panneau de configuration des options Internet.

3 Cliquez sur **Security** (Sécurité).

4 Cliquez sur **Sites de confiance** > **Sites**.

5 Ajoutez le nom DNS du serveur d'applications d'identité.

Par exemple : `rbpm.mycompany.com`

6 Cliquez sur **Ajouter**, puis sur **Fermer**.

7 Cliquez sur **Personnaliser le niveau...**

8 Sous **Authentification utilisateur**, sélectionnez **Connexion automatique avec le nom d'utilisateur et le mot de passe actuel**.

9 Cliquez sur **OK**.

10 Dans Options Internet, cliquez sur **Avancé**.

11 Sous sécurité, sélectionnez **Activer l'authentification Windows intégrée**.

12 Répétez cette procédure pour l'ordinateur de chaque utilisateur final à qui vous souhaitez fournir un accès SSO aux applications d'identité et à Identity Reporting.

28 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 15.8, « Configuration des paramètres pour les applications d'identité », page 235.

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.

29 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 la communication SSL sur le serveur Tomcat, vous pouvez obtenir des certificats de deux manières :

- Certificat émis par une autorité de certification (CA) approuvée externe
- Certificat auto-signé

29.1 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 à la Section 29.2, « Création d'un fichier Keystore et d'une demande de signature de certificat », page 342.
❑	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 à la Section 29.4, « Activation de SSL avec un certificat auto-signé », page 344. 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 29.3, « Activation de SSL avec un certificat signé d'une autorité de certification externe », page 343.
❑	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 29.6, « Mise à jour des paramètres SSL pour le serveur d'applications », page 351 et à la Section 29.7, « Mise à jour des paramètres SSL dans l'utilitaire de configuration », page 352.

29.2 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.

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 : `C:\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 C:\NetIQ\idm\apps\tomcat\conf
   export PATH=C:\NetIQ\idm\apps\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 : `C:\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 29.3, « Activation de SSL avec un certificat signé d'une autorité de certification externe », page 343.
- Pour le certificat auto-signé, reportez-vous à la Section 29.4, « Activation de SSL avec un certificat auto-signé », page 344.

29.3 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 29.2, « Création d'un fichier Keystore et d'une demande de signature de certificat », page 342.

Pour utiliser un certificat signé et SSL :

1 Copiez le certificat dans le répertoire de configuration de votre serveur d'applications. Par exemple : `C:\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 : `C:\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 aussi les certificats signés à l'emplacement du fichier cacerts de Java. Par exemple :

```
keytool -import -trustcacerts -alias root -keystore
C:\NetIQ\idm\jre\lib\security\cacerts -file IDMTESTREE.der
```

5 Mettez à jour les paramètres SSL pour le serveur d'applications. Pour ce faire, reportez-vous à la Section 29.6, « Mise à jour des paramètres SSL pour le serveur d'applications », page 351.

6 Mettez à jour les paramètres SSL dans l'utilitaire de configuration. Pour plus d'informations, reportez-vous à la Section 29.7, « Mise à jour des paramètres SSL dans l'utilitaire de configuration », page 352.

7 Mettez à jour les paramètres SSL pour Self Service Password Reset. Pour plus d'informations, reportez-vous à la Section 29.8, « Mise à jour des paramètres SSL pour SSPR », page 353

8 Relancez Tomcat.

29.4 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.

29.4.1 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 : `C:\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
C:\NetIQ\idm\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.jks
```

Exemples :

```
keytool -list -v -alias root -keystore IDMkey.jks
```

Le serveur répertorie les certificats.

29.4.2 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 la Section 29.2, « Création d'un fichier Keystore et d'une demande de signature de certificat », page 342

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 29.2, « Création d'un fichier Keystore et d'une demande de signature de certificat », page 342.

   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 : `C:\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
C:\NetIQ\idm\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 à la Section 29.6, « Mise à jour des paramètres SSL pour le serveur d'applications », page 351.

10 Mettez à jour les paramètres SSL dans l'utilitaire de configuration. Pour plus d'informations, reportez-vous à la Section 29.7, « Mise à jour des paramètres SSL dans l'utilitaire de configuration », page 352.

11 Mettez à jour les paramètres SSL pour Self Service Password Reset. Pour plus d'informations, reportez-vous à la Section 29.8, « Mise à jour des paramètres SSL pour SSPR », page 353

12 Relancez Tomcat.

29.5 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.

29.5.1 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 Copiez la clé privée et les certificats créés à l'Étape 3 et à l'Étape 4 aux emplacements suivants, en fonction de vos composants :

Composant	Chemin Windows
Moteur Identity Manager	`C:\NetIQ\idm\NDS\DIBFiles`

Chargeur distant	Répertoire d'installation du chargeur distant :
	`C:\NetIQ\idm\RemoteLoader`
	OU
	`C:\NetIQ\idm\RemoteLoader\64bit`
	OU
	`C:\NetIQ\idm\RemoteLoader\32bit`

Chargeur distant .NET	`C:\NetIQ\idm\RemoteLoader.NET`
Agent de dissémination	`C:\NetIQ\idm\FanoutAgent`

9 Redémarrez les services Identity Manager.

29.5.2 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\UserApplication\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.

29.6 Mise à jour des paramètres SSL pour le serveur d'applications

Le serveur d'applications qui héberge les applications d'identité et Identity Reporting doit être configuré pour prendre en charge les communications SSL. Cette section explique comment mettre à jour un serveur d'applications Tomcat, à savoir le serveur d'applications par défaut.

1. Arrêtez Tomcat, s'il est en cours d'exécution.
2. Configurez le port SSL du serveur Tomcat.

   Par exemple, le port connecteur pour SSL est `8543`. Modifiez le fichier `server.xml` qui se trouve dans le répertoire `C:\NetIQ\idm\apps\tomcat\conf`.

   ```
   <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" />
   ```

   où:

   keystoreFile

   Indique le chemin d'accès au fichier `userapp.keystore`, situé par défaut dans le répertoire `C:\NetIQ\idm\apps\tomcat\conf\userapp.keystore`.

   keystorePass

   Spécifie le mot de passe du fichier `userapp.keystore`.

   De même, mettez à jour l'attribut `redirectPort` sur `8543` et enregistrez le fichier `server.xml`.
3. Accédez au répertoire `conf` de Tomcat, situé par défaut à l'emplacement `C:\NetIQ\idm\apps\tomcat\conf`.
4. Vérifiez que le répertoire `conf` contient un fichier Keystore. Par exemple : `idmapps.keystore`.

   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 29.2, « Création d'un fichier Keystore et d'une demande de signature de certificat », page 342.
5. Dans un éditeur de texte, ouvrez le fichier `server.xml` situé dans le répertoire `conf`.
6. Ajoutez les lignes suivantes au fichier `server.xml` :

   ```
   <Connector port="port_number" protocol="HTTP/1.1" maxThreads="150"
   SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
   sslProtocol="TLS" keystoreFile="path_to_file/filename.keystore"
   keystorePass="password"
   ```

   Par exemple :

   ```
   <Connector port="8543" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="C:\NetIQ\idm\apps\tomcat\conf\idmapps.keystore"
   keystorePass="encrypted_password"
   ```

NetIQ recommande de spécifier un mot de passe chiffré plutôt qu'un mot de passe en texte clair pour le paramètre keystorePass. Pour plus d'informations sur l'utilisation de mots de passe chiffrés et en texte clair dans les communications SSL, reportez-vous à la documentation Securing Tomcat (Sécurisation de Tomcat).

7 Démarrez Tomcat.

29.7 Mise à jour des paramètres SSL dans l'utilitaire de configuration

Lorsque vous installez les applications d'identité et Identity Reporting, vous devez indiquer *https* pour la méthode de communication. Par exemple : « *Protocole » page 213*. Toutefois, après l'installation, vous pouvez utiliser l'utilitaire de configuration de RBPM pour vous assurer que les applications communiquent avec SSL. Pour plus d'informations sur ces paramètres, reportez-vous au Chapitre 15.8, « Configuration des paramètres pour les applications d'identité », page 235.

1 Arrêtez Tomcat à l'aide du fichier `services.msc`.

2 Accédez à l'utilitaire de configuration de RBPM, situé par défaut dans le répertoire d'installation des applications d'identité. Par exemple : `C:\NetIQ\idm\apps\UserApplication`.

3 À l'invite de commande, exécutez l'utilitaire de configuration (`configupdate.bat`) :

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 à l'aide du fichier `services.msc`.

29.8 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 :

```
C:\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
```

30 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 :

30.1 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.

30.2 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.

30.2.1 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).

30.2.2 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 30.2.3, « Création de l'objet Stratégie de mot de passe dans le coffre-fort d'identité », page 356 et à la Section 30.2.4, « Création d'une stratégie de mot de passe personnalisée », page 357.

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.

30.2.3 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 au coffre-fort d'identité, importez les attributs à partir du fichier en exécutant `ldapmodify.exe` à partir du répertoire `install/utilities` du kit d'installation Identity Manager.

30.2.4 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 30.2.3, « Création de l'objet Stratégie de mot de passe dans le coffre-fort d'identité », page 356.

30.2.5 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.

30.3 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.

30.4 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.

30.5 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).

30.6 Activation d'Identity Manager

Certains composants Identity Manager s'activent automatiquement lors de votre première connexion. D'autres composants requièrent une procédure d'activation.

30.6.1 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 utiliser, activez l'ensemble de pilotes qui contient un pilote. Vous pouvez activer n'importe quelle arborescence avec la référence.

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 **Finish** (Terminer).

REMARQUE : Identity Manager n'affiche pas l'édition correcte d'Identity Manager après l'activation de la modification d'ensemble.

30.6.2 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.

30.6.3 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 30.6.1, « Installation d'une référence d'activation de produit », page 359. Pour plus d'informations à propos des pilotes, reportez-vous au site Web de documentation des pilotes Identity Manager.

30.6.4 Activation de composants spécifiques Identity Manager

Cette section fournit des informations sur l'activation de composants spécifiques pour Identity Manager.

Activation de Designer

Lorsque vous activez le moteur ou les pilotes Identity Manager, vous activez également Designer.

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 Micro Focus Customer Center** (Visiter 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.

IX Mise à niveau d'Identity Manager

Cette section fournit des informations pour la mise à niveau des composants Identity Manager. Pour migrer les données existantes vers un nouveau serveur, reportez-vous à la Partie X, « Migration des données Identity Manager vers une nouvelle installation », page 403. Pour plus d'informations sur la différence entre une mise à niveau et une migration, reportez-vous à la Section 31.2, « Notions de mise à niveau et de migration », page 367.

31 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.

31.1 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. Passez en revue les différences entre une mise à niveau et une migration. Pour plus d'informations, reportez-vous à la Section 31.2, « Notions de mise à niveau et de migration », page 367.
❑	2. Effectuez la mise à niveau vers Identity Manager 4.5.6. Si vous possédez une version antérieure à la version 4.5.6, vous ne pouvez pas effectuer la mise à niveau ou la migration vers la version 4.7. Pour plus d'informations, reportez-vous au Guide d'installation de NetIQ Identity Manager 4.5.
❑	3. Assurez-vous que vous disposez de la dernière version du kit d'installation pour mettre à niveau Identity Manager. Reportez-vous à la Section 5.5, « Téléchargement des fichiers d'installation », page 45.
❑	4. Renseignez-vous sur les interactions entre les différents composants Identity Manager. Pour plus d'informations, reportez-vous au Partie I, « Introduction », page 17.
❑	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 à la Chapitre 6, « Considérations relatives à l'installation », page 49 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 31.5, « Sauvegarde de la configuration actuelle », page 371.
❑	7. Effectuez la mise à niveau vers la version la plus récente de Designer. Pour plus d'informations, reportez-vous à la Section 32.1, « Mise à niveau de Designer », page 375.

	Éléments de la liste de contrôle
❑	8. Installez la dernière version d'iManager ou effectuez la mise à niveau vers la dernière version. Pour plus d'informations, reportez-vous à l'une des sections suivantes : ◆ **Installation** : « Installation d'iManager » page 143 ◆ **Mise à niveau** : « Mise à niveau d'iManager » page 376
❑	9. Sur le serveur exécutant Identity Manager, mettez à niveau edirectory vers la version la plus récente et installez les derniers correctifs. Si vous mettez à niveau eDirectory 9.0 ou une version ultérieure dans un environnement où le dernier chargeur distant 64 bits a déjà été mis à niveau, l'installation d'eDirectory échoue et le chargeur distant cesse de fonctionner. Pour vous assurer que le chargeur distant fonctionne correctement, effectuez la procédure suivante avant de mettre à niveau eDirectory : 1. Arrêtez le chargeur distant et ses instances. 2. Désinstallez le RPM `novell-DXMLopensslx`. 3. Installez eDirectory 9.1 ou version ultérieure. 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. Mettez à jour les plug-ins iManager en fonction de la version d'iManager. Pour plus d'informations, reportez-vous à la Section 32.2.4, « Mise à jour des plug-ins iManager après une mise à niveau ou une réinstallation », page 379.
❑	11. Arrêtez les pilotes associés au serveur sur lequel vous avez installé le moteur Identity Manager. Pour plus d'informations, reportez-vous à la Section 9.4.1, « Arrêt des pilotes », page 93.
❑	12. Mettez à niveau le moteur Identity Manager. Pour plus d'informations, reportez-vous à la Section 32.4, « Mise à niveau du moteur Identity Manager », page 380. **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 35.4, « Migration du moteur Identity Manager vers un nouveau serveur », page 411.
❑	13. (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 32.3, « Mise à niveau du chargeur distant », page 379.
❑	14. (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 32.8, « Mise à niveau des pilotes Identity Manager », page 394. 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.
❑	15. (Conditionnel) Si le composant OSP n'est pas installé, installez-le. Pour plus d'informations, reportez-vous à la Partie 13, « Installation du composant Single Sign-on », page 169.
❑	16. (Conditionnel) Si le composant SSPR n'est pas installé, installez-le. Pour plus d'informations, reportez-vous à la Partie 14, « Installation du composant de gestion des mots de passe », page 177. **REMARQUE :** installez SSPR si vous utilisez le fournisseur hérité de gestion des mots de passe. Pour plus d'informations, reportez-vous à la Section 4.4.2, « Présentation du fournisseur hérité pour la gestion des mots de passe », page 33.

	Éléments de la liste de contrôle
❑	17. Mettez à niveau l'application utilisateur, le tableau de bord Identity Manager, OSP, SSPR et Identity Reporting à l'aide du programme de mise à niveau. Pour plus d'informations, reportez-vous à la Section 32.5, « Mise à niveau des applications d'identité et d'Identity Reporting », page 381. Vous pouvez aussi mettre à niveau ces composants manuellement. Pour plus d'informations, reportez-vous à la Partie X, « Migration des données Identity Manager vers une nouvelle installation », page 403.
❑	18. Mettez à niveau le module de création de rapports Identity et les pilotes associés. Pour plus d'informations, reportez-vous à la Section 32.6, « Mise à niveau d'Identity Reporting », page 392.
❑	19. Démarrez les pilotes associés aux applications d'identité et le moteur Identity Manager. Pour plus d'informations, reportez-vous à la Section 9.4.2, « Lancement des pilotes », page 94.
❑	20. (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 à la Section 32.9, « Ajout de nouveaux serveurs à l'ensemble de pilotes », page 396.
❑	21. (Conditionnel) Si vous disposez de stratégies et de règles personnalisées, restaurez vos paramètres personnalisés. Pour plus d'informations, reportez-vous à la Section 32.10, « Restauration de stratégies et de règles personnalisées sur le pilote », page 398.
❑	22. Activez votre solution Identity Manager mise à niveau. Pour plus d'informations, reportez-vous à la Section 30.6, « Activation d'Identity Manager », page 359.

31.2 Notions de mise à niveau et de migration

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 401.

31.3 Ordre de mise à niveau

Vous devez mettre à niveau les composants Identity Manager dans l'ordre suivant :

1. Designer
2. iManager
3. Sentinel Log Management for IGA
4. Coffre-fort d'identité
5. Chargeur distant/moteur Identity Manager
6. Plug-ins iManager
7. Composants Tomcat et PostgreSQL
8. Single Sign-On (fournisseur d'authentification unique One)
9. SSPR (réinitialisation du mot de passe en self-service)
10. Applications d'identité (pour l'édition avancée)
11. Identity Reporting
12. Analyzer

Pour plus d'informations à propos des derniers chemins de mise à niveau pris en charge, consultez les Notes de version relatives à votre version sur le site Web de documentation d'Identity Manager 4.6.

31.4 Chemins de mise à niveau pris en charge

Identity Manager 4.7 prend en charge la mise à niveau à partir des versions 4.5.x et 4.6.x. 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 31.4.1, « Mise à niveau à partir des versions 4.6.x d'Identity Manager », page 368
- Section 31.4.2, « Mise à niveau à partir des versions 4.5.x d'Identity Manager », page 370

31.4.1 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).

Composant	Version de base	Version mise à jour
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. 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.
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. 3. Mettez à niveau SLM for IGA. 4. Mettez à jour les paquetages de pilote de passerelle de services gérés et des services de collecte de données. 5. Installez Identity Rerporting 4.7. 6. 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

31.4.2 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).
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. 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. 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. Installez Identity Rerporting 4.7. 7. Créez une stratégie de synchronisation des données à partir de la page IDMDCS.

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

31.5 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 31.5.1, « Exportation du projet Designer », page 372
- Section 31.5.2, « Exportation de la configuration des pilotes », page 373

31.5.1 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 372
- « Création d'un nouveau projet à partir du coffre-fort d'identité » page 372

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.

31.5.2 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 373
- « Utilisation d'iManager pour créer une exportation du pilote » page 374

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.

32 Mise à niveau des composants Identity Manager

Cette section fournit des informations spécifiques pour la mise à niveau de certains composants Identity Manager. Vous pourriez, par exemple, souhaiter mettre à niveau Designer vers la dernière version sans mettre à niveau iManager. Cette section décrit également des procédures susceptibles d'être nécessaires après une mise à niveau.

32.1 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 Designer à partir du média Identity Manager (`\products\Designer\install.exe`)
4. Sélectionnez la langue dans laquelle vous souhaitez installer Designer, puis lisez et acceptez l'accord de licence.
5. Indiquez le répertoire d'installation de Designer, puis cliquez sur **Oui** dans le message indiquant que Designer est déjà installé.
6. Indiquez si vous souhaitez créer des raccourcis sur votre bureau ou dans le menu du bureau.
7. Lisez le résumé, puis cliquez sur **Installer**.
8. Consultez les notes de version, puis cliquez sur **Suivant**.
9. Sélectionnez l'option de lancement de Designer, puis cliquez sur **Terminé**.
10. Spécifiez un emplacement pour votre espace de travail Designer, puis cliquez sur **OK**.
11. Cliquez sur **OK** dans le message avertissant que votre projet doit être fermé et converti.
12. Dans la vue **Projet**, développez le projet, puis double-cliquez sur **Le projet doit être converti**.
13. Examinez les étapes effectuées par l'assistant de conversion de projet, puis cliquez sur **Suivant**.

14 Spécifiez un nom pour la sauvegarde de votre projet, puis cliquez sur **Suivant**.

15 Passez en revue le résumé de la procédure de conversion, puis cliquez sur **Convertir**.

16 Passez en revue le résumé une fois la conversion terminée, puis cliquez sur **Ouvrir**.

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).

32.2 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.

Si vous utilisez eDirectory 9.1, mettez à niveau votre version d'iManager vers la version 3.1. Les fichiers d'installation d'iManager 3.1 se trouvent dans le répertoire `<répertoire_extraction_iso>\products\iManager277\installs\win`.

La procédure de mise à niveau inclut les tâches suivantes :

- Section 32.2.1, « Mise à niveau d'iManager sous Windows », page 376
- Section 32.2.2, « Mise à jour des services basés sur le rôle », page 378
- Section 32.2.3, « Réinstallation ou migration des plug-ins pour Plug-in Studio », page 379
- Section 32.2.4, « Mise à jour des plug-ins iManager après une mise à niveau ou une réinstallation », page 379

32.2.1 Mise à niveau d'iManager sous Windows

Si le programme d'installation d'iManager Server détecte une version précédemment installée d'iManager, il se peut qu'il vous invite à la mettre à niveau. Si vous acceptez la mise à niveau, le programme remplace les versions existantes de JRE et de Tomcat par les dernières versions. Cette opération effectue également la mise à niveau d'iManager vers la dernière version.

Avant la mise à niveau d'iManager, assurez-vous que l'ordinateur répond aux conditions préalables et à la configuration système requise. Pour plus d'informations, consultez les sources suivantes :

- Les notes de version accompagnant la mise à jour.
- Pour iManager, reportez-vous à la section « Considérations relatives à l'installation du serveur iManager » page 146
- Pour iManager Workstation, reportez-vous à la section « Considérations relatives à l'installation du poste de travail iManager » page 147

REMARQUE : la procédure de mise à niveau utilise les valeurs de port HTTP et de port SSL configurées dans la version précédente d'iManager.

Pour installer iManager Server sous Windows :

1. Connectez-vous en tant qu'utilisateur avec privilèges d'administrateur à l'ordinateur sur lequel vous souhaitez mettre à niveau iManager.
2. (Conditionnel) Si vous avez modifié les fichiers de configuration `server.xml` et `context.xml`, enregistrez une copie de sauvegarde de ces fichiers à un autre emplacement avant d'effectuer la mise à niveau.

   La procédure de mise à niveau remplace les fichiers de configuration.
3. Sur le site Web de téléchargement NetIQ, sélectionnez la version d'iManager désirée, puis téléchargez le fichier `win.zip` dans un répertoire sur votre serveur. Par exemple, `iMan_277_win.zip`.
4. Extrayez le fichier `win.zip` dans le dossier iManager.
5. Exécutez `iManagerInstall.exe` situé par défaut dans le dossier *répertoire_extraction*`\iManager\installs\win`.
6. Dans la fenêtre de bienvenue d'iManager, sélectionnez une langue, pus cliquez sur **OK**.
7. Dans la fenêtre **Introduction**, cliquez sur **Next** (Suivant).
8. Acceptez l'accord de licence, puis cliquez sur **Suivant**.
9. (Facultatif) Pour utiliser des adresses IPv6 avec iManager, cliquez sur **Oui** dans la fenêtre **Activer IPv6**.

   Vous pouvez activer des adresses IPv6 après la mise à niveau d'iManager. Pour plus d'informations, reportez-vous à la Section 11.3.2, « Configuration d'iManager pour les adresses IPv6 après l'installation », page 158.
10. Cliquez sur **Next** (Suivant).
11. À l'invite de mise à niveau, sélectionnez **Mise à niveau**.
12. (Conditionnel) Consultez la fenêtre présentant un **résumé de la détection**.

    La fenêtre présentant un **résumé de la détection** affiche la dernière version du conteneur de servlets et du logiciel JVM qu'iManager utilisera après sa mise à niveau.
13. Cliquez sur **Next** (Suivant).
14. Lisez la page **Résumé avant installation**, puis cliquez sur **Installer**.

    La procédure de mise à niveau peut prendre plusieurs minutes. Il se peut qu'il ajoute de nouveaux fichiers pour les composants iManager ou modifie la configuration d'iManager. Pour plus d'informations, consultez les notes de version de la mise à niveau.
15. (Conditionnel) Si la fenêtre **Installation terminée** affiche le message d'erreur suivant, exécutez la procédure suivante :

    ```
    The installation of iManager version is complete, but some errors occurred
    during the install.
    Please see the installation log Log file path for details. Press "Done" to quit
    the installer.
    ```

    15a Notez le chemin d'accès au fichier journal indiqué dans le message d'erreur.

    15b Dans la fenêtre **Installation terminée**, cliquez sur **Terminé** Terminé.

    15c Ouvrez le fichier journal.

    15d (Conditionnel) Si vous trouvez l'erreur suivante dans le fichier journal, vous pouvez ignorer le message d'erreur. L'installation s'est bien déroulée et iManager fonctionne correctement.

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class
com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The process
cannot access the file because it is being used by another process)
```

15e (Conditionnel) Si le fichier ne contient pas l'erreur indiquée à l'Étape 21d, NetIQ vous recommande de recommencer l'installation.

16 Cliquez sur **Terminer**.

17 Une fois l'initialisation d'iManager terminée, cliquez sur le premier lien de la page de mise en route, puis connectez-vous. Pour plus d'informations, reportez-vous à la section Accessing iManager (Accès à iManager) du manuel *NetIQ iManager Administration Guide* (Guide d'administration de NetIQ iManager 2.7.7).

18 (Conditionnel) Si vous avez effectué des copies de sauvegarde des fichiers de configuration `server.xml` et `context.xml` avant de démarrer la procédure de mise à niveau, remplacez les nouveaux fichiers de configuration par les copies de sauvegarde.

32.2.2 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**. Pour plus d'informations, reportez-vous à la Section 11.1.3, « Présentation de l'installation des plug-ins d'iManager », page 145.
- 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.

32.2.3 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.

32.2.4 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. Pour plus d'informations, reportez-vous à la Section 11.1.3, « Présentation de l'installation des plug-ins d'iManager », page 145.

1 Ouvrez iManager.

2 Accédez à **Configurer > Installation de plug-ins > Modules de plug-in Novell disponibles**.

3 Mettez à jour les plug-ins.

32.3 Mise à niveau du chargeur distant

Si vous exécutez le chargeur distant, vous devez mettre à niveau ses fichiers.

REMARQUE : avant de mettre à niveau le chargeur distant .Net, assurez-vous d'avoir correctement installé toutes les mises à jour Windows sur votre système.

---

1 Créez une sauvegarde des fichiers de configuration du chargeur distant. L'emplacement par défaut des fichiers est `C:\...\RemoteLoader\`*`nomchargeurdistant`*`-config.txt`.

2 Vérifiez que les pilotes sont bien arrêtés. Pour connaître les instructions, reportez-vous à la Section 9.4.1, « Arrêt des pilotes », page 93.

3 Arrêtez le service ou le daemon du chargeur distant pour chaque pilote.

- **Windows :** dans la console du chargeur distant, sélectionnez l'instance du chargeur distant, puis cliquez sur **Arrêter**.
- **Chargeur distant Java :** `dirxml_jremote -config` *`chemin_vers_fichier_config`* `-u`

4 Arrêtez le processus Icache à l'aide du Gestionnaire des tâches Windows.

5 (Conditionnel) Pour exécuter une installation silencieuse sur un serveur Windows, assurez-vous que le fichier `silent.properties` inclut le chemin d'accès au répertoire qui contient les fichiers installés du chargeur distant. Par exemple :

```
X64_CONNECTED_SYSTEM_LOCATION=c:\novell\remoteloader\64bit
```

Le programme d'installation ne détecte pas le chemin d'accès par défaut de l'installation précédente.

6 Exécutez le programme d'installation du chargeur distant.

La procédure d'installation met à jour les fichiers et les binaires avec la version actuelle. Pour plus d'informations, reportez-vous à la Partie III, « Installation du moteur Identity Manager », page 55.

7 Une fois l'installation terminée, vérifiez que vos fichiers de configuration contiennent bien les informations de votre environnement.

8 (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 9 page 380.

9 Lancez le service ou le daemon du chargeur distant pour chaque pilote.

- **Chargeur distant Java** : `dirxml_jremote -config` *`chemin_accès_fichier_configuration`*
- **Windows** : dans la console du chargeur distant, sélectionnez l'instance du chargeur distant, puis cliquez sur **Démarrer**.

32.4 Mise à niveau du moteur Identity Manager

lorsque vous mettez à niveau le moteur Identity Manager ou mettez à jour séparément une méthode SAML, iMonitor affiche les indicateurs d'état actuel et non actuel pour les méthodes SAML. Vous pouvez ignorer l'indicateur d'état non actuel, dans la mesure où eDirectory utilise correctement la méthode mise à jour. La procédure de mise à niveau du moteur redémarre eDirectory, qui, en interne, prend soin d'utiliser la méthode SAML mise à jour. Si vous mettez à jour séparément une méthode SAML, redémarrez manuellement le serveur eDirectory pour utiliser la méthode SAML mise à jour.

Assurez-vous que le fichier de cache ne contienne aucun événement avant d'entamer 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 du cache de travail existants du pilote MapDB (dx*). 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

Après avoir mis à niveau le chargeur distant et les services basés sur le rôle, vous pouvez mettre à niveau le moteur Identity Manager. La procédure de mise à niveau met à jour les fichiers du module d'interface du pilote stockés dans le système de fichiers sur l'ordinateur hôte.

1. Vérifiez que les pilotes sont bien arrêtés. Pour plus d'informations, reportez-vous à la Section 9.4.1, « Arrêt des pilotes », page 93.
2. Lancez le programme d'installation du moteur Identity Manager à partir de `IDM`*`version`*`_Win:\products\IDM\Windows\setup\idm_install.exe`.
3. Sélectionnez la langue à utiliser pour l'installation.
4. Lisez, puis acceptez l'accord de licence.
5. Pour mettre à jour le moteur Identity Manager et les fichiers du module d'interface du pilote, sélectionnez les options suivantes :
   - **Serveur Identity Manager**
   - **Plug-ins iManager pour Identity Manager**
   - **Pilotes**
6. Spécifiez un utilisateur et le mot de passe utilisateur avec droits d'administrateur sur eDirectory au format LDAP.
7. Lisez le résumé, puis cliquez sur **Installer**.
8. Lisez le résumé de l'installation, puis cliquez sur **Terminé**.

32.5 Mise à niveau des applications d'identité et d'Identity Reporting

Cette section fournit des informations sur la mise à niveau des applications d'identité et des logiciels pris en charge, 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
- Identity Reporting

NetIQ fournit un programme de mise à niveau pour ces composants. Ce programme se trouve dans le répertoire `products\CommonApplication\` du paquetage d'installation d'Identity Manager. Accédez au répertoire qui contient le fichier `ApplicationUpgrade.exe`.

Après la mise à niveau, les composants sont mis à niveau vers les versions suivantes :

- Tomcat – `8.5.27`
- ActiveMQ – `5.15.2`
- Java – `1.80_162`
- One SSO Provider – `6.2.1`
- Self-Service Password Reset – `4.2.0.4`

- Applications d'identité– `4.7.0`
- Identity Reporting – `6.0.0`

Cette section fournit des informations concernant les rubriques suivantes :

32.5.1 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.xml` 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.

32.5.2 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 une mise à niveau ou une migration vers Identity Manager 4.7 à partir d'une version antérieure à la version 4.5.6. Pour plus d'informations sur la mise à niveau vers Identity Manager 4.5, reportez-vous à la section Mise à niveau d'Identity Manager du *Guide d'installation de NetIQ Identity Manager*.
- **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.

  Sur un serveur Windows, le programme de mise à niveau stocke les fichiers temporaires dans un répertoire spécifié dans la variable d'environnement `%temp%`. Si ce répertoire ne dispose pas de l'espace requis, définissez les variables d'environnement TEMP et TMP sur un répertoire de votre système de fichiers qui dispose de l'espace suffisant. Le programme de mise à niveau sera redirigé vers ce répertoire pour stocker les fichiers de ce répertoire.

  Pour définir ces variables d'environnement sur un autre répertoire, procédez comme suit avant de démarrer la mise à niveau :

  1. Ouvrez l'invite de commande, puis entrez la commande suivante :

     ```
     SET TMP=D:\custom_tmp
     SET TEMP=D:\custom_tmp
     ```

     où `D:\custom_tmp` est le chemin vers le répertoire qui dispose de suffisamment d'espace.

REMARQUE : pour un environnement en grappe, 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.

  REMARQUE : assurez-vous d'avoir installé le serveur d'applications Tomcat à l'aide d'un programme d'installation fourni à des fins de commodité lors de l'installation d'Identity Manager. La procédure de mise à niveau vous permet uniquement de mettre à niveau l'instance Tomcat installée à l'aide du programme d'installation fourni à des fins de commodité.

- **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 « Mise à niveau de la base de données PostgreSQL » page 384.
- **Les applications d'identité et les pilotes Identity Reporting sont mis à niveau :** assurez-vous d'avoir mis à niveau les pilotes suivants pour les applications d'identité et Identity Reporting.
  - Pilote d'application utilisateur
  - Pilote de rôles et de ressources
  - Pilote de passerelle système gérée
  - Pilote de service de collecte de données

  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).
- **L'administrateur dispose des privilèges d'accès les plus élevés :** fournit les privilèges d'accès les plus élevés à l'administrateur.
- **Les paramètres du contrôle de compte utilisateur sont modifiés en Ne jamais m'avertir) :**

  accédez à **Panneau de configuration > Comptes d'utilisateurs** et **Modifier les paramètres de contrôle du compte d'utilisateur** sur **Ne jamais m'avertir**.
- **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.

  Par exemple : `set CATALINA_OPTS="-Dsspr.applicationPath=C:\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. Accédez à **Your ID > Configuration Manager** (Votre ID > Gestionnaire de configuration) dans le menu déroulant.
  3. Cliquez sur **LocalDB**.
  4. Cliquez sur **Download LocalDB** (Télécharger la base de données locale).

32.5.3 Mise à niveau de la base de données PostgreSQL

IMPORTANT : la procédure de mise à niveau peut prendre un certain temps en fonction de la taille de la base de données. Par conséquent, planifiez votre mise à niveau en conséquence.

1. Arrêtez le service PostgreSQL en cours d'exécution sur votre serveur.
2. Renommez le répertoire `postgres` à partir de l'emplacement `C:\Netiq\idm\apps`.

   Par exemple, modifiez `postgres` pour le renommer `postgresql_9_3`.
3. Installez la version de PostgreSQL prise en charge sur votre système d'exploitation.

   Vous devez choisir un emplacement différent de l'emplacement d'installation actuel de PostgreSQL.

   3a Montez le fichier image `Identity_Manager_4.7_Windows.iso` et accédez au répertoire `products\CommonApplication\postgre_tomcat_install` contenant les fichiers d'installation de PostgreSQL.

   3b Installez l'application PostgreSQL en exécutant le fichier TomcatPostgreSQL.exe.

   Sélectionnez uniquement l'option **PostgreSQL** pendant l'installation.

   REMARQUE : n'indiquez pas les détails de la base de données sur la page **Détails de PostgreSQL**. Assurez-vous que les options **Créer un compte de connexion à la base de données** et **Créer une base de données vide** sont désélectionnées.
4. Arrêtez le service PostgreSQL que vous venez d'installer. Accédez à **Services**, recherchez le service PostgreSQL 9.6 et arrêtez-le.

   REMARQUE : les utilisateurs appropriés peuvent effectuer des opérations d'arrêt après avoir procédé à une authentification valide.
5. Modifiez les autorisations pour le répertoire PostgreSQL qui vient d'être installé en effectuant les opérations suivantes :

   Créez un utilisateur `postgres` :

   1. Accédez à **Panneau de configuration > Comptes d'utilisateurs > Comptes d'utilisateurs > Gérer les comptes**.
   2. Cliquez sur **Ajouter un compte d'utilisateur**.
   3. Sur la page Ajouter un utilisateur, spécifiez `postgres` en tant que nom d'utilisateur et indiquez un mot de passe pour l'utilisateur.

   Octroyez des autorisations sur les répertoires PostgreSQL existants et récemment installés à l'utilisateur `postgres` :

   1. Cliquez avec le bouton droit sur le répertoire PostgreSQL et accédez à **Propriétés > Sécurité > Modifier**.
   2. Sélectionnez **Contrôle total** pour l'utilisateur afin de fournir des autorisations complètes.
   3. Cliquez sur **Appliquer**.
6. Accédez au répertoire PostgreSQL en tant qu'utilisateur `postgres`.
   1. Connectez-vous au serveur en tant qu'utilisateur `postgres`.

      Avant de vous connecter, vérifiez que l'utilisateur `postgres` peut se connecter au serveur Windows en vérifiant si une connexion à distance est autorisée pour cet utilisateur.
   2. Ouvrez une invite de commande et définissez `PGPASSWORD` à l'aide de la commande suivante :

```
set PGPASSWORD=<your pg password>
```

3. Accédez au répertoire PostgreSQL que vous venez d'installer.

   Par exemple : `C:\Users\postgres>cd C:\NetIQ\idm\apps1\postgresql962\bin`.

7 Mettez à niveau PostgreSQL à partir du nouveaux répertoire `bin` PostgreSQL. Exécutez la commande suivante, puis cliquez sur **Entrée**.

```
pg_upgrade.exe --old-datadir "C:\NetIQ\idm\apps1\postgres\data" --new-datadir
"C:\NetIQ\idm\apps1\postgresql962\data" --old-bindir
"C:\NetIQ\idm\apps1\postgres\bin" --new-bindir
"C:\NetIQ\idm\apps1\postgresql962\bin"
```

8 Démarrez le service de base de données PostgreSQL mis à niveau.

Accédez à **Services**, recherchez le service PostgreSQL 9.6 et démarrez-le.

REMARQUE : les utilisateurs appropriés peuvent effectuer des opérations de démarrage après avoir procédé à une authentification valide.

---

9 Désactivez l'ancien service PostgreSQL pour veiller à ce que le service ne démarre pas automatiquement.

10 (Facultatif) Supprimez les anciens fichiers de données du répertoire `bin` du nouveau service PostgreSQL installé.

1. Connectez-vous en tant qu'utilisateur `postgres`.
2. Accédez au répertoire bin et exécutez les fichiers `analyze_new_cluster.bat` et `delete_old_cluster.bat`.

   Par exemple : `C:\NetIQ\idm\apps1\postgresql961\bin`

REMARQUE : vous ne devez exécuter cette étape que si vous souhaitez supprimer les anciens fichiers de données.

32.5.4 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.

32.5.5 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 Effectuez le déploiement et redémarrez le pilote.

10 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.
- Si vous installez tous les modèles de notification lors de la mise à niveau du paquetage de pilote d'application utilisateur, déployez les objets **Collection de notification par défaut** sur votre serveur Identity Manager.

32.5.6 Utilisation de la procédure guidée de mise à niveau

La procédure suivante décrit comment mettre à niveau les applications d'identité, OSP, SSPR, Tomcat, ActiveMQ et Identity Reporting à l'aide de l'assistant.

1 Connectez-vous au serveur sur lequel vous voulez exécuter la procédure de mise à niveau.

2 Montez le fichier image `.iso`, accédez au répertoire contenant le fichier exécutable de mise à niveau, situé par défaut dans le répertoire `products\CommonApplication\`.

3 Lancez le programme de mise à niveau. Cliquez avec le bouton droit sur le fichier exécutable `ApplicationUpgrade.exe`, puis sélectionnez **Exécuter en tant qu'administrateur**.

4 Sur la page **Introduction**, passez en revue les composants Identity Manager que vous pouvez mettre à niveau, puis cliquez sur **Suivant**.

5 Lisez et acceptez l'accord de licence, puis cliquez sur **Suivant**.

6 Passez en revue la page **Applications déployées**, puis cliquez sur **Suivant**.

Cette page répertorie les composants actuellement installés ainsi que leurs versions. Si d'autres applications sont déployées sur le serveur, la procédure de mise à niveau affiche un avertissement indiquant que ces applications risquent de ne pas fonctionner correctement après la mise à niveau.

Vous devez les restaurer manuellement à partir de la sauvegarde créée par la procédure de mise à niveau.

7 Pour poursuivre la mise à niveau, cliquez sur **Suivant**.

8 Terminez la procédure guidée en utilisant les paramètres ci-dessous. Ce programme propage automatiquement les valeurs des composants existants. Veillez à spécifier les valeurs adéquates pour les paramètres.

- **Dossier d'installation du fournisseur d'authentification unique One**

  Représente le chemin d'un répertoire dans lequel le programme de mise à niveau crée les fichiers d'application pour OSP. Si le chemin n'est pas correct, accédez à l'emplacement auquel OSP est installé.

- **Dossier d'installation de SSPR**

  Représente le chemin d'un répertoire dans lequel le programme de mise à niveau crée les fichiers d'application pour SSPR. Si le chemin n'est pas correct, accédez à l'emplacement auquel SSPR est installé.

- **Dossier d'installation de l'application utilisateur**

  Représente le chemin d'un répertoire dans lequel le programme de mise à niveau crée les fichiers d'application pour l'application utilisateur. Si le chemin n'est pas correct, accédez à l'emplacement auquel l'application utilisateur est installée.

- **Connexion à la base de données**

  Représente les paramètres pour la connexion à la base de données de l'application utilisateur. Les applications d'identité se connectent également à cette base de données. Le programme de mise à niveau inclut ces informations dans le fichier de configuration de l'application utilisateur.

  Plate-forme de la base de données

  Représente la plate-forme de la base de données de l'application utilisateur.

  Hôte de la base de données

  Spécifie le nom ou l'adresse IP du serveur qui héberge l'application utilisateur.

  Port de la base de données

  Spécifie le port utilisé par le serveur de base de données pour communiquer avec l'application utilisateur.

  Fichier JAR du pilote de base de données

  Spécifie le fichier JAR pour la plate-forme de base de données.

  Le fournisseur de la base de données fournit le fichier JAR du pilote, qui représente le fichier JAR pour le serveur de base de données. Par exemple, pour PostgreSQL, vous pouvez spécifier le fichier `postgresql-9.4-1212.jdbc42.jar`, situé par défaut dans le dossier `C:\NetIQ\idm\apps\postgres`. De même, spécifiez les fichiers JAR appropriés pour votre plate-forme de base de données.

- **(Conditionnel) Connexion à la base de données de création de rapports**

  Représente les paramètres de connexion à la base de données d'Identity Reporting.

  Hôte de la base de données

  Spécifie le nom ou l'adresse IP du serveur qui héberge l'application utilisateur.

  Port de la base de données

  Spécifie le port utilisé par le serveur de base de données pour communiquer avec l'application utilisateur.

  Nom de la base de données

  Indique le nom de la base de données. Par défaut, le nom de la base de données est `idmrptdb`.

- **(Conditionnel) Références de la base de données de création de rapports**

  Utilisateur de la base de données d'Identity Reporting

  Indique le nom d'un compte qui permet à l'application utilisateur d'accéder à des données et de les modifier dans les bases de données. Par défaut, le nom d'utilisateur de la base de données est `postgres`.

  Mot de passe de la base de données de création de rapports

  Indique le mot de passe pour le nom d'utilisateur spécifié.

  Mise à niveau de la base de données de création de rapports

  Mettre à niveau la base de données maintenant : le programme de mise à niveau met à jour le schéma des tables de la base de données de création de rapports dans le cadre de la procédure de mise à niveau.

Mettre à niveau la base de données au démarrage de l'application : le programme de mise à niveau laisse des instructions pour mettre à jour le schéma des tables de la base de données au premier démarrage de l'application utilisateur après la mise à niveau.

Écrire SQL dans un fichier : génère un script SQL que l'administrateur de la base de données peut exécuter pour mettre à jour les base de données. Si vous choisissez cette option, vous devez également spécifier un nom pour le **Fichier de schéma**. Le paramètre se trouve dans la configuration **Fichier de sortie SQL**. Vous pouvez sélectionner cette option si vous ne disposez pas des autorisations nécessaires pour créer ou modifier une base de données dans votre environnement. Pour plus d'informations sur la création de tableaux avec le fichier, reportez-vous à la Section 15.7.2, « Création manuelle du schéma de base de données », page 224.

Fichier JAR du pilote de base de données

Spécifie le fichier JAR pour la plate-forme de base de données.

Le fournisseur de la base de données fournit le fichier JAR du pilote, qui représente le fichier JAR pour le serveur de base de données. Par exemple, pour PostgreSQL, vous pouvez spécifier le fichier `postgresql-9.4-1212.jdbc42.jar`, situé par défaut dans le dossier `C:\NetIQ\idm\apps\postgres`. De même, spécifiez les fichiers JAR appropriés pour votre plate-forme de base de données.

- **Mettre à niveau la base de données**

  Mettre à niveau la base de données maintenant

  Le programme de mise à niveau met à jour le schéma des tables de la base de données dans le cadre de la procédure de mise à niveau.

  Mettre à niveau la base de données au démarrage de l'application

  Le programme de mise à niveau laisse des instructions pour mettre à jour le schéma des tables de la base de données au premier démarrage de l'application utilisateur après la mise à niveau.

  Écrire SQL dans un fichier

  Génère un script SQL que l'administrateur de la base de données peut exécuter pour mettre à jour les base de données. Si vous choisissez cette option, vous devez également spécifier un nom pour le **Fichier de schéma**. Le paramètre se trouve dans la configuration **Fichier de sortie SQL**. Vous pouvez sélectionner cette option si vous ne disposez pas des autorisations nécessaires pour créer ou modifier une base de données dans votre environnement. Pour plus d'informations sur la création de tableaux avec le fichier, reportez-vous à la Section 15.7.2, « Création manuelle du schéma de base de données », page 224.

- **Administrateur de la base de données**

  Représente le nom et le mot de passe de l'administrateur de la base de données.

  Nom d'utilisateur de la base de données

  Spécifie le compte d'un administrateur de la base de données qui peut créer des tables de base de données, des vues et d'autres artefacts.

  Mot de passe

  Spécifie le mot de passe de l'administrateur de la base de données.

- **Connexion à la base de données de création de rapports**

  Représente le nom et le mot de passe de l'hôte de l'administrateur de la base de données.

  Nom d'utilisateur de la base de données

  Spécifie le compte d'un administrateur de la base de données qui peut créer des tables de base de données, des vues et d'autres artefacts.

Mot de passe

Spécifie le mot de passe de l'administrateur de la base de données.

9 Passez en revue la page **Résumé avant la mise à niveau**, puis cliquez sur **Installer**.

La procédure de mise à jour arrête le service Tomcat et démarre la mise à niveau, laquelle peut prendre un certain temps.

10 Une fois la procédure de mise à niveau terminée, passez en revue les fichiers journaux correspondants à l'emplacement `/tmp/rbpm_upgrade/` et si vous devez mettre à jour quelques configurations manuellement, reportez-vous à la Section 32.5.7, « Tâches postérieures à la mise à niveau », page 389.

En fonction de l'endroit où vous avez installé les composants, le processus crée le répertoire de sauvegarde à cet emplacement et ajoute un horodatage (indiquant le moment de la sauvegarde) au répertoire sauvegardé.

Exemples :

- Tomcat – `C:\NetIQ\idm\apps\tomcat_backup_02262018_033634`
- OSP et SSPR - `C:\NetIQ\idm\apps\osp_sspr_backup_02262018_033634`
- ActiveMQ - `C:\NetIQ\idm\apps\activemq_backup_02262018_033634`
- Application utilisateur - `C:\NetIQ\idm\apps\UserApplication_backup_02262018_033634`
- Identity Reporting - `C:\NetIQ\idm\apps\IdentityReporting_backup_02262018_033634`

32.5.7 Tâches postérieures à la mise à niveau

Après la mise à niveau des applications d'identité, veuillez effectuer les opérations suivantes :

Vous devez également restaurer manuellement les paramètres personnalisés pour Tomcat, SSPR, OSP ou les applications d'identité.

Effectuez les opérations post-mise à niveau pour les composants requis :

- « Java » page 389
- « Tomcat » page 390
- « Applications d'identité » page 391
- « One SSO Provider » page 391
- « Self-Service Password Reset » page 391
- « Kerberos » page 392

Java

Vérifiez que les certificats situés à l'emplacement du nouveau JRE mis à niveau (`jre/lib/security/cacerts`) correspondent à ceux se trouvant à l'emplacement de l'ancien JRE. Importez manuellement les certificats manquants dans votre fichier `cacerts`.

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 : `C:\NetIQ\idm\apps\jre`.

---

2 Vérifiez que l'emplacement d'origine de JRE est `tomcat\bin\setenv.bat`.

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 `C:\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 à l'emplacement `C:\NetIQ\eDirectory\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 <User Application certificate alias> -
srckeystore  <backup cacert> -srcstorepass changeit -destkeystore
C:\NetIQ\eDirectory\jre\lib\security\cacerts
```

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 mettez à niveau Identity Manager à partir de la version 4.5.6, vous devez créer manuellement les index composés pour chaque attribut que vous souhaitez utiliser pour trier les utilisateurs dans le tableau de bord Identity Manager. Reportez-vous à la section « Création d'index composés » page 217.

1 Lancez le fichier de l'utilitaire configupdate (`configupdate.bat`).

   Dans le fichier `configupdate.bat.properties`, assurez-vous que la valeur `use_console` est définie sur `false` (faux).

2 Connectez-vous au serveur du coffre-fort d'identité et acceptez le certificat eDirectory.

3 Sous l'onglet **Clients SSO**, accédez à **RBPM**, puis cliquez sur **Afficher les options avancées**.

4 Définissez l'option **Configuration SAML RBPM à eDirectory** sur Auto.

One SSO Provider

Par défaut, l'entrée `LogHost` située dans le fichier `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.

Self-Service Password Reset

Après la mise à niveau de SSPR, mettez à jour le paramètre de client SSO à l'aide de l'utilitaire de mise à jour de configuration. Pour plus d'informations, reportez-vous au point « Self Service Password Reset » page 255 de la Section 15.8.5, « Paramètres des clients SSO », page 252.

Pour mettre à jour les détails de configuration de SSPR, procédez comme suit :

1 Connectez-vous au portail SSPR en tant qu'administrateur.

2 Mettez à jour les détails du serveur d'audit :

   2a Accédez à **YourID > Configuration Editor** (Éditeur de configuration) et spécifiez le mot de passe de configuration.

   2b Sélectionnez **Settings > Auditing > Audit Forwarding > Syslog Audit Server Certificates** (Paramètres > Audit > Réacheminement d'audit > Certificats de serveur d'audit Syslog).

   2c Importez ces certificats depuis le serveur, puis cliquez sur **Save** (Enregistrer).

3 Importez **LocalDB** dans SSPR :

   3a Accédez à **YourID > Configuration Manager** (Votre ID > Gestionnaire de configuration) dans le menu déroulant.

   3b Cliquez sur **LocalDB**.

   3c Cliquez sur **Import (Upload) LocalDB Archive File** (Importer [Télécharger] le fichier d'archive LocalDB).

4 (Conditionnel) Pour restreindre la configuration de SSPR :

   4a Accédez à **YourID > Configuration Manager** (Votre ID > Gestionnaire de configuration) dans la liste.

   4b Cliquez sur **Restreindre la configuration**.

5 Pour configurer les autorisations de l'administrateur pour SSPR, reportez-vous à la Section 14.2.3, « Tâches de post-installation », page 184.

Pour vérifier si la mise à niveau a réussi, lancez les composants mis à niveau.

Par exemple, lancez le tableau de bord Identity Manager, puis cliquez sur **À propos de**. Vérifiez si l'application affiche la nouvelle version, par exemple **4.7.0**.

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.

32.6 Mise à niveau d'Identity Reporting

Identity Reporting inclut deux pilotes. De même, vous devrez peut-être migrer le contenu de NetIQ Event Auditing Service vers Sentinel Log Management for IGA. Effectuez la mise à niveau dans l'ordre suivant :

1. Mettez à niveau le paquetage de pilotes pour les services de collecte de données.
2. Mettez à niveau le paquetage de pilotes pour le service de passerelle système gérée.
3. Migrez vers Sentinel Log Management for IGA
4. Mettez à niveau Identity Reporting

32.6.1 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, **Managed System Gateway Base package 2.0.0.20120509205929**.

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 Terminez la configuration du pilote. Pour plus d'informations, reportez-vous aux sections suivantes :

- Section 19.1.2, « Configuration du pilote de la passerelle système gérée (MSG, Managed System Gateway) », page 278
- Section 19.1.3, « Configuration du pilote pour le service de collecte de données (DCS, Data Collection Service) », page 279

10 Répétez la procédure de l'Étape 2 à l'Étape 9 pour mettre à niveau le paquetage pour le pilote du service de collecte de données.

11 Assurez-vous que les pilotes de passerelle système gérée et du service de collecte de données sont connectés à la version d'Identity Manager mise à niveau.

32.6.2 Mise à niveau d'Identity Reporting

Avant de procéder à la mise à niveau d'Identity Reporting, vous devez mettre à niveau les applications d'identité et SLM for IGA. Pour mettre à niveau la version 4.0.2 ou ultérieure d'Identity Reporting, installez la nouvelle version sur l'ancienne. Pour plus d'informations, reportez-vous à la section « Installation d'Identity Reporting » page 265.

32.6.3 Modification des références à reportRunner dans la base de données

Après la mise à niveau d'Identity Reporting et avant le premier démarrage de Tomcat, veillez à mettre à jour les références de reportRunner à partir de la base de données.

1 Arrêtez Tomcat.

2 Accédez au répertoire d'installation d'Identity Reporting et renommez le dossier `reportContent` en `ORG-reportContent`.

Par exemple : `C:\NetIQ\idm\apps\IdentityReporting`.

3 Nettoyez les répertoires temporaire et de travail sous le dossier Tomcat.

4 Connectez-vous à la base de données PostgreSQL.

4a Recherchez les références à reportRunner dans les tables suivantes :

- `idm_rpt_cfg.idmrpt_rpt_params`
- `idm_rpt_cfg.idmrpt_definition`

4b Émettez les instructions de suppression suivantes :

```
DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE
rpt_def_id='com.novell.content.reportRunner';

DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE
def_id='com.novell.content.reportRunner';
```

5 Démarrez Tomcat.

Vérifiez dans les journaux si les rapports sont régénérés avec le bon reportRunner.

6 Connectez-vous à Identity Reporting et exécutez les rapports.

32.6.4 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.

32.7 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 de correctif, par exemple `analyzer_4.6_patch1_20121128.zip`, à partir du site Web de téléchargement 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, par exemple **4.6 Update 1** et l'ID du Build **20121128**.

32.8 Mise à niveau des pilotes Identity Manager

NetIQ propose le nouveau contenu de pilote par le biais de **paquetages** plutôt que de fichiers de configuration de pilote. 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).

REMARQUE : si vous mettez à niveau la version 3.*x* du pilote de l'application utilisateur vers le paquetage version 4.0.2 de l'application utilisateur, Designer installe à la fois la version 3.*x* et la version 4.0 des stratégies du même pilote. Le fait d'avoir à la fois les stratégies 3.*x* et 4.0 dans le catalogue du paquetage peut entraîner le dysfonctionnement de Designer. Supprimez les stratégies 3.*x* et conservez les stratégies 4.0.

Vous pouvez mettre à niveau vos pilotes vers des paquetages de l'une des manières suivantes :

- Section 32.8.1, « Création d'un nouveau pilote », page 395
- Section 32.8.2, « Remplacement du contenu existant par du contenu issu de paquetages », page 395
- Section 32.8.3, « Conservation du contenu actuel et ajout de nouveau contenu avec des paquetages », page 396

32.8.1 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.

32.8.2 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 31.5.2, « Exportation de la configuration des pilotes », page 373.

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 32.10, « Restauration de stratégies et de règles personnalisées sur le pilote », page 398.

32.8.3 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 31.5.2, « Exportation de la configuration des pilotes », page 373.

   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.

32.9 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.

32.9.1 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 Designer, ignorez cette étape et allez à la Section 35.3.1, « Copie des informations spécifiques au serveur dans Designer », page 409. 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**.

32.9.2 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

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).

32.10 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.

- Section 32.10.1, « Utilisation de Designer pour restaurer les stratégies et les règles personnalisées sur le pilote », page 398
- Section 32.10.2, « Utilisation d'iManager pour restaurer les stratégies et les règles personnalisées sur le pilote », page 399

32.10.1 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 9.4.2, « Lancement des pilotes », page 94. 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.

32.10.2 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 9.4.2, « Lancement des pilotes », page 94. 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.

33 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 `dib` du coffre-fort d'identité `C:\Novell\NDS\DIBFiles`.
   - **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 `C:\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.bat` 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 `192.99.17.22`
  - **Port TCP du serveur OAuth**
  - **Le serveur OAuth utilise TLS/SSL.**
- Configuration de l'authentification
  - **Fichier Keystore OAuth**. Par exemple, `C:\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://192.99.17.22:8180/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://192.99.179.202:8180/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 235.

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 363. Pour plus d'informations sur la différence entre la mise à niveau et la migration, reportez-vous à la Section 31.2, « Notions de mise à niveau et de migration », page 367.

34 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.

34.1 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 31.2, « Notions de mise à niveau et de migration », page 367.
❑	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 à la Partie I, « Introduction », page 17.
❑	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 Chapitre 6, « Considérations relatives à l'installation », page 49 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 7.1.2, « Conditions préalables et considérations relatives à l'installation du coffre-fort d'identité », page 58.
❑	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 35.4, « Migration du moteur Identity Manager vers un nouveau serveur », page 411.
❑	7. Installez Identity Manager sur le nouveau serveur. Pour plus d'informations, reportez-vous à la section « Planification de l'installation d'Identity Manager » page 37.
❑	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 32.3, « Mise à niveau du chargeur distant », page 379.
❑	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 35.1, « Liste de contrôle pour la migration d'Identity Manager », page 407.
❑	10. Ajoutez le nouveau serveur à l'ensemble de pilotes. Pour plus d'informations, reportez-vous à la Section 32.9.1, « Ajout du nouveau serveur à l'ensemble de pilotes », page 397.
❑	11. Modifiez les informations spécifiques du serveur pour chaque pilote. Pour plus d'informations, reportez-vous à la Section 35.3.1, « Copie des informations spécifiques au serveur dans Designer », page 409.

	Éléments de la liste de contrôle
❑	12. (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 35.3, « Copie des informations spécifiques du serveur pour l'ensemble de pilotes », page 409
❑	13. Mettez à jour vos pilotes au format du paquetage. Pour plus d'informations, reportez-vous à la Section 32.8, « Mise à niveau des pilotes Identity Manager », page 394.
❑	14. (Conditionnel) Si vous disposez de stratégies et de règles personnalisées, restaurez vos paramètres personnalisés. Pour plus d'informations, reportez-vous à la Section 32.10, « Restauration de stratégies et de règles personnalisées sur le pilote », page 398.
❑	15. Supprimez l'ancien serveur de l'ensemble de pilotes. Pour plus d'informations, reportez-vous à la Section 32.9.2, « Suppression de l'ancien serveur de l'ensemble de pilotes », page 397.
❑	16. Activez votre solution Identity Manager mise à niveau. Pour plus d'informations, reportez-vous à la Section 30.6, « Activation d'Identity Manager », page 359.

34.2 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 9.4.1, « Arrêt des pilotes », page 93
- Section 9.4.2, « Lancement des pilotes », page 94

35 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 :

35.1 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 5.3.4, « Configuration recommandée pour le serveur », page 43 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 au Chapitre 15, « Installation des applications d'identité », page 189.
❑	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 35.2, « Préparation de votre projet Designer pour la migration », page 408.

	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 35.4, « Migration du moteur Identity Manager vers un nouveau serveur », page 411.
❑	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 à la Section 35.5, « Migration du pilote d'application utilisateur », page 411.
❑	9. Créez un nouveau pilote de service de rôles et de ressources. Vous ne pouvez pas migrer un pilote existant du service de rôles et de ressources. Pour plus d'informations, reportez-vous à la Section 15.6.3, « Création du pilote du service de rôles et de ressources », page 222.
❑	10. Déployez les deux pilotes dans le coffre-fort d'identité. Pour plus d'informations, reportez-vous à la Section 15.6.4, « Déploiement des pilotes de l'application utilisateur », page 223.
❑	11. Mettez à niveau les applications d'identité. Pour plus d'informations, reportez-vous à la Section 32.5, « Mise à niveau des applications d'identité et d'Identity Reporting », page 381.
❑	12. 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 35.7.1, « Vidage du cache du navigateur », page 413.
❑	13. (Conditionnel) Restaurez vos paramètres personnalisés pour SharedPagePortlet. Pour plus d'informations, reportez-vous à la Section 35.7.3, « Mise à jour du paramètre Timeout maximum pour SharedPagePortlet », page 414.
❑	14. 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 35.7.4, « Désactivation du paramètre de requête automatique pour les groupes », page 414.

35.2 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.

35.3 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 35.3.1, « Copie des informations spécifiques au serveur dans Designer », page 409
- Section 35.3.2, « Modification des informations spécifiques au serveur dans iManager », page 410
- Section 35.3.3, « Modification des informations spécifiques au serveur pour l'application utilisateur », page 411

35.3.1 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 9.4.2, « Lancement des pilotes », page 94.

35.3.2 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.

35.3.3 Modification des informations spécifiques au serveur pour l'application utilisateur

Vous devez reconfigurer l'application utilisateur pour qu'elle reconnaisse le nouveau serveur. Exécutez le fichier `configupdate.bat`.

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. Dans une invite de commande, lancez l'utilitaire de mise à jour de la configuration (`configupdate.bat`).
3. Spécifiez les valeurs telles que décrites au Chapitre 15.8, « Configuration des paramètres pour les applications d'identité », page 235.

35.4 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 Administering Replicas (Administration de répliques) de *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory).
3. Installez le moteur Identity Manager sur le nouveau serveur.

   Pour plus d'informations, reportez-vous à la Partie III, « Installation du moteur Identity Manager », page 55.

35.5 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.

35.5.1 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**.

35.5.2 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**.

35.5.3 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.

35.6 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.
- 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, reportez-vous à la Section 4.4, « Utilisation de la gestion des mots de passe en self-service dans Identity Manager », page 32.

Pour plus d'informations sur la mise à niveau des applications d'identité, reportez-vous à la Section 32.5, « Mise à niveau des applications d'identité et d'Identity Reporting », page 381.

35.7 Fin de la migration des applications d'identité

Après la mise à niveau ou la migration des applications d'identité, terminez la procédure de migration.

35.7.1 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.

35.7.2 Utilisation du fournisseur hérité ou d'un fournisseur externe pour la gestion des mots de passe

Par défaut, Identity Manager utilise SSPR pour la gestion des mots de passe. Toutefois, pour utiliser vos stratégies de mot de passe existantes, vous pouvez utiliser le fournisseur hérité interne d'Identity Manager. Vous pouvez également utiliser un fournisseur externe. Pour plus d'informations sur la configuration d'Identity Manager pour ces fournisseurs, reportez-vous à l'une des sections suivantes :

- « Utilisation du fournisseur hérité pour la gestion des mots de passe oubliés » page 231
- « Utilisation d'un système externe pour la gestion des mots de passe oubliés » page 233

35.7.3 Mise à jour du paramètre Timeout maximum pour SharedPagePortlet

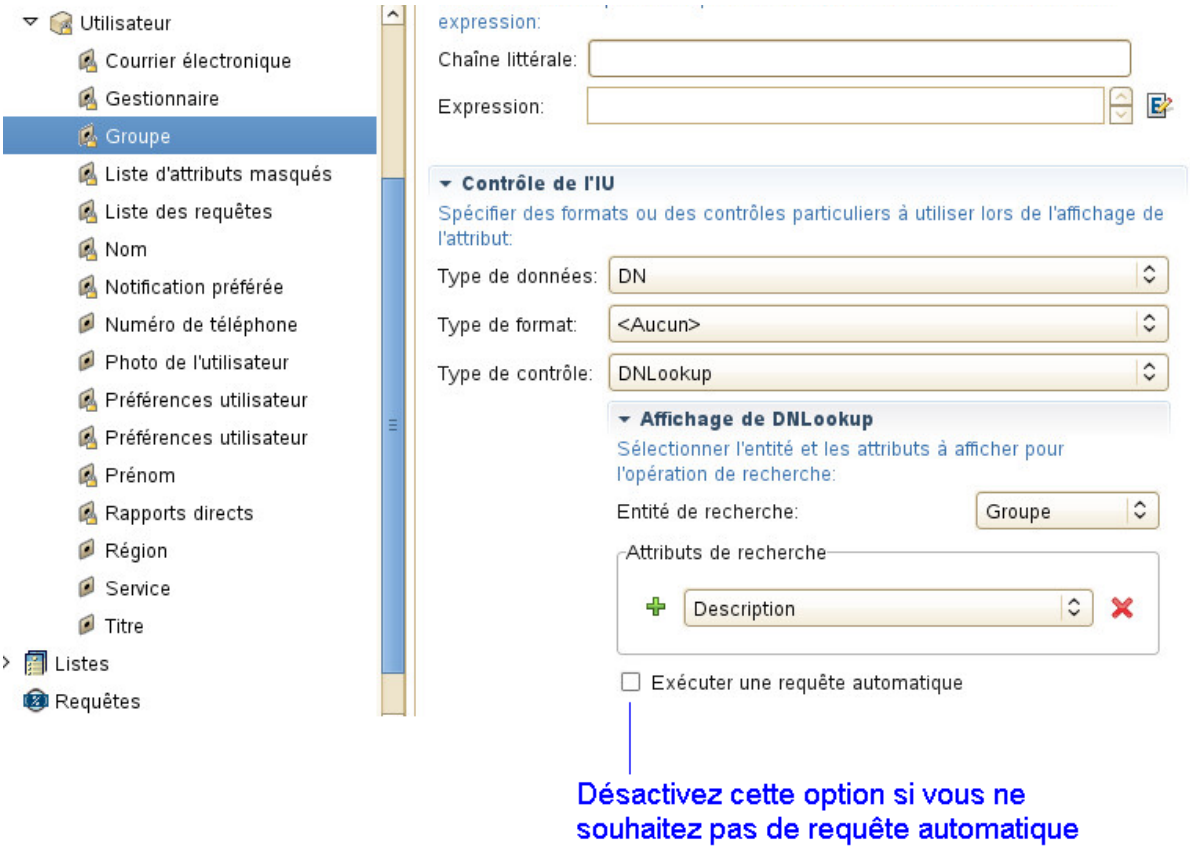
Si vous avez personnalisé l'un des paramètres ou l'une des préférences par défaut de SharedPagePortlet, il a été enregistré dans votre base de données et ce paramètre est écrasé. Par conséquent, l'accès à l'onglet Self-service d'identité ne permet pas toujours de mettre en surbrillance la page partagée 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**.

35.7.4 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 :



Désactivez cette option si vous ne souhaitez pas de requête automatique

36 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.

36.1 Désinstallation du coffre-fort d'identité

Avant de désinstaller le coffre-fort d'identité, vous devez comprendre la structure de votre arborescence eDirectory et connaître les emplacements des répliques. Par exemple, vous devez savoir si votre arborescence comporte plusieurs serveurs.

1. (Conditionnel) Si votre arborescence eDirectory comporte plusieurs serveurs, procédez comme suit :

   1a (Conditionnel) Si le serveur sur lequel vous avez installé eDirectory contient des répliques maîtresses, désignez, avant de supprimer eDirectory, un autre serveur dans l'anneau de répliques qui deviendra un maître.

   Pour plus d'informations, reportez-vous à la section « Managing Partitions and Replicas » (Gestion des partitions et des répliques) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory).

   1b (Conditionnel) Si l'arborescence sur le serveur sur lequel vous avez installé eDirectory contient l'unique copie d'une partition, fusionnez cette partition avec la partition parente ou ajoutez une réplique de cette partition sur un autre serveur et désignez ce dernier le détenteur de la réplique maîtresse.

   Pour plus d'informations, reportez-vous à la section « Managing Partitions and Replicas » (Gestion des partitions et des répliques) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory).

   1c Contrôlez l'état de santé de la base de données eDirectory. Corrigez les erreurs éventuelles 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. Pour désinstaller le coffre-fort d'identité :

   Utilisez l'option du Panneau de configuration permettant d'ajouter et de supprimer des programmes. Par exemple, sous Windows Server 2012 R2, cliquez sur **Programmes et fonctionnalités**. Cliquez avec le bouton droit sur **NetIQ eDirectory**, puis cliquez sur **Désinstaller**.

3 (Conditionnel) Si votre arborescence eDirectory comporte plusieurs serveurs, procédez comme suit :

3a Supprimez tous les objets spécifiques au serveur encore présents dans l'arborescence.

3b Vérifiez à nouveau l'état de santé pour vous assurer que le serveur a bien été supprimé de l'arborescence.

Pour plus d'informations, reportez-vous à la section « Préservation de l'état de santé d'eDirectory » du *Guide d'administration de NetIQ eDirectory*.

36.2 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 « Keeping eDirectory Healthy » (Maintenance de l'état de santé de eDirectory) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

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.

36.3 Désinstallation du moteur Identity Manager

Lorsque vous installez le moteur Identity Manager, la procédure d'installation place un script de désinstallation sur le serveur 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 36.2, « Suppression d'objets du coffre-fort d'identité », page 418.

Pour désinstaller le moteur Identity Manager sur un serveur Windows, utilisez l'option du Panneau de configuration permettant d'ajouter et de supprimer des programmes. Par exemple, sous Windows 2012 R2, cliquez sur **Programmes et fonctionnalités**. Cliquez avec le bouton droit sur **Identity Manager**, puis cliquez sur **Désinstaller**.

36.4 Désinstallation du chargeur distant

Lorsque vous installez le chargeur distant, la procédure d'installation place un script de désinstallation sur le serveur. Ce script vous permet de supprimer l'ensemble des services, paquetages et répertoires créés pendant l'installation.

Pour désinstaller le chargeur distant sur un serveur Windows, utilisez l'option du Panneau de configuration permettant d'ajouter et de supprimer des programmes.

36.5 Désinstallation des applications d'identité

Vous devez désinstaller chaque composant du module de provisioning basé sur les rôles (RBPM), comme les pilotes et la base de données.

Si vous devez désinstaller les composants d'exécution associés à RBPM, le programme de désinstallation redémarre automatiquement votre serveur, à moins que vous n'exécutiez le programme de désinstallation en mode silencieux sous Windows. Vous devez redémarrer manuellement le serveur Windows.

REMARQUE : avant de désinstaller le module RBPM, désinstallez le moteur Identity Manager. Pour plus d'informations, reportez-vous à la Section 36.3, « Désinstallation du moteur Identity Manager », page 418.

36.5.1 Suppression des pilotes pour le module de provisioning basé sur les rôles

Vous pouvez utiliser Designer ou iManager pour supprimer le pilote de l'application utilisateur et celui du service de rôles et de ressources.

1. Arrêtez les pilotes de l'application utilisateur et du service de rôles et de ressources. En fonction du composant utilisé, effectuez l'une des opérations suivantes :
   - **Designer :** 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 du pilote, puis cliquez sur **Arrêter le pilote**.
2. Supprimez les pilotes de l'application utilisateur et du service de rôles et de ressources. En fonction du composant utilisé, effectuez l'une des opérations suivantes :
   - **Designer :** 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.

36.5.2 Désinstallation des applications d'identité

Vous devez désinstaller l'application utilisateur et sa base de données de Tomcat. Cette procédure explique comment supprimer l'application utilisateur et sa base de données de Tomcat et PostgreSQL. Si vous utilisez un autre serveur d'applications et une autre base de données, reportez-vous à la documentation du produit pour connaître la procédure à suivre.

IMPORTANT : soyez prudent lorsque vous supprimez l'application utilisateur, car le processus supprime tous les dossiers et fichiers se trouvant dans le dossier où ont été installés les scripts et les fichiers accompagnant l'application utilisateur. Si vous supprimez les fichiers, il se peut que vous désinstalliez involontairement Tomcat ou PostgreSQL. Par exemple, le dossier de désinstallation est généralement `C:\NetIQ\idm\apps\UserApplication`. Ce dossier contient également les dossiers de Tomcat et PostgreSQL.

---

1. Connectez-vous au serveur sur lequel vous avez installé l'application utilisateur.
2. Ouvrez l'option du Panneau de configuration permettant d'ajouter et de supprimer des programmes. Par exemple, sous Windows Server 2012 R2, cliquez sur **Programmes et fonctionnalités**.
3. Cliquez avec le bouton droit sur **l'application utilisateur Identity Manager**, puis cliquez sur **Désinstaller**.

36.6 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 36.6.1, « Suppression des pilotes de création de rapports », page 420.
2. Supprimez Identity Reporting. Pour plus d'informations, reportez-vous à la Section 36.6.2, « Désinstallation d'Identity Reporting », page 421.
3. Supprimez Sentinel. Pour plus d'informations, reportez-vous à la section Désinstallation de Sentinel du Guide d'installation de NetIQ Identity Manager pour Linux.

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.

36.6.1 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.

36.6.2 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 36.6.1, « Suppression des pilotes de création de rapports », page 420.

IMPORTANT : avant d'exécuter le programme de désinstallation d'Identity Reporting, vérifiez que vous avez copié vos rapports générés se trouvant dans le répertoire d'installation de Reporting à un autre emplacement sur votre ordinateur, car la procédure de désinstallation supprime tous les fichiers et dossiers du répertoire où Reporting était installé. Par exemple, le dossier d'installation de Reporting est `C:\NetIQ\idm\apps\IDMReporting`.

Pour désinstaller Identity Reporting, employez l'utilitaire du Panneau de configuration permettant d'ajouter et de supprimer des programmes. Par exemple, sous Windows Server 2012 R2, cliquez sur **Programmes et fonctionnalités**. Cliquez avec le bouton droit sur **Identity Reporting**, puis cliquez sur **Désinstaller**.

36.7 Désinstallation d'Analyzer

1 Fermez Analyzer.

2 Désinstallez Analyzer.

Utilisez l'option du Panneau de configuration permettant d'ajouter et de supprimer des programmes. Par exemple, sous Windows Server 2008, cliquez sur **Programmes et fonctionnalités**. Cliquez avec le bouton droit sur **Analyzer pour Identity Manager**, puis cliquez sur **Désinstaller**.

36.8 Désinstallation d'iManager

Cette section explique comment désinstaller iManager et iManager Workstation. Il n'est pas nécessaire de respecter un ordre spécifique pour désinstaller iManager ou les composants tiers associés. NetIQ recommande de prendre note des considérations suivantes concernant la désinstallation de l'un de ces composants :

- Si vous désinstallez le serveur Web ou le conteneur de servlet, vous ne serez plus en mesure d'exécuter iManager.
- Quelle que soit la plate-forme, le programme de désinstallation supprime uniquement les fichiers qu'il a installés initialement. En d'autres termes, il ne supprime pas les fichiers créés par l'application pendant son fonctionnement. Par exemple, les fichiers journaux et les fichiers de configuration créés automatiquement pendant l'exécution de Tomcat.

- Le programme de désinstallation ne supprime pas les fichiers qui ont été créés ni les fichiers modifiés au sein de la structure de répertoires qui ont été ajoutés initialement pendant l'installation. Cela permet de s'assurer que le programme de désinstallation ne supprime pas des données par inadvertance.
- La désinstallation d'iManager n'affecte aucune configuration RBS définie dans votre arborescence. Il ne supprime pas les fichiers journaux ni le contenu personnalisé.

IMPORTANT : avant de désinstaller iManager, sauvegardez votre contenu personnalisé ainsi que tous les autres fichiers iManager spéciaux que vous souhaitez conserver. Par exemple, les plug-ins personnalisés.

36.8.1 Désinstallation d'iManager sous Windows

Pour désinstaller des composants iManager, utilisez l'option du Panneau de configuration permettant d'ajouter et de supprimer des programmes. Les conditions suivantes s'appliquent à la procédure de désinstallation :

- L'option du panneau de configuration répertorie Tomcat et NICI séparément d'iManager. Si vous ne les utilisez plus, désinstallez ces programmes.
- Si eDirectory est installé sur le même serveur qu'iManager, ne désinstallez pas NICI. eDirectory a besoin de NICI pour fonctionner.
- Lors de la désinstallation d'iManager, le programme vous demande si vous souhaitez supprimer tous les fichiers d'iManager. Si vous sélectionnez **Oui**, le programme supprime les fichiers, y compris tout le contenu personnalisé. Il ne supprime toutefois pas les objets RBS 2.7. de l'arborescence eDirectory, et l'état du schéma reste inchangé.

36.8.2 Désinstallation d'iManager Workstation

Pour désinstaller iManager Workstation, supprimez le répertoire dans lequel vous avez extrait les fichiers.

36.9 Désinstallation de Designer

1. Fermez Designer.
2. Désinstallez Designer en fonction du système d'exploitation :

   Utilisez l'option du Panneau de configuration permettant d'ajouter et de supprimer des programmes. Par exemple, sous Windows Server 2008, cliquez sur **Programmes et fonctionnalités**. Cliquez avec le bouton droit sur **Designer pour Identity Manager**, puis cliquez sur **Désinstaller**.

37 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.

37.1 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
La procédure de mise à niveau ne définit pas le compte d'administration de l'application utilisateur par défaut en tant que `cn=uaadmin.ou=sa.o=data`. L'erreur suivante est consignée dans le fichier catalina.out. `AuthorizationManagerService [RBPM] Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.com.novell.srvprv.spi.security.IDMAuthorizationException: Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.at com.novell.idm.security.authorization.ldap.LdapRightsUtil.getPropertyRights(LdapRightsUtil.java:152)` `Unable to fetch roles from edirectory in the predefined time set.`	1. Accédez au fichier `setenv.bat` et modifiez la valeur de la propriété `-Dncpclient_req_timeout` sur *1150* dans l'entrée `CATALINA_OPTS`. 2. Relancez Tomcat.
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. Exécutez la commande suivante à partir du répertoire d'installation (par défaut, `C:\NetIQ\idm\apps\UserApplication\`) : `configupdate.bat`

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**. Exécutez la commande suivante à partir du répertoire d'installation (par défaut, `C:\NetIQ\idm\apps\UserApplication\`) : `configupdate.bat`

37.2 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.

37.3 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.

37.4 Dépannage de l'erreur de requête de la page SSPR

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
SSPR signale une erreur de fonctionnement de requête de la page Ce problème se produit lorsque vous cliquez sur le bouton **Précédent** alors que vous êtes sur une page SSPR. SSPR affiche un message de séquence incorrecte dans le journal d'erreurs SSPR similaire à ce qui suit : `ERROR, password.pwm.servlet.TopServlet, 5035 ERROR_INCORRECT_REQUEST_SEQUENCE (expectedPageID=3, submittedPageID=4, url=<some sspr url>`	Désactivez la détection du bouton Précédent à partir de **Gestionnaire de configuration de SSPR > Paramètres > Sécurité > Sécurité Web**. **REMARQUE :** la modification de ce paramètre n'a aucun effet sur les utilisateurs finaux.

Pour les problèmes d'ordre général rencontrés lors de l'authentification ou de la connexion aux applications d'identité, reportez-vous à *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager - Guide de l'administrateur des applications d'identité).

A Exemple de solution de déploiement en cluster Identity Manager sous Windows

Cette annexe fournit des instructions détaillées sur la façon de configurer Identity Manager dans un environnement en cluster sur une plate-forme Windows 2012 R2.

A.1 Conditions préalables

Les versions 8.8.8 SP9 ou 9.0.2 d'eDiretory ou des services ultérieurs sont en cours d'exécution dans un environnement de cluster Windows 2012 R2. Pour obtenir des informations détaillées sur la configuration d'une grappe eDirectory, reportez-vous à la section Mise en grappe des services eDirectory sur Windows du *Guide d'Installation de NetIQ eDirectory*.

REMARQUE : eDirectory ne prend pas en charge l'équilibrage de la charge à l'aide de plusieurs noeuds de grappe. La mise en grappe eDirectory est uniquement prévue dans le cadre de la fonctionnalité de basculement.

A.2 Configuration de NetIQ Identity Manager sur une grappe eDirectory

Cette section part du principe que vous avez déjà configuré une grappe eDirectory.

Utilisez la procédure suivante pour configurer Identity Manager dans un environnement de grappe eDirectory.

1. Dans le **gestionnaire de grappes**, définissez la priorité des rôles mis en grappe eDirectory sur **No Auto Start** (Pas de démarrage automatique) sur le noeud principal.
2. Arrêtez le noeud secondaire.
3. Installez le moteur Identity Manager sur le noeud principal en sélectionnant l'option **Serveur méta-annuaire** dans l'assistant d'installation d'Identity Manager.

   IMPORTANT : veillez à installer le moteur Identity Manager dans un espace de stockage local.

   ---
4. L'assistant d'installation d'Identity Manager arrête le rôle de grappe eDirectory pendant l'installation. Lorsque ce rôle est arrêté, ce rôle peut présenter un état d'échec. Après l'installation, démarrez le rôle de grappe eDirectory à partir du **gestionnaire de grappes**.
5. Définissez la priorité requise pour le rôle eDirectory mis en grappe et activez le noeud secondaire.

6 Installez le moteur Identity Manager sur un noeud secondaire à l'aide de la commande `DCLUSTER_INSTALL`.

Par exemple, `idm_install.exe -DCLUSTER_INSTALL="true"`

A.3 Mise en grappe du chargeur distant

1 Installez le chargeur distant sur les noeuds de grappe principal et secondaire.

REMARQUE : pour le noeud principal et secondaire, vérifiez que le chargeur distant est installé au même emplacement que l'espace de stockage partagé.

2 (Conditionnel) Si vous utilisez des communications sécurisées avec le chargeur distant, stockez tous les certificats SSL dans un espace de stockage partagé.

3 Avant de créer le rôle de grappe du chargeur distant, ouvrez la console du chargeur distant et sélectionnez **Remote Loader as a Windows Service** (Chargeur distant en tant que service Windows).

4 Dans le **gestionnaire de grappes**, sous **Rôles**, créez un nouveau rôle de grappe de chargeur distant.

Spécifiez les informations suivantes pour le rôle :

Role Type (Type de rôle) : service générique

Service Select (Sélection d'un service) : instance du chargeur distant enregistrée en tant que service Windows.

Name (Nom) : nom de rôle de la grappe

Adresse : spécifiez une adresse IP publique

Select Storage (Sélectionnez un espace de stockage) : stockage de grappe partagé

Paramètres de réplication du registre :

1. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\RLConsole`
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\DirXML Remote Loader\Command port 8000`

   Spécifiez le chemin d'accès au registre de l'instance du chargeur distant que vous souhaitez mettre en grappe.
3. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\PassSync`

REMARQUE

- Par défaut, chaque rôle de grappe n'accepte qu'un seul service Windows. Par conséquent, spécifiez un port de commande et un chemin de registre unique correspondant à chaque instance du chargeur distant.
- Le filtre de mot de passe du pilote Active Directory n'est pas pris en charge dans une grappe Windows.

B Configuration d'un environnement multiserveur

Après avoir installé le coffre-fort d'identité, vous pouvez configurer l'annuaire et employer l'utilitaire DHost pour créer, démarrer et arrêter des 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.

B.1 Modification de l'arborescence eDirectory et du serveur de répliques

Une fois le coffre-fort d'identité installé, vous pouvez le configurer à l'aide de l'utilitaire DHost. Pour pouvoir employer 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 7.4, « Configuration du coffre-fort d'identité après l'installation », page 80.

Lorsque vous employez l'utilitaire DHost, 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 DHost 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 Encrypted Replication (Réplication chiffrée) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

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

B.2 Ajout d'une nouvelle arborescence au coffre-fort d'identité

Lorsque vous créez une arborescence dans le coffre-fort d'identité, vous pouvez spécifier une adresse IPv6 pour la nouvelle arborescence, si votre serveur de coffre-fort d'identité prend déjà en charge les adresses IPv6.

B.3 Ajout d'un serveur à une arborescence existante

Vous pouvez ajouter un serveur à une arborescence existante en exécutant le programme d'installation d'eDirectory.

B.4 Suppression du coffre-fort d'identité et de sa base de données du serveur

1. Accédez au répertoire `dsreports`.
2. Supprimez les fichiers HTML que vous avez précédemment créé à l'aide d'iMonitor.

B.5 Suppression d'un objet Serveur eDirectory et des services Annuaire d'une arborescence

L'utilitaire DHost permet de supprimer d'une arborescence les services Annuaire et l'objet Serveur. Pour plus d'informations, reportez-vous au *Guide d'administration de NetIQ eDirectory*.