

---

# NetIQ® Identity Manager

## Guide du programme d'installation intégré

Février 2017

## **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/>.

**Copyright (C) 2017 NetIQ Corporation. Tous droits réservés.**

---

# Table des matières

À propos de ce guide et de la bibliothèque	5
À propos de NetIQ Corporation	7
<b>1 Introduction</b>	<b>9</b>
1.1 Différences entre la procédure d'installation intégrée et les programmes d'installation autonomes	9
1.2 Présentation du processus d'installation intégré	10
1.2.1 Serveur Identity Manager	11
1.2.2 Applications d'identité	11
1.2.3 Identity Reporting	12
1.2.4 Sentinel Log Management for Identity Governance and Administration	12
1.2.5 iManager	13
1.2.6 Designer	13
1.2.7 Analyzer	13
1.3 Présentation de la structure par défaut du coffre-fort d'identité	14
1.3.1 Conteneur système	16
1.3.2 Conteneur de données	16
1.3.3 Conteneur de sécurité	16
<b>2 Planification de l'installation d'Identity Manager</b>	<b>17</b>
2.1 Liste de contrôle de l'installation	17
2.2 Considérations relatives à l'utilisation du programme d'installation intégré	18
2.3 Conditions préalables et configuration système requise	19
2.3.1 Conditions préalables	19
2.3.2 Configuration système requise	20
2.3.3 Composants pouvant être installés	21
2.3.4 Emplacements d'installation par défaut	22
<b>3 Installation d'Identity Manager</b>	<b>25</b>
3.1 Téléchargement du fichier ISO	25
3.2 Utilisation d'un même mot de passe pour tous les paramètres configurés lors de la procédure d'installation intégrée	25
3.3 Utilisation de l'assistant d'installation	26
3.4 Installation silencieuse	27
<b>4 Configuration des composants Identity Manager</b>	<b>29</b>
4.1 Considérations relatives à la configuration des composants	29
4.2 Utilisation de l'assistant de configuration	30
4.3 Modification du fichier de propriétés pour la configuration en mode silencieux	32
4.4 Configuration en mode silencieux	33
<b>5 Présentation des paramètres de configuration</b>	<b>35</b>
5.1 Coffre-fort d'identité	35
5.1.1 Création d'une nouvelle arborescence	35
5.1.2 Ajout à une arborescence existante	37

5.2	Serveur Identity Manager . . . . .	39
5.3	Sentinel Log Management for IGA . . . . .	40
5.4	Applications d'identité . . . . .	40
5.5	Module Novell Identity Reporting . . . . .	42
5.6	Outils . . . . .	44
<b>6</b>	<b>Dernières étapes de la procédure d'installation intégrée</b>	<b>45</b>
6.1	Assignment de l'objet de stratégie de mot de passe aux ensembles de pilotes . . . . .	45
6.1.1	Création de l'objet de stratégie de mot de passe . . . . .	45
6.1.2	Assignment de l'objet de stratégie de mot de passe . . . . .	46
6.2	Configuration des composants Identity Manager . . . . .	46
<b>7</b>	<b>Activation des produits Identity Manager</b>	<b>47</b>
7.1	Achat d'une licence de produit Identity Manager . . . . .	47
7.2	Installation d'une référence d'activation de produit . . . . .	47
7.3	Affichage des activations de produits pour Identity Manager et les pilotes . . . . .	48
7.4	Activation des pilotes Identity Manager . . . . .	48
7.5	Activation d'Analyzer . . . . .	49
7.6	Activation de Designer et de l'administrateur d'assignation de rôles . . . . .	49
<b>8</b>	<b>Désinstallation d'Identity Manager</b>	<b>51</b>
<b>9</b>	<b>Dépannage</b>	<b>53</b>
9.1	Emplacement des fichiers journaux et de propriétés . . . . .	53
9.2	Dépannage en cas d'échec de la configuration . . . . .	53
9.3	Dépannage des problèmes liés au chargeur distant sous Windows . . . . .	53
9.4	Dépannage en cas de désinstallation . . . . .	54

# À propos de ce guide et de la bibliothèque

Le présent *guide du programme d'installation intégré* fournit des instructions pour l'installation du produit NetIQ Identity Manager (Identity Manager) à l'aide du programme d'installation intégré. Ce document contient de nombreuses références au [Guide d'installation de NetIQ Identity Manager](#), lequel fournit des informations détaillées sur l'installation d'Identity Manager avec des programmes d'installation autonomes.

## Public

Les informations contenues dans ce manuel sont destinées aux architectes et administrateurs d'identités qui souhaitent installer Identity Manager afin d'évaluer ce produit en tant que 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 :	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
États-Unis et Canada :	1-888-323-6768
Courrier électronique :	<a href="mailto:info@netiq.com">info@netiq.com</a>
Site Web :	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacter le support technique

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

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

## 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](http://www.netiq.com/documentation). Vous pouvez également envoyer un message électronique à l'adresse [Documentation-Feedback@netiq.com](mailto: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](http://community.netiq.com).



# 1 Introduction

NetIQ propose deux méthodes d'installation et de configuration d'Identity Manager dans votre environnement : une solution d'installation intégrée et des programmes d'installation spécifiques pour chaque composant ou groupe de composants. Le **programme d'installation intégré** vous permet d'installer et de configurer tous les composants en appliquant des valeurs par défaut à la plupart des paramètres. Ces paramètres sont utiles pour les installations standard. NetIQ recommande de conserver ces paramètres pour votre installation.

Vous pouvez utiliser le programme d'installation intégré pour installer tous les composants sur un ordinateur Linux ou Windows, à l'exception du composant NetIQ Sentinel Log Management for Identity Governance and Administration, qui ne peut être installé que sur les ordinateurs Linux. Optez pour les **programmes d'installation autonomes** pour installer un ou plusieurs composants Identity Manager séparément, ou si vous souhaitez personnaliser de nombreux paramètres.

Avant de poursuivre, assurez-vous de bien connaître les différents composants Identity Manager. Pour plus d'informations, reportez-vous à la section [Aperçu des composants Identity Manager](#) du *Guide d'installation de NetIQ Identity Manager*.

## 1.1 Différences entre la procédure d'installation intégrée et les programmes d'installation autonomes

Les informations suivantes peuvent vous aider à déterminer si vous devez utiliser le programme d'installation intégré ou l'un des programmes d'installation autonomes.

### Programme d'installation intégré

NetIQ recommande d'utiliser ce programme lorsque vous souhaitez évaluer Identity Manager ou créer un environnement de test. Le programme permet de rassembler tous les composants nécessaires en une seule procédure d'installation. Le programme d'installation intégré présente les caractéristiques suivantes :

- ♦ il peut être exécuté sur les plates-formes Red Hat Enterprise Linux (RHEL) 7.3 ou version ultérieure, SUSE Linux Enterprise Server (SLES) 12 SP1 ou version ultérieure, ou Windows 2012 R2 ;
- ♦ il applique les valeurs par défaut pour la plupart des paramètres ;
- ♦ il installe tous les composants dans un environnement de serveur unique ;
- ♦ il utilise PostgreSQL 9.6.x pour tous les systèmes d'exploitation pris en charge
- ♦ il utilise Apache Tomcat pour tous les systèmes d'exploitation pris en charge.

---

**IMPORTANT** : l'utilisation du programme d'installation intégré fait l'objet des restrictions suivantes :

- ♦ il ne doit pas être utilisé pour installer Identity Manager sur les plates-formes RHEL 6.x et SLES 11 ou ultérieures.

Pour installer les composants Identity Manager pris en charge sur ces plates-formes, utilisez plutôt les programmes d'installation de composants individuels. Pour savoir quels composants sont pris en charge sur quelles plates-formes, reportez-vous au manuel [Guide d'installation de NetIQ Identity Manager](#).

- ♦ il ne doit pas être exécuté en mode console ;
  - ♦ il ne doit pas être utilisé pour installer Identity Manager Standard Edition ;
  - ♦ il ne doit pas être utilisé dans un environnement en grappe ;
  - ♦ il ne doit pas être utilisé dans un environnement de production.
- 

### Programmes d'installation autonomes

NetIQ recommande l'utilisation de cette option pour les environnements de production et de déploiement temporaire de votre solution de gestion des identités. Les programmes d'installation autonomes vous offrent plus de flexibilité pour la configuration de votre environnement. Ce processus présente les caractéristiques suivantes :

- ♦ il permet de personnaliser les paramètres des composants ;
- ♦ il permet d'installer des composants dans des environnements distribués ;
- ♦ il prend en charge plusieurs plates-formes de base de données ;
- ♦ prise en charge de plusieurs serveurs d'applications ;
- ♦ création d'un environnement de production pris en charge ;

Pour plus d'informations sur l'utilisation du processus d'installation autonome, reportez-vous au [Guide d'installation de NetIQ Identity Manager](#).

## 1.2 Présentation du processus d'installation intégré

Le processus d'installation intégré exécute en interne les programmes d'installation des différents composants Identity Manager. Le programme d'installation fournit des valeurs par défaut pour les paramètres les plus courants dans un environnement à serveur unique. Ces paramètres sont utilisés dans les installations classiques. NetIQ recommande de conserver ces paramètres pour votre installation. Si vous installez les composants Identity Manager dans un environnement distribué, exécutez le programme d'installation intégré sur chaque ordinateur et spécifiez le composant à installer.

Lorsque vous lancez la procédure d'installation, vous pouvez définir un mot de passe que la procédure appliquera à tous les paramètres de mot de passe des composants installés. Lors de l'installation, des paramètres par défaut sont appliqués aux composants. Vous pouvez modifier ces paramètres par défaut au cours de la procédure d'installation ou ultérieurement. Par exemple, lorsque vous lancez le processus, vous pouvez définir le mot de passe que vous souhaitez appliquer à toutes les valeurs de mot de passe.

---

**REMARQUE** : il est impossible d'utiliser la procédure d'installation intégrée pour mettre à niveau une installation existante.

---

Les sections suivantes décrivent les composants que vous pouvez installer avec ce processus, ainsi que leurs valeurs par défaut.

## 1.2.1 Serveur Identity Manager

Cette option permet d'installer les composants Identity Manager suivants :

- ♦ Coffre-fort d'identité
- ♦ Moteur Identity Manager
- ♦ Plug-ins iManager
- ♦ Pilotes Identity Manager
- ♦ Chargeur distant
- ♦ Agent Fan-out

---

**REMARQUE :** s'applique uniquement au pilote JDBC Fan-out. Lorsque cette option est sélectionnée, le programme d'installation 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).

---

Par défaut, le compte administrateur du coffre-fort d'identité est `admin`. Vous pouvez modifier cette valeur pendant la configuration des composants. La procédure d'installation crée automatiquement une arborescence pour le coffre-fort d'identité. Pour plus d'informations, reportez-vous à la [Section 1.3, « Présentation de la structure par défaut du coffre-fort d'identité », page 14](#).

## 1.2.2 Applications d'identité

Cette option permet d'installer les composants Identity Manager et les logiciels complémentaires suivants :

- ♦ Administrateur de catalogue
- ♦ Home and Provisioning Dashboard
- ♦ Module de provisioning basé sur les rôles (RBPM)
- ♦ Pilote de service de rôle et de ressource
- ♦ Application utilisateur
- ♦ Pilote d'application utilisateur
- ♦ One SSO Provider
- ♦ PostgreSQL
- ♦ Réinitialisation de mot de passe en self-service (SSPR, Self Service Password Reset)
- ♦ Tomcat

---

**REMARQUE :** si vous choisissez d'installer RBPM en mode silencieux ou d'interface utilisateur graphique, assurez-vous que les options Identity Reporting et Sentinel Log Management for IGA sont également sélectionnées.

---

La procédure d'installation fournit un environnement Oracle JRE, des versions Open Source du serveur Web Apache Tomcat, d'Apache ActiveMQ et du serveur de base de données PostgreSQL comme base pour le fonctionnement d'Identity Manager. Le programme d'installation vous permet d'installer ces composants sans avoir à les télécharger séparément. Toutefois, NetIQ ne propose pas de support aux entreprises pour ces composants.

NetIQ recommande d'utiliser un serveur d'applications d'entreprise pour les environnements de déploiement temporaire et de production, et d'utiliser ce programme d'installation pour la création d'environnements de développement. NetIQ ne fournit aucune mise à jour pour ces composants et n'offre aucun service de support, d'administration, de configuration ou de réglage les concernant. Pour toute demande de support, contactez le fournisseur tiers du composant.

La procédure d'installation crée les comptes et bases de données suivants :

Élément par défaut	Description
idmuserappdb	Base de données pour les applications d'identité
idmadmin	Compte administrateur de la base de données idmuserappdb
uaadmin	Compte administrateur de l'application utilisateur

La procédure d'installation crée et configure également le pilote de l'application utilisateur et celui du service de rôles et de ressources. Pour configurer des pilotes supplémentaires, reportez-vous au [site Web de documentation des pilotes Identity Manager](#).

Pour plus d'informations sur les applications d'identité, reportez-vous aux sections [Présentation des composants de gestion du provisioning des utilisateurs](#) et [Installation des applications d'identité](#) du [Guide d'installation de NetIQ Identity Manager](#).

## 1.2.3 Identity Reporting

Cette option permet d'installer les composants Identity Manager suivants :

- ♦ Module Novell Identity Reporting
- ♦ Pilote de passerelle système gérée (MSGW, Managed System Gateway)
- ♦ Pilote pour le service de collecte de données (DCS, Data Collection Service)

Même s'il se peut que vous disposiez de plusieurs types de systèmes d'audit d'événements, Identity Reporting ne peut communiquer qu'avec un seul service d'audit d'événements. Pour consigner des événements, Identity Reporting doit pouvoir accéder à la base de données SIEM installée en même temps que Sentinel.

Pour plus d'informations sur Identity Reporting, reportez-vous aux sections [Identity Reporting](#) et [Installation d'Identity Reporting](#) du [Guide d'installation de NetIQ Identity Manager](#).

## 1.2.4 Sentinel Log Management for Identity Governance and Administration

Cette option installe Sentinel Log Management for IGA sur la nouvelle base de données PostgreSQL.

**IMPORTANT** : sous Linux, NetIQ vous impose d'installer Sentinel Log Management for IGA et Identity Reporting sur le même ordinateur si vous effectuez l'opération à l'aide du programme d'installation intégré. Si vous installez ces composants à l'aide de programmes d'installation de composants individuels, vous pouvez les installer sur le même ordinateur ou dans un environnement distribué.

Sentinel Log Management for IGA vous permet d'afficher les événements et d'interagir avec ceux-ci. Vous pouvez par exemple exécuter les opérations suivantes :

- ♦ Configurer la collecte de données pour les sources d'événements comme syslog, les audits, etc.
- ♦ Afficher des événements en temps réel
- ♦ Corréler des données d'événement
- ♦ Transférer des événements

Pour plus d'informations sur Sentinel Log Management for IGA, reportez-vous à la section [Installation et gestion de Sentinel Log Management for Identity Governance and Administration](#) du [Guide d'installation de NetIQ Identity Manager](#).

## 1.2.5 iManager

Cette option permet d'installer iManager ainsi que son client pour les postes de travail. Au cours du processus de configuration, vous pouvez modifier les ports qu'iManager utilise par défaut pour les communications. Pour plus d'informations sur iManager, reportez-vous aux sections [iManager](#) et [Installation d'iManager](#) du [Guide d'installation de NetIQ Identity Manager](#).

## 1.2.6 Designer

Cette option permet d'installer Designer sur l'ordinateur local. Designer ne comporte pas de paramètres programmables par l'utilisateur. Pour plus d'informations sur Designer, reportez-vous aux sections [Designer pour Identity Manager](#) et [Planification de l'installation de Designer](#) du [Guide d'installation de NetIQ Identity Manager](#).

## 1.2.7 Analyzer

Cette option permet d'installer Analyzer sur l'ordinateur local. Analyzer ne comporte pas de paramètres programmables par l'utilisateur. Pour plus d'informations sur Analyzer, reportez-vous aux sections [Analyzer pour Identity Manager](#) et [Installation d'Analyzer](#) du [Guide d'installation de NetIQ Identity Manager](#).

## 1.3 Présentation de la structure par défaut du coffre-fort d'identité

Pour s'adapter à la plupart des déploiements d'Identity Manager, la procédure d'installation intégrée crée une structure par défaut pour le coffre-fort d'identité.

Figure 1-1 Structure par défaut du coffre-fort d'identité

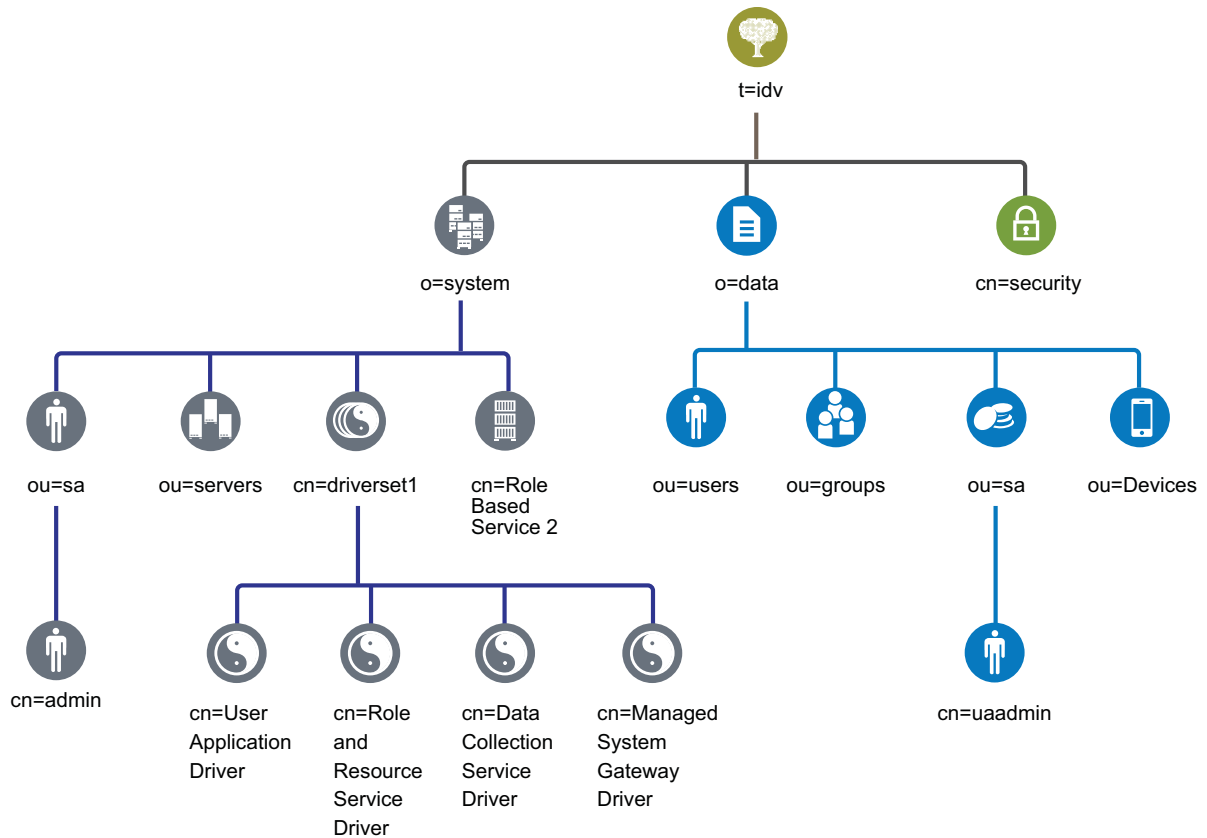


Tableau 1-1 Description des objets du coffre-fort d'identité

Objet	Description
t=idv	Nom de l'arborescence eDirectory. Par exemple, idv.
o=system	Tous les objets du système Identity Manager se trouvent dans l'organisation Système. Seuls les administrateurs doivent avoir accès à ce conteneur et à tous ses sous-conteneurs. Pour plus d'informations, reportez-vous à la <a href="#">Section 1.3.1, « Conteneur système », page 16</a> .
ou=sa.o=system	C'est dans le conteneur ou=sa.o=system que sont stockés tous les utilisateurs du système. Les utilisateurs du système sont ses administrateurs, les administrateurs de pilotes et les autres administrateurs.
cn=admin.ou=sa.o=system	Il s'agit du compte administrateur de l'arborescence.
ou=servers.o=system	Ce conteneur stocke les objets Serveur ainsi que tous les objets associés aux serveurs. Il vous est ainsi possible de séparer les objets Serveur des autres objets du système.

Objet	Description
cn=driverset1.o=system	L'objet Ensemble de pilotes contient tous les objets Pilote. Les objets Ensemble de pilotes sont placés directement dans le conteneur Système.
cn=User Application Driver.cn=driverset1.o=system	Le pilote d'application utilisateur gère toutes les tâches liées à l'application utilisateur.
cn=Role and Resource Service Driver.cn=driverset1.o=system	Le pilote du service de rôles et de ressources gère toutes les tâches associées au module de provisioning basé sur les rôles (RBPM).
cn=Data Collection Service Driver.cn=driverset1.o=system	Le pilote du service de collecte des données (DCS) gère des tâches associées au module Identity Reporting.
cn=Managed System Gateway Driver.cn=driverset1.o=system	Le pilote de passerelle système gérée (MSGW) gère des tâches associées au module Identity Reporting.
cn=Role Based Service 2.o=system	Ce conteneur stocke des objets qui permettent d'exploiter iManager dans Identity Manager.
o=data	Tous les objets Données d'Identity Manager se trouvent dans l'organisation Données. Les administrateurs doivent veiller à ce que tous les utilisateurs aient accès à ce conteneur et à l'ensemble de ses sous-conteneurs. Pour plus d'informations, reportez-vous à la <a href="#">Section 1.3.2, « Conteneur de données », page 16</a> .
ou=users.o=data	Conteneur par défaut pour tous les objets Utilisateur dans le coffre-fort d'identité.
ou=groups.o=data	Conteneur par défaut pour tous les objets Groupe dans le coffre-fort d'identité.
ou=sa.o=data	Conteneur par défaut pour les comptes de service, superutilisateur et administrateur de rôles utilisés par l'application utilisateur, le module de provisioning basé sur les rôles et le module Identity Reporting.
cn=uaadmin.ou=sa.o=data	Objet Administrateur des applications utilisateur.
ou=Devices.o=data	Conteneur par défaut pour les périphériques.
cn=security	Le conteneur de sécurité contient tous les objets de sécurité de l'arborescence et d'Identity Manager. Assurez-vous que seuls les administrateurs ont accès à ce conteneur et à tous ses sous-conteneurs. Pour plus d'informations, reportez-vous à la <a href="#">Section 1.3.3, « Conteneur de sécurité », page 16</a> .

Cette structure par défaut est surtout utile dans le cadre d'une installation dans un seul environnement. Par exemple, elle est particulièrement indiquée pour les petits et moyens déploiements d'Identity Manager. Les environnements multi-tenants peuvent présenter une structure légèrement différente. En outre, les arborescences vastes et distribuées ne peuvent pas être structurées de cette façon.

Identity Manager 4.0 et ses versions ultérieures utilisent la plupart du temps des conteneurs Organisation, de sorte que les utilisateurs, les groupes et les administrateurs de service sont placés dans le même conteneur. Utilisez les organisations (o=) autant que possible et réservez les unités organisationnelles (ou=) aux situations où elles sont vraiment pertinentes. La structure d'Identity Manager est conçue pour garantir une grande évolutivité grâce à trois éléments principaux : le conteneur système, le conteneur de données et le conteneur de sécurité.

## 1.3.1 Conteneur système

Le conteneur système est une organisation. Par défaut, il est désigné en tant que `o = system`. Ce conteneur comprend toutes les informations techniques et de configuration pour votre coffre-fort d'identité ainsi que pour le système Identity Manager. Le conteneur système comporte les quatre sous-conteneurs principaux suivants :

### **ou=sa**

Le conteneur d'administrateurs de services contient des objets administratifs pour le coffre-fort d'identité et les pilotes. Seuls les administrateurs peuvent accéder à la sous-arborescence du système. L'administrateur du coffre-fort d'identité par défaut est `admin.sa.system`. Les objets de ce conteneur peuvent être désignés par l'abréviation « `sa` » ou par les termes administrateurs de service / superutilisateurs / comptes de service.

### **Serveurs**

Les objets Serveur comportent divers objets associés devant résider dans le même conteneur que l'objet Serveur. À mesure que vous ajoutez des serveurs dans votre arborescence, parcourir tous les objets peut s'avérer fastidieux.

Tous les objets Serveur doivent se trouver sous le conteneur `servers.system`. Toutefois, un administrateur peut créer des conteneurs de serveurs individuels pour chaque serveur déployé dans l'environnement. Le nom du conteneur est celui de l'objet Serveur.

Cette structure est conçue pour favoriser l'évolutivité. Tous les objets associés au serveur (volumes, licences, certificats) y sont placés afin de vous aider à trouver facilement les objets dont vous avez besoin.

### **Ensembles de pilotes**

Les ensembles de pilotes sont créés en tant que partition distincte au cours de la configuration du moteur Identity Manager. Le coffre-fort d'identité stocke les objets Ensemble de pilotes dans le conteneur système. Cette structure vous permet d'évoluer en ajoutant des ensembles de pilotes au conteneur système. Les services basés sur les rôles pour iManager sont également stockés dans le conteneur système.

## 1.3.2 Conteneur de données

Le conteneur de données comprend les groupes, les utilisateurs, les administrateurs de rôles, les périphériques et d'autres objets. Il s'agit des données qui constituent votre système. Les groupes, utilisateurs et conteneurs d'administrateurs de services sont des unités organisationnelles. Vous pouvez avoir des unités organisationnelles supplémentaires pour structurer vos données selon vos pratiques organisationnelles. Par exemple, le conteneur d'administrateurs de service (`ou=sa`) contient tous les objets Administrateur de l'application utilisateur ainsi que les comptes d'administrateur de service.

## 1.3.3 Conteneur de sécurité

Le conteneur Sécurité est un conteneur spécifique créé lors de l'installation du coffre-fort d'identité. Il est désigné en tant que `cn=security` au lieu de `dc`, `o` ou `ou`. Ce conteneur contient tous les objets de sécurité pour le coffre-fort d'identité. Par exemple, il comprend l'autorité de certification et les stratégies de mot de passe.



# 2 Planification de l'installation d'Identity Manager

Cette section fournit des informations qui peuvent être utiles pour planifier votre environnement Identity Manager, notamment les conditions préalables et la configuration système requise pour chaque composant Identity Manager. Il n'est pas nécessaire d'installer les composants sur le même ordinateur. Cependant, le programme d'installation intégré ne prend pas en charge l'installation d'Identity Manager dans un environnement en grappe.

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 de 90 jours ou ultérieurement.

## 2.1 Liste de contrôle de l'installation

La liste de contrôle suivante indique les principales étapes pour planifier l'installation d'Identity Manager dans un environnement de test ou d'évaluation.

Éléments de la liste de contrôle	
<input type="checkbox"/>	1. Renseignez-vous sur les interactions entre les différents composants Identity Manager. Pour plus d'informations, reportez-vous à la <a href="#">Chapitre 1, « Introduction », page 9</a> .
<input type="checkbox"/>	2. Consultez les considérations relatives à l'installation de ces composants pour vous assurer que les ordinateurs respectent toutes les exigences et conditions préalables : <ul style="list-style-type: none"><li>♦ Conditions préalables relatives à la procédure d'installation intégrée : <a href="#">Section 2.2, « Considérations relatives à l'utilisation du programme d'installation intégré », page 18</a>.</li><li>♦ Conditions préalables pour chaque composant : <a href="#">Section 2.3, « Conditions préalables et configuration système requise », page 19</a>.</li></ul> <p><b>IMPORTANT :</b> les applications d'identité et les fonctions Identity Reporting nécessitent que Sentinel Log Management for IGA soit installé à des fins d'audit des événements. Sentinel ne peut être installé que sur un ordinateur Linux. Si vous utilisez des ordinateurs Windows, vous devez disposer d'au moins un ordinateur Linux pour y installer Sentinel.</p>
<input type="checkbox"/>	3. Passez en revue les composants, logiciels et paramètres par défaut que la procédure d'installation intégrée ajoutera à vos serveurs. Pour plus d'informations, reportez-vous au <a href="#">Chapitre 5, « Présentation des paramètres de configuration », page 35</a> .
<input type="checkbox"/>	4. Vérifiez la configuration par défaut définie pour le coffre-fort d'identité. Pour plus d'informations, reportez-vous à la <a href="#">Section 1.3, « Présentation de la structure par défaut du coffre-fort d'identité », page 14</a> .
<input type="checkbox"/>	5. (Conditionnel) Si vous installez des composants dans un environnement Red Hat Enterprise Linux 7.x, assurez-vous que l'ordinateur dispose des bibliothèques adéquates. Pour plus d'informations, reportez-vous à la section <a href="#">Installing Identity Manager on an RHEL 7.x Server</a> (Installation d'Identity Manager sur un serveur RHEL 6.x) du manuel <a href="#">NetIQ Identity Manager Setup Guide</a> (Guide d'installation de NetIQ Identity Manager).

---

## Éléments de la liste de contrôle

---

- ☐ 6. Lancez la procédure d'installation intégrée :
    - ♦ Pour effectuer une installation guidée, reportez-vous à la [Section 3.3, « Utilisation de l'assistant d'installation », page 26](#).
    - ♦ Pour effectuer une installation silencieuse, reportez-vous à la [Section 3.4, « Installation silencieuse », page 27](#).
  - ☐ 7. Configurez les composants installés :
    - ♦ Pour un processus guidé, reportez-vous à la [Section 4.2, « Utilisation de l'assistant de configuration », page 30](#).
    - ♦ Pour une configuration en mode silencieux, reportez-vous à la [Section 4.4, « Configuration en mode silencieux », page 33](#).
  - ☐ 8. Terminez l'installation. Pour plus d'informations, reportez-vous au [Chapitre 6, « Dernières étapes de la procédure d'installation intégrée », page 45](#).
  - ☐ 9. Activez Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 7, « Activation des produits Identity Manager », page 47](#).
- 

## 2.2 Considérations relatives à l'utilisation du programme d'installation intégré

Cette section décrit les considérations à prendre en compte si vous envisagez d'utiliser le programme d'installation intégré pour installer tous les composants Identity Manager. Sauf indication contraire, les serveurs et les postes de travail doivent également respecter les conditions préalables répertoriées dans la [Section 2.3, « Conditions préalables et configuration système requise », page 19](#).

- ☐ Il est impossible d'utiliser la procédure d'installation intégrée pour mettre à niveau une installation existante.
- ☐ Les composants tels que les applications d'identité ou Identity Reporting nécessitent l'utilisation du serveur d'application Apache Tomcat. Le programme d'installation intégré installe automatiquement une version prise en charge de Tomcat lorsque l'un des composants ou les deux sont spécifiés pour l'installation.
- ☐ Lors de l'installation des applications d'identité, le programme d'installation intégré nécessite également l'installation d'Identity Reporting.
- ☐ Si vous souhaitez installer tous les composants sur un seul ordinateur, il doit s'agir d'un ordinateur Linux. Si vous utilisez des ordinateurs Windows, vous devez disposer d'au moins un ordinateur Linux pour l'installation de Sentinel Log Management for IGA. Les applications d'identité et Identity Reporting vous demande d'installer Sentinel Log Management for IGA à des fins d'audit.
- ☐ Le programme d'installation intégré installe eDirectory 9.0.2 avec le Hotfix 2 appliqué. Il installe également iManager 3.0.2 Patch 1 qui est compatible avec cette version d'eDirectory. Pour utiliser eDirectory 8.8.8 Patch 9 Hotfix 2 et iManager 2.7.7 Patch 9, installez-les à l'aide des programmes d'installation des composants. Pour plus d'informations, reportez-vous au [Guide d'installation de NetIQ Identity Manager](#).

## 2.3 Conditions préalables et configuration système requise

Vous pouvez installer tous les composants sur un seul ordinateur à des fins d'évaluation, ou utiliser le programme d'installation intégré pour installer les différents composants sur plusieurs systèmes et plates-formes. Pour ce faire, vous devez exécuter le programme d'installation intégré à plusieurs reprises, en sélectionnant à chaque fois les composants souhaités.

### 2.3.1 Conditions préalables

Vérifiez que les conditions suivantes sont remplies avant de lancer le programme d'installation intégré.

#### Toutes les plates-formes

---

**IMPORTANT :** Sentinel Log Management for Identity Governance and Administration (IGA) ne peut être installé que dans des environnements Linux. Si vous voulez évaluer les applications d'identité et les fonctions Identity Reporting dans Identity Manager, vous devez installer Sentinel Log Management for IGA sur un ordinateur Linux avant toute utilisation du programme d'installation intégré sur un ordinateur Windows.

---

- ☐ Avant d'installer eDirectory, vous devez disposer d'une méthode pour résoudre les noms d'arborescence en adresses de renvois du serveur. NetIQ recommande d'utiliser pour ce faire des services SLP (Service Location Protocol). Les versions de NetIQ eDirectory antérieures à la version 8.8 intégraient SLP dans le paquetage d'installation. En revanche, dans les versions ultérieures, les services SLP doivent être installés séparément. Pour plus d'informations, reportez-vous à la section [Utilisation d'OpenSLP ou d'un fichier hosts.nds pour résoudre les noms d'arborescence](#) du [Guide d'installation de NetIQ Identity Manager](#).
- ☐ Pour permettre un fonctionnement optimal de l'infrastructure eDirectory, vous devez configurer une adresse IP statique sur le serveur. Si vous utilisez des adresses DHCP sur le serveur, les performances d'eDirectory risquent d'être imprévisibles. Assurez-vous que le nom DNS de l'ordinateur peut être résolu. Si ce n'est pas le cas, ajoutez une entrée pour cet ordinateur dans le fichier `/etc/hosts` afin de permettre la résolution du nom DNS.
- ☐ Synchronisez l'heure de tous les serveurs du réseau. NetIQ recommande d'utiliser le protocole NTP (Network Time Protocol).

#### Linux

- ☐ (Conditionnel) Si vous installez des composants dans un environnement Red Hat Enterprise Linux 7.x, assurez-vous que l'ordinateur dispose des bibliothèques adéquates. Pour plus d'informations, reportez-vous à la section [Installing Identity Manager on an RHEL 7.x Server](#) (Installation d'Identity Manager sur un serveur RHEL 6.x) du manuel [NetIQ Identity Manager Setup Guide](#) (Guide d'installation de NetIQ Identity Manager).
- ☐ (Conditionnel) Pour une installation guidée sur des plates-formes SUSE Linux Enterprise Server 12 SP1 ou ultérieures, assurez-vous que les bibliothèques suivantes soient installées sur l'ordinateur :
  - ♦ `libXtst6-32bit-1.2.1-4.4.1.x86_64`
  - ♦ `libXrender-32bit`
  - ♦ `libXi6-32bit`

En général, vous pouvez télécharger les fichiers `.rpm` à partir d'un site Web tel que <http://rpmfind.net/linux>. Par exemple, vous pouvez télécharger `libXtst6-32bit-1.2.1-4.4.1.x86_64.rpm` à partir de cette [page Web](#).

- ☐ Assurez-vous que le fichier RPM `unzip` est installé sur toutes les plates-formes Linux que vous utilisez.
- ☐ Le fichier `/etc/hosts` ne peut contenir qu'une seule adresse de boucle. S'il existe plusieurs adresses de bouclage, supprimez les adresses superflues à l'aide d'un éditeur afin de corriger la configuration. Par exemple :

```
127.0.0.1 localhost.localdomain localhost #loopback
#127.0.0.2 server1
192.0.2.1 server1
```

## Windows

- ☐ Pour installer Identity Manager avec le programme d'installation intégré, vous devez disposer de droits d'administrateur sur l'ordinateur Windows.
- ☐ Avant de lancer la procédure d'installation, assurez-vous que votre système d'exploitation Windows dispose des Service Packs les plus récents.

### 2.3.2 Configuration système requise

Les exigences suivantes s'appliquent lorsque vous installez tous les composants, ou la plupart des composants, sur le même ordinateur. Si vous souhaitez connaître les exigences applicables à un composant particulier, reportez-vous à la section relative aux [remarques et conditions préalables à l'installation](#) du *Guide d'installation de NetIQ Identity Manager*.

Référez-vous aux informations suivantes pour vous assurer que vous pouvez installer et configurer votre système Identity Manager sans problème.

Catégorie	Configuration requise
Processeur	Ordinateur multiprocesseur avec un processeur de 2 GHz
Mémoire	6 Go au minimum
Espace disque	40 Go au minimum
	<b>REMARQUE</b> : il faut aussi compter de l'espace disque supplémentaire pour la configuration et le chargement des données. L'espace requis dépend des systèmes connectés et du nombre d'objets contenus dans le coffre-fort d'identité.
Système d'exploitation	Un ou plusieurs des systèmes suivants : <ul style="list-style-type: none"><li>♦ SLES 12 SP1 ou version ultérieure (64 bits)</li><li>♦ RHEL 7.3 ou version ultérieure (64 bits)</li><li>♦ Windows Server 2012 R2 (64 bits)</li></ul>

Catégorie	Configuration requise
Systèmes virtuels	<p>L'un des systèmes suivants :</p> <ul style="list-style-type: none"> <li>♦ Hyper-V dans Windows Server 2012 R2</li> <li>♦ VMWare ESXi 5.5</li> </ul> <p><b>IMPORTANT :</b> NetIQ prend en charge Identity Manager sur les systèmes virtuels d'entreprise prenant officiellement en charge les systèmes d'exploitation où sont exécutés les produits NetIQ. Tant que les fournisseurs de systèmes virtuels indiquent officiellement prendre en charge ces systèmes d'exploitation, NetIQ prend en charge l'intégralité de la pile Identity Manager sur ces derniers.</p>
Hot Fix de système d'exploitation	Avant d'installer Identity Manager, NetIQ vous recommande d'appliquer les derniers correctifs du système d'exploitation à l'aide de l'outil de mise à jour automatique fourni par le fabricant.
Navigateurs Web	<p><b>Ordinateur de bureau :</b> (au minimum)</p> <ul style="list-style-type: none"> <li>♦ Apple Safari 9</li> <li>♦ Google Chrome 51 ou version ultérieure</li> <li>♦ Microsoft Internet Explorer 11 ou version ultérieure, Edge</li> <li>♦ Mozilla FireFox 46 ou version ultérieure</li> </ul> <p><b>iPad :</b> (au minimum)</p> <ul style="list-style-type: none"> <li>♦ Safari 9 ou version ultérieure sous iOS 9, 10</li> </ul> <p><b>REMARQUE :</b> pour accéder aux applications, les cookies doivent être activés pour le navigateur. Si les cookies sont désactivés, le produit ne fonctionne pas.</p>

### 2.3.3 Composants pouvant être installés

Par défaut, le programme d'installation intégré installe les composants Identity Manager suivants :

**Tableau 2-1** Composants Identity Manager et leur version installée par le programme d'installation intégré

Composants Identity Manager	Version
Coffre-fort d'identité (eDirectory)	9.0.2 Hotfix 2
Moteur Identity Manager	4.6
Chargeur distant	4.6
One SSO Provider	6.1.3
Self-Service Password Reset	4.1.0
Kit de développement Java Oracle	1.8.0_112
Apache Tomcat	8.5.9
PostgreSQL	9.6.10
Apache ActiveMQ	5.14

Composants Identity Manager	Version
iManager et les plug-ins	3.0.2 Patch 1
Applications d'identité	4.6
Sentinel Log Management for IGA	8.0.0.1
Module Novell Identity Reporting	5.5
Designer	4.6
Analyzer	4.6

## 2.3.4 Emplacements d'installation par défaut

Le programme d'installation intégré installe les composants Identity Manager aux emplacements spécifiés dans le [Tableau 2-2](#). Sur un ordinateur Windows, vous pouvez spécifier l'emplacement d'installation des composants. Sur les ordinateurs Linux, la procédure d'installation enregistre les composants dans des emplacements prédéfinis.

**Tableau 2-2** Emplacements d'installation par défaut définis par le programme d'installation intégré

Composants Identity Manager	Chemins d'installation par défaut
<b>Linux</b>	
Coffre-fort d'identité (eDirectory)	/opt/novell/eDirectory
Moteur Identity Manager	/opt/novell/eDirectory
Chargeur distant	/opt/novell/dirxml
Agent Fan-out	/opt/novell/dirxml/fanoutagent
Sentinel Log Management for IGA	/opt/novell/sentinel (Linux uniquement)
JRE	/opt/netiq/idm/jre
Tomcat	/opt/netiq/idm/apps/tomcat
PostgreSQL	/opt/netiq/idm/apps/postgres
ActiveMQ	/opt/netiq/idm/apps/activemq
OSP	/opt/netiq/idm/apps/osp
SSPR	/opt/netiq/idm/apps/sspr
Application utilisateur	/opt/netiq/idm/apps/UserApplication
Applications d'identité	/opt/netiq/idm/apps
Identity Reporting	/opt/netiq/idm/apps/IDMReporting
iManager et les plug-ins	/var/opt/novell/iManager
Analyzer	/opt/netiq/idm/tools/Analyzer
Designer	/opt/netiq/idm/tools/Designer
<b>Windows</b>	

<b>Composants Identity Manager</b>	<b>Chemins d'installation par défaut</b>
Coffre-fort d'identité (eDirectory)	C:\NetIQ\IdentityManager\NDS
Moteur Identity Manager	C:\NetIQ\IdentityManager\NDS
Chargeur distant	C:\NetIQ\IdentityManager\RemoteLoader
Agent Fan-out	C:\NetIQ\IdentityManager\FanoutAgent
JRE	C:\NetIQ\IdentityManager\jre
Tomcat	C:\NetIQ\IdentityManager\apps\tomcat
PostgreSQL	C:\NetIQ\IdentityManager\apps\posgres
OSP	C:\NetIQ\IdentityManager\apps\osp
SSPR	C:\NetIQ\IdentityManager\apps\sspr
ActiveMQ	C:\NetIQ\IdentityManager\apps\activemq
Application utilisateur	C:\NetIQ\IdentityManager\apps\UserApplication
Identity Reporting	C:\NetIQ\IdentityManager\apps\IDMReporting
iManager	C:\NetIQ\IdentityManager\iManager
Analyzer	C:\NetIQ\IdentityManager\tools\Analyzer
Designer	C:\NetIQ\IdentityManager\tools\Designer





# 3 Installation d'Identity Manager

Le programme d'installation intégré installe les fichiers binaires de tous les composants Identity Manager et configure ceux-ci. Vous pouvez installer les composants et les configurer simultanément, ou effectuer ces deux procédures séparément.

## 3.1 Téléchargement du fichier ISO

Vous devez télécharger les fichiers d'installation à partir du site de téléchargement de NetIQ.

**Pour télécharger le fichier .iso :**

- 1 Accédez au [site Web de téléchargement de NetIQ](#).
- 2 Dans le menu **Product or Technology** (Produit ou technologie), sélectionnez **Identity Manager**.
- 3 Dans le champ **Select Version** (Sélectionner version), sélectionnez **Identity Manager 4.6**, puis cliquez sur **Submit Query** (Envoyer).
- 4 Cliquez sur le lien **Identity Manager 4.6**, puis sur **Proceed to download** (Lancer le téléchargement).
- 5 Connectez-vous avec votre ID NetIQ Customer Center.
- 6 Sélectionner le fichier `.iso` correspondant à votre plate-forme, puis suivez les instructions à l'écran pour télécharger le fichier.

Les fichiers d'installation intégrée (`install.exe` ou `install.bin`) se trouvent à la racine des fichiers `.iso` d'Identity Manager. Accédez aux fichiers d'installation d'Identity Manager , soit en montant le fichier `.iso`, soit en utilisant le DVD que vous avez créé à partir de ce fichier `.iso`.

## 3.2 Utilisation d'un même mot de passe pour tous les paramètres configurés lors de la procédure d'installation intégrée

Pour la plupart des composants Identity Manager, il est nécessaire d'indiquer un mot de passe lors de la phase de configuration. Pour accélérer la configuration, vous pouvez indiquer au processus d'appliquer le même mot de passe pour tous les paramètres configurés par le programme d'installation intégré.

Le mot de passe doit contenir au moins six caractères.

### Linux

Avant d'appeler le programme d'installation ou de configuration, entrez la commande suivante :

```
export USER_SUPPLIED_PASSWORD=password
```

Par exemple :

```
export USER_SUPPLIED_PASSWORD=test123
```

## Windows

Effectuez l'une des opérations suivantes :

- ♦ Sous **Propriétés système > Variables d'environnement**, ajoutez `USER_SUPPLIED_PASSWORD` et spécifiez une valeur pour cette variable.
- ♦ Avant d'appeler le programme d'installation ou de configuration, entrez la commande suivante :

```
set USER_SUPPLIED_PASSWORD=password
```

Par exemple :

```
set USER_SUPPLIED_PASSWORD=test123
```

## 3.3 Utilisation de l'assistant d'installation

La procédure suivante indique comment installer Identity Manager sur une plate-forme Linux ou Windows à l'aide de l'assistant d'installation. Pour effectuer une installation en mode silencieux sans surveillance, reportez-vous à la [Section 3.4, « Installation silencieuse », page 27](#).

Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise, détaillées dans la [Section 2.1, « Liste de contrôle de l'installation », page 17](#). Référez-vous également aux dernières notes de version pour obtenir des informations utiles pour l'installation.

Si vous le souhaitez, vous pouvez spécifier un mot de passe que la procédure d'installation utilisera pour configurer la plupart des mots de passe requis pour Identity Manager.

### Pour installer Identity Manager à l'aide de l'assistant :

- 1 Connectez-vous en tant qu'utilisateur root ou administrateur à l'ordinateur sur lequel vous souhaitez installer les composants.
- 2 Montez le fichier `.iso` ou créez un DVD à partir de ce fichier `.iso`. Pour plus d'informations, reportez-vous à la [Section 3.1, « Téléchargement du fichier ISO », page 25](#).
- 3 (Facultatif) Indiquez à la procédure d'installation d'appliquer le même mot de passe à tous les paramètres configurés par le programme d'installation intégré. Pour plus d'informations, reportez-vous à la [Section 3.2, « Utilisation d'un même mot de passe pour tous les paramètres configurés lors de la procédure d'installation intégrée », page 25](#).
- 4 À partir du répertoire racine du fichier `.iso`, accédez aux fichiers d'installation, puis effectuez l'une des opérations suivantes :
  - ♦ **Linux** : entrez la commande `./install.bin`
  - ♦ **Windows** : exécutez `install.exe`
- 5 Sur la page de titre, sélectionnez la langue de votre choix dans la liste déroulante, puis cliquez sur **OK**.
- 6 Sur la page d'introduction, passez en revue les différents composants Identity Manager que vous pouvez installer, puis cliquez sur **Suivant**.
- 7 Lisez et acceptez l'accord de licence, puis cliquez sur **Suivant**.

---

**REMARQUE** : avant de pouvoir accepter l'accord de licence, vous devez le lire jusqu'au bout en faisant défiler la page jusqu'à la fin du texte.

---

- 8 Spécifiez les composants que vous souhaitez installer sur le serveur local, puis cliquez sur **Suivant**.

Pour plus d'informations sur les composants disponibles, reportez-vous à la [Section 1.2, « Présentation du processus d'installation intégré », page 10](#).

- 9 (Conditionnel) Pour un serveur Windows, spécifiez le dossier d'installation, puis cliquez sur **Suivant**.
- 10 Lisez le résumé avant installation, puis cliquez sur **Installer**.

---

**REMARQUE** : selon les composants sélectionnés, l'exécution de la procédure d'installation peut prendre un certain temps.

---

- 11 Une fois l'installation terminée, effectuez l'une des opérations suivantes pour configurer les composants installés :
  - ♦ **Pour configurer immédiatement les composants** : sélectionnez **Continuer**.
  - ♦ **Pour reporter la configuration** : désélectionnez la case **Continue Now** (Continuer).

---

**REMARQUE** : si vous souhaitez reporter la configuration, ne redémarrez pas l'ordinateur et ne procédez ni au redémarrage ni à l'arrêt d'un quelconque service tant que vous n'avez pas configuré les composants Identity Manager.

---

Vous pouvez modifier les paramètres de configuration à tout moment. Cependant, vous devez spécifier de nombreux paramètres avant de pouvoir exécuter Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 4, « Configuration des composants Identity Manager », page 29](#).

---

**REMARQUE** : certains composants, tels que Designer et Analyzer, ne nécessitent pas de configuration.

---

- 12 Cliquez sur **Terminer**.

## 3.4 Installation silencieuse

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 provenant des fichiers de propriétés. Pour effectuer une installation guidée, reportez-vous à la [Section 3.3, « Utilisation de l'assistant d'installation », page 26](#). Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise, détaillées dans la [Section 2.1, « Liste de contrôle de l'installation », page 17](#). Référez-vous également aux dernières notes de version pour obtenir des informations utiles pour l'installation.

Si vous le souhaitez, vous pouvez spécifier un mot de passe que la procédure d'installation utilisera pour configurer les mots de passe Single Sign-on requis pour Identity Manager. Pour plus d'informations, reportez-vous à la [Section 4.1, « Considérations relatives à la configuration des composants », page 29](#).

**Pour effectuer une installation en mode silencieux :**

- 1 Connectez-vous en tant qu'utilisateur `root` ou administrateur à l'ordinateur sur lequel vous souhaitez installer les composants.
- 2 Une fois que vous avez monté le fichier `.iso`, accédez au répertoire contenant les fichiers d'installation. Par défaut, il s'agit du répertoire `<chemin_ISO_extraît>/install/profiles/install.properties`.

- 3 Modifiez le fichier `install.properties` servant à l'installation en mode silencieux, qui se trouve par défaut dans l'un des répertoires suivants :
  - ♦ **Linux** : `install/propfiles`
  - ♦ **Windows** : `install\propfiles`
- 4 Accédez au répertoire contenant les fichiers d'installation, qui se trouve par défaut dans le répertoire `install`.
- 5 Modifiez le fichier `install.properties` servant à l'installation en mode silencieux, qui se trouve par défaut dans l'un des répertoires suivants :
  - ♦ **Linux** : `install/propfiles`
  - ♦ **Windows** : `install\propfiles`
- 6 (Facultatif) Indiquez à la procédure d'installation d'appliquer le même mot de passe à tous les paramètres configurés par le programme d'installation intégré. Pour plus d'informations, reportez-vous à la [Section 3.2, « Utilisation d'un même mot de passe pour tous les paramètres configurés lors de la procédure d'installation intégrée », page 25](#).
- 7 Pour exécuter l'installation en mode silencieux, lancez l'une des commandes suivantes :
  - ♦ **Linux** : `install.bin -i silent -f <chemin_ISO_extraît>/install/propfiles/install.properties`
  - ♦ **Windows** : `install.exe -i silent -f <chemin_ISO_extraît>/install/propfiles/install.properties`
- 8 (Conditionnel) Pour continuer la configuration, entrez les valeurs suivantes dans le fichier `install.properties` :
  - ♦ Spécifiez `CONTINUE_CONFIGURE=true`.
  - ♦ Spécifiez le chemin d'accès du fichier de configuration dans la propriété `CONFIGURE_PROPERTY_FILE`. Par exemple, si vous configurez une nouvelle arborescence, spécifiez `configure_new_tree.properties`. Spécifiez `configure_existing_tree.properties` pour une arborescence existante. Pour plus d'informations, reportez-vous au [Chapitre 4, « Configuration des composants Identity Manager », page 29](#).
- 9 (Conditionnel) Pour configurer les composants ultérieurement, exécutez une des commandes suivantes :
  - ♦ **Linux** : `configure.bin -i silent -f <chemin_ISO_extraît>/install/propfiles/configure_<new/existing>_tree.properties`
  - ♦ **Windows** : `configure.exe -i silent -f <chemin_ISO_extraît>/install/propfiles/configure_<new/existing>_tree.properties`

# 4 Configuration des composants Identity Manager

Vous pouvez laisser la procédure d'installation intégrée vous guider tout au long de la configuration des composants Identity Manager installés, ou opter pour une configuration en mode silencieux. Certains composants, tels que Designer et Analyzer, ne nécessitent pas de configuration. Pour plus d'informations sur les paramètres de configuration, reportez-vous au [Chapitre 5, « Présentation des paramètres de configuration »](#), page 35.

---

## REMARQUE

- ♦ Pour garantir que les utilisateurs pourront se connecter aux applications d'identité, le processus de configuration applique un exemple de stratégie de mot de passe à `admin.sa.system`, `uaadmin.sa.data` et `users.data`. Dans le cadre de cette opération, le processus active également le paramètre **Autoriser l'administrateur à récupérer les mots de passe** dans les options de récupération de mot de passe.
  - ♦ Le programme d'installation intégré fournit des valeurs par défaut pour les paramètres les plus courants dans un environnement monoserveur. Ces paramètres sont utilisés dans les installations classiques. NetIQ recommande de conserver ces paramètres pour votre installation.
- 

## 4.1 Considérations relatives à la configuration des composants

Avant d'utiliser la procédure d'installation intégrée pour configurer les composants installés, prenez connaissance des considérations suivantes :

- ♦ Vous ne pouvez configurer que les composants installés sur l'ordinateur local.
- ♦ Avant toute installation ou configuration, vous pouvez indiquer au processus d'appliquer le même mot de passe pour tous les paramètres configurés par le programme d'installation intégré. Pour plus d'informations, reportez-vous à la [Section 3.2, « Utilisation d'un même mot de passe pour tous les paramètres configurés lors de la procédure d'installation intégrée »](#), page 25.
- ♦ Assurez-vous que le fichier `/etc/hosts` contient les entrées correspondant à l'adresse de boucle 127.0.0.1 et à l'adresse IP réelle. Pour plus d'informations, reportez-vous à la section [Section 2.3, « Conditions préalables et configuration système requise »](#), page 19.
- ♦ Si vous configurez les applications d'identité et composants Identity Reporting, vous devez sélectionner **Paramètres avancés** et modifier tous les champs contenant la mention `localhost` afin qu'ils correspondent à une adresse IP ou un nom DNS valide. Si vous ne modifiez pas la valeur `localhost`, la configuration échoue.
- ♦ Si vous ne configurez que le serveur Identity Manager, ajoutez manuellement les informations relatives au serveur de consignation dans les fichiers `logevent.conf` (Linux) et `logevent.cfg` (Windows). La procédure d'installation intégrée n'ajoute les informations du serveur de consignation à ces fichiers que lorsque vous configurez les applications d'identité ou le module Identity Reporting.

- ♦ Par défaut, Sentinel Log Management for IGA utilise le port 8643. Toutefois, vous pouvez configurer Sentinel Log Management for IGA pour utiliser un autre port après l'installation. Pour plus d'informations, reportez-vous à la section [Modification de la configuration après l'installation](#) du Guide d'installation et de configuration de NetIQ Sentinel.
- ♦ Avant d'ajouter un serveur secondaire à une arborescence existante, vous devez procéder à une vérification de l'état de santé. La procédure d'installation intégrée ne peut pas effectuer cette vérification de l'état de santé pour vous.
- ♦ Lorsque vous ajoutez un serveur secondaire à l'arborescence, le serveur reçoit uniquement une copie de la racine et sa propre partition de l'ensemble de pilotes.
  - ♦ Si vous utilisez également le pilote du service de collecte des données en tant que pilote principal sur ce second serveur, le pilote ne peut pas voir les modifications d'objets qu'il doit inclure dans les rapports. Pour configurer le pilote du service de collecte des données sur ce serveur, reportez-vous à la section [Configuration du pilote pour le service de collecte de données \(DCS, Data Collection Service\)](#) du Guide d'installation de NetIQ Identity Manager.
  - ♦ Si le pilote du service de collecte des données se trouve sur ce serveur de section, il doit contenir une copie de la partition de l'arborescence pour fonctionner.

Pour plus d'informations sur les valeurs de configuration, reportez-vous au [Chapitre 5, « Présentation des paramètres de configuration »](#), page 35.

## 4.2 Utilisation de l'assistant de configuration

L'assistant de configuration vous guide tout au long de la configuration de chacun des composants Identity Manager que vous avez sélectionnés lorsque vous avez effectué l'installation.

### Pour configurer les composants Identity Manager :

- (Conditionnel) Pour ajouter un serveur secondaire à une arborescence existante, exécutez la procédure suivante :
  - 1a Accédez à l'utilitaire ndscheck, qui se trouve par défaut dans l'un des répertoires suivants :
    - ♦ **Linux** : `/opt/novell/eDirectory/bin/ndscheck`
    - ♦ **Windows** : `emplacement_installation\NDS`
  - 1b Spécifiez les paramètres obligatoires et exécutez la commande suivante :
 

```
ndscheck [-h nom_d'hôte port] [-a admin_FDN] [-w mot_de_passe]
```
- (Conditionnel) Si vous venez de terminer l'[Étape 12 page 27](#) de la procédure d'installation, passez à l'[Étape 6 page 30](#).
- (Facultatif) Indiquez au processus de configuration d'appliquer le même mot de passe pour tous les paramètres configurés par le programme d'installation intégré. Pour plus d'informations, reportez-vous à la [Section 3.2, « Utilisation d'un même mot de passe pour tous les paramètres configurés lors de la procédure d'installation intégrée »](#), page 25.
- (Conditionnel) Pour lancer la configuration manuellement, effectuez l'une des opérations suivantes :
  - ♦ **Linux (interface graphique)** : entrez la commande `./configure.bin`
  - ♦ **Windows** : exécutez `configure.exe`
- Sur la page de titre, sélectionnez la langue de votre choix dans la liste déroulante, puis cliquez sur **OK**.
- Passez en revue les composants installés sur votre système, puis cliquez sur **Suivant**.

- 7 Sélectionnez les composants que vous souhaitez configurer sur le serveur local, puis cliquez sur **Suivant**.
- 8 Utilisez les informations suivantes pour configurer les différents composants :
- ♦ **Coffre-fort d'identité** : indiquez si vous souhaitez créer une nouvelle arborescence dans le coffre-fort d'identité ou en modifier une existante ; configurez ensuite l'arborescence pour votre environnement. Pour plus d'informations, reportez-vous à la [Section 5.1, « Coffre-fort d'identité », page 35](#).
  - ♦ **Sentinel Log Management for IGA** : spécifiez les informations de configuration de Sentinel Log Management for IGA. Pour plus d'informations, reportez-vous au [Section 5.3, « Sentinel Log Management for IGA », page 40](#).
- 
- IMPORTANT** : Sentinel Log Management for IGA ne peut être installé que sur des ordinateurs Linux. Toutefois, vous devez disposer d'une version de Sentinel opérationnelle pour configurer le module Identity Reporting.
- 
- ♦ **Applications d'identité** : spécifiez les informations de configuration de vos applications d'identité. Vous devez inclure l'adresse IP ou le nom DNS d'un serveur d'audit, sans quoi la configuration échoue. Pour plus d'informations, reportez-vous à la [Section 5.4, « Applications d'identité », page 40](#).
- 
- IMPORTANT** : vous devez sélectionner **Paramètres avancés** et modifier tous les champs contenant la mention `localhost` afin qu'ils correspondent à une adresse IP ou un nom DNS valide. Si vous ne remplacez pas le paramètre par défaut `localhost`, la configuration échoue.
- 
- ♦ **(Conditionnel) Serveur Identity Manager** : si vous effectuez l'installation dans une arborescence eDirectory existante, spécifiez les informations du serveur Identity Manager existant. Pour plus d'informations, reportez-vous à la [Section 5.2, « Serveur Identity Manager », page 39](#).
  - ♦ **Module Novell Identity Reporting** : pour utiliser le module Identity Reporting, vous devez avoir installé et configuré Sentinel. Vous ne pouvez installer Sentinel que sur un ordinateur Linux. Si vous utilisez un ordinateur Windows, vous devez installer Sentinel sur un ordinateur Linux avant toute configuration du module Identity Reporting sur un ordinateur Windows.  
  
Spécifiez les informations de configuration de votre module Identity Reporting. Pour plus d'informations, reportez-vous à la [Section 5.5, « Module Novell Identity Reporting », page 42](#).
  - ♦ **Outils** : Linux uniquement. Sélectionnez **Paramètres avancés** pour modifier les ports HTTP par défaut. Pour plus d'informations, reportez-vous à la [Section 5.6, « Outils », page 44](#).
- 9 Cliquez sur **Suivant** pour lancer la configuration des différents composants.
- 10 Passez en revue le résumé des informations de configuration, puis cliquez sur **Configurer**.
- 11 Lisez le résumé de la configuration, puis cliquez sur **Terminé**.

---

**REMARQUE** : si des erreurs se sont produites lors de la configuration, le programme d'installation intégré indique l'emplacement des journaux d'installation. Consultez les journaux d'installation pour connaître la raison de l'échec de la configuration.

---



## 4.3 Modification du fichier de propriétés pour la configuration en mode silencieux

Vous pouvez exécuter une configuration en mode silencieux des composants Identity Manager en créant ou en modifiant un fichier de propriétés reprenant les paramètres nécessaires à l'exécution de la configuration pour chaque composant. Le média Identity Manager fournit deux exemples de fichiers que vous pouvez utiliser si vous avez installé tous les composants sur un même serveur.

### Pour modifier le fichier de propriétés :

- 1 (Conditionnel) Si vous avez installé tous les composants sur le même serveur, modifiez l'un des exemples de fichiers de propriétés fournis pour la configuration en mode silencieux, qui se trouvent par défaut dans l'un des répertoires suivants :

- ♦ **Linux** : `install/propfiles`
- ♦ **Windows** : `install\propfiles`

Par exemple, utilisez le fichier `configure_new_tree.properties` pour créer une arborescence.

- 2 (Conditionnel) Si vous n'avez pas installé tous les composants sur le même serveur, procédez de la manière suivante pour créer un fichier de propriétés pour les composants installés :

#### 2a Exécutez la commande suivante :

```
./install.bin -i silent -DSELECTED_PRODUCTS=components_to_be_configured -f filename.properties
```

où `filename.properties` désigne l'un des exemples de fichiers de propriétés.

Le programme vérifie que les composants sont installés, puis génère une liste de paramètres obligatoires pour ces composants.

- 2b Utilisez la sortie de la commande présentée à l'[Étape 2a](#) pour créer un fichier de propriétés.
  - 2c Ajouter une variable `SELECTED_PRODUCTS` au fichier, puis indiquez quels composants vous souhaitez configurer.
- 3 Dans le fichier de propriétés, définissez les paramètres pour les composants installés. Pour plus d'informations, reportez-vous au [Chapitre 5, « Présentation des paramètres de configuration », page 35](#).
  - 4 Ajoutez les variables de mot de passe suivantes au fichier de propriétés :

Variable de mot de passe	Compte utilisateur ou service concerné
IA_IDVAULT_ADMIN_PASSWORD	Administrateur du coffre-fort d'identité
IA_RBPM_POSTGRESDB_PASSWORD	Administrateur de la base de données des applications d'identité (idmadmin)
IA_RBPM_USERAPPADMIN_PASSWORD	Administrateur de l'application utilisateur (uaadmin)
IA_REPORTING_NOVL_DB_USER_PASSWORD	Administrateur de la base de données Identity Reporting
IA_REPORTING_IDM_SERVER_PASSWORD	Utilisateur du serveur Identity Reporting (idmrptsrv)
IA_REPORTING_IDM_USER_PASSWORD	Utilisateur Identity Reporting (idmrptuser)
-DUSER_SUPPLIED_PASSWORD	Service Single Sign-on



Si vous avez inclus la variable `duser_supplied_password` lorsque vous avez lancé l'installation en mode silencieux, le programme a déjà appliqué cette valeur pour les mots de passe Single Sign-on.

5 Enregistrez, puis fermez le fichier.

## 4.4 Configuration en mode silencieux

Vous pouvez exécuter une configuration en mode silencieux des composants Identity Manager en créant un fichier de propriétés reprenant les paramètres nécessaires à l'exécution de la configuration pour chaque composant. Le média Identity Manager fournit deux exemples de fichiers que vous pouvez utiliser si vous avez installé tous les composants sur un même serveur.

Pour plus d'informations sur les paramètres pouvant être configurés, reportez-vous au [Chapitre 5, « Présentation des paramètres de configuration »](#), page 35.

**Pour effectuer une configuration en mode silencieux :**

- 1 (Conditionnel) Pour ajouter un serveur secondaire à une arborescence existante, exécutez la procédure suivante :
  - 1a Accédez à l'utilitaire `ndsccheck`, qui se trouve par défaut dans l'un des répertoires suivants :
    - ♦ **Linux** : `/opt/novell/eDirectory/bin/ndsccheck`
    - ♦ **Windows** : `emplacement_installation\NDS`
  - 1b Spécifiez les paramètres obligatoires et exécutez la commande suivante :

```
ndsccheck [-h nom_d'hôte port] [-a admin_FDN] [-w mot_de_passe]
```
- 2 (Facultatif) Indiquez au processus de configuration d'appliquer le même mot de passe pour tous les paramètres configurés par le programme d'installation intégré. Pour plus d'informations, reportez-vous à la [Section 3.2, « Utilisation d'un même mot de passe pour tous les paramètres configurés lors de la procédure d'installation intégrée »](#), page 25.
- 3 Pour lancer la configuration en mode silencieux, entrez l'une des commandes suivantes :
  - ♦ **Linux** : `configure.bin -i silent -f <chemin_ISO_extrait>/install/propfiles/configure_new_tree.properties`
  - ♦ **Windows** : `configure.exe -i silent -f <chemin_ISO_extrait>/install/propfiles/configure_new_tree.properties`



# 5 Présentation des paramètres de configuration

Cette section définit les paramètres que vous devez spécifier pour configurer de manière adéquate votre installation d'Identity Manager. Vous pouvez utiliser le programme d'installation pour configurer les composants immédiatement après leur installation.

---

**REMARQUE :** pour la plupart des composants, vous devez spécifier un mot de passe. Vous pouvez utiliser le même mot de passe pour chacun des paramètres. Pour ce faire, spécifiez le mot de passe à utiliser lorsque vous lancez la procédure d'installation. Pour plus d'informations, reportez-vous aux instructions d'installation.

---

## 5.1 Coffre-fort d'identité

Cette section définit les paramètres de l'arborescence eDirectory utilisée pour le coffre-fort d'identité. Certains paramètres s'appliquent uniquement à la configuration d'une nouvelle arborescence et non à celle d'une arborescence existante. Par ailleurs, le programme affiche les paramètres de base. Pour afficher tous les paramètres, cliquez sur **Paramètres avancés**.

### 5.1.1 Création d'une nouvelle arborescence

Utilisez les paramètres suivants si vous ne disposez pas d'une arborescence eDirectory existante. Tous les paramètres de cette section sont destinés à créer une nouvelle arborescence.

#### Créer une arborescence

Sélectionnez cette option pour créer une nouvelle arborescence eDirectory pour votre coffre-fort d'identité.

#### Nom de l'arborescence

Permet de spécifier le nom de l'arborescence à créer. Ce nom doit satisfaire aux conditions suivantes :

- ♦ Le nom de l'arborescence doit être unique sur votre réseau.
- ♦ Le nom de l'arborescence doit se composer de 2 à 32 caractères.
- ♦ Le nom de l'arborescence doit uniquement contenir des caractères de type lettres (a-zA-Z), chiffres (0-9), tirets (-) et traits de soulignement (\_).

Si vous utilisez plusieurs arborescences, établissez une norme au sein de l'entreprise pour l'attribution des noms afin de faciliter les éventuelles fusions d'arborescences ultérieures.

#### Mot de passe de l'administrateur

Permet de spécifier le mot de passe de l'objet Administrateur. Par exemple, `netiq123`. Le programme d'installation attribue ce mot de passe à l'objet Administrateur créé.

## Paramètres avancés

Tous les autres paramètres se trouvent sous **Paramètres avancés**. Si vous n'apportez pas de modifications aux **Paramètres avancés**, le programme de configuration utilise les paramètres par défaut enregistrés.

### Administrateur du coffre-fort d'identité

Permet de spécifier le nom distinctif relatif (RDN) de l'objet Administrateur de l'arborescence qui possède les droits complets, au moins sur le contexte auquel ce serveur est ajouté. Le nom par défaut est `admin`.

Le programme d'installation utilise ce compte pour effectuer toutes les opérations dans l'arborescence.

### Port NCP

*Uniquement applicable aux serveurs Linux*

Permet de spécifier le port NCP (NetWare Core Protocol) que le coffre-fort d'identité utilise pour communiquer avec les composants Identity Manager. La valeur par défaut est 524.

### Port 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.

Pour plus d'informations sur l'utilisation de LDAP, reportez-vous à la section [Utilisation du protocole LDAP pour communiquer avec le coffre-fort d'identité](#) du [Guide d'installation de NetIQ Identity Manager](#).

### Port LDAP sécurisé

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. Pour plus d'informations sur l'utilisation de LDAP, reportez-vous à la section [Utilisation du protocole LDAP pour communiquer avec le coffre-fort d'identité](#) du [Guide d'installation de NetIQ Identity Manager](#).

### Port HTTP

Permet de spécifier le port sur lequel la pile HTTP fonctionne en texte clair. La valeur par défaut est 8028.

Les ports définis pour la pile HTTP doivent être différents de ceux que vous utilisez pour iManager. Pour plus d'informations, reportez-vous au [Guide d'administration de NetIQ iManager](#).

### Port HTTP sécurisé

Permet de spécifier le port sur lequel la pile HTTP fonctionne à l'aide du protocole TLS/SSL. La valeur par défaut est 8030.

Les ports définis pour la pile HTTP doivent être différents de ceux que vous utilisez pour iManager. Pour plus d'informations, reportez-vous au [Guide d'administration de NetIQ iManager](#).

### Chemin de l'instance eDirectory

*Uniquement applicable aux serveurs Linux*

Permet de spécifier le chemin de cette instance eDirectory sur ce serveur. Le chemin d'accès par défaut est `/var/opt/novell/eDirectory`. Vous pouvez exécuter plusieurs instances eDirectory sur un même serveur.

### Chemin du répertoire DIB

Permet de spécifier le chemin d'accès de l'emplacement du système local auquel vous souhaitez installer les fichiers de la base de données des informations de l'annuaire (DIB). Par défaut, le programme d'installation place ces fichiers aux emplacements suivants :

- ♦ **Linux** : /var/opt/novell/eDirectory/data/dib
- ♦ **Windows** : C:\NetIQ\IdentityManager\NDS\DIBFiles\

Les fichiers de données DIB correspondent aux fichiers de votre base de données eDirectory. 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.

---

**IMPORTANT** : sous Windows, les fichiers DIB doivent se trouver dans le répertoire \NDS. Si vous modifiez l'emplacement par défaut des fichiers DIB sous Windows, la configuration du moteur Identity Manager échoue.

---

### Exiger TLS pour les liaisons simples avec un mot de passe

(Facultatif) Indiquez si le coffre-fort d'identité doit utiliser le protocole TLS (Transport Layer Security) lors de la réception de requêtes LDAP en texte clair. Cette option est activée par défaut.

### Activer Secretstore

*Uniquement applicable aux serveurs Windows*

(Facultatif) Indiquez si SecretStore doit être activé pendant la configuration d'eDirectory. Pour plus d'informations, reportez-vous à la section [Intégration de SecretStore dans eDirectory](#) du [Guide d'installation de NetIQ eDirectory](#).

## 5.1.2 Ajout à une arborescence existante

Si vous disposez déjà d'une arborescence eDirectory, utilisez les paramètres suivants pour ajouter ce nouveau serveur à l'arborescence existante.

---

**IMPORTANT** : assurez-vous toutefois de bien comprendre les implications de l'ajout d'un nouveau serveur à une arborescence existante. Pour plus d'informations, reportez-vous à la [Section 4.1](#), « [Considérations relatives à la configuration des composants](#) », page 29.

---

### Ajouter à une arborescence existante

Sélectionnez cette option si vous disposez d'une arborescence existante que vous souhaitez modifier pour l'utiliser avec le coffre-fort d'identité.

### Nom de l'arborescence existante

Indiquez le nom de l'arborescence eDirectory.

### Adresse du serveur existant

Indiquez l'adresse IP du serveur qui contient la réplique maîtresse de la partition racine.

### Numéro du port existant

Spécifiez le port NCP du serveur spécifié ci-dessus. Le port par défaut pour NCP est 524.

### **DN du contexte du serveur existant**

Indiquez le DN LDAP du contexte dans lequel vous souhaitez que ce serveur soit placé dans votre arborescence existante. La valeur par défaut est ou=servers,o=system au sein de la structure du coffre-fort d'identité créée par le programme d'installation intégré. Pour plus d'informations, reportez-vous à la [Section 1.3, « Présentation de la structure par défaut du coffre-fort d'identité »](#), page 14.

### **Nom de l'administrateur du serveur existant**

Indiquez le nom de l'administrateur eDirectory. Le nom par défaut est admin. Pour plus d'informations, reportez-vous à la [Section 1.3, « Présentation de la structure par défaut du coffre-fort d'identité »](#), page 14.

### **DN du contexte administrateur du serveur existant**

Indiquez le DN LDAP du contexte dans lequel est placé l'administrateur eDirectory dans l'arborescence existante. La valeur par défaut est ou=sa,o=system au sein de la structure du coffre-fort d'identité créée par le programme d'installation intégré. Pour plus d'informations, reportez-vous à la [Section 1.3, « Présentation de la structure par défaut du coffre-fort d'identité »](#), page 14.

### **Mot de passe de l'administrateur du serveur existant**

Indiquez le mot de passe de l'administrateur eDirectory.

### **Paramètres avancés**

Tous les autres paramètres se trouvent sous **Paramètres avancés**. Si vous n'apportez pas de modifications aux **Paramètres avancés**, le programme de configuration utilise les paramètres par défaut enregistrés.

#### **Port LDAP**

Permet de spécifier le port sur lequel l'arborescence eDirectory existante doit être à l'écoute des requêtes LDAP en texte clair. La valeur par défaut est 389.

Pour plus d'informations sur l'utilisation de LDAP, reportez-vous à la section [Utilisation du protocole LDAP pour communiquer avec le coffre-fort d'identité](#) du [Guide d'installation de NetIQ Identity Manager](#).

#### **Port LDAP sécurisé**

Permet de spécifier le port sur lequel l'arborescence eDirectory existante doit être à l'écoute des requêtes LDAP à l'aide du protocole SSL (Secure Sockets Layer). La valeur par défaut est 636.

Pour plus d'informations sur l'utilisation de LDAP, reportez-vous à la section [Utilisation du protocole LDAP pour communiquer avec le coffre-fort d'identité](#) du [Guide d'installation de NetIQ Identity Manager](#).

#### **Port HTTP**

Permet de spécifier le port sur lequel la pile HTTP fonctionne en texte clair. La valeur par défaut est 8028.

Les ports définis pour la pile HTTP doivent être différents de ceux que vous utilisez pour iManager. Pour plus d'informations, reportez-vous au manuel [NetIQ Manager Administration Guide](#) (Guide d'administration du catalogue NetIQ Identity Manager).

#### **Port HTTP sécurisé**

Permet de spécifier le port sur lequel la pile HTTP fonctionne à l'aide du protocole TLS/SSL. La valeur par défaut est 8030.

Les ports définis pour la pile HTTP doivent être différents de ceux que vous utilisez pour iManager. Pour plus d'informations, reportez-vous au [Guide d'administration de NetIQ iManager](#).

### Chemin du répertoire DIB

Permet de spécifier le chemin d'accès de l'emplacement du système local auquel vous souhaitez installer les fichiers de la base de données des informations de l'annuaire (DIB). Par défaut, le programme d'installation place ces fichiers aux emplacements suivants :

- ♦ **Linux** : /var/opt/novell/eDirectory/data/dib
- ♦ **Windows** : C:\NetIQ\IdentityManager\NDS\DIBFiles\

Les fichiers de données DIB correspondent aux fichiers de votre base de données eDirectory. 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.

---

**IMPORTANT** : sous Windows, les fichiers DIB doivent se trouver dans le répertoire \NDS. Si vous modifiez l'emplacement par défaut des fichiers DIB sous Windows, la configuration du moteur Identity Manager échoue.

---

### Exiger TLS pour les liaisons simples avec un mot de passe

(Facultatif) Indiquez si le coffre-fort d'identité doit utiliser le protocole TLS (Transport Layer Security) lors de la réception de requêtes LDAP en texte clair. Cette option est activée par défaut.

### Activer Secretstore

*Uniquement applicable aux serveurs Windows*

(Facultatif) Indiquez si SecretStore doit être activé pendant la configuration d'eDirectory. Pour plus d'informations, reportez-vous à la section [Intégration de SecretStore dans eDirectory](#) du [Guide d'installation de NetIQ eDirectory](#).

## 5.2 Serveur Identity Manager

Le programme d'installation intégré n'affiche les champs relatifs au **serveur Identity Manager** que dans le cas où vous choisissez d'ajouter votre serveur à une arborescence eDirectory existante.

---

**IMPORTANT** : le programme d'installation intégré ne prend pas en charge les mises à niveau. Si vous disposez déjà d'un déploiement d'Identity Manager, vous devez utiliser les programmes d'installation standard pour mettre à niveau de votre solution Identity Manager. Pour plus d'informations, reportez-vous à la section [Mise à niveau d'Identity Manager](#) du [Guide d'installation de NetIQ Identity Manager](#).

---

### Nom de l'ensemble de pilotes

Indiquez un nom pour le nouvel objet Ensemble de pilotes d'Identity Manager. Cet objet doit être créé pour qu'Identity Manager puisse fonctionner. Si vous créez une nouvelle arborescence, le programme d'installation intégré crée cet objet pour vous.

### DN du contexte de l'ensemble de pilotes

Indiquez le DN LDAP du conteneur dans lequel vous souhaitez créer cet objet Ensemble de pilotes. L'emplacement par défaut est o=system au sein de la structure du coffre-fort d'identité créée par le programme d'installation intégré. Pour plus d'informations, reportez-vous à la [Section 1.3, « Présentation de la structure par défaut du coffre-fort d'identité », page 14](#).

## 5.3 Sentinel Log Management for IGA

Sentinel Log Management for IGA permet d'auditer vos composants Identity Manager. Ce composant doit être installé et en cours d'exécution avant de configurer les applications d'identité et Identity Reporting. Sinon, la configuration de ces composants échoue.

### Mot de passe Sentinel

Spécifiez le mot de passe de l'administrateur Sentinel. La procédure d'installation se charge de créer ce compte.

---

**REMARQUE** : sur un serveur SLES, le mot de passe doit respecter la stratégie de mot de passe des systèmes.

---

### Mot de passe dbauser

Permet de spécifier le mot de passe pour le compte `admin` qui peut modifier l'entrepôt d'informations d'identité. La procédure d'installation se charge de créer ce compte.

---

**REMARQUE** : sur un serveur SLES, le mot de passe doit respecter la stratégie de mot de passe des systèmes.

---

### Paramètres avancés

Tous les autres paramètres se trouvent sous **Paramètres avancés**. Si vous n'apportez pas de modifications aux **Paramètres avancés**, le programme de configuration utilise les paramètres par défaut enregistrés.

## 5.4 Applications d'identité

Cette section définit les paramètres des applications d'identité, telles que l'application utilisateur. Le programme affiche les paramètres de base. Pour afficher tous les paramètres, cliquez sur **Paramètres avancés**.

---

**IMPORTANT** : vous devez sélectionner **Paramètres avancés** et modifier tous les champs contenant la mention `localhost` afin qu'ils correspondent à une adresse IP ou un nom DNS valide. Si vous ne remplacez pas le paramètre par défaut `localhost`, la configuration échoue.

---

### Hôte du serveur OSP

Permet de spécifier le nom DNS ou l'adresse IP du serveur sur lequel vous envisagez d'installer OSP, et qui devient alors le serveur d'authentification LDAP. N'utilisez pas le terme `localhost`.

Pour plus d'informations sur OSP, reportez-vous à la section [Utilisation de l'accès Single Sign-on dans Identity Manager](#) du [Guide d'installation de NetIQ Identity Manager](#).

### Mot de passe OSP Keystore

Permet de spécifier le mot de passe que vous souhaitez créer pour le chargement du nouveau keystore sur le serveur OAuth.

Ce mot de passe doit être composé d'au moins six caractères.



### Mot de passe de configuration SSPR

Permet de spécifier le mot de passe que vous souhaitez créer pour configurer SSPR (Self-Service Password Reset).

Par défaut, SSPR ne demande pas de mot de passe pour la configuration. Or, sans mot de passe, tout utilisateur qui peut se connecter à SSPR peut également modifier les paramètres de configuration.

### Mot de passe du service

Permet de spécifier le mot de passe du client Single Sign-on utilisé par SSPR, les applications d'identité et Identity Reporting.

Ce mot de passe doit être composé d'au moins six caractères.

### Mot de passe de l'administrateur des applications d'identité

Permet de spécifier le mot de passe de l'administrateur de l'application utilisateur. La procédure d'installation crée ce compte dans le coffre-fort d'identité et lui confère les droits nécessaires pour effectuer des tâches administratives sur le conteneur d'utilisateurs de l'application utilisateur. Ce paramètre présente les caractéristiques suivantes :

- ♦ Par défaut, le nom du compte est `uaadmin`.
- ♦ Si vous avez démarré le serveur d'applications hébergeant l'application utilisateur, vous ne pouvez pas modifier ce paramètre à l'aide des fichiers `configupdate.sh` ou `configupdate.bat`.
- ♦ Pour modifier cette assignation après avoir déployé l'application, utilisez la page **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 [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (NetIQ Identity Manager - Guide de l'administrateur des applications d'identité).

### Mot de passe de l'utilisateur de la base de données idmadmin

Permet de spécifier le mot de passe de l'administrateur de la base de données des applications d'identité.

Par défaut, le nom du compte est `idmadmin`.

### Port d'arrêt de Tomcat

Permet de spécifier le port que vous souhaitez utiliser pour arrêter correctement toutes les applications Web et Tomcat. La valeur par défaut est 8105.

### Port HTTP Tomcat

Permet de spécifier le port que le serveur Tomcat doit utiliser pour communiquer avec les ordinateurs clients. La valeur par défaut est 8080. Pour utiliser SSL, la valeur par défaut est 8443. Pour plus d'informations, reportez-vous à la section [Activation de SSL avec un certificat signé](#) du [Guide d'installation de NetIQ Identity Manager](#).

### Port de redirection Tomcat

(Conditionnel) Si vous n'utilisez pas les protocoles TLS/SSL, permet de spécifier le port sur lequel le serveur d'applications redirige les requêtes qui nécessitent un transport SSL. La valeur par défaut est 8543.

### Port AJP Tomcat

(Facultatif) Permet de spécifier le port que le serveur d'applications doit utiliser pour communiquer avec un connecteur Web à l'aide du protocole AJP au lieu de HTTP. La valeur par défaut est 8109.

Utilisez ce paramètre lorsque vous souhaitez que le serveur d'applications gère le contenu statique se trouvant dans l'application Web, ou si vous souhaitez utiliser la fonctionnalité de traitement SSL du serveur d'applications.

### Hôte du serveur d'audit

Permet de spécifier le nom DNS ou l'adresse IP du serveur qui héberge la base de données SIEM utilisée par Sentinel et Identity Reporting (l'entrepôt d'informations d'identité). N'utilisez pas `localhost`.

---

**IMPORTANT :** vous devez installer et exécuter votre serveur d'audit avant de commencer à configurer les applications d'identité. Si le programme d'installation intégré ne peut pas communiquer avec le serveur d'audit, la configuration échoue.

---

### Paramètres avancés

Tous les autres paramètres se trouvent sous **Paramètres avancés**. Vous devez modifier le contenu du champ **Hôte des applications d'identité** en remplaçant `localhost` par une adresse IP ou un nom DNS. Si vous n'apportez pas de modifications aux **Paramètres avancés**, le programme de configuration utilise les paramètres par défaut enregistrés et la configuration échoue.

### Administrateur des applications d'identité

Permet de spécifier le nom du compte administrateur pour les applications d'identité. La valeur par défaut est `uaadmin`.

### Hôte des applications d'identité

Permet de spécifier l'URL de connexion au client de l'application utilisateur sur le serveur d'applications. N'utilisez pas le terme `localhost`.

## 5.5 Module Novell Identity Reporting

Cette section définit les paramètres du module Identity Reporting. Le programme affiche les paramètres de base. Pour afficher tous les paramètres, cliquez sur **Paramètres avancés**.

---

**IMPORTANT :** le module Identity Reporting nécessite Sentinel. Ce dernier s'exécute uniquement sur des ordinateurs Linux. Si vous effectuez l'installation sur un ordinateur Windows, vous devez installer Sentinel sur un ordinateur Linux avant de commencer à configurer le module Identity Reporting sous Windows.

---

### Port de passerelle système gérée

Permet de spécifier le port que le pilote MSGW doit utiliser pour communiquer avec le coffre-fort d'identité.

La valeur par défaut est 7707.

### Hôte du service de collecte de données

Permet de spécifier le nom DNS ou l'adresse IP du serveur qui héberge le service de collecte de données. N'utilisez pas le terme `localhost`.

### Paramètres avancés

Tous les autres paramètres se trouvent sous **Paramètres avancés**. Si vous n'apportez pas de modifications aux **Paramètres avancés**, le programme de configuration utilise les paramètres par défaut enregistrés.

### Activer la recherche dans les sous-conteneurs

Indiquez si les modules Identity Reporting doivent prendre en charge les recherches dans les sous-conteneurs. Cette option est activée par défaut.

### Utiliser des connexions LDAP sécurisées

Indiquez si vous souhaitez que le serveur communique via une connexion LDAP sécurisée. Vous devez également spécifier le **port LDAP**.

### Port LDAP

Permet de spécifier le port à utiliser pour communiquer avec le serveur qui héberge le coffre-fort d'identité. Indiquez la même valeur que celle que vous avez utilisée pour l'option **port LDAP sécurisé** dans la [Section 5.1, « Coffre-fort d'identité », page 35](#).

Vous pouvez aussi spécifier un port en texte clair pour les communications non sécurisées. Si vous optez pour cette dernière option, ne sélectionnez pas **Utiliser des connexions LDAP sécurisées**.

### Valeur d'expiration du jeton (en minutes)

Indiquez la durée pendant laquelle un jeton d'authentification doit être conservé. La valeur par défaut est de 60 minutes.

### Conservation des rapports terminés : durée et unités

Sélectionnez la durée pendant laquelle le module Identity Reporting doit conserver les rapports finalisés avant de les supprimer. Par exemple, pour une période de conservation de six mois, sélectionnez **Mois** pour la durée et 6 pour les unités.

### Attribut de login du sous-conteneur

Indique l'attribut de connexion qu'Identity Manager utilise pour effectuer des recherches dans la sous-arborescence du conteneur d'utilisateurs spécifié lors de la collecte de données destinées à la création de rapports. La valeur par défaut est `cn`.

---

**REMARQUE** : si vous spécifiez un DN qui inclut des caractères spéciaux, il se peut que vous ayez besoin d'insérer des séquences d'échappement devant ces caractères. Pour plus d'informations, reportez-vous au document [RFC 2253/4514 Section 2](#).

---

### Hôte du serveur SMTP

Permet de spécifier le nom DNS ou l'adresse IP du serveur de messagerie que le module Identity Reporting doit utiliser pour envoyer des notifications. La valeur par défaut est `localhost`. Remplacez-la par une adresse IP ou un nom DNS valide.

### Port du serveur SMTP

Permet de spécifier le numéro de port du serveur de messagerie. La valeur par défaut est 435.

### ID utilisateur SMTP

(Conditionnel) Si vous avez recours à l'authentification pour les communications avec le serveur de messagerie, spécifiez l'adresse électronique que vous souhaitez utiliser pour cette authentification.

Vous devez également sélectionner l'option **Exiger l'authentification du serveur pour SMTP**.

### Mot de passe de l'utilisateur SMTP

Permet de spécifier le mot de passe associé à l'adresse électronique que vous souhaitez utiliser pour l'authentification.

### Adresse électronique par défaut

Permet de spécifier l'adresse électronique que vous souhaitez que le module Identity Reporting utilise pour émettre des notifications par message électronique.

### Utiliser SSL pour SMTP

Permet d'indiquer si vous souhaitez utiliser SSL pour les communications avec le serveur de messagerie. Par défaut, cette option n'est pas activée.

### Exiger l'authentification du serveur pour SMTP

Permet d'indiquer si vous souhaitez utiliser l'authentification pour les communications avec le serveur de messagerie.

Vous devez également définir les valeurs des champs **ID utilisateur SMTP** et **Mot de passe de l'utilisateur SMTP**. Par défaut, cette option n'est pas activée.

## 5.6 Outils

Cette section définit les paramètres des différents outils Identity Manager : iManager, Analyzer et Designer. À l'heure actuelle, seul iManager offre des paramètres programmables. Ces paramètres n'apparaissent que sur les ordinateurs Linux pendant la configuration. Pour afficher les paramètres, cliquez sur **Paramètres avancés**.

---

**REMARQUE** : les ports définis pour la pile HTTP doivent être différents de ceux que vous utilisez pour le coffre-fort d'identité. Pour plus d'informations, reportez-vous au [Guide d'administration de NetIQ iManager](#).

---

### Port HTTP

Permet de spécifier le numéro du port de la pile utilisé par iManager pour les communications en texte clair. La valeur par défaut est 8080.

### Port HTTP sécurisé

Permet de spécifier le numéro du port de la pile utilisé par iManager pour les communications via le protocole TLS/SSL. La valeur par défaut est 8443.

# 6 Dernières étapes de la procédure d'installation intégrée

À l'issue de l'exécution du programme d'installation intégré, les composants Identity Manager ont été installés et la configuration de base est terminée. Toutefois, pour que les différents composants soient entièrement opérationnels, vous devez encore créer des pilotes et effectuer des étapes de configuration supplémentaires.

## 6.1 Assignation de l'objet de stratégie de mot de passe aux ensembles de pilotes

Vous devez assigner l'objet `DirXML-PasswordPolicy` à chaque ensemble de pilotes dans une arborescence dans le coffre-fort d'identité. Le processus d'installation intégré n'ajoute pas l'objet de stratégie au coffre-fort d'identité. Vous pouvez cependant créer l'objet.

- ♦ [Section 6.1.1, « Création de l'objet de stratégie de mot de passe », page 45](#)
- ♦ [Section 6.1.2, « Assignation de l'objet de stratégie de mot de passe », page 46](#)

### 6.1.1 Création de l'objet de stratégie de mot de passe

Si l'objet `DirXML-PasswordPolicy` n'existe pas dans le coffre-fort d'identité, procédez comme suit pour le créer.

- 1 Dans un éditeur de texte, créez un fichier LDIF (LDAP Data Interchange Format) avec les attributs suivants :

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: <driverset LDAP dn>
```

---

**REMARQUE :** si vous copiez le contenu tel quel, vous risquez d'introduire des caractères spéciaux masqués dans le fichier. Si un message d'erreur de type `ldif_record() = 17` s'affiche lors de l'ajout de ces attributs au coffre-fort d'identité, insérez un espace supplémentaire entre les deux DN.

---

- 2 Pour ajouter l'objet `DirMXL-PasswordPolicy` dans le coffre-fort d'identité, importez les attributs du fichier en effectuant l'une des opérations suivantes :

**Linux :**

Accédez au répertoire contenant l'utilitaire `ldapmodify` et entrez la commande suivante :

```
ldapmodify -x -c -h hostname_or_IP_address -p 389 -D  
"cn=admin,ou=sa,o=system" -w password -f path_to_ldif_file
```

Par exemple :

```
ldapmodify -x -ZZ -c -h server1.test.com -p 389 -D  
"cn=admin,ou=sa,o=system" -w test123 -f /root/dirxmlpasswordpolicy.ldif
```

Par défaut, l'utilitaire `ldapmodify` est situé dans le répertoire `/opt/novell/eDirectory/bin`.

**Windows :**

Exécutez le fichier `ldapmodify.exe` à partir du répertoire `install/utilities` du kit d'installation d'Identity Manager.

## 6.1.2 Assignation de l'objet de stratégie de mot de passe

Vous devez assigner l'objet `DirMXL-PasswordPolicy` à chaque ensemble de pilotes d'une arborescence. Pour plus d'informations, reportez-vous à la section [Creating Password Policies](#) (Création de stratégies de mot de passe) du manuel [Password Management Administration Guide](#) (Guide d'administration 3.3.2 pour la gestion des mots de passe).

## 6.2 Configuration des composants Identity Manager

Après l'installation, vous devez configurer certains composants Identity Manager.

- ♦ **Pilotes :** pour chaque pilote, il existe un manuel expliquant comment procéder à son installation et à sa configuration. Pour plus d'informations, reportez-vous au [site Web de documentation des pilotes Identity Manager](#).
- ♦ **Applications d'identité :** vous devez configurer les différentes applications d'identité afin qu'elles fonctionnent dans votre environnement. Pour plus d'informations, reportez-vous aux guides suivants :
  - ♦ [Guide d'installation de NetIQ Identity Manager](#)
  - ♦ [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (Guide de l'administrateur des applications d'identité de NetIQ Identity Manager)
- ♦ **Identity Reporting :** vous devez configurer Identity Reporting pour votre environnement. Pour plus d'informations, reportez-vous au [Guide de l'administrateur de NetIQ Identity Reporting](#).

# 7 Activation des produits Identity Manager

Les informations de cette section expliquent le fonctionnement de l'activation pour les composants Identity Manager. Les composants Identity Manager doivent être activés dans les 90 jours à compter de l'installation, faute de quoi ils ne fonctionnent plus. À n'importe quel moment au cours de ces 90 jours, ou ultérieurement, vous pouvez choisir d'activer les produits Identity Manager. Utilisez les informations présentées dans les sections suivantes pour activer les composants Identity Manager.

## 7.1 Achat d'une licence de produit Identity Manager

Pour acheter une licence de produit Identity Manager afin de l'activer, reportez-vous à la [page Web du guide d'achat de NetIQ Identity Manager \(https://www.netiq.com/products/identity-manager/advanced/how-to-buy/\)](https://www.netiq.com/products/identity-manager/advanced/how-to-buy/).

Une fois la licence de 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 oubliez votre ID client ou ne l'avez pas reçu, contactez votre représentant commercial.

## 7.2 Installation d'une référence d'activation de produit

Installez la référence d'activation de produit via iManager.

**Pour installer la référence d'activation du produit :**

- 1 Une fois la licence achetée, NetIQ vous envoie un message électronique incluant votre ID client. Ce message contient également, sous la section Order Detail (Détail de la commande), un lien vers le site auprès duquel vous pouvez obtenir votre référence. Cliquez sur le lien pour accéder à ce site.
- 2 Cliquez sur le lien de téléchargement de licence et effectuez l'une des opérations suivantes :
  - ♦ Enregistrez le fichier de référence d'activation de produit à un emplacement adéquat.  
ou
  - ♦ Ouvrez le fichier de référence d'activation du produit, puis copiez son contenu dans le Presse-papiers.  
  
Copiez attentivement le contenu et veillez à n'inclure aucune ligne ni aucun espace supplémentaire. 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 (-) de la référence (FIN DE LA RÉFÉRENCE D'ACTIVATION DU PRODUIT-----).
- 3 Ouvrez iManager.
- 4 Sélectionnez **Identity Manager > Présentation de Identity Manager**.
- 5 Recherchez et sélectionnez un ensemble de pilotes dans la structure de l'arborescence.

- 6 Sur la page Présentation d'Identity Manager, cliquez sur l'ensemble des 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 activer un composant Identity Manager, puis cliquez sur **Suivant**.
- 9 Effectuez l'une des opérations suivantes :
  - ♦ Indiquez l'emplacement dans lequel vous avez enregistré les références d'activation d'Identity Manager, puis cliquez sur **Suivant**.
  - ou
  - ♦ Collez le contenu des références d'activation d'Identity Manager dans la zone de texte, puis cliquez sur **Suivant**.
- 10 Cliquez sur **Terminer**.


---

**REMARQUE** : vous devez activer chaque ensemble de pilotes qui contient un pilote. Vous pouvez activer n'importe quelle arborescence avec la référence.

---

## 7.3 Affichage 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 moteur et les pilotes Identity Manager :

- 1 Ouvrez iManager.
- 2 Cliquez sur **Identity Manager > Présentation d'Identity Manager**.
- 3 Recherchez et sélectionnez un ensemble de pilotes dans la structure de l'arborescence, puis cliquez sur  pour lancer la recherche.
- 4 Sur la page Présentation d'Identity Manager, cliquez sur l'ensemble de pilotes pour lequel vous souhaitez afficher les informations d'activation.
- 5 Sur la page Présentation de l'ensemble des 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.

---

**REMARQUE** : après l'installation d'une référence d'activation de produit valide pour un ensemble de pilotes, il est possible que la mention **Activation requise** apparaisse encore en regard du nom du pilote. Dans ce cas, redémarrez le pilote et le message devrait disparaître.

---

## 7.4 Activation des pilotes Identity Manager

Le produit Identity Manager que vous avez acheté inclut les références d'activation de plusieurs pilotes communs et pilotes de service.

- ♦ **Pilotes de service** : les pilotes de service suivants sont activés en même temps que le moteur Identity Manager :
  - ♦ Service de collecte de données
  - ♦ Services de droits



- ♦ Fournisseur d'ID
- ♦ Service de boucle
- ♦ Passerelle système gérée
- ♦ Service de tâche manuelle
- ♦ Service nul
- ♦ Service de rôles
- ♦ Application utilisateur
- ♦ Ordre de travail
- ♦ **Pilotes courants** : les pilotes communs suivants sont activés en même temps que le moteur Identity Manager :
  - ♦ Active Directory
  - ♦ ADAM
  - ♦ eDirectory
  - ♦ GroupWise
  - ♦ LDAP
  - ♦ Lotus Notes

Les activations de tous les autres pilotes Identity Manager doivent être achetées séparément. Les activations de pilotes sont vendues en tant que modules d'intégration Identity Manager. Un module d'intégration Identity Manager peut contenir un ou plusieurs pilotes. Vous recevez une référence d'activation de produit pour chaque module d'intégration Identity Manager acheté.

Vous devez effectuer les étapes décrites à la [Section 7.2, « Installation d'une référence d'activation de produit »](#), [page 47](#) pour chaque module afin d'activer les pilotes.

## 7.5 Activation d'Analyzer

Lors du premier démarrage d'Analyzer, vous êtes invité à l'activer. Si vous ne l'activez pas, vous ne pouvez pas utiliser Analyzer.

## 7.6 Activation de Designer et de l'administrateur d'assignation de rôles

Designer et l'administrateur de l'assignation de rôles ne requièrent pas d'activation en dehors de celle du moteur et des pilotes Identity Manager.



# 8

## Désinstallation d'Identity Manager

Vous pouvez désinstaller tous les composants Identity Manager installés à l'aide de l'assistant de désinstallation d'Identity Manager. Pour plus d'informations sur la désinstallation de chaque composant Identity Manager, reportez-vous à la section [Désinstallation des composants Identity Manager](#) du *Guide d'installation de NetIQ Identity Manager*.



# 9 Dépannage

Utilisez les informations suivantes pour résoudre les problèmes relatifs au programme d'installation intégré.

## 9.1 Emplacement des fichiers journaux et de propriétés

Le tableau suivant contient l'emplacement du journal d'installation (`ii_install.log`), du journal de configuration (`ii_configure.log`) et des fichiers de propriétés. À chaque composant installé correspond un fichier de propriétés.

Plate-forme	Fichiers journaux	Installation des fichiers de propriétés
Windows	<code>&lt;emplacement_installation&gt;\install\logs</code>  L'emplacement par défaut est <code>C:\netiq\IdentityManager\install\logs</code>	<code>&lt;emplacement_installation&gt;\install\propfiles</code>  L'emplacement par défaut est <code>C:\netiq\IdentityManager\install\logs\propfiles\</code>
Linux	<code>/var/opt/netiq/idm/install/logs</code>	<code>/var/opt/netiq/idm/install/logs/propfiles/</code>

## 9.2 Dépannage en cas d'échec de la configuration

Utilisez les informations suivantes pour remédier à un échec de la configuration des composants :

**Problème :** La configuration des applications d'identité échoue.

**Opérations suggérées :** Accédez aux fichiers journaux. Recherchez le mot `localhost`. Si vous trouvez ce mot dans les fichiers journaux, cela signifie qu'au cours de la configuration, vous n'avez pas remplacé la valeur par défaut `localhost` par une adresse IP ou un nom DNS valide sous **Paramètres avancés**. Relancez la configuration en fournissant une adresse IP ou un nom DNS valide sous **Paramètres avancés**.

## 9.3 Dépannage des problèmes liés au chargeur distant sous Windows

Par défaut, le programme d'installation intégré installe tous les composants Identity Manager dans le répertoire `C:\NetIQ`. Tous les pilotes utilisent le répertoire `C:\Novell` par défaut. Cependant, vous pouvez rendre les pilotes opérationnels en modifiant manuellement le répertoire par défaut des pilotes.

**Pour faire fonctionner les pilotes du chargeur distant :**

- 1 Lancez la console du chargeur distant.

- 2 Ajoutez une instance du pilote approprié.
- 3 Modifiez le chemin d'accès par défaut en remplaçant C:\Novell par C:\NetIQ.
- 4 Poursuivez la configuration en suivant les étapes habituelles.

## 9.4 Dépannage en cas de désinstallation

Les informations suivantes peuvent vous aider à résoudre les problèmes de désinstallation. Si le problème persiste, contactez votre représentant NetIQ.

**Problème :** Un message indique que la procédure de désinstallation est incomplète, mais le fichier journal ne contient aucun échec.

**Opérations suggérées :** Le processus n'a pas pu supprimer le répertoire `netiq` qui contient les fichiers d'installation par défaut. Vous pouvez supprimer ce répertoire manuellement si vous avez déjà supprimé tous les logiciels NetIQ de votre ordinateur.