

## Guide du programme d'installation intégré

# Novell® Identity Manager

**4.0**

15 octobre 2010

[www.novell.com](http://www.novell.com)



## Mentions légales

Novell, Inc. exclut toute garantie relative au contenu ou à l'utilisation de cette documentation. En particulier, Novell ne garantit pas que cette documentation est exhaustive ni exempte d'erreurs. Novell, Inc. se réserve en outre le droit de réviser cette publication à tout moment et sans préavis.

Par ailleurs, Novell exclut toute garantie relative à tout logiciel, notamment toute garantie, expresse ou implicite, que le logiciel présenterait des qualités spécifiques ou qu'il conviendrait à un usage particulier. Novell se réserve en outre le droit de modifier à tout moment tout ou partie des logiciels Novell, sans notification préalable de ces modifications à quiconque.

Tous les produits ou informations techniques fournis dans le cadre de ce contrat peuvent être soumis à des contrôles d'exportation aux États-Unis et à la législation commerciale d'autres pays. Vous vous engagez à respecter toutes les réglementations de contrôle des exportations et à vous procurer les licences et classifications nécessaires pour exporter, réexporter ou importer des produits livrables. Vous acceptez de ne pas procéder à des exportations ou à des réexportations vers des entités figurant sur les listes noires d'exportation en vigueur aux États-Unis ou vers des pays terroristes ou soumis à un embargo par la législation américaine en matière d'exportations. Vous acceptez de ne pas utiliser les produits livrables pour le développement prohibé d'armes nucléaires, de missiles ou chimiques et biologiques. Reportez-vous à la [page Web des services de commerce international de Novell \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) pour plus d'informations sur l'exportation des logiciels Novell. Novell décline toute responsabilité dans le cas où vous n'obtiendriez pas les autorisations d'exportation nécessaires.

Copyright © 2010 Novell, Inc. Tous droits réservés. Cette publication ne peut être reproduite, photocopiée, stockée sur un système de recherche documentaire ou transmise, même en partie, sans le consentement écrit explicite préalable de l'éditeur.

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
États-Unis  
[www.novell.com](http://www.novell.com)

*Documentation en ligne* : pour accéder à la documentation en ligne la plus récente de ce produit et des autres produits Novell ou pour obtenir des mises à jour, reportez-vous au [site Novell de documentation \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

## **Marques de Novell**

Pour connaître les marques commerciales de Novell, reportez-vous à la [liste des marques commerciales et des marques de service de Novell \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

## **Éléments tiers**

Toutes les marques commerciales de fabricants tiers appartiennent à leur propriétaire respectif.



# Table des matières

<b>À propos de ce guide</b>	<b>7</b>
<b>1 Présentation du programme d'installation intégré</b>	<b>9</b>
1.1 Programmes d'installation intégré et autonome . . . . .	9
1.2 Configuration des pilotes . . . . .	10
<b>2 Composants Identity Manager</b>	<b>11</b>
2.1 Serveur méta-annuaire (coffre-fort d'identité, moteur méta-annuaire et chargeur distant) . . .	12
2.1.1 Processeurs pris en charge . . . . .	12
2.1.2 Systèmes d'exploitation du serveur . . . . .	12
2.2 Audit et création de rapports . . . . .	13
2.3 Application utilisateur . . . . .	14
2.4 Administrateur d'assignation de rôles . . . . .	15
2.5 iManager, Designer et Analyzer . . . . .	15
2.6 Navigateurs Web . . . . .	15
2.7 Structure du coffre-fort d'identité . . . . .	16
2.7.1 Sécurité . . . . .	17
2.7.2 Données . . . . .	17
2.7.3 Système . . . . .	17
<b>3 Configuration système requise</b>	<b>19</b>
3.1 Plates-formes prises en charge . . . . .	19
3.2 Ressources requises . . . . .	20
<b>4 Installation d'Identity Manager</b>	<b>21</b>
4.1 Obtention du fichier ISO sur le site de téléchargement . . . . .	21
4.2 Nouvelle installation à partir d'un média physique ou d'un fichier ISO . . . . .	22
4.2.1 Installation . . . . .	22
4.2.2 Configuration . . . . .	24
4.3 Installation et configuration en mode silencieux . . . . .	31
4.3.1 Installation en mode silencieux . . . . .	31
4.3.2 Configuration en mode silencieux . . . . .	32
<b>5 Activation des produits Novell Identity Manager</b>	<b>33</b>
5.1 Achat d'une licence de produit Identity Manager . . . . .	33
5.2 Installation d'une référence d'activation de produit . . . . .	33
5.3 Affichage des activations de produits pour Identity Manager et les pilotes . . . . .	34
5.4 Activation des pilotes Identity Manager . . . . .	35
5.5 Activation d'Analyzer . . . . .	35
5.6 Activation de Designer et de l'administrateur d'assignation de rôles . . . . .	36
<b>6 Mise à niveau d'Identity Manager</b>	<b>37</b>
6.1 Création d'une sauvegarde de la configuration actuelle . . . . .	37

6.1.1	Vérification de l'actualité de votre projet Designer . . . . .	37
6.1.2	Création d'une exportation des pilotes . . . . .	39
6.2	Arrêt des pilotes . . . . .	40
6.2.1	Utilisation de Designer pour arrêter les pilotes . . . . .	40
6.2.2	Utilisation d'iManager pour arrêter les pilotes . . . . .	40
6.3	Mise à niveau de Designer . . . . .	41
6.4	Mise à niveau du serveur méta-annuaire (coffre-fort d'identité, moteur méta-annuaire et chargeur distant) . . . . .	41
6.5	Mise à niveaux de pilotes vers des paquetages . . . . .	43
6.5.1	Création d'un nouveau pilote . . . . .	43
6.5.2	Remplacement du contenu existant par du contenu issu de paquetages . . . . .	43
6.5.3	Conservation du contenu actuel et ajout de nouveau contenu avec des paquetages . . . . .	44
6.6	Restauration de stratégies et de règles personnalisées pour le pilote . . . . .	45
6.6.1	Utilisation de Designer pour restaurer les stratégies et les règles personnalisées sur le pilote . . . . .	45
6.6.2	Utilisation d'iManager pour restaurer les stratégies et les règles personnalisées sur le pilote . . . . .	46
6.7	Déploiement du projet converti . . . . .	47
6.8	Lancement des pilotes . . . . .	47
6.8.1	Utilisation de Designer pour lancer les pilotes . . . . .	47
6.8.2	Utilisation d'iManager pour démarrer les pilotes . . . . .	47
<b>7</b>	<b>Dépannage d'Identity Manager</b>	<b>49</b>
<b>8</b>	<b>Désinstallation d'Identity Manager</b>	<b>55</b>

# À propos de ce guide

Novell Identity Manager 4.0 est un service de partage et de synchronisation de données qui permet à des applications, annuaires et bases de données de partager des informations. Il relie des informations dispersées et permet d'établir des stratégies qui régissent les mises à jour automatiques de certains systèmes en cas de changement d'identités.

Identity Manager est à la base du provisioning des comptes, de la sécurité, du Single Sign-on, du self-service utilisateur, de l'authentification, des autorisations, des workflows automatisés et des services Web. Il permet d'intégrer, de gérer et de contrôler vos informations d'identité distribuées, de manière à proposer les bonnes ressources aux bonnes personnes.

Ce guide explique comment installer, mettre à niveau ou désinstaller un système Identity Manager utile à votre environnement.

- ♦ [Chapitre 1, « Présentation du programme d'installation intégré », page 9](#)
- ♦ [Chapitre 2, « Composants Identity Manager », page 11](#)
- ♦ [Chapitre 3, « Configuration système requise », page 19](#)
- ♦ [Chapitre 4, « Installation d'Identity Manager », page 21](#)
- ♦ [Chapitre 5, « Activation des produits Novell Identity Manager », page 33](#)
- ♦ [Chapitre 6, « Mise à niveau d'Identity Manager », page 37](#)
- ♦ [Chapitre 7, « Dépannage d'Identity Manager », page 49](#)
- ♦ [Chapitre 8, « Désinstallation d'Identity Manager », page 55](#)

## Public

Ce guide est destiné aux administrateurs, aux consultants et aux ingénieurs réseau qui planifient et installent Identity Manager dans un environnement de réseau.

## Commentaires

Nous souhaiterions connaître vos commentaires et suggestions sur ce guide et les autres documentations fournies avec ce produit. Utilisez la fonction Commentaires proposée au bas de chaque page de la documentation en ligne ou accédez à la page Web [www.novell.com/documentation/feedback.html](http://www.novell.com/documentation/feedback.html) (en anglais).

## Mises à jour de la documentation

Vous trouverez la version la plus récente de ce document sur le [site Web de la documentation relative à Identity Manager](http://www.novell.com/documentation/idm40/index.html) (<http://www.novell.com/documentation/idm40/index.html>).

## Documentation complémentaire

Pour obtenir une documentation supplémentaire sur Identity Manager, reportez-vous au [site Web de documentation d'Identity Manager](http://www.novell.com/documentation/idm40/index.html) (<http://www.novell.com/documentation/idm40/index.html>).

Pour obtenir de la documentation sur l'application utilisateur, reportez-vous au [site Web de documentation d'Identity Manager](http://www.novell.com/documentation/idm40/index.html) (<http://www.novell.com/documentation/idm40/index.html>).





# Présentation du programme d'installation intégré

# 1

Identity Manager 4.0 assure la mise en conformité efficace, ainsi qu'une réduction des coûts pour la gestion des identités et du provisioning depuis l'environnement du centre de données vers le cloud. Le programme d'installation intégré facilite le déploiement d'Identity Manager 4.0 pour les administrateurs et les consultants. Il s'agit d'un programme d'installation simplifié pour vous aider à configurer un système, car il ne nécessite pas d'installation individuelle de chaque composant.

- ♦ [Section 1.1, « Programmes d'installation intégré et autonome », page 9](#)
- ♦ [Section 1.2, « Configuration des pilotes », page 10](#)

## 1.1 Programmes d'installation intégré et autonome

**Tableau 1-1** Comparaison des programmes d'installation intégré et autonome

Fonctions	Intégré	Autonome
Structure de l'arborescence	La structure de l'arborescence est prédéfinie pour correspondre à la plupart des déploiements d'Identity Manager. Pour plus d'informations sur la structure de l'arborescence, reportez-vous à la <a href="#">Section 2.7, « Structure du coffre-fort d'identité », page 16</a> .	La structure de l'arborescence est personnalisable.
Installation personnalisée de pilotes	Par défaut, tous les pilotes sont installés.	L'installation personnalisée des pilotes est prise en charge.
Ensemble de pilotes	Créé en tant que partition distincte lors de la configuration du serveur méta-annuaire.	Non créé. Peut être créé manuellement à l'aide d'iManager.
Installation non-root	Non prise en charge.	L'installation non-root de certains composants est prise en charge.
Installation du plug-in iManager	Installé automatiquement.	Installé manuellement.
Dépendances	Gère automatiquement les dépendances.	Les dépendances sont gérées manuellement.
Durée de l'installation	Automatise plusieurs étapes manuelles pour configurer rapidement le système.	Nécessite généralement plus de temps.

Fonctions	Intégré	Autonome
Options de sélection utilisateur	L'interface utilisateur comporte moins d'options et requiert donc moins de sélections utilisateur. Plusieurs options utilisent des valeurs par défaut.	L'interface utilisateur compte plusieurs options. Vous devez donc bien connaître les différents composants.
Vérifications des plates-formes prises en charge	Vérifie en interne les différences de plate-forme.	N'effectue pas de vérification de plate-forme.
Gestion des incohérences	Expérience utilisateur cohérente pour tous les composants et plates-formes.	Incohérences possibles.
Phases d'installation et de configuration	Phases d'installation et de configuration séparées.	Diffère selon les composants.

Si vous créez une solution Identity Manager où vous devez installer un ou plusieurs composants Identity Manager séparément ou qui nécessite de nombreuses options personnalisées, reportez-vous au [Guide d'installation de la structure d'Identity Manager 4.0](#) pour obtenir de l'aide. Pour des instructions concernant l'installation, reportez-vous à la section « [Installation](#) » du manuel [Guide d'installation de la structure d'Identity Manager 4.0](#).

Le programme d'installation intégré sert principalement aux nouvelles installations d'Identity Manager 4.0. Pour plus d'informations sur la mise à niveau d'une installation existante, reportez-vous au [Chapitre 6, « Mise à niveau d'Identity Manager », page 37](#).

Actuellement, le programme d'installation intégré prend en charge deux types de modes d'installation : interface graphique et silencieux. Le mode console n'est pas pris en charge.

## 1.2 Configuration des pilotes

Les composants suivants d'Identity Manager 4.0 peuvent être installés et configurés à l'aide du programme d'installation intégré.

- ♦ Serveur méta-annuaire (coffre-fort d'identité, moteur méta-annuaire et chargeur distant)
- ♦ Module de provisioning basé sur les rôles
- ♦ Module Novell Identity Reporting
- ♦ Service d'audit d'événements
- ♦ Administrateur d'assignation de rôles
- ♦ iManager
- ♦ Designer
- ♦ Analyzer

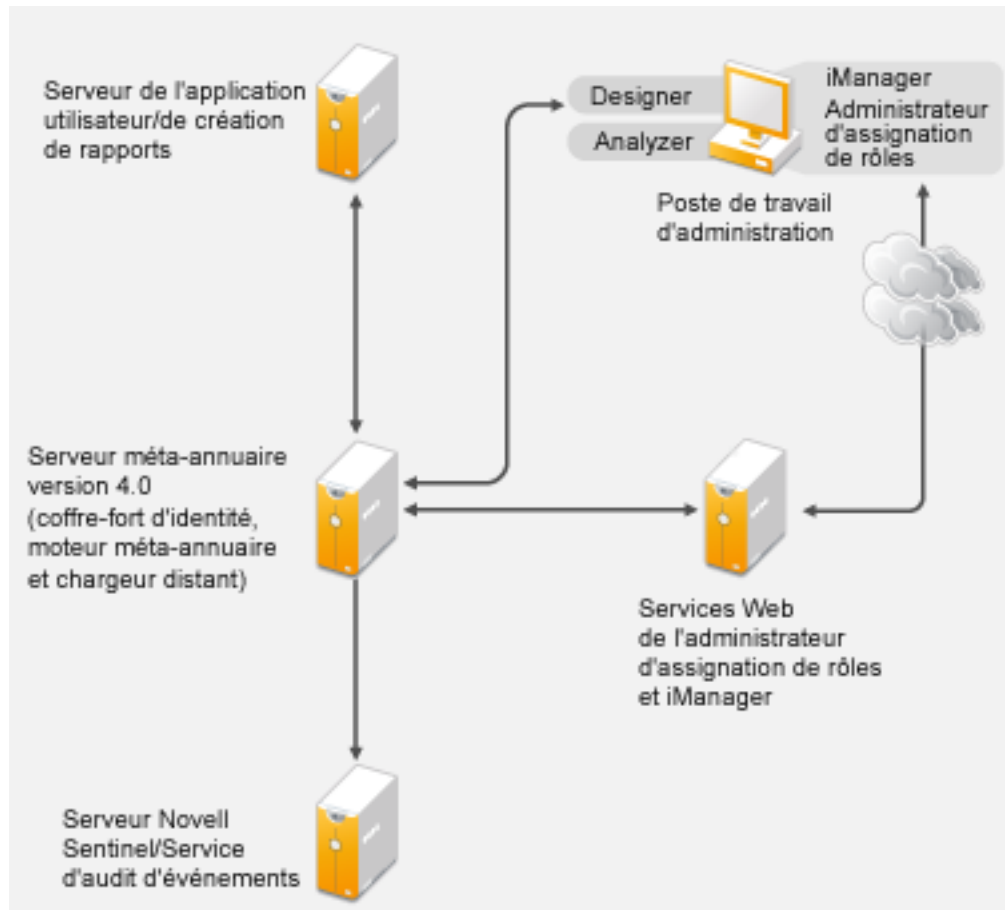
Le programme d'installation intégré configure les pilotes requis pour le module de provisioning basé sur les rôles et le module Identity Reporting. Pour configurer des périphériques supplémentaires, reportez-vous au [site Web de documentation sur les pilotes Identity Manager 4.0 \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).

# Composants Identity Manager

# 2

Vous pouvez installer les composants suivants à l'aide du programme d'installation intégré d'Identity Manager. Les composants Identity Manager ne doivent pas nécessairement être installés sur le même système. La [Figure 2-1](#) montre les plates-formes et les systèmes pris en charge.

**Figure 2-1** Composants du programme d'installation intégré d'Identity Manager



- ◆ [Section 2.1, « Serveur métadirectory \(coffre-fort d'identité, moteur métadirectory et chargeur distant\) »](#), page 12
- ◆ [Section 2.2, « Audit et création de rapports »](#), page 13
- ◆ [Section 2.3, « Application utilisateur »](#), page 14
- ◆ [Section 2.4, « Administrateur d'assignation de rôles »](#), page 15
- ◆ [Section 2.5, « iManager, Designer et Analyzer »](#), page 15
- ◆ [Section 2.6, « Navigateurs Web »](#), page 15
- ◆ [Section 2.7, « Structure du coffre-fort d'identité »](#), page 16

## 2.1 Serveur méta-annuaire (coffre-fort d'identité, moteur méta-annuaire et chargeur distant)

Le serveur méta-annuaire traite les événements des pilotes, qu'ils soient configurés pour utiliser le chargeur distant ou non.

Au cours de l'installation d'Identity Manager, eDirectory est automatiquement installé.

- ♦ [Section 2.1.1, « Processeurs pris en charge », page 12](#)
- ♦ [Section 2.1.2, « Systèmes d'exploitation du serveur », page 12](#)

### 2.1.1 Processeurs pris en charge

Les processeurs répertoriés ci-dessous sont ceux utilisés au cours du test d'Identity Manager.

Les processeurs 32 bits pris en charge pour Linux (SUSE Linux Enterprise Server) et Windows sont les suivants :

- ♦ Intel x86-32
- ♦ AMD x86-32

Les processeurs 64 bits pris en charge pour Linux (SUSE Linux Enterprise Server) et Windows sont les suivants :

- ♦ Intel EM64T
- ♦ AMD Athlon64
- ♦ AMD Opteron

Le processeur SPARC est utilisé pour le test de Solaris.

### 2.1.2 Systèmes d'exploitation du serveur

Vous pouvez installer le moteur méta-annuaire en tant qu'application 32 bits sur un système d'exploitation 32 bits et en tant qu'application 64 bits sur un système d'exploitation 64 bits. Le [Tableau 2-1](#) contient une liste des systèmes d'exploitation du serveur pris en charge sur lesquels le serveur méta-annuaire peut s'exécuter.

**Tableau 2-1** *Systèmes d'exploitation pris en charge pour le serveur*

Version du système d'exploitation du serveur	Notes
Windows Server 2003 SP2 (32 bits)	Le serveur méta-annuaire s'exécute uniquement en mode 32 bits.
Windows Server 2008 R2 (64 bits)	Le serveur méta-annuaire s'exécute uniquement en mode 64 bits.

Version du système d'exploitation du serveur	Notes
SUSE Linux Enterprise Server 10 SP3 (32 et 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits. Novell conseille d'appliquer les derniers correctifs pour les systèmes d'exploitation en passant par le système de mises à jour automatisées du fabricant avant d'installer Identity Manager.
SUSE Linux Enterprise Server 11 (32 et 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits. Novell conseille d'appliquer les derniers correctifs pour les systèmes d'exploitation en passant par le système de mises à jour automatisées du fabricant avant d'installer Identity Manager.
Solaris 10 (64 bits)	Le serveur méta-annuaire s'exécute uniquement en mode 64 bits.
Solaris Zones	Le serveur méta-annuaire s'exécute uniquement en mode 64 bits.

**Tableau 2-2** *Systèmes d'exploitation de virtualisation pris en charge*

Version du système d'exploitation du serveur	Notes
Xen	Xen est pris en charge lorsque la machine virtuelle Xen exécute SLES 10/SLES 11 en tant que système d'exploitation invité en mode paravirtualisé.
Virtualisation de Windows Server 2008 R2 avec Hyper-V	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.
VMware ESX	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.

Le chargeur distant vous offre une souplesse de configuration pour votre solution Identity Manager. Il prend en charge les modes 32 et 64 bits. Par défaut, le programme d'installation détecte la version du système d'exploitation, puis installe la version correspondante du chargeur distant. Le [Tableau 2-1 page 12](#) liste les systèmes d'exploitation pris en charge pour le chargeur distant.

Identity Manager 4.0 permet la coexistence des chargeurs distants 32 et 64 bits sur un système d'exploitation 64 bits. Si vous mettez à niveau un chargeur distant 32 bits installé sur un système d'exploitation 64 bits, le processus met à niveau le chargeur distant 32 bits et installe également le chargeur distant 64 bits. Vous pouvez disposer à la fois d'un chargeur distant 32 bits et d'un chargeur 64 bits sur la même machine.

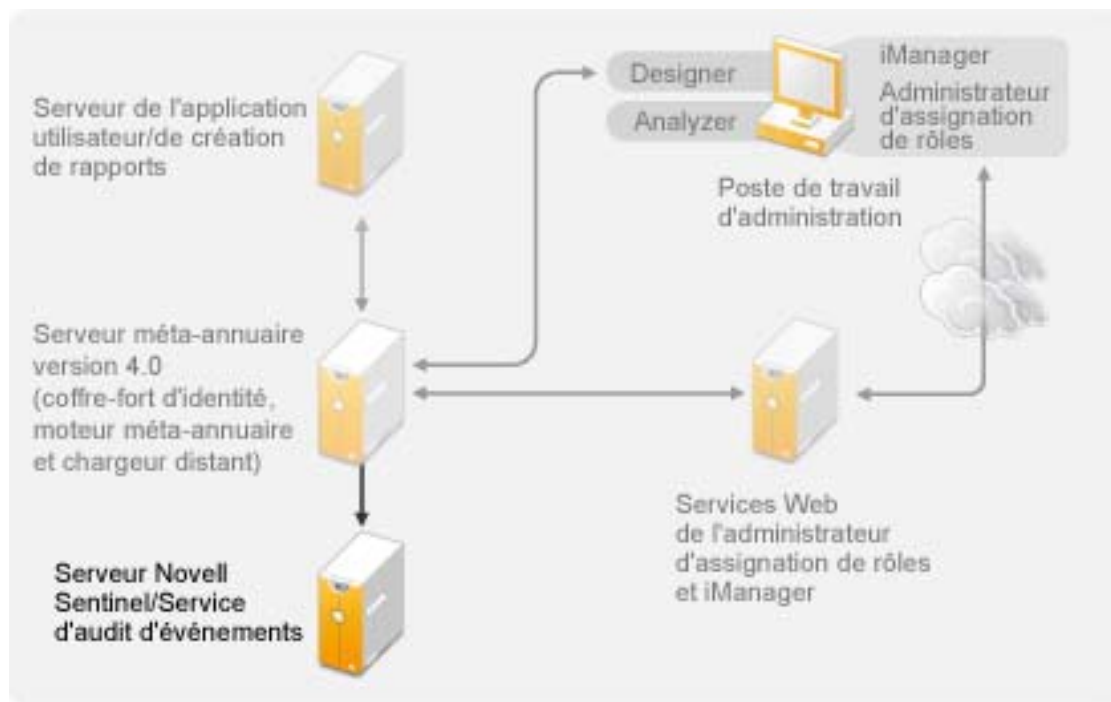
## 2.2 Audit et création de rapports

L'ajout des fonctions d'audit et de création de rapports permet de respecter les normes auxquelles de nombreuses sociétés doivent se conformer. Vous pouvez créer des suivis d'audit pour tous les événements que vous devez suivre et générer des rapports afin de respecter les normes d'audit de votre société.

Le module Novell Identity Reporting et Novell Sentinel sont deux outils distincts qui permettent de rassembler des informations d'audit et de création de rapports concernant Identity Manager.

Le module Identity Reporting est un composant d'Identity Manager 4.0. Novell Sentinel n'est pas fourni avec Identity Manager, mais constitue un composant facultatif que vous pouvez ajouter à votre système Identity Manager.

**Figure 2-2** Audit et création de rapports



Pour plus d'informations sur le module Identity Reporting, reportez-vous au manuel [Identity Reporting Module Guide](#) (Guide du module Novell Identity Reporting). Pour obtenir des informations de configuration concernant Sentinel avec Identity Manager, reportez-vous au manuel [Identity Manager 4.0 Reporting Guide for Novell Sentinel](#) (Guide de création de rapports d'Identity Manager 4.0 pour Novell Sentinel). Pour plus d'informations sur la configuration système requise pour Novell Sentinel, reportez-vous au [Guide d'installation de Novell Sentinel \(http://www.novell.com/documentation/sentinel6/index.html\)](http://www.novell.com/documentation/sentinel6/index.html).

## 2.3 Application utilisateur

L'application utilisateur Identity Manager vous permet d'accéder aux informations, rôles, ressources et fonctionnalités d'Identity Manager. Votre administrateur système détermine les détails de ce que vous pouvez afficher et faire dans l'application utilisateur Identity Manager.

Le module de provisioning basé sur les rôles utilise JBoss et PostgreSQL comme serveur d'applications et base de données.

Reportez-vous au manuel [Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0](#) pour obtenir une liste de la configuration système requise pour l'application utilisateur.

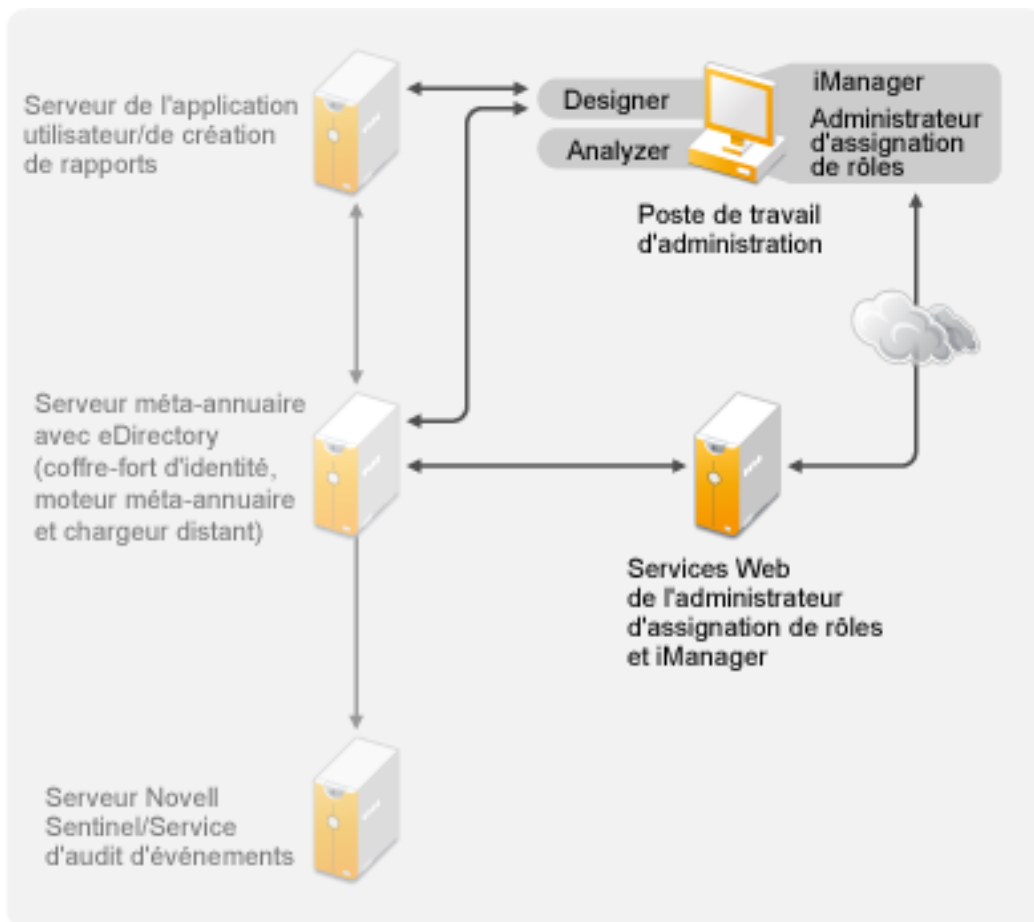
## 2.4 Administrateur d'assignation de rôles

L'administrateur d'assignation de rôles vous permet d'assigner des rôles système gérés, des rôles composites ainsi que des profils (appelés collectivement autorisations) à des rôles Identity Manager. Lorsqu'un utilisateur est assigné à un rôle via le module de provisioning basé sur les rôles Identity Manager, il reçoit toutes les autorisations assignées à ce rôle. Reportez-vous au manuel [Novell Identity Manager Role Mapping Administrator 2.0 User Guide](#) (Guide de l'utilisateur de l'administrateur d'assignation de rôles version 2.0 de Novell Identity Manager) pour plus d'informations.

## 2.5 iManager, Designer et Analyzer

Pour installer iManager, Designer, Analyzer et l'administrateur d'assignation de rôles, sélectionnez-les individuellement à l'aide des cases à cocher sur la page Sélectionner les composants de l'installation. La [Figure 2-3](#) illustre ces composants.

**Figure 2-3** Outils pour Identity Manager



## 2.6 Navigateurs Web

Les navigateurs Web pris en charge pour gérer Identity Manager sont les suivants :

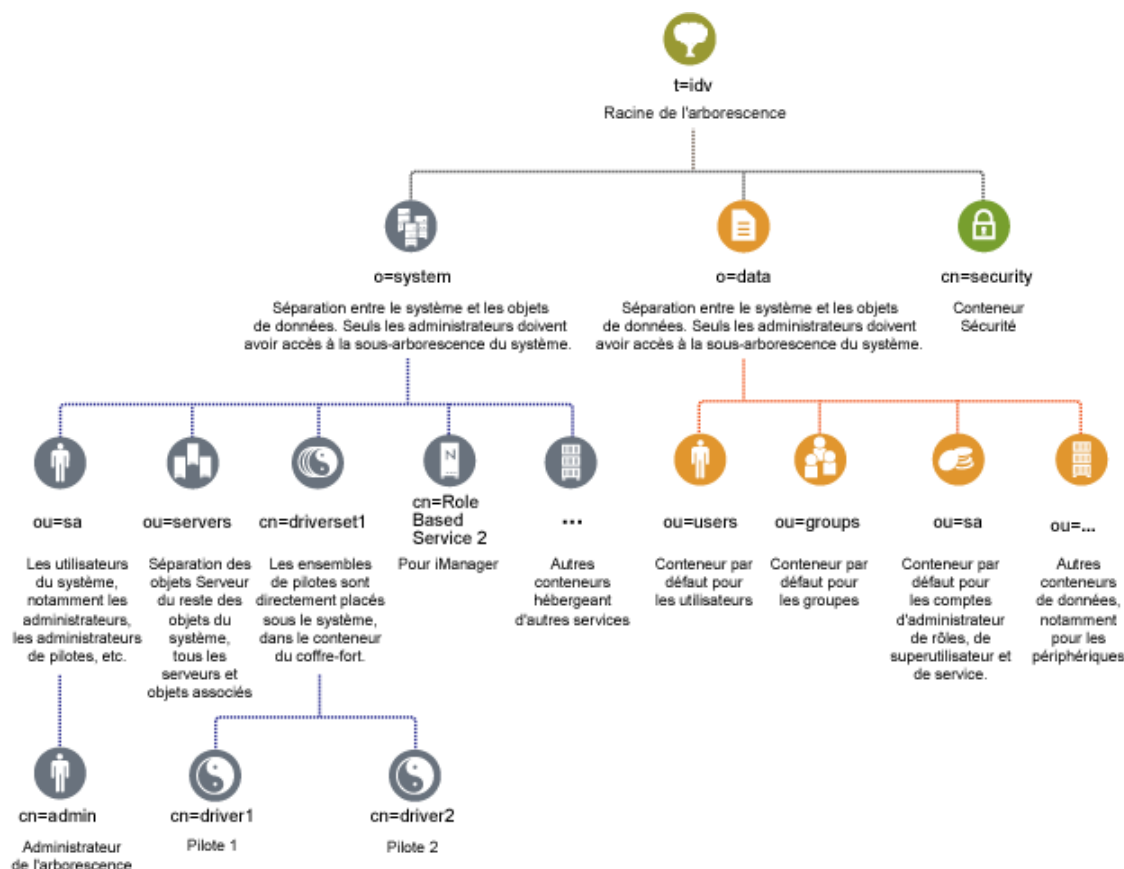
- ♦ Internet Explorer 6 SP2

- ♦ Internet Explorer 7 et 8
- ♦ Firefox 3, 3.5.x et 3.6.x

## 2.7 Structure du coffre-fort d'identité

La structure du coffre-fort d'identité est prédéfinie de manière à correspondre à la plupart de vos déploiements Identity Manager.

Figure 2-4 Structure du coffre-fort d'identité



La Figure 2-4 montre la structure du coffre-fort d'identité pour Identity Manager. Cette structure est surtout utile pour une installation dans un seul environnement. Il s'agit de la structure par défaut des 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. Le type de structure d'arborescence est créé lorsque vous créez une nouvelle arborescence via le programme d'installation intégré.

Identity Manager 4.0 utilise la plupart du temps des conteneurs Organisation, de sorte que les utilisateurs, les groupes et les administrateurs de services sont placés dans le même conteneur. Utilisez les organisations autant que possible et réservez les unités organisationnelles aux situations où elles sont vraiment pertinentes. La structure d'Identity Manager 4.0 est conçue pour garantir l'évolutivité grâce à trois composants principaux :

- ♦ [Section 2.7.1, « Sécurité », page 17](#)



- ♦ [Section 2.7.2, « Données », page 17](#)
- ♦ [Section 2.7.3, « Système », page 17](#)

## 2.7.1 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.

## 2.7.2 Données

Le conteneur de données contient les groupes, les utilisateurs, les administrateurs de rôles, les périphériques, etc. 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.

### **ou=sa**

Le conteneur d'administrateurs de services (`ou=sa`) contient tous les objets Administrateur de l'application utilisateur et les comptes d'administrateur de services.

## 2.7.3 Système

Le conteneur système est une organisation. 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 quatre sous-conteneurs principaux :

- ♦ `sa` ou administrateurs de services / superutilisateur / comptes de services ;
- ♦ serveurs ;
- ♦ ensembles de pilotes ;
- ♦ services.

### **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`.

### **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. Tous les objets associés au serveur (volumes, licences, certificats) sont en place et il est plus facile de retrouver ceux dont vous avez besoin.

Cette structure est conçue pour l'évolutivité. Ainsi, que vous ayez 10 ou 100 serveurs, vous pouvez facilement trouver les objets associés à un seul serveur.

### **Ensembles de pilotes**

Les ensembles de pilotes sont créés en tant que partition distincte au cours de la configuration du serveur méta-annuaire. Tous les objets Ensemble de pilotes sont stockés dans le conteneur système. Votre système Identity Manager 4.0 peut compter plusieurs ensembles de pilotes. 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.

# Configuration système requise

# 3

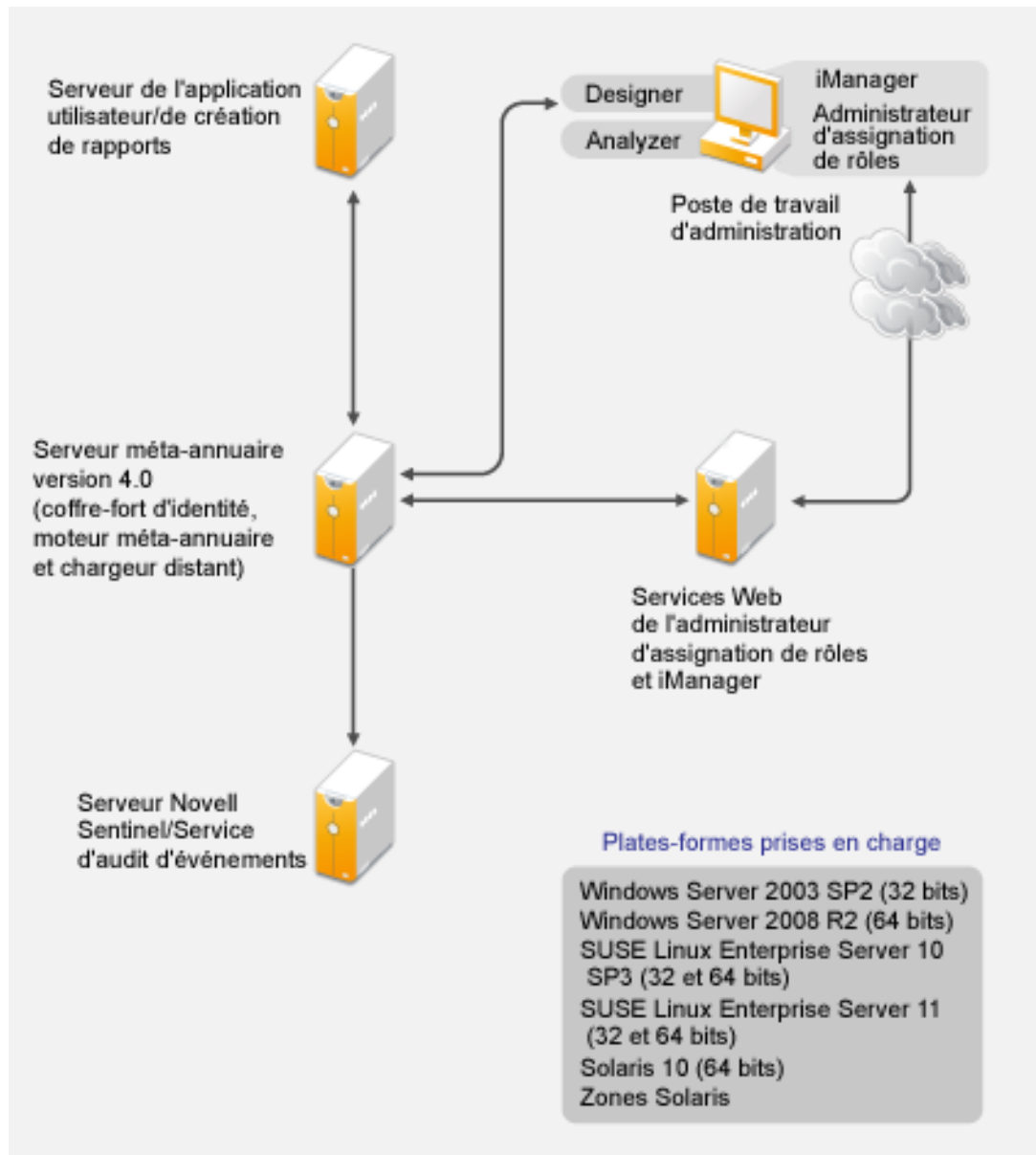
Les composants de Novell Identity Manager peuvent être installés sur plusieurs systèmes et plates-formes.

- ♦ [Section 3.1, « Plates-formes prises en charge », page 19](#)
- ♦ [Section 3.2, « Ressources requises », page 20](#)

## 3.1 Plates-formes prises en charge

La [Figure 3-1](#) montre les plates-formes prises en charge par le programme d'installation intégré de Novell Identity Manager 4.0.

**Figure 3-1** Configuration système requise pour le programme d'installation intégré d'Identity Manager



- ♦ Le programme d'installation intégré n'installe ni ne configure les composants Identity Manager sur les plates-formes Red Hat Linux. Pour l'installation des composants Identity Manager sur Red Hat Linux et d'autres plates-formes prises en charge, reportez-vous à la documentation spécifique au produit.
- ♦ Avec Identity Manager 4.0, le service d'audit d'événements n'est pris en charge que sur la plate-forme Linux.
- ♦ Avec Identity Manager 4.0, seul le serveur méta-annuaire est pris en charge sous Solaris.
- ♦ Avec le programme d'installation intégré, le module de provisioning basé sur les rôles et le module Identity Reporting ne peuvent être installés que sur une machine équipée du coffre-fort d'identité.
- ♦ Certaines options de composants individuels nécessitant une sélection de l'utilisateur sont différentes selon la plate-forme.

## 3.2 Ressources requises

Outre les exigences de plate-forme mentionnées ci-dessus, veillez à disposer des ressources suivantes pour installer et configurer tous les composants Identity Manager :

- ♦ 2048 Mo de RAM.
- ♦ 10 Go d'espace disque disponible pour installer tous les composants.
- ♦ Espace disque supplémentaire pour configurer et charger les données. Ce paramètre peut varier en fonction des systèmes connectés.
- ♦ Un serveur multiprocesseur avec processeur de 2 GHz est préférable.

---

**Remarque :** ces spécifications peuvent varier selon votre environnement de déploiement.

---

# Installation d'Identity Manager

# 4

Vous pouvez installer et configurer tous les composants simultanément ou en plusieurs fois à l'aide du programme d'installation intégré. Si vous souhaitez installer chaque composant séparément, utilisez le programme d'installation de la structure d'Identity Manager qui dispose de programmes d'installation différents pour chaque composant et installez les composants dans l'ordre stipulé à la section « [Installation d'Identity Manager](#) » du *Guide d'installation de la structure d'Identity Manager 4.0*. Pour obtenir une explication des différents composants, reportez-vous au guide *Présentation d'Identity Manager 4.0*.

Pour obtenir une liste des différents composants installés par le programme d'installation intégré d'Identity Manager, reportez-vous au [Chapitre 1, « Présentation du programme d'installation intégré », page 9](#). Pour des informations détaillées sur chaque composant, reportez-vous au guide *Présentation d'Identity Manager 4.0*.

Les sections suivantes ne fournissent pas d'instructions d'installation pas à pas, car l'interface d'installation est très explicite. En revanche, elles donnent des informations sur les étapes importantes du processus au cours desquelles vous pourriez avoir besoin d'aide.

- ♦ [Section 4.1, « Obtention du fichier ISO sur le site de téléchargement », page 21](#)
- ♦ [Section 4.2, « Nouvelle installation à partir d'un média physique ou d'un fichier ISO », page 22](#)
- ♦ [Section 4.3, « Installation et configuration en mode silencieux », page 31](#)

Pour plus d'informations sur la mise à niveau d'une installation existante d'Identity Manager, reportez-vous au [Chapitre 6, « Mise à niveau d'Identity Manager », page 37](#).

## 4.1 Obtention du fichier ISO sur le site de téléchargement

Vous pouvez télécharger une copie d'évaluation d'Identity Manager et l'utiliser gratuitement durant 90 jours. Les composants Identity Manager doivent être activés dans les 90 jours à compter de l'installation, faute de quoi ils ne fonctionneront plus. À tout moment, durant ces 90 jours ou ultérieurement, vous pouvez choisir d'acheter une licence de produit et d'activer Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 5, « Activation des produits Novell Identity Manager », page 33](#).

Pour télécharger Identity Manager et ses services :

- 1 Allez sur le [site Web de téléchargements Novell \(http://download.novell.com\)](http://download.novell.com).
- 2 Dans le menu *Produit (Product) ou Technologie (Technologie)*, sélectionnez *Novell Identity Manager*, puis cliquez sur *Search (Rechercher)*.
- 3 Sur la page des téléchargements Novell Identity Manager, cliquez sur le bouton *Télécharger* à côté du fichier souhaité. Le [Tableau 4-1](#) contient une description de chaque fichier.

Selon vos besoins, sélectionnez une image ISO appropriée. Chaque image ISO contient les versions 32 et 64 bits du produit.

- 4 Suivez les invites à l'écran pour télécharger le fichier vers un répertoire de votre ordinateur.

- 5 Recommencez à partir de l'[Étape 3](#) jusqu'à ce que vous ayez téléchargé tous les fichiers dont vous avez besoin.
- 6 Montez le fichier `.iso` téléchargé en tant que volume ou utilisez ce fichier `.iso` pour créer un DVD du logiciel. Si vous n'avez pas encore vérifié la validité du support que vous avez gravé, vous pouvez le faire à l'aide de l'option *Vérification du support*.

**Tableau 4-1** Images ISO d'Identity Manager

ISO	Plate-forme	Description
<code>windows_identity_manager_enterprise_4.0.iso</code>	Windows	Contient l'image DVD pour le serveur méta-annuaire, Designer, iManager, l'administrateur d'assignation de rôles, d'Analyzer, du module Novell Identity Reporting et du module de provisioning basé sur les rôles.
<code>linux_identity_manager_enterprise_4.0.iso</code>	Linux	Contient l'image DVD pour le serveur méta-annuaire, le service d'audit d'événements, Designer, iManager, l'administrateur d'assignation de rôles, Analyzer, le module Identity Reporting et le module de provisioning basé sur les rôles.
<code>solaris_identity_manager_enterprise_4.0.iso</code>	Solaris	Contient l'image DVD pour le serveur méta-annuaire. Les autres composants ne sont pas pris en charge sur la plate-forme Solaris.

## 4.2 Nouvelle installation à partir d'un média physique ou d'un fichier ISO

Le programme d'installation intégré vous aide à installer les fichiers binaires pour les composants Identity Manager et à configurer ces derniers.

- ♦ [Section 4.2.1, « Installation », page 22](#)
- ♦ [Section 4.2.2, « Configuration », page 24](#)

### 4.2.1 Installation

- 1 Accédez aux fichiers d'installation d'Identity Manager 4.0, soit en montant le fichier `.iso`, soit en utilisant le DVD que vous avez créé à partir de ce fichier `.iso`.

Pour plus d'informations, reportez-vous à la [Section 4.1, « Obtention du fichier ISO sur le site de téléchargement », page 21](#).

- 2 Accédez au répertoire de montage et démarrez l'installation à l'aide du programme approprié pour votre plate-forme.

**Linux :** `./install.bin`

**Solaris :** `./install.bin`

Pour exécuter le fichier binaire, saisissez `./install.bin`.

**Windows :** `install.exe`

- 3 Les informations suivantes permettent de terminer l'installation :

**Introduction :** sélectionnez la langue de votre installation, puis vérifiez quels composants vous pouvez installer.

**Accord de licence :** lisez, puis acceptez l'accord de licence.

**Sélectionner les composants :** sélectionnez les composants à installer. Les options sont les suivantes :

- ♦ Coffre-fort d'identité
- ♦ Module de provisioning basé sur les rôles
- ♦ Module Novell Identity Reporting
- ♦ Service d'audit d'événements
- ♦ Administrateur d'assignation de rôles
- ♦ iManager
- ♦ Designer
- ♦ Analyzer

---

**Remarque :** si vous sélectionnez le module de provisioning basé sur les rôles ou le module Identity Reporting pour installation, Designer est automatiquement sélectionné, car le programme d'installation utilise Designer en interne pour créer la configuration du pilote. Vous ne pouvez pas installer le module de provisioning basé sur les rôles et le module Identity Reporting sur un système différent dépourvu du coffre-fort d'identité. Vous devez toujours installer ces deux modules sur la même machine. JBoss et PostgreSQL sont utilisés comme serveur d'applications et base de données.

---

**Personnaliser les produits sélectionnés :** sélectionnez cette option si vous souhaitez installer le chargeur distant avec le serveur méta-annuaire.

**Choisir le dossier d'installation :** spécifiez le dossier de base dans lequel Identity Manager et ses composants sont installés. Cette option n'est applicable qu'à Windows.

Les installations Linux/UNIX ont un chemin d'installation prédéfini. Le programme d'installation intégré installe les composants dans les chemins d'installation prédéfinis suivants :

- ♦ eDirectory et Identity Manager : `/opt/novell/eDirectory`
- ♦ Module de provisioning basé sur les rôles, module de création de rapports, administrateur d'assignation de rôles, Designer et Analyzer : `/opt/novell/idm`
- ♦ Service d'audit d'événements : `/opt/novell/sentinel_eas`

**Résumé avant installation :** lisez la page de résumé avant installation, qui contient des informations sur les composants sélectionnés. Pour modifier ces paramètres, cliquez sur *Précédent*.

**Résumé de l'installation terminée :** lisez le résumé post-installation pour vérifier l'état d'installation des composants sélectionnés et l'emplacement du fichier journal pour chacun d'eux. Reportez-vous au [Tableau 4-2 page 31](#) pour plus d'informations sur l'emplacement des fichiers journaux.

**Poursuivre avec la configuration :** (facultatif) cette case à cocher n'est activée que lorsque les composants sélectionnés sont configurables. Si vous souhaitez poursuivre avec la configuration, passez à la [Section 4.2.2, « Configuration », page 24](#). Sinon, décochez cette case.

## 4.2.2 Configuration

Vous pouvez configurer les composants Identity Manager que vous avez déjà installés à l'aide du programme d'installation intégré. Vérifiez que vous avez terminé la [Section 4.2.1, « Installation », page 22](#) avant de poursuivre la configuration.

Pour configurer les composants Identity Manager :

- 1 Si vous continuez depuis l'[Étape 3 page 22](#) de la procédure d'installation, passez à l'[Étape 2](#). Si ce n'est pas le cas, démarrez la configuration avec le programme adapté à votre plate-forme :

**Linux :** `./configure.bin`

**Solaris :** `./configure.bin`

Pour exécuter le fichier binaire, saisissez `./configure.bin`.

**Windows :** `configure.exe`

- 2 Sélectionnez les composants que vous souhaitez configurer et cliquez sur *Suivant*.
- 3 Sélectionnez l'une des options suivantes pour effectuer la configuration des composants Identity Manager :
  - ♦ [« Création d'une nouvelle arborescence » page 24](#)
  - ♦ [« Ajout à une arborescence existante » page 28](#)

### Création d'une nouvelle arborescence

Les champs qui apparaissent dépendent des composants sélectionnés pour configuration à la page précédente.

- 1 Utilisez les informations suivantes pour configurer vos composants Identity Manager si vous avez choisi de créer une nouvelle arborescence.
  - ♦ [« Coffre-fort d'identité » page 24](#)
  - ♦ [« Coffre-fort d'identité > Avancé » page 25](#)
  - ♦ [« Module de provisioning basé sur les rôles \(RBPM\) » page 25](#)
  - ♦ [« Module de provisioning basé sur les rôles \(RBPM\) > Avancé » page 26](#)
  - ♦ [« Module Novell Identity Reporting » page 26](#)
  - ♦ [« Module Identity Reporting > Avancé » page 26](#)
  - ♦ [« Service d'audit d'événements » page 27](#)
  - ♦ [« Service d'audit d'événements > Avancé » page 28](#)
  - ♦ [« iManager > Avancé » page 28](#)
- 2 Examinez le résumé avant configuration, puis cliquez sur *Configurer*.
- 3 Examinez la page de résumé de configuration, puis cliquez sur *Terminé*.

Si des problèmes se sont produits lors de la configuration, parcourez les journaux de configuration. Pour plus d'informations, reportez-vous à la section [« Emplacement des fichiers journaux et de propriétés » page 31](#).

#### Coffre-fort d'identité

Remplissez les champs suivants pour créer une nouvelle arborescence :



**Nouveau nom d'arborescence** : spécifiez un nom pour la nouvelle arborescence.

**Mot de passe de l'administrateur** : spécifiez un mot de passe pour l'administrateur du coffre-fort d'identité.

**Confirmer le mot de passe de l'administrateur** : spécifiez à nouveau le mot de passe de l'administrateur du coffre-fort d'identité.

Coffre-fort d'identité > Avancé

Sélectionnez *Avancé* si vous souhaitez personnaliser l'arborescence créée. Renseignez les champs suivants pour personnaliser l'arborescence :

**Nom de l'administrateur** : spécifiez le nom de l'administrateur du coffre-fort d'identité.

**Port NCP** : laissez la valeur par défaut de 524 pour le port NCP ou modifiez-la. NCP est le principal protocole de communications eDirectory.

**Port LDAP** : laissez la valeur par défaut de 389 pour le port LDAP ou modifiez-la.

**Port sécurisé LDAP** : laissez la valeur par défaut de 636 pour le port sécurisé LDAP ou modifiez-la.

**Port HTTP** : laissez la valeur par défaut de 8028 pour le port HTTP ou modifiez-la.

**Port sécurisé HTTP** : laissez la valeur par défaut de 8030 pour le port sécurisé HTTP ou modifiez-la.

**Chemin de l'instance** : si votre serveur est de type Linux/UNIX, vous pouvez exécuter plusieurs instances d'eDirectory sur un seul serveur. Spécifiez le chemin de cette instance d'eDirectory sur ce serveur. Le chemin d'accès par défaut est `/var/opt/novell/eDirectory`.

**Chemin du répertoire DIB** : spécifiez le chemin de votre base de données eDirectory (DIB). L'emplacement par défaut de la DIB est :

- ♦ **Linux/UNIX** : `/var/opt/novell/eDirectory/data/dib`
- ♦ **Windows** : `c:\Novell\IdentityManager\NDS\DIBFiles\`

---

**Remarque** : les fichiers DIB doivent toujours résider dans le dossier `\NDS`. Si vous modifiez l'emplacement par défaut de la DIB sous Windows, par exemple `\NDS\DIBFiles\`, la configuration du serveur méta-annuaire échoue.

---

**Exiger TLS pour les liaisons simples avec un mot de passe** : sélectionnez cette option pour que toutes les connexions LDAP se fassent sur le port sécurisé (636 par défaut). Si vous désélectionnez cette option, les utilisateurs qui s'authentifient auprès du serveur LDAP sur le port en texte clair (389 par défaut) transmettent leur mot de passe en texte clair. Pour plus d'informations, reportez-vous à la section « [Communicating with eDirectory through LDAP](http://www.novell.com/documentation/edir88/edirin88/data/a7f08yl.html) » (<http://www.novell.com/documentation/edir88/edirin88/data/a7f08yl.html>) (Communication avec eDirectory via LDAP) du manuel *Novell eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html>) (Guide d'installation de Novell eDirectory 8.8).

Module de provisioning basé sur les rôles (RBPM)

Renseignez les champs suivants pour configurer le module RBPM ainsi que votre service d'audit d'événements (EAS), lequel fait partie du module Identity Reporting :

**Adresse du serveur EAS :** spécifiez le nom DNS ou l'adresse IP du serveur qui héberge le service EAS. Vous pouvez utiliser ce serveur ou en ajouter un autre.

**Mot de passe de l'utilisateur de la base de données idmadmin :** spécifiez le mot de passe de l'utilisateur de la base de données. Cette dernière stocke les informations destinées aux rapports.

**Confirmer le mot de passe de l'utilisateur de la base de données idmadmin :** spécifiez à nouveau le mot de passe de l'utilisateur de la base de données.

**Mot de passe de l'application utilisateur :** spécifiez le mot de passe de l'application utilisateur.

**Confirmer le mot de passe de l'application utilisateur :** spécifiez à nouveau le mot de passe de l'application utilisateur.

Module de provisioning basé sur les rôles (RBPM) > Avancé

Sélectionnez *Avancé* si vous souhaitez personnaliser la configuration du module RBPM.

**Adresse de l'application utilisateur :** spécifiez le nom DNS ou l'adresse IP du serveur qui héberge l'application utilisateur.

**Utilisateur de l'application utilisateur :** spécifiez un nom pour l'administrateur de l'application utilisateur.

Module Novell Identity Reporting

Renseignez les champs suivants pour configurer le module Identity Reporting :

**Mot de passe de l'utilisateur idmrptsrv :** spécifiez le mot de passe de l'utilisateur idmrptsrv. L'utilisateur idmrptsrv est le propriétaire des schémas et objets de la base de données destinés à la création de rapports.

**Mot de passe idmrptuser :** spécifiez le mot de passe de l'utilisateur idmrptuser. Il s'agit d'un utilisateur disposant d'un accès en lecture seule aux données de création de rapports.

**Mot de passe dbauser :** spécifiez le mot de passe de l'utilisateur dbauser (administrateur de la base de données).

**Port de passerelle système gérée :** spécifiez le port sur lequel le pilote de passerelle système gérée communique.

**Adresse du service de collecte de données :** indiquez l'adresse IP ou le nom DNS du serveur du service de collecte de données.

Module Identity Reporting > Avancé

Sélectionnez *Avancé* pour personnaliser la configuration du module Identity Reporting. Renseignez les champs suivants pour personnaliser le module Identity Reporting :

**Activer la recherche dans les sous-conteneurs :** sélectionnez cette option pour permettre au module Identity Reporting d'effectuer des recherches dans les sous-conteneurs afin de réunir des informations destinées à des rapports.

**Plate-forme du serveur d'applications :** spécifiez le type de serveur d'applications que vous utilisez avec le module de provisioning basé sur les rôles. Les plates-formes prises en charge sont JBoss, WebSphere et WebLogic.

**Adresse de l'hôte de la base de données :** spécifiez le nom DNS ou l'adresse IP du serveur qui exécute votre base de données.

**Nom du fichier du pilote JDBC PostgreSQL :** spécifiez `postgresql-8.4-701.jdbc4.jar` comme nom de fichier du pilote PostgreSQL JDBC.

**Emplacement du pilote JDBC PostgreSQL :** spécifiez l'emplacement du fichier `.jar` du pilote JDBC PostgreSQL. L'emplacement par défaut est le suivant :

- ♦ **Linux/UNIX :** `/opt/novell/sentinel_eas/lib/`
- ♦ **Windows :** `c:\Novell\idm\sentinel_eas\lib`

**Adresse du serveur LDAP :** indiquez l'adresse IP et le port du serveur LDAP.

**Port LDAP sécurisé :** indiquez si le serveur communique via une connexion LDAP sécurisée.

**Valeur d'expiration du jeton (en minutes) :** indiquez le nombre de minutes de conservation du jeton pour authentification.

**Unité de création de rapports :** sélectionnez *Jour*, *Semaine* ou *Mois*.

**Valeur de conservation du rapport :** indiquez la durée de conservation d'un rapport. Si l'unité de création de rapports est définie sur *Jour* et que la valeur de conservation du rapport est de 1, les rapports sont conservés 1 jour avant d'être supprimés.

**Attribut de login du sous-conteneur :** si vous activez les recherches de sous-conteneur, vous devez fournir l'attribut de login utilisé pour la recherche dans la sous-arborescence du conteneur des utilisateurs.

**Adresse du serveur SMTP :** spécifiez le nom DNS ou l'adresse IP du serveur SMTP pour configurer les messages électroniques en vue des notifications de rapports.

**Port du serveur SMTP :** laissez la valeur par défaut de 456 pour le port du serveur SMTP ou modifiez-la.

**Adresse électronique de l'utilisateur SMTP :** spécifiez l'adresse électronique à utiliser pour l'authentification, lorsque cette dernière est activée.

**Mot de passe de l'utilisateur SMTP :** indiquez le mot de passe de l'utilisateur SMTP.

**Confirmer le mot de passe de l'utilisateur SMTP :** indiquez à nouveau le mot de passe de l'utilisateur SMTP.

**Adresse électronique par défaut :** spécifiez une adresse électronique par défaut à utiliser, si la personne qui exécute le rapport ne dispose pas d'une adresse électronique spécifiée dans le coffre-fort d'identité.

**SMTP utilise SSL :** sélectionnez cette option si le serveur SMTP utilise une connexion SSL.

**Authentification du serveur requise :** sélectionnez cette option si l'authentification est requise pour le serveur SMTP.

Service d'audit d'événements

Remplissez les champs suivants pour configurer le service d'audit d'événements :

**Mot de passe de l'administrateur :** indiquez le mot de passe de l'administrateur.

**Confirmer le mot de passe de l'administrateur :** indiquez à nouveau le mot de passe de l'administrateur.

**Mot de passe de l'administrateur de la base de données :** indiquez le mot de passe de l'administrateur de la base de données.

**Confirmer le mot de passe de l'administrateur de la base de données :** indiquez à nouveau le mot de passe de l'administrateur de la base de données.

Service d'audit d'événements > Avancé

Sélectionnez *Avancé* pour personnaliser la configuration du service d'audit d'événements :

**Port PostgreSQL :** laissez la valeur par défaut de 15432 pour le port PostgreSQL ou modifiez-la.

**Activer le réacheminement des ports :** sélectionnez cette option pour activer le réacheminement des ports ou désélectionnez-la pour le désactiver.

iManager > Avancé

Il n'existe que des options de configuration avancées pour iManager. Sélectionnez *Avancé* pour afficher ces options :

**Port HTTP :** laissez la valeur par défaut de 8080 pour le port non sécurisé ou modifiez-la.

**Port sécurisé HTTP :** laissez la valeur par défaut de 8443 pour le port sécurisé ou modifiez-la.

### **Ajout à une arborescence existante**

Les champs qui apparaissent dépendent des composants que vous avez choisi de configurer à la page précédente.

**1** Utilisez les informations suivantes pour configurer les composants Identity Manager si vous avez choisi d'ajouter ce serveur à une arborescence existante.

- ♦ « Coffre-fort d'identité » page 28
- ♦ « Coffre-fort d'identité > Avancé » page 29
- ♦ « Serveur méta-annuaire » page 30
- ♦ « Module de provisioning basé sur les rôles (RBPM) » page 30
- ♦ « Module de provisioning basé sur les rôles (RBPM) > Avancé » page 30
- ♦ « Module Novell Identity Reporting » page 30
- ♦ « Service d'audit d'événements » page 30
- ♦ « iManager > Avancé » page 31

**2** Examinez la page de résumé de configuration, puis cliquez sur *Terminé*.

Si des problèmes se sont produits durant la configuration, parcourez les journaux de configuration. Pour plus d'informations, reportez-vous à la section « [Emplacement des fichiers journaux et de propriétés](#) » page 31.

### **Coffre-fort d'identité**

Renseignez les champs suivants pour permettre à votre serveur de contacter un coffre-fort d'identité existant :

**Adresse du serveur existant :** spécifiez l'adresse IP d'un serveur de votre arborescence existante.

**Numéro de port du serveur 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 du conteneur si vous souhaitez que ce serveur soit placé dans votre arborescence existante. Par exemple, ou=server,o=system.

**DN administrateur du serveur existant :** spécifiez le DN de l'utilisateur qui dispose de droits d'administrateur complets sur votre arborescence.

Sous Windows, le nom d'administrateur du serveur existant est le nom d'administrateur de l'arborescence existante et le DN de contexte d'administrateur du serveur existant est le DN du LDAP de contexte d'administrateur de l'arborescence existante.

**Mot de passe de l'administrateur du serveur existant :** indiquez le mot de passe de l'administrateur spécifié ci-dessus.

Coffre-fort d'identité > Avancé

Sélectionnez *Avancé* pour personnaliser ce coffre-fort d'identité. Renseignez les champs suivants pour personnaliser le coffre-fort d'identité :

**Port NCP :** laissez la valeur par défaut de 524 pour le port NCP ou modifiez-la. NCP est le principal protocole de communications eDirectory.

**Port LDAP :** laissez la valeur par défaut de 389 pour le port LDAP ou modifiez-la.

**Port sécurisé LDAP :** laissez la valeur par défaut de 636 pour le port sécurisé LDAP ou modifiez-la.

**Port HTTP :** laissez la valeur par défaut de 8028 pour le port HTTP ou modifiez-la.

**Port sécurisé HTTP :** laissez la valeur par défaut de 8030 pour le port sécurisé HTTP ou modifiez-la.

**Chemin de l'instance :** si votre serveur est de type Linux/UNIX, vous pouvez exécuter sur celui-ci plusieurs instances d'eDirectory. Spécifiez le chemin de cette instance d'eDirectory sur ce serveur. Le chemin d'accès par défaut est `/var/opt/novell/eDirectory/data`.

**Chemin du répertoire DIB :** spécifiez le chemin de votre base de données eDirectory (DIB). L'emplacement par défaut de la DIB est :

- ♦ **Linux/UNIX :** `/var/opt/novell/eDirectory/data/DIB`
- ♦ **Windows :** `c:\Novell\Identity Manager\NDS\DIBfiles\`

---

**Remarque :** les fichiers DIB doivent toujours résider dans le dossier `\NDS`. Si vous modifiez l'emplacement par défaut de la DIB sous Windows, par exemple `\NDS\DIBfiles\`, la configuration du serveur méta-annuaire échoue.

---

**Exiger TLS pour les liaisons simples avec un mot de passe :** sélectionnez cette option pour que toutes les connexions LDAP se fassent sur le port sécurisé (636 par défaut). Si vous désélectionnez cette option, les utilisateurs qui s'authentifient auprès du serveur LDAP sur le port en texte clair (389 par défaut) transmettent leur mot de passe en texte clair. Pour plus d'informations, reportez-vous à la section « [Communicating with eDirectory through LDAP](http://www.novell.com/documentation/) » (<http://www.novell.com/documentation/>)

[edir88/edirin88/data/a7f08yl.html](http://www.novell.com/documentation/edir88/edirin88/data/a7f08yl.html)) (Communication avec eDirectory via LDAP) du manuel *Novell eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html>) (Guide d'installation de Novell eDirectory 8.8).

**Activer la réplication codée :** sélectionnez cette option si vous souhaitez que la réplication de votre arborescence soit codée. Pour plus d'informations, reportez-vous à la section « [Réplication codée](http://www.novell.com/documentation/edir88/edir88/data/bs6rydy.html) » (<http://www.novell.com/documentation/edir88/edir88/data/bs6rydy.html>) dans le *Guide d'administration de Novell eDirectory 8.8* (<http://www.novell.com/documentation/edir88/edir88/data/a2iii88.html>).

### Serveur méta-annuaire

**Nom de l'ensemble de pilotes :** spécifiez le nom du nouvel ensemble de pilotes créé au cours de la configuration du serveur méta-annuaire. Assurez-vous de ne pas utiliser un ensemble de pilotes existant.

**DN du contexte de l'ensemble de pilotes :** spécifiez le contexte où le nouvel ensemble est créé dans votre arborescence.

### Module de provisioning basé sur les rôles (RBPM)

Renseignez les champs suivants pour configurer le module RBPM ainsi que votre service d'audit d'événements (EAS), lequel fait partie du module Identity Reporting :

**Adresse du serveur EAS :** spécifiez le nom DNS ou l'adresse IP du serveur qui héberge le service EAS. Vous pouvez utiliser ce serveur ou en ajouter un autre.

**Mot de passe de l'utilisateur de la base de données idmadmin :** spécifiez le mot de passe de l'utilisateur de la base de données. Cette dernière stocke les informations destinées aux rapports.

**DN de l'administrateur de l'application utilisateur :** spécifiez le DN pour l'administrateur de l'application utilisateur au format LDAP.

**Mot de passe de l'administrateur de l'application utilisateur :** spécifiez le mot de passe de l'application utilisateur.

### Module de provisioning basé sur les rôles (RBPM) > Avancé

Les options de configuration avancées du module RBPM sont identiques pour les configurations de nouvelle arborescence et d'arborescence existante. Reportez-vous à la section « [Module de provisioning basé sur les rôles \(RBPM\) > Avancé](#) » page 26.

### Module Novell Identity Reporting

Les options de configuration du module Identity Reporting sont identiques pour les configurations de nouvelle arborescence et d'arborescence existante. Reportez-vous aux sections « [Module Novell Identity Reporting](#) » page 26 et « [Module Identity Reporting > Avancé](#) » page 26.

### Service d'audit d'événements

Les options de configuration du service d'audit d'événements sont identiques pour les configurations de nouvelle arborescence et d'arborescence existante. Reportez-vous aux sections « [Service d'audit d'événements](#) » page 27 et « [Service d'audit d'événements > Avancé](#) » page 28.

## iManager > Avancé

Les options de configuration d'iManager sont identiques pour les configurations de nouvelle arborescence et d'arborescence existante. Reportez-vous à la section « [iManager > Avancé](#) » page 28.

### Emplacement des fichiers journaux et de propriétés

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

**Tableau 4-2** Emplacement des fichiers journaux et de propriétés après installation et configuration

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:\Novell\IdentityManager\install\ logs</code>	<code>&lt;emplacement_installation&gt;install\propfiles</code>  L'emplacement par défaut est <code>C:\Novell\IdentityManager\install \logs\propfiles\</code>
Linux/ Solaris	<code>/var/opt/novell/idm/install/logs</code>	<code>/var/opt/novell/idm/install/logs/ propfiles/</code>

## 4.3 Installation et configuration en mode silencieux

- ♦ [Section 4.3.1, « Installation en mode silencieux », page 31](#)
- ♦ [Section 4.3.2, « Configuration en mode silencieux », page 32](#)

### 4.3.1 Installation en mode silencieux

Afin d'exécuter une installation en mode silencieux des composants Identity Manager, vous devez créer un fichier de propriétés reprenant les paramètres nécessaires à l'exécution de l'installation. Un exemple de fichier est disponible sur le média Identity Manager :

- ♦ **Linux :** `./install/propfiles/install.properties`
- ♦ **Solaris :** `./install/propfiles/install.properties`
- ♦ **Windows :** `\install\propfiles\install.properties`

Lancez l'installation en mode silencieux à l'aide du programme convenant à votre plate-forme :

- ♦ **Linux :** `./install.bin -i silent -f <nom_fichier>.properties`
- ♦ **Solaris :** `./install.bin -i silent -f <nom_fichier>.properties`  
Pour exécuter le fichier binaire, saisissez `./install.bin -i silent -f  
<nom_fichier>.properties.`
- ♦ **Windows :** `\install.exe -i silent -f <nom_fichier>.properties`

L'installation en mode silencieux prend en charge les variables de mot de passe suivantes en tant que variables environnementales. Si les variables de mot de passe ne sont pas transmises via l'environnement, vous devez les ajouter au fichier `silent.properties`.

**Serveur méta-annuaire :** `IA_IDVAULT_ADMIN_PASSWORD`.

**Module de provisioning basé sur les rôles :** `IA_RBPM_POSTGRESQL_DB_PASSWORD` et `IA_RBPM_USERAPPADMIN_PASSWORD`.

**Module Novell Identity Reporting :** `IA_REPORTING_NOVL_DB_USER_PASSWORD`, `IA_REPORTING_IDM_USER_PASSWORD` et `IA_REPORTING_IDM_SERVER_PASSWORD`.

**Service d'audit d'événements :** `IA_EAS_ADMIN_PWD` et `IA_EAS_DBA_PWD`.

### 4.3.2 Configuration en mode silencieux

Vous pouvez également 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. Deux exemples de fichiers sont disponibles sur le média Identity Manager. L'un sert à créer une nouvelle arborescence, l'autre à ajouter ce serveur à une arborescence existante.

- ♦ **Linux :** reportez-vous à l'emplacement suivant.
  - ♦ `./install/propfiles/configure_new_tree.properties`
  - ♦ `./install/propfiles/configure_existing_tree.properties`
- ♦ **Solaris :** reportez-vous à l'emplacement suivant.
  - ♦ `./install/propfiles/configure_new_tree.properties`
  - ♦ `./install/propfiles/configure_existing_tree.properties`
- ♦ **Windows :** reportez-vous à l'emplacement suivant.
  - ♦ `\install\propfiles\configure_new_tree.properties`
  - ♦ `IDM4.0_Win:\install\propfiles\configure_existing_tree.properties`

Lancez la configuration en mode silencieux à l'aide du programme approprié pour votre plateforme :

- ♦ **Linux :** `./configure.bin -i silent -f <nom_fichier>.properties`
- ♦ **Solaris :** `./configure.bin -i silent -f <nom_fichier>.properties`  
Pour exécuter le fichier binaire, saisissez `./configure.bin -i silent -f <nom_fichier>.properties`.
- ♦ **Windows :** `\configure.exe -i silent -f <nom_fichier>.properties`



# Activation des produits Novell Identity Manager

# 5

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.

Vous pouvez activer les composants Identity Manager en effectuant les tâches suivantes :

- ♦ [Section 5.1, « Achat d'une licence de produit Identity Manager », page 33](#)
- ♦ [Section 5.2, « Installation d'une référence d'activation de produit », page 33](#)
- ♦ [Section 5.3, « Affichage des activations de produits pour Identity Manager et les pilotes », page 34](#)
- ♦ [Section 5.4, « Activation des pilotes Identity Manager », page 35](#)
- ♦ [Section 5.5, « Activation d'Analyzer », page 35](#)
- ♦ [Section 5.6, « Activation de Designer et de l'administrateur d'assignation de rôles », page 36](#)

## 5.1 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 Novell Identity Manager \(http://www.novell.com/products/identitymanager/howtobuy.html\)](http://www.novell.com/products/identitymanager/howtobuy.html).

Une fois la licence de produit achetée, Novell vous envoie votre ID client par message électronique. Ce dernier message contient également une URL vers le site Novell auprès duquel vous pouvez obtenir une référence d'activation de produit. Si vous ne vous en souvenez pas ou si vous ne recevez pas votre ID client, appelez le centre d'activation Novell au 1-800-418-8373 aux États-Unis. Dans les autres pays, appelez le 1-801-861-8373. (Les appels effectués avec l'indicatif 801 vous seront facturés.) Vous pouvez également [discuter en ligne avec nous \(http://support.novell.com/chat/activation\)](http://support.novell.com/chat/activation).


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

Installez la référence d'activation de produit via iManager.

- 1 Une fois la licence achetée, Novell vous envoie un message électronique avec votre ID client. Ce message contient également un lien sous la section Détail de la commande 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 Cliquez sur  pour naviguer jusqu'à un ensemble de pilotes dans l'arborescence et le sélectionner.
- 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.

---

## 5.3 Affichage des activations de produits pour Identity Manager et les pilotes

Pour chaque ensemble de pilotes, vous pouvez afficher les références d'activation du produit installé pour le moteur méta-annuaire et les pilotes Identity Manager :

- 1 Ouvrez iManager.
- 2 Cliquez sur *Identity Manager > Présentation d'Identity Manager*.
- 3 Cliquez sur  pour rechercher et sélectionner 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 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 nécessaire » apparaisse encore en regard du nom du pilote. Dans ce cas, redémarrez le pilote et le message devrait disparaître.

---

## 5.4 Activation des pilotes Identity Manager

Votre achat Identity Manager comprend des activations pour des pilotes de service et plusieurs pilotes courants.

- ♦ **Pilotes de service :** les pilotes de service suivants sont activés en même temps que le serveur méta-annuaire :
  - ♦ 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 courants suivants sont activés en même temps que le serveur méta-annuaire :
  - ♦ 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 5.2, « Installation d'une référence d'activation de produit »](#), page 33 pour chaque module afin d'activer les pilotes.

## 5.5 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. Pour plus d'informations, reportez-vous à la section « [Activating Analyzer](#) » (Activation d'Analyzer) dans le manuel *Analyzer 1.2 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 1.2 pour Identity Manager).

## **5.6 Activation de Designer et de l'administrateur d'assignation de rôles**

Designer et l'administrateur d'assignation de rôles ne requièrent pas d'activation en dehors de celle du serveur méta-annuaire ou des pilotes.

# Mise à niveau d'Identity Manager

# 6

Vous pouvez utiliser le programme d'installation intégré pour mettre à niveau le coffre-fort d'identité et le serveur méta-annuaire. Si le module de provisioning basé sur les rôles est installé ou si vous le migrez sur du nouveau matériel, reportez-vous à la section « [Mise à niveau ou migration](#) » du *Guide d'installation de la structure d'Identity Manager 4.0*.

- ♦ [Section 6.1, « Création d'une sauvegarde de la configuration actuelle », page 37](#)
- ♦ [Section 6.2, « Arrêt des pilotes », page 40](#)
- ♦ [Section 6.3, « Mise à niveau de Designer », page 41](#)
- ♦ [Section 6.4, « Mise à niveau du serveur méta-annuaire \(coffre-fort d'identité, moteur méta-annuaire et chargeur distant\) », page 41](#)
- ♦ [Section 6.5, « Mise à niveaux de pilotes vers des paquetages », page 43](#)
- ♦ [Section 6.6, « Restauration de stratégies et de règles personnalisées pour le pilote », page 45](#)
- ♦ [Section 6.7, « Déploiement du projet converti », page 47](#)
- ♦ [Section 6.8, « Lancement des pilotes », page 47](#)

## 6.1 Création d'une sauvegarde de la configuration actuelle

Avant de procéder à la mise à niveau, il est important de créer une sauvegarde de la configuration actuelle de votre système Identity Manager. Il existe deux façons de créer une sauvegarde :

- ♦ [Section 6.1.1, « Vérification de l'actualité de votre projet Designer », page 37](#)
- ♦ [Section 6.1.2, « Création d'une exportation des pilotes », page 39](#)

### 6.1.1 Vérification de l'actualité de votre projet Designer

Un projet Designer contient le schéma ainsi que toutes les informations de configuration de pilote. La création d'un projet contenant votre solution Identity Manager permet d'exporter tous les pilotes en une seule étape au lieu de créer un fichier d'exportation distinct pour chaque pilote.

- ♦ [« Exportation du projet actuel » page 37](#)
- ♦ [« Création d'un nouveau projet à partir du coffre-fort d'identité » page 38](#)

#### Exportation du projet actuel

Si vous avez déjà un projet Designer, vérifiez que les informations contenues dans ce projet sont synchronisées avec celles contenues dans le coffre-fort d'identité.

- 1 Dans Designer, ouvrez votre projet.
- 2 Dans Modeler, cliquez avec le bouton droit sur le coffre-fort d'identité, puis sélectionnez *Activité en direct > Comparer*.
- 3 Évaluez le projet et actualisez toutes les différences, puis cliquez sur *OK*.

Pour plus d'informations, reportez-vous à la section « [Using the Compare Feature When Deploying](#) » (Utilisation de la fonction de comparaison lors du déploiement) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

- 4 Dans la barre d'outils, sélectionnez *Projet > Exporter*.
- 5 Cliquez sur *Sélectionner tout* pour sélectionner toutes les ressources à exporter.
- 6 Sélectionnez l'emplacement où vous voulez sauvegarder le projet et son format, puis cliquez sur *Terminer*.

Enregistrez le projet à n'importe quel emplacement, excepté l'espace de travail actuel. Lorsque vous effectuez la mise à niveau vers Designer, vous devez créer un nouvel emplacement d'espace de travail. Pour plus d'informations, reportez-vous à la section « [Exporting a Project](#) » (Exportation d'un projet) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

### Création d'un nouveau projet à partir du coffre-fort d'identité

Si vous n'avez pas de projet Designer de votre solution Identity Manager actuelle, vous devez créer un projet en tant que sauvegarde de votre solution actuelle.

- 1 Installez Designer 4.0.  
Vous pouvez créer un projet Identity Manager 3.6x avec Designer 4.0. Pour plus d'informations, reportez-vous à la section « [Installation de Designer](#) » du *Guide d'installation de la structure d'Identity Manager 4.0*.
- 2 Lancez Designer, puis déterminez un emplacement pour votre espace de travail.
- 3 Sélectionnez s'il faut rechercher des mises à niveau en ligne, puis cliquez sur *OK*.
- 4 Sur la page de bienvenue, cliquez sur *Lancer Designer*.
- 5 Dans la barre d'outils, sélectionnez *Projet > Importer un projet > Coffre-fort d'identité*.
- 6 Indiquez un nom pour le projet, puis sélectionnez soit l'emplacement par défaut pour votre projet, soit un emplacement différent que vous définirez.
- 7 Cliquez sur *Suivant*.
- 8 Indiquez l'information de connexion au coffre-fort d'identité :  
**Nom d'hôte** : indiquez l'adresse IP ou le nom DNS du serveur de coffre-fort d'identité.  
**Nom d'utilisateur** : indiquez le DN de l'utilisateur pour l'authentification au coffre-fort d'identité.  
**Mot de passe** : indiquez le mot de passe de l'utilisateur d'authentification.
- 9 Cliquez sur *Suivant*.
- 10 Laissez le schéma de coffre-fort d'identité et la collection de notification par défaut cochés.
- 11 Développez la collection de notification par défaut et décochez les langues dont vous n'avez pas besoin.  
Les collections de notification par défaut sont traduites vers beaucoup de langues différentes. Vous pouvez importer toutes les langues ou sélectionner seulement celles que vous utilisez.
- 12 Cliquez sur *Parcourir*, puis naviguez jusqu'à un ensemble de pilotes à importer et sélectionnez-le.

- 13 Répétez l'[Étape 12](#) pour chaque ensemble de pilotes dans ce coffre-fort d'identité, puis cliquez sur *Terminer*.
- 14 Une fois l'importation du projet terminée, cliquez sur *OK*.
- 15 Si vous n'avez qu'un seul coffre-fort d'identité, vous avez terminé. Si vous avez plusieurs coffres-forts d'identité, continuez avec l'[Étape 16](#).
- 16 Dans la barre d'outils, cliquez sur *Activité en direct > Importer*.
- 17 Répétez la procédure de l'[Étape 8](#) à l'[Étape 14](#) pour chaque coffre-fort d'identité supplémentaire.

## 6.1.2 Création d'une exportation des pilotes


La création d'une exportation des pilotes réalise une sauvegarde de votre configuration actuelle. Toutefois, Designer ne crée actuellement pas de sauvegarde des pilotes de droits basés sur les rôles et les stratégies. Utilisez iManager pour vérifier l'exportation du pilote de droits basés sur les rôles.

- ♦ [« Utilisation de Designer pour créer une exportation du pilote » page 39](#)
- ♦ [« Utilisation d'iManager pour créer une exportation du pilote » page 39](#)

### Utilisation de Designer pour créer une exportation du pilote

- 1 Vérifiez que votre projet dans Designer dispose de la version la plus récente de votre pilote.  
Pour connaître les instructions, reportez-vous à la section [« Importing a Library, a Driver Set, or a Driver from the Identity Vault »](#) (Importation d'une bibliothèque, d'un pilote ou d'un ensemble de pilotes à partir du coffre-fort d'identité) du manuel [Designer 4.0 for Identity Manager 4.0 Administration Guide](#) (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).
- 2 Dans Modeler, cliquez avec le bouton droit de la souris sur la ligne du pilote que vous mettez à niveau.
- 3 Sélectionnez *Exporter dans un fichier de configuration*.
- 4 Naviguez jusqu'à l'emplacement dans lequel enregistrer le fichier de configuration, puis cliquez sur *Enregistrer*.
- 5 Cliquez sur *OK* sur la page des résultats.
- 6 Répétez la procédure de l'[Étape 1](#) à l'[Étape 5](#) pour chaque pilote.

### Utilisation d'iManager pour créer une exportation du pilote

- 1 Dans iManager, sélectionnez *Identity Manager > Présentation d'Identity Manager*.
- 2 Naviguez jusqu'à l'emplacement de l'arborescence dans lequel rechercher les objets Ensemble des pilotes et sélectionnez-le, puis cliquez sur l'icône de recherche .
- 3 Cliquez sur l'objet Ensemble des pilotes contenant le pilote à mettre à niveau.
- 4 Cliquez sur le pilote à mettre à niveau, puis cliquez sur *Exporter*.
- 5 Cliquez sur *Suivant*, puis choisissez *Exporter toutes les stratégies contenues, qu'elles soient liées ou non à la configuration*.
- 6 Cliquez sur *Suivant*, puis sur *Enregistrer sous*.
- 7 Sélectionnez *Enregistrer sur le disque*, puis cliquez sur *OK*.




- 8 Cliquez sur *Terminer*.
- 9 Répétez la procédure de l'Étape 1 à l'Étape 8 pour chaque pilote.

## 6.2 Arrêt des pilotes



Avant de mettre des fichiers à niveau, vous devez arrêter les pilotes.

- ♦ [Section 6.2.1, « Utilisation de Designer pour arrêter les pilotes », page 40](#)
- ♦ [Section 6.2.2, « Utilisation d'iManager pour arrêter les pilotes », page 40](#)

### 6.2.1 Utilisation de Designer pour arrêter les pilotes

- 1 Sélectionnez l'objet  Coffre-fort d'identité sous l'onglet *Aperçu*.
- 2 Dans la barre d'outils *Modeler*, cliquez sur l'icône *Arrêter tous les pilotes* .  
Ceci arrête tous les pilotes faisant partie du projet.
- 3 Configurez les pilotes en mode démarrage manuel pour qu'ils ne démarrent pas tant que la procédure de mise à niveau n'est pas terminée :
  - 3a Double-cliquez sur l'icône du pilote  dans l'onglet *Aperçu*.
  - 3b Sélectionnez *Configuration du pilote > Options de démarrage*.
  - 3c Sélectionnez *Manuel*, puis cliquez sur *OK*.
  - 3d Répétez la procédure de l'Étape 3a à l'Étape 3c pour chaque pilote.

### 6.2.2 Utilisation d'iManager pour arrêter les pilotes

- 1 Dans *iManager*, sélectionnez *Identity Manager > Présentation d'Identity Manager*.
- 2 Naviguez jusqu'à l'emplacement de l'arborescence dans lequel rechercher les objets Ensemble des pilotes et sélectionnez-le, puis cliquez sur l'icône de recherche .
- 3 Cliquez sur l'objet Ensemble des pilotes.
- 4 Cliquez sur *Pilotes > Arrêter tous les pilotes*.
- 5 Répétez la procédure de l'Étape 2 à l'Étape 4 pour chaque objet Ensemble des pilotes.
- 6 Configurez les pilotes en mode démarrage manuel pour qu'ils ne démarrent pas tant que la procédure de mise à niveau n'est pas terminée :
  - 6a Dans *iManager*, sélectionnez *Identity Manager > Présentation d'Identity Manager*.
  - 6b Naviguez jusqu'à l'emplacement de l'arborescence dans lequel rechercher les objets Ensemble des pilotes et sélectionnez-le, puis cliquez sur l'icône de recherche .
  - 6c Cliquez sur l'objet Ensemble des pilotes.
  - 6d Dans l'angle supérieur droit de l'icône du pilote, cliquez sur *Modifier les propriétés*.
  - 6e Sur la page Configuration du pilote, sous *Options de démarrage*, sélectionnez *Manuel*, puis cliquez sur *OK*.
  - 6f Répétez la procédure de l'Étape 6a à l'Étape 6e pour chaque pilote dans l'arborescence.



## 6.3 Mise à niveau de Designer

Avant de mettre Designer à niveau, vérifiez de bien exporter vos projets afin d'en générer une sauvegarde. Pour des instructions concernant la procédure d'exportation de votre projet, reportez-vous à la section « [Exporting a Project](#) » (Exportation d'un projet) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

Designer ne peut être installé que sous Windows ou Linux. Si votre moteur méta-annuaire est installé sous Solaris, Designer doit l'être sur un serveur distinct.

Pour mettre à niveau Designer :

- 1 Lancez le programme d'installation de Designer depuis le média Identity Manager :  
**Linux** : `./products/Designer/install`  
Pour exécuter le fichier binaire, saisissez `./install`.  
**Windows** : `\products\Designer\install.exe`
- 2 Sélectionnez la langue dans laquelle installer Designer, puis lisez et acceptez l'accord de licence.
- 3 Indiquez le répertoire où Designer est installé, puis cliquez sur *Oui* dans le message annonçant que Designer est déjà installé.
- 4 Indiquez si les raccourcis doivent être placés sur le bureau ou dans le menu du bureau.
- 5 Lisez le résumé puis cliquez sur *Installer*.
- 6 Lisez le fichier lisezmoi, puis cliquez sur *Suivant*.
- 7 Sélectionnez l'option de lancement de Designer, puis cliquez sur *Terminé*.
- 8 Spécifiez un emplacement pour votre espace de travail Designer, puis cliquez sur *OK*.
- 9 Cliquez sur *OK* dans le message avertissant que votre projet doit être fermé et converti.
- 10 Dans la vue du projet, développez le projet, puis double-cliquez sur *Le projet doit être converti*.
- 11 Examinez les étapes effectuées par l'assistant de conversion de projet, puis cliquez sur *Suivant*.
- 12 Spécifiez un nom pour la sauvegarde de votre projet, puis cliquez sur *Suivant*.
- 13 Lisez le résumé du déroulement de la conversion, puis cliquez sur *Convertir*.
- 14 Parcourez le résumé lorsque la conversion est terminée, puis cliquez sur *Ouvrir*.

Designer est mis à niveau et le projet est converti au format actuel.

## 6.4 Mise à niveau du serveur méta-annuaire (coffre-fort d'identité, moteur méta-annuaire et chargeur distant)

Une fois les composants de prise en charge mis à niveau, c'est le serveur méta-annuaire qui est mis à niveau. Au cours de ce processus, les fichiers du module d'interface pilote stockés dans le système de fichiers sont mis à jour.

- 1 Vérifiez que les pilotes sont bien arrêtés. Pour connaître les instructions, reportez-vous à la [Section 6.2, « Arrêt des pilotes », page 40](#).
- 2 Arrêtez manuellement le processus lcache.

- 3 Si vous effectuez une mise à niveau depuis Identity Manager 3.6 ou une version supérieure, exécutez l'utilitaire NrfCaseUpdate pour prendre en charge la recherche en casse mixte de rôles et de ressources.

Si vous n'exécutez pas l'utilitaire NrfCaseUpdate, la mise à niveau du serveur méta-annuaire échoue. Pour plus d'informations sur l'exécution de l'utilitaire NrfCaseUpdate, reportez-vous à la section « [Exécution de l'utilitaire NrfCaseUpdate](#) » du *Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0*.

---

**Remarque :** vous ne devez pas exécuter l'utilitaire NrfCaseUpdate si vous ne mettez à niveau que le chargeur distant.

---

- 4 Lancez le programme d'installation intégré depuis le média Identity Manager :

- ♦ **Linux :** ./install.bin

- ♦ **Solaris :** ./install.bin

Pour exécuter le fichier binaire, saisissez ./install.bin.

- ♦ **Windows :** install.exe

- 5 Sélectionnez la langue dans laquelle effectuer la mise à niveau, puis cliquez sur *OK*.
- 6 Lisez et acceptez l'accord de licence, puis cliquez sur *Suivant*.
- 7 Cliquez sur *Mettre à niveau* pour mettre à niveau le coffre-fort d'identité et le serveur méta-annuaire, puis cliquez sur *Suivant*.
- 8 Sélectionnez *Serveur méta-annuaire*, puis cliquez sur *Suivant*.  
Le coffre-fort d'identité est mis à jour automatiquement.
- 9 Spécifiez le nom d'un utilisateur disposant de droits d'administrateur complets sur le coffre-fort d'identité au format LDAP.
  - ♦ **Linux/UNIX :** spécifiez les paramètres *DN de l'administrateur* et *Mot de passe de l'administrateur*.
  - ♦ **Windows :** spécifiez les paramètres *DN de l'administrateur*, *Nom du conteneur* et *Mot de passe de l'administrateur*.
- 10 Indiquez le mot de passe de l'utilisateur disposant de droits d'administrateur sur le coffre-fort d'identité, puis cliquez sur *Suivant*.

---

**Remarque :** l'[Étape 9](#) et l'[Étape 10](#) ne sont pas applicables à la mise à niveau du chargeur distant.

---

- 11 Parcourez le résumé avant mise à niveau, puis cliquez sur *Installer*.

- 12 Lisez le résumé de mise à niveau, puis cliquez sur *Terminé*.

Vous pouvez consulter le fichier journal de mise à niveau (ii\_upgrade.log) à l'emplacement suivant :

- ♦ **Linux/UNIX :** /var/opt/novell/idm/install/logs

- ♦ **Windows :** C:\Novell\IdentityManager\install\logs

Les chemins repris sont les chemins d'installation par défaut.

## 6.5 Mise à niveaux de pilotes vers des paquetages

Les paquetages constituent la nouvelle fonction de gestion de contenu d'Identity Manager 4.0. Ils contiennent les bases des stratégies de création de pilotes. Tous les nouveaux éléments de contenu de pilote sont fournis via des paquetages au lieu de fichiers de configuration de pilote.

Les paquetages sont gérés, tenus à jour et créés par le biais de Designer. iManager prend en charge les paquetages, mais les changements apportés au contenu de pilote via iManager ne sont pas pris en compte dans Designer. Pour plus d'informations sur la gestion des paquetages, reportez-vous à la section « [Managing the Identity Manager Content](#) » (Gestion du contenu d'Identity Manager) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

Il existe trois manières différentes de mettre à niveau vos pilotes vers des paquetages :

- ♦ [Section 6.5.1, « Création d'un nouveau pilote », page 43](#)
- ♦ [Section 6.5.2, « Remplacement du contenu existant par du contenu issu de paquetages », page 43](#)
- ♦ [Section 6.5.3, « Conservation du contenu actuel et ajout de nouveau contenu avec des paquetages », page 44](#)

### 6.5.1 Création d'un nouveau pilote

La manière la plus simple de mettre à niveau les pilotes vers des paquetages est de supprimer votre pilote existant et d'en créer un nouveau avec des paquetages. Ajoutez toutes les fonctionnalités de pilote que vous souhaitez avec des paquetages. Reportez-vous au guide de chaque pilote pour les étapes de création d'un nouveau pilote avec des paquetages. La procédure est différente pour chaque pilote. Pour obtenir des instructions, reportez-vous au [site Web de documentation des pilotes Identity Manager](http://www.novell.com/documentation/idm40drivers/) (<http://www.novell.com/documentation/idm40drivers/>).

### 6.5.2 Remplacement du contenu existant par du contenu issu de paquetages

Si vous devez créer des associations créées par le pilote, vous ne devez pas supprimer et recréer le pilote. Vous pouvez remplacer le contenu de pilote existant par des paquetages.

- 1** Créez une sauvegarde du pilote et tout le contenu personnalisé dans le pilote.  
Pour obtenir des instructions, reportez-vous à la section [Section 6.1.2, « Création d'une exportation des pilotes », page 39](#).
- 2** Dans Designer, supprimez tous les objets stockés dans le pilote. Supprimez les stratégies, les filtres, les droits et tous les autres éléments stockés dans le pilote.
- 3** Importez les paquetages de pilotes dans le catalogue de paquetages.  
Pour obtenir des instructions, reportez-vous à la section « [Importing Packages into the Package Catalog](#) » (Importation de paquetages dans le catalogue de paquetages) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).
- 4** Installez les paquetages sur le pilote.

Pour obtenir des instructions, consultez le guide de chaque pilote sur le [site Web de documentation des pilotes Identity Manager](http://www.novell.com/documentation/idm40drivers/) (<http://www.novell.com/documentation/idm40drivers/>).

- 5 Ajoutez les paquetages de base, obligatoires et facultatifs au pilote pour obtenir la fonctionnalité souhaitée. Ces étapes sont spécifiques à chaque pilote.

Pour plus d'instructions, consultez le guide de chaque pilote sur le [site Web de documentation des pilotes Identity Manager](http://www.novell.com/documentation/idm40drivers/) (<http://www.novell.com/documentation/idm40drivers/>).

- 6 Restaurez les éventuelles stratégies et règles personnalisées sur le pilote.

Pour obtenir des instructions, reportez-vous à la [Section 6.6, « Restauration de stratégies et de règles personnalisées pour le pilote »](#), page 45.

Le pilote fonctionne à présent comme auparavant, mais son contenu est issu de paquetages et non plus d'un fichier de configuration.

### 6.5.3 Conservation du contenu actuel et ajout de nouveau contenu avec des paquetages

Vous pouvez garder le pilote tel qu'il est actuellement et lui ajouter de nouvelles fonctionnalités par le biais de paquetages, pour autant que celles-ci n'empiètent pas sur la fonction actuelle du pilote. Lorsque vous installez un paquetage, ce dernier peut écraser des stratégies existantes et ainsi empêcher le pilote de fonctionner.

Pour ajouter du contenu nouveau au pilote à l'aide de paquetages :

- 1 Créez une sauvegarde du pilote et de tout son contenu personnalisé.

Pour obtenir des instructions, reportez-vous à la [Section 6.1.2, « Création d'une exportation des pilotes »](#), page 39.

- 2 Importez les paquetages de pilotes dans le catalogue de paquetages.

Pour obtenir des instructions, reportez-vous à la section « [Importing Packages into the Package Catalog](#) » (Importation de paquetages dans le catalogue de paquetages) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

- 3 Installez les paquetages sur le pilote.

Pour obtenir des instructions, consultez le guide de chaque pilote sur le [site Web de documentation des pilotes Identity Manager](http://www.novell.com/documentation/idm40drivers/) (<http://www.novell.com/documentation/idm40drivers/>).

- 4 Ajoutez les paquetages souhaités au pilote. Ces étapes sont spécifiques à chaque pilote.

Pour obtenir des instructions, reportez-vous au [site Web de documentation des pilotes Identity Manager](http://www.novell.com/documentation/idm40drivers/) (<http://www.novell.com/documentation/idm40drivers/>).

Le pilote contient la nouvelle fonctionnalité ajoutée par les paquetages.

## 6.6 Restauration de stratégies et de règles personnalisées pour le pilote

Si vous disposez de stratégies ou de règles personnalisées, vous pouvez les restaurer sur le pilote une fois que vous avez déposé le nouveau fichier de configuration du pilote. Si ces stratégies ont des noms différents, elles restent stockées dans le pilote mais leurs liens sont cassés et doivent être rétablis.

- ♦ [Section 6.6.1, « Utilisation de Designer pour restaurer les stratégies et les règles personnalisées sur le pilote », page 45](#)
- ♦ [Section 6.6.2, « Utilisation d'iManager pour restaurer les stratégies et les règles personnalisées sur le pilote », page 46](#)


### 6.6.1 Utilisation de Designer pour restaurer les stratégies et les règles personnalisées sur le pilote

Vous pouvez ajouter les stratégies dans l'ensemble de stratégies de deux manières :

- ♦ [« Ajout d'une stratégie personnalisée via la vue Aperçu » page 45](#)
- ♦ [« Ajout d'une stratégie personnalisée via la vue Afficher le flux de stratégie » page 46](#)

Effectuez ces procédures dans un environnement de test avant de déplacer le pilote dans votre environnement de production.

#### Ajout d'une stratégie personnalisée via la vue Aperçu

- 1 Dans la vue *Aperçu*, choisissez le pilote mis à niveau pour afficher la vue *Ensemble de stratégies*.
- 2 Cliquez avec le bouton droit de la souris sur l'icône de l'ensemble de stratégie  là où vous devez restaurer la stratégie personnalisée sur le pilote, puis choisissez *Nouveau > À partir de la copie*.
- 3 Naviguez jusqu'à la stratégie personnalisée, puis sélectionnez-la et cliquez sur *OK*.
- 4 Indiquez le nom de la stratégie personnalisée, puis cliquez sur *OK*.
- 5 Cliquez sur *Oui* dans le message de conflit de fichier pour enregistrer votre projet.
- 6 Lorsque le Générateur de stratégies ouvre la stratégie, vérifiez que les informations sont correctes dans la stratégie copiée.
- 7 Répétez la procédure de l'[Étape 2](#) à l'[Étape 6](#) pour chaque stratégie personnalisée à restaurer pour le pilote.
- 8 Lancez le pilote et testez-le.

Pour plus d'informations sur le lancement du pilote, reportez-vous à la [Section 6.8, « Lancement des pilotes », page 47](#). Pour plus d'informations sur le test du pilote, reportez-vous à la section [« Testing Policies with Policy Simulator »](#) (Test des stratégies avec le simulateur de stratégies) dans *Policies in Designer 4.0* (Stratégies dans Designer 4.0).


- 9 Une fois que vous avez vérifié que les stratégies fonctionnent, déplacez le pilote vers l'environnement de production.

## Ajout d'une stratégie personnalisée via la vue Afficher le flux de stratégie

- 1 Dans la vue *Aperçu*, sélectionnez le pilote mis à niveau, puis cliquez sur l'icône *Afficher le flux de stratégie*.
- 2 Cliquez avec le bouton droit de la souris sur l'ensemble de stratégies dans lequel vous devez restaurer la stratégie personnalisée sur le pilote, puis choisissez *Ajouter une stratégie > Copier existant*.
- 3 Naviguez jusqu'à la stratégie personnalisée, puis sélectionnez-la et cliquez sur *OK*.
- 4 Indiquez le nom de la stratégie personnalisée, puis cliquez sur *OK*.
- 5 Cliquez sur *Oui* dans le message de conflit de fichier pour enregistrer votre projet.
- 6 Lorsque le Générateur de stratégies ouvre la stratégie, vérifiez que les informations sont correctes dans la stratégie copiée.
- 7 Répétez la procédure de l'[Étape 2](#) à l'[Étape 6](#) pour chaque stratégie personnalisée à restaurer pour le pilote.
- 8 Lancez le pilote et testez-le.  
  
Pour plus d'informations sur le lancement du pilote, reportez-vous à la [Section 6.8, « Lancement des pilotes », page 47](#). Pour plus d'informations sur le test du pilote, reportez-vous à la section « [Testing Policies with Policy Simulator](#) » (Test des stratégies avec le simulateur de stratégies) dans *Policies in Designer 4.0* (Stratégies dans Designer 4.0).
- 9 Une fois que vous avez vérifié que les stratégies fonctionnent, déplacez le pilote vers l'environnement de production.

## 6.6.2 Utilisation d'iManager pour restaurer les stratégies et les règles personnalisées sur le pilote

Effectuez cette procédure dans un environnement de test avant de déplacer le pilote dans votre environnement de production.

- 1 Dans iManager, sélectionnez *Identity Manager > Présentation d'Identity Manager*.
- 2 Naviguez jusqu'à l'emplacement de l'arborescence dans lequel rechercher les objets Ensemble des pilotes et sélectionnez-le, puis cliquez sur l'icône de recherche .
- 3 Cliquez sur l'objet Ensemble des pilotes contenant le pilote mis à niveau.
- 4 Cliquez sur l'icône du pilote, puis choisissez l'ensemble de stratégies dans lequel restaurer la stratégie personnalisée.
- 5 Cliquez sur *Insérer*.
- 6 Sélectionnez *Utiliser une stratégie existante*, puis naviguez jusqu'à la stratégie personnalisée et sélectionnez-la.
- 7 Cliquez sur *OK*, puis sur *Fermer*.
- 8 Répétez la procédure de l'[Étape 3](#) à l'[Étape 7](#) pour chaque stratégie personnalisée à restaurer pour le pilote.
- 9 Lancez le pilote et testez-le.

Pour plus d'informations sur le lancement du pilote, reportez-vous à la [Section 6.8, « Lancement des pilotes », page 47](#). Il n'existe pas de simulateur de stratégie dans iManager. Pour tester les stratégies, faites intervenir des événements qui les exécutent. Vous pouvez, par exemple, créer un utilisateur, le modifier ou le supprimer.

- 10 Une fois que vous avez vérifié que les stratégies fonctionnent, déplacez le pilote vers l'environnement de production.

## 6.7 Déploiement du projet converti




Déployez le projet Designer converti dans le coffre-fort d'identité. Pour plus d'informations, reportez-vous à la section « [Deploying and Exporting](#) » (Déploiement et exportation) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

## 6.8 Lancement des pilotes

Une fois tous les composants Identity Manager mis à niveau, vous devez redémarrer les pilotes. Il est également important de tester les pilotes après leur exécution pour vérifier que toutes les stratégies continuent à fonctionner.


- ♦ [Section 6.8.1, « Utilisation de Designer pour lancer les pilotes », page 47](#)
- ♦ [Section 6.8.2, « Utilisation d'iManager pour démarrer les pilotes », page 47](#)

### 6.8.1 Utilisation de Designer pour lancer les pilotes

- 1 Sélectionnez l'objet Coffre-fort d'identité  dans l'onglet *Aperçu*.
- 2 Cliquez sur l'icône *Démarrer tous les pilotes*  dans la barre d'outils Modeler. Ceci lance tous les pilotes du projet.
- 3 Définissez les options de démarrage des pilotes :
  - 3a Double-cliquez sur l'icône du pilote  dans l'onglet *Aperçu*.
  - 3b Sélectionnez *Configuration du pilote > Option de démarrage*.
  - 3c Sélectionnez *Démarrage auto* ou choisissez votre méthode préférée pour lancer le pilote, puis cliquez sur *OK*.
  - 3d Répétez la procédure de l'[Étape 3a](#) à l'[Étape 3c](#) pour chaque pilote.
- 4 Testez les pilotes pour vérifier que les stratégies fonctionnent comme prévu.


Pour plus d'informations sur la manière de tester vos stratégies, reportez-vous à la section « [Testing Policies with Policy Simulator](#) » (Test des stratégies avec le simulateur de stratégies) dans *Policies in Designer 4.0* (Stratégies dans Designer 4.0).

### 6.8.2 Utilisation d'iManager pour démarrer les pilotes

- 1 Dans iManager, sélectionnez *Identity Manager > Présentation d'Identity Manager*.
- 2 Naviguez jusqu'à l'emplacement de l'arborescence dans lequel rechercher les objets Ensemble des pilotes et sélectionnez-le, puis cliquez sur l'icône de recherche .
- 3 Cliquez sur l'objet Ensemble des pilotes.
- 4 Cliquez sur *Pilotes > Démarrer tous les pilotes* pour lancer tous les pilotes simultanément.

ou

Dans la partie supérieure droite de l'icône du pilote, cliquez sur *Lancer le pilote* pour lancer chaque pilote individuellement.

- 5** Si vous disposez de plusieurs pilotes, répétez la procédure de l'[Étape 2](#) à l'[Étape 4](#).
- 6** Définissez les options de démarrage des pilotes :
  - 6a** Dans iManager, sélectionnez *Identity Manager > Présentation d'Identity Manager*.
  - 6b** Naviguez jusqu'à l'emplacement de l'arborescence dans lequel rechercher les objets Ensemble des pilotes et sélectionnez-le, puis cliquez sur l'icône de recherche .
  - 6c** Cliquez sur l'objet Ensemble des pilotes.
  - 6d** Dans l'angle supérieur droit de l'icône du pilote, cliquez sur *Modifier les propriétés*.
  - 6e** Dans la page Configuration du pilote, sous *Options de démarrage*, sélectionnez *Démarrage auto* ou choisissez votre méthode préférée de lancement du pilote, puis cliquez sur *OK*.
  - 6f** Répétez la procédure de l'[Étape 6b](#) à l'[Étape 6e](#) pour chaque pilote.
- 7** Testez les pilotes pour vérifier que les stratégies fonctionnent comme prévu.

Il n'existe pas de simulateur de stratégie dans iManager. Pour tester les stratégies, faites intervenir des événements qui les exécutent. Vous pouvez, par exemple, créer un utilisateur, le modifier ou le supprimer.



# Dépannage d'Identity Manager

# 7

Gardez à l'esprit les informations suivantes lorsque vous installez Identity Manager à l'aide du programme d'installation intégré :

- ♦ « Problèmes d'installation » page 49
- ♦ « Transmission de paramètres obligatoires lors de la configuration » page 50
- ♦ « La configuration échoue si le fichier hôte contient l'entrée 127.0.0.2 » page 50
- ♦ « Le programme d'installation génère l'exception java.io.FileNotFoundException » page 50
- ♦ « Le nom de l'arborescence est généré automatiquement lorsqu'il existe déjà » page 51
- ♦ « Installation du serveur secondaire » page 51
- ♦ « Les services ne fonctionnent pas » page 51
- ♦ « Détection de l'état actuel du système » page 51
- ♦ « Le programme d'installation intégré peut se bloquer lors de la mise à niveau d'Identity Manager » page 51
- ♦ « L'installation de distribution d'exécution Windows peut forcer un redémarrage en cas d'échec d'installation » page 52
- ♦ « Problème de processus lcache lors de la mise à niveau d'Identity Manager » page 52
- ♦ « La mise à niveau échoue sous Windows Server 2003 » page 52
- ♦ « Configuration du fichier ISO extrait via des outils d'extraction ISO tiers sous UNIX » page 52
- ♦ « L'activation de XDAS diminue les performances » page 52
- ♦ « Problèmes de désinstallation de composant Identity Manager » page 53

## Problèmes d'installation

Action : Si des erreurs se produisent durant l'installation d'Identity Manager, veuillez à vous reporter aux fichiers journaux en fonction de votre plate-forme :

- ♦ **Linux/Solaris** : /var/opt/novell/idm/install/logs/
- ♦ **Windows** : L'emplacement par défaut est C:\novell\IdentityManager\install\logs\. Vous pouvez modifier l'emplacement des fichiers journaux en vous basant sur l'emplacement d'installation que vous spécifiez.

Action : Afin de détecter les échecs courants, reportez-vous au fichier `ii_install.log` pour les problèmes d'installation, `ii_configure.log` pour les problèmes de configuration et `ii_uninstall.log` pour les problèmes de désinstallation. Dans les fichiers journaux, recherchez le texte `exitValue = xxx`. Si la valeur n'est pas 0, une exécution de commande particulière a échoué, ce qui à son tour génère un fichier journal. Reportez-vous à ce fichier journal pour plus de détails sur l'échec.

Par exemple,

```

"/home/siva/build/products/Reporting/IDMReport.bin" -
DIA_USER_JRE_HOME="/opt/nov
ell/idm/jre" -i silent -f "/tmp/
idmreporting_configure.properties"
execute command
    exitValue = 1
log file location    :/tmp/idmreporting_configure.properties
log file location    :/opt/novell/idm/rbpm/IDMReporting//
RPT_Install.log

```

L'extrait ci-dessus du fichier `ii_install.log` indique que la commande a échoué, car `exitValue` est égal à 1 (différent de zéro). Pour une analyse plus détaillée, reportez-vous au fichier `/opt/novell/idm/rbpm/IDMReporting/RPT_Install.log` tel qu'affiché dans la commande.

### Transmission de paramètres obligatoires lors de la configuration

Source : Lors de la configuration, le programme d'installation peut afficher le message d'erreur suivant après spécification des paramètres de configuration :

```

Some of the inputs are not proper. They are highlighted in
Red.

```

Cause possible : Selon le paramètre mis en évidence, la cause du message d'erreur peut être l'une des suivantes :

- ◆ Le numéro de port est déjà en cours d'utilisation.
- ◆ Le nom d'hôte DNS transmis n'est pas valide.
- ◆ Le format du DN est incorrect.

Action : Procédez comme suit :

- ◆ Utilisez un numéro de port différent si le port est déjà en cours d'utilisation.
- ◆ Indiquez un nom DNS ou une adresse IP valide si vous ne souhaitez pas spécifier de nom DNS.
- ◆ Vérifiez qu'un DN valide est spécifié au format LDAP.

### La configuration échoue si le fichier hôte contient l'entrée 127.0.0.2

Cause possible : Si le fichier `/etc/hosts` compte une entrée comprenant l'adresse de boucle 127.0.0.2, le certificat IP par défaut est créé pour cette adresse.

Action : Deux solutions sont possibles :

- ◆ Modifiez le fichier `/etc/hosts` si le fichier hôte compte une entrée comprenant l'adresse de boucle 127.0.0.2.

Par exemple, le nom d'hôte 127.0.0.2. Commentez-le et veillez à ce que l'entrée de l'adresse IP réelle soit dans le fichier.

### Le programme d'installation génère l'exception `java.io.FileNotFoundException`

Cause possible : Si le répertoire `tmp` du système n'est pas présent, le programme d'installation génère cette exception peu après avoir appelé le programme d'installation.

Action : Créez le répertoire `tmp` du système.

### Le nom de l'arborescence est généré automatiquement lorsqu'il existe déjà

Source : Le programme d'installation intégré tente de générer automatiquement le nom de l'arborescence si ce nom existe déjà.

### Installation du serveur secondaire

Explication : Le programme d'installation intégré ajoute la réplique qui héberge l'objet Serveur sur toutes les installations de serveur secondaire. Il attend l'activation de la réplique.

### Les services ne fonctionnent pas

Explication : Certains services peuvent ne pas fonctionner parce que les ports dont ils ont besoin sont occupés.

Action : Veillez à ce que les ports suivants soient libres avant de démarrer l'installation. Exécutez la commande `netstat -anp | egrep` pour vérifier si ces ports sont libres.

```
netstat -anp | egrep
': (524|389|636|8028|8030|8090|8000|7707|8006
|8009|8081|8443|8009|8080|8443|1199|1198|119
0|3973|4544|4545|4546|4557|4812|4813|8109|81
83|8180|8543|29007|37022|8180|10013|10014|61
616|61617|1514|15432|5556|1289|1443|1468) '
```

### Détection de l'état actuel du système

Explication : Assurez-vous de sauvegarder le fichier d'état du programme d'installation. Le fichier d'état intégré est un fichier de configuration important utilisé par le programme d'installation pour diverses informations, telles que l'état actuel du système, ainsi que les composants installés, configurés ou désinstallés.

Action : Sauvegardez le fichier d'état en procédant comme suit :

- ♦ **Linux/Solaris** : Exécutez `/etc/opt/novell/idm/install/conf/install_state.conf`.
- ♦ **Windows** : Exécutez `C:\Novell\conf\install_state.conf`.

### Le programme d'installation intégré peut se bloquer lors de la mise à niveau d'Identity Manager

Cause possible : Avant de mettre à niveau Identity Manager sous Windows, le programme d'installation intégré essaie d'arrêter tous les services dépendants. Parfois, le programme d'installation se bloque lorsqu'il arrête le service DHost.

Action : Pour poursuivre la mise à niveau, arrêtez manuellement le service DHost à partir du Gestionnaire des tâches.

## L'installation de distribution d'exécution Windows peut forcer un redémarrage en cas d'échec d'installation

Explication : L'installation du méta-annuaire échoue et émet le message suivant dans le fichier *<Emplacement installation>\ii\_install.log* :

```
: \Users\Administrator\IDM4\products\Directory\x64\windows\x64\redist_pkg\vcredist_x86.exe" /q:a /c:"msiexec /i vcredist.msi /qn /l C:\Users\ADMINI~1\AppData\Local\Temp\vcredist32_Windows_x64_Install.log"
execute command exitValue = 3010
```

Action : Le code d'erreur 3010 renvoyé par l'exécutable vcledist correspond à une réussite, vous devez donc redémarrer la machine Windows. Après le processus de redémarrage, relancez le programme d'installation et celle-ci se poursuit normalement. Le redémarrage de la machine n'affecte pas les installations réussies précédentes.

## Problème de processus lcache lors de la mise à niveau d'Identity Manager

Source : Après la mise à niveau d'Identity Manager, l'agent de la plate-forme peut ne pas consigner les événements comme souhaité. Ce problème est dû au fait que l'agent de la plate-forme n'est pas mis à niveau au cours de la mise à niveau sous Linux. Sous Windows et Solaris, l'agents de la plate-forme est mis à niveau vers la dernière version, mais le nouvel agent de plate-forme a différents ports par défaut, ce qui nécessite un redémarrage du processus lcache.

Action : Arrêtez manuellement lcache avant de lancer la mise à niveau.

## La mise à niveau échoue sous Windows Server 2003

Explication : La mise à niveau d'Identity Manager 3.6.1 sur eDirectory 8.8 SP5 échoue sur une machine Windows 2k3 32 bits si :

- ♦ un antivirus Symantec est installé et activé ;
- ♦ la configuration est sur un pilote assigné.

Action : Copiez les fichiers installables sur une machine locale et effectuez l'installation.

## Configuration du fichier ISO extrait via des outils d'extraction ISO tiers sous UNIX

Explication : La configuration du programme d'installation intégré d'Identity Manager 4.0 échoue si le fichier ISO est extrait par des outils d'extraction ISO tiers sur UNIX.

Action : Pour une configuration réussie, utilisez la commande `mount -o loop`.

## L'activation de XDAS diminue les performances

Cause possible : Si la consigne d'événements XDAS est activée, les performances du moteur Identity Manager sont diminuées sans configuration SLP.

Action : SLP doit être correctement configuré et en état de fonctionnement pour éviter d'affecter les performances.

## Problèmes de désinstallation de composant Identity Manager

Source : L'option de désinstallation est désactivée lorsque vous retentez la désinstallation avec le fichier `uninstall.bin`.

Action : Exécutez les programmes de désinstallation de composant individuel comme suit :

- ♦ **Linux/Solaris** : exécutez la commande suivante pour désinstaller les composants individuels :
  - ♦ **Méta-annuaire** : désinstallez la structure d'Identity Manager :

```
/root/idm/Uninstall_Identity_Manager/  
Uninstall_Identity_Manager
```

désinstallez le coffre-fort d'identité :

```
/opt/novell/eDirectory/sbin/nds-uninstall
```
  - ♦ **JBoss** : exécutez la commande suivante :

```
$IA_RBPM_POSTGRESQL_INSTALL_PATH$/  
JBossPostgreSQL_Uninstaller/Uninstall_JBossPostgreSQL
```
  - ♦ **Module de provisioning basé sur les rôles** : exécutez la commande suivante :

```
java -jar /opt/novell/idm/rbpm/RemoveUserApp/  
uninstaller.jar
```
  - ♦ **Module Novell Identity Reporting** : exécutez la commande suivante :

```
/opt/novell/idm/rbpm/Uninstall_Identity_Reporting/  
Uninstall_Identity_Reporting
```
  - ♦ **Service d'audit d'événements** : exécutez la commande suivante :

```
/opt/novell/sentinel_eas/Uninstall_Event_Auditing  
Service/Uninstall_Event_Auditing_Service
```
  - ♦ **Administrateur d'assignation de rôles** : exécutez la commande suivante :

```
/opt/novell/idm/rma/rma-uninstall.sh -s
```
  - ♦ **Designer** : exécutez la commande suivante :

```
/opt/novell/idm/Designer/UninstallDesigner/Uninstall  
Designer_for_Identity_Manager
```
  - ♦ **Analyzer** : exécutez la commande suivante :

```
/opt/novell/idm/Analyzer/UninstallAnalyzer/Uninstall  
Analyzer_for_Identity_Manager
```
  - ♦ **iManager** : exécutez la commande suivante :

```
/var/opt/novell/tomcat5/webapps/nps/UninstallerData/  
UninstalliManager
```
- ♦ **Windows** : hormis pour l'administrateur d'assignation de rôles, désinstallez tous les composants à partir de *Windows* > *Ajout/Suppression de programmes*. Pour désinstaller l'administrateur d'assignation de rôles, exécutez le fichier `C:\novell\IdentityManager\RMA\rma-uninstall.bat` depuis l'invite de commande.



# Désinstallation d'Identity Manager

# 8

Le script de désinstallation désinstalle tous les composants Identity Manager installés à l'aide du programme d'installation intégré. Si vous souhaitez désinstaller un seul composant, reportez-vous à la section « [Désinstallation d'Identity Manager](#) » du *Guide d'installation de la structure d'Identity Manager 4.0*.

Veillez à ce que les variables d'environnement JAVA\_HOME et PATH pointent vers Java avant que le programme d'installation intégré soit appelé.

Pour désinstaller les composants Identity Manager :

- 1 Exécutez la désinstallation à l'aide du programme adéquat pour votre plate-forme :

- ♦ **Linux** : `./Uninstall_Identity Manager Components.bin`

Le fichier binaire se situe à l'emplacement `/opt/novell/idm/Uninstall_Identity Manager Components.bin`.

- ♦ **Solaris** : `./Uninstall_Identity Manager Components.bin`

Le fichier binaire se situe à l'emplacement `/opt/novell/idm/Uninstall_Identity Manager Components.bin`.

- ♦ **Windows** : `Uninstall_Identity Manager Components.exe`

Le programme de désinstallation est situé à l'emplacement `<emplacement installation>\Uninstall_Identity Manager Components.exe`. Cliquez sur *Ajout/Suppression* de programmes et désinstallez les composants Identity Manager.

---

**Remarque** : la désinstallation du coffre-fort d'identité ne supprime pas tous les fichiers après désinstallation. Reportez-vous à la [documentation de désinstallation d'eDirectory](http://www.novell.com/documentation/edir88/edirin88/data/bnn8twh.html) (<http://www.novell.com/documentation/edir88/edirin88/data/bnn8twh.html>) pour plus d'informations.

---

- 2 Cochez la case pour chaque composant à désinstaller, puis cliquez sur *Suivant*.

- 3 Spécifiez les références pour chacun de ces composants au format LDAP, puis cliquez sur *Suivant*.

Le programme de désinstallation a besoin des références pour déconfigurer les composants avant désinstallation.

- 4 Lisez le résumé concernant la désinstallation des composants, puis cliquez sur *Désinstaller*.

Si vous devez modifier la liste des composants sélectionnés, cliquez sur *Précédent* et apportez vos modifications.

- 5 Parcourez la page Résumé de désinstallation terminée qui affiche la liste des composants qui ont été désinstallés, puis cliquez sur *Terminé* pour terminer le processus de désinstallation.

