

Guide d'installation

Novell® Identity Manager

4.0

15 octobre 2010

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 © 2007-2010 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

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

À propos de ce guide	9
Partie I Planification	11
1 Mise en place d'un environnement de développement	13
2 Création d'un plan de projet	15
2.1 Phase de découverte	15
2.1.1 Définition des processus d'entreprise actuels	16
2.1.2 Définition de l'action de la solution Identity Manager sur les processus d'entreprise actuels	17
2.1.3 Identification des principales parties prenantes professionnelles et techniques	18
2.1.4 Interrogation de toutes les parties prenantes	18
2.1.5 Création d'une stratégie de haut niveau et d'un chemin d'exécution conforme	19
2.2 Phase d'analyse des besoins et de la conception	19
2.2.1 Définition des besoins de votre entreprise	20
2.2.2 Analyse de vos processus d'entreprise	22
2.2.3 Conception d'un modèle de données d'entreprise	22
2.3 Démonstration de faisabilité	24
2.4 Validation et préparation des données	24
2.5 Pilote de production	25
2.6 Planification du déploiement vers la production	25
2.7 Déploiement vers la production	25
3 Directives techniques	27
3.1 Instructions pour les outils de gestion	28
3.1.1 Instructions pour Analyser	29
3.1.2 Instructions pour Designer	29
3.1.3 Instructions pour iManager	29
3.1.4 Instructions pour l'administrateur d'assignation de rôles	29
3.2 Instructions pour le serveur méta-annuaire	30
3.3 Instructions pour eDirectory	31
3.3.1 Objets Identity Manager dans eDirectory	31
3.3.2 Réplication des objets nécessaires à Identity Manager sur le serveur	32
3.3.3 Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents	33
3.4 Application utilisateur	36
3.5 Instructions pour l'audit et la création de rapport	37
Partie II Installation	39
4 Liste de vérification pour un système Identity Manager de base	41
4.1 Conditions préalables	42
4.2 Planification	42
4.3 Installation	42

4.4	Configuration du pilote avec le chargeur distant	43
4.5	Configuration de pilotes sans chargeur distant	43
4.6	Configuration supplémentaire	44
5	Où se procurer Identity Manager	45
6	Configuration système requise	49
6.1	eDirectory et iManager	50
6.2	Serveur méta-annuaire	51
6.2.1	Processeurs pris en charge	52
6.2.2	Systèmes d'exploitation du serveur	52
6.3	Chargeur distant	53
6.4	Application utilisateur	55
6.5	Audit et création de rapports	56
6.6	Postes de travail	57
6.6.1	Plates-formes des postes de travail	58
6.6.2	Navigateurs Web	58
6.6.3	Ressources requises	58
7	Installation d'Identity Manager	59
7.1	Installation d'Analyzer	59
7.2	Installation de Designer	60
7.3	Installation d'eDirectory	60
7.4	Installation d'iManager	61
7.5	Installation du serveur méta-annuaire	61
7.5.1	Installation non-root du serveur méta-annuaire	63
7.5.2	Installation en mode silencieux du serveur méta-annuaire	65
7.6	Installation du chargeur distant	66
7.6.1	Configuration requise	66
7.6.2	Pilotes pris en charge	66
7.6.3	Procédure d'installation	67
7.6.4	Installation silencieuse du chargeur distant	69
7.6.5	Installation du chargeur distant Java sous UNIX ou Linux	70
7.6.6	Coexistence de chargeurs distants 32 et 64 bits	71
7.7	Installation du module de provisioning basé sur les rôles	71
7.8	Installation d'un pilote personnalisé	71
7.9	Installation de l'administrateur d'assignation de rôles	71
7.10	Installation du module Identity Reporting ou de Sentinel	72
7.11	Installation d'Identity Manager dans un environnement en grappe	73
8	Activation des produits Novell Identity Manager	75
8.1	Achat d'une licence de produit Identity Manager	75
8.2	Installation d'une référence d'activation de produit	75
8.3	Affichage des activations de produits pour Identity Manager et les pilotes	76
8.4	Activation des pilotes Identity Manager	77
8.5	Activation d'Analyzer	77
8.6	Activation de Designer et de l'administrateur d'assignation de rôles	78

9 Dépannage d'Identity Manager	79
Partie III Mise à niveau ou migration	85
10 Nouveautés	87
10.1 Module Identity Reporting	87
10.2 Nouveaux pilotes	87
10.2.1 Pilote SharePoint (chargeur distant .NET)	87
10.2.2 Pilote Salesforce.com	88
10.3 Prise en charge de l'audit XDAS	88
10.4 Remplacement des fichiers de configuration de pilote par des paquetages	88
10.5 Administrateur d'assignation de rôles	88
10.6 Analyzer	88
10.7 Programme d'installation intégré	89
11 Mise à niveau et migration	91
11.1 Mise à niveau	91
11.2 Migration	92
11.3 Plusieurs serveurs associés à un seul ensemble de pilotes	92
12 Versions prises en charge et configuration système requise pour les mises à niveau et migrations	93
12.1 Mises à niveau	93
12.1.1 Versions prises en charge pour les mises à niveau	93
12.1.2 Configuration système requise	94
12.2 Migrations	94
12.2.1 Versions prises en charge pour les migrations	94
12.2.2 Configuration système requise	94
13 Réalisation d'une mise à niveau	95
13.1 Liste de contrôle de mise à niveau	95
13.2 Création d'une sauvegarde de la configuration actuelle	97
13.2.1 Vérification de l'actualité de votre projet Designer	98
13.2.2 Création d'une exportation des pilotes	99
13.3 Mise à niveau d'iManager	100
13.4 Arrêt des pilotes	101
13.4.1 Utilisation de Designer pour arrêter les pilotes	101
13.4.2 Utilisation d'iManager pour arrêter les pilotes	101
13.5 Mise à niveau d'Analyzer	102
13.6 Mise à niveau de Designer	102
13.7 Mise à niveau du serveur méta-annuaire et des fichiers de module d'interface pilote	103
13.8 Mise à niveau du chargeur distant	104
13.9 Mise à niveau des pilotes vers des paquetages	104
13.9.1 Création d'un nouveau pilote	105
13.9.2 Remplacement du contenu existant par le contenu des paquetages	105
13.9.3 Conservation du contenu existant et ajout de nouveau contenu à l'aide des paquetages	106
13.10 Restauration de stratégies et de règles personnalisées sur le pilote	107
13.10.1 Utilisation de Designer pour restaurer les stratégies et les règles personnalisées sur le pilote	107

13.10.2	Utilisation d'iManager pour restaurer les stratégies et les règles personnalisées sur le pilote	108
13.11	Superposition du nouveau pilote sur le fichier de configuration de pilote existant (obsolète)	109
13.11.1	Utilisation de Designer pour superposer le nouveau pilote sur le fichier de configuration de pilote existant	109
13.11.2	Utilisation d'iManager pour superposer le nouveau pilote sur le fichier de configuration de pilote existant	110
13.12	Déploiement du projet converti	110
13.13	Lancement des pilotes	110
13.13.1	Utilisation de Designer pour lancer les pilotes	111
13.13.2	Utilisation d'iManager pour démarrer les pilotes	111
14	Exécution d'une migration	113
14.1	Liste de contrôle de migration	113
14.2	Ajout du nouveau serveur à l'ensemble de pilotes	115
14.3	Modification des informations spécifiques du serveur	115
14.3.1	Modification des informations spécifiques du serveur dans Designer	116
14.3.2	Modification des informations spécifiques du serveur dans iManager	116
14.4	Suppression de l'ancien serveur de l'ensemble de pilotes	117
14.4.1	Utilisation de Designer pour retirer l'ancien serveur de l'ensemble de pilotes	117
14.4.2	Utilisation d'iManager pour retirer l'ancien serveur de l'ensemble de pilotes	117
14.4.3	Déclassement de l'ancien serveur	118
Partie IV	Désinstallation d'Identity Manager	119
15	Désinstallation des composants d'Identity Manager	121
15.1	Suppression d'objets dans eDirectory	121
15.2	Désinstallation du serveur méta-annuaire	122
15.2.1	Désinstallation sous Linux/UNIX	122
15.2.2	Désinstallation sous Windows	122
15.3	Désinstallation du chargeur distant	122
15.3.1	Désinstallation sous Linux/UNIX	122
15.3.2	Désinstallation sous Windows	123
15.4	Désinstallation du module de provisioning basé sur les rôles	123
15.4.1	Suppression des pilotes	123
15.4.2	Désinstallation de l'application utilisateur	123
15.4.3	Désinstallation du serveur d'applications et de la base de données	124
15.5	Désinstallation des composants du module Identity Reporting	125
15.5.1	Suppression des pilotes de création de rapports	125
15.5.2	Désinstallation du module Identity Reporting	125
15.5.3	Désinstallation du service d'audit d'événements	125
15.6	Désinstallation d'iManager	126
15.7	Désinstallation d'eDirectory	126
15.8	Désinstallation d'Analyzer	127
15.9	Désinstallation de Designer	127
15.10	Désinstallation de l'administrateur d'assignation de rôles	128

À propos de ce guide

Novell Identity Manager 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 régiront 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 planifier, installer ou mettre à niveau un système Identity Manager utile à votre environnement.

- ♦ [Partie I, « Planification », page 11](#)
 - ♦ [Chapitre 1, « Mise en place d'un environnement de développement », page 13](#)
 - ♦ [Chapitre 2, « Création d'un plan de projet », page 15](#)
 - ♦ [Chapitre 3, « Directives techniques », page 27](#)
- ♦ [Partie II, « Installation », page 39](#)
 - ♦ [Chapitre 4, « Liste de vérification pour un système Identity Manager de base », page 41](#)
 - ♦ [Chapitre 5, « Où se procurer Identity Manager », page 45](#)
 - ♦ [Chapitre 6, « Configuration système requise », page 49](#)
 - ♦ [Chapitre 7, « Installation d'Identity Manager », page 59](#)
 - ♦ [Chapitre 8, « Activation des produits Novell Identity Manager », page 75](#)
- ♦ [Partie III, « Mise à niveau ou migration », page 85](#)
 - ♦ [Chapitre 10, « Nouveautés », page 87](#)
 - ♦ [Chapitre 11, « Mise à niveau et migration », page 91](#)
 - ♦ [Chapitre 12, « Versions prises en charge et configuration système requise pour les mises à niveau et migrations », page 93](#)
 - ♦ [Chapitre 13, « Réalisation d'une mise à niveau », page 95](#)
 - ♦ [Chapitre 14, « Exécution d'une migration », page 113](#)
- ♦ [Partie IV, « Désinstallation d'Identity Manager », page 119](#)

Public

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

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 de la documentation supplémentaire sur les pilotes Identity Manager, reportez-vous au [site Web de documentation des pilotes Identity Manager \(http://www.novell.com/documentation/idm40drivers/index.html\)](http://www.novell.com/documentation/idm40drivers/index.html).

Pour obtenir la documentation relative à l'application utilisateur, reportez-vous au [site Web de documentation du module de provisioning basé sur les rôles Identity Manager \(http://www.novell.com/documentation/idmrbpm40/index.html\)](http://www.novell.com/documentation/idmrbpm40/index.html).

Planification

Identity Manager 4.0 vous aide à gérer les identités et les ressources de votre entreprise. Il automatise également de nombreux processus d'entreprise qui sont actuellement exécutés manuellement.

Si vous avez des questions concernant les différents composants d'une solution Identity Manager, reportez-vous au guide *Présentation d'Identity Manager 4.0*, qui fournit des informations détaillées sur chaque composant.

Pour créer une solution Identity Manager efficace dans votre environnement, vous devez commencer par la planifier et la concevoir. La planification présente deux aspects majeurs : la mise en place d'un laboratoire de test pour se familiariser avec les produits et la création d'un plan de projet pour mettre en oeuvre une solution Identity Manager. Lorsque vous créez le plan de projet, vous définissez le processus d'entreprise ainsi qu'une planification de mise en oeuvre. La plupart des sociétés disposent de différents processus d'entreprise, gérés par diverses personnes. Une solution Identity Manager complète affecte la plupart de ces processus. Il est extrêmement important de prendre le temps de planifier une solution Identity Manager, de sorte qu'elle soit correctement mise en oeuvre dans votre environnement.

Si vous créez une solution Identity Manager dont tous les composants résident sur le même serveur, reportez-vous au *Guide du programme d'installation intégré d'Identity Manager 4.0* pour vous aider à l'installer. Il s'agit d'un programme d'installation simplifié qui vous permet de configurer votre système plus rapidement.

Il est vivement recommandé d'engager un expert Identity Manager pour vous aider dans chaque phase de la mise en oeuvre de votre solution. Pour plus d'informations sur les options de partenariat, accédez au [site Web Novell Solution Partner \(http://www.novell.com/partners/\)](http://www.novell.com/partners/). Novell Education offre également des cours sur la mise en oeuvre d'Identity Manager.

- ♦ [Chapitre 1, « Mise en place d'un environnement de développement », page 13](#)
- ♦ [Chapitre 2, « Création d'un plan de projet », page 15](#)
- ♦ [Chapitre 3, « Directives techniques », page 27](#)

Mise en place d'un environnement de développement

1

Pour aboutir à un plan utile, vous devez vous familiariser avec les produits Identity Manager avant de démarrer la phase de planification du déploiement. La configuration d'un environnement de développement dans lequel vous pouvez tester, analyser et développer votre solution Identity Manager vous permet de vous familiariser avec chaque composant et de découvrir des problèmes imprévus qui peuvent survenir.

Par exemple, lorsque vous synchronisez des informations entre deux systèmes, celles-ci sont présentées différemment sur chacun d'entre eux. En modifiant ces données et en examinant la façon dont elles se synchronisent entre les deux systèmes, vous pouvez voir si ce changement affecte les autres systèmes qui utilisent ces informations.

La configuration d'un environnement de développement vous permet également et surtout de vérifier que vos solutions fonctionnent avant de les appliquer à des données en direct. Identity Manager manipule et supprime des données. L'environnement de test permet d'apporter des modifications sans perdre les données présentes dans l'environnement de production.

Il est conseillé de configurer un environnement de développement pour chaque déploiement d'Identity Manager. Chaque déploiement est différent. Il existe différents systèmes, stratégies et processus d'entreprise à intégrer dans la solution Identity Manager. L'environnement de déploiement permet de créer la solution la mieux adaptée à chaque situation.

L'outil le plus important à utiliser pour développer votre solution Identity Manager s'intitule Designer. Il permet de recueillir toutes les informations concernant votre environnement, puis de les exploiter pour créer une solution Identity Manager adaptée à vos besoins. Utilisez Designer au cours des différentes phases de la planification, afin de recueillir toutes les informations. Designer simplifie la création d'un plan de projet contenant les informations d'entreprise et les données techniques. Pour en savoir plus sur Designer, reportez-vous au manuel [Designer 4.0 for Identity Manager 4.0 Administration Guide](#) (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

Pour configurer votre environnement de développement, retrouvez les informations dans le [Chapitre 4, « Liste de vérification pour un système Identity Manager de base », page 41](#). Il s'agit d'une liste de vérifications de tous les composants d'Identity Manager. Elle vous permet de vous assurer que vous avez installé et configuré tous les composants d'Identity Manager que vous pouvez utiliser pour développer un plan de projet. Utilisez les informations fournies au [Chapitre 3, « Directives techniques », page 27](#) pour configurer votre environnement de développement et vous documenter sur les aspects techniques à prendre en compte au moment d'installer et de configurer chaque composant d'Identity Manager.

Une fois votre environnement de développement créé, vous pouvez générer le plan de projet afin de mettre en place la solution Identity Manager. Créez le plan du projet à l'aide des informations présentes dans le [Chapitre 2, « Création d'un plan de projet », page 15](#).

Création d'un plan de projet

2

Ce document de planification offre une vue d'ensemble des activités qui sont généralement réalisées dans le cadre d'un projet Identity Manager, depuis son initiation jusqu'à son déploiement complet en production. La mise en oeuvre d'une stratégie Identity Manager nécessite que vous définissiez la nature de vos processus d'entreprise actuels, les besoins de ces processus et les parties prenantes de votre environnement, que vous conceviez une solution, que vous obteniez l'adhésion des parties prenantes et que vous testiez et déployiez la solution. Cette section vise à vous donner les informations nécessaires concernant le processus afin que vous puissiez optimiser les performances d'Identity Manager.

Cette section n'est pas exhaustive ; elle ne présente pas toutes les configurations possibles et doit être adaptée selon les besoins des clients. Chaque environnement est différent et nécessite une certaine souplesse dans le type d'activités utilisé.

- ♦ [Section 2.1, « Phase de découverte », page 15](#)
- ♦ [Section 2.2, « Phase d'analyse des besoins et de la conception », page 19](#)
- ♦ [Section 2.3, « Démonstration de faisabilité », page 24](#)
- ♦ [Section 2.4, « Validation et préparation des données », page 24](#)
- ♦ [Section 2.5, « Pilote de production », page 25](#)
- ♦ [Section 2.6, « Planification du déploiement vers la production », page 25](#)
- ♦ [Section 2.7, « Déploiement vers la production », page 25](#)

2.1 Phase de découverte

La solution Identity Manager touche de nombreux aspects de votre activité. Pour parvenir à une solution efficace, vous devez prendre le temps de définir l'ensemble de vos processus d'entreprise, puis d'identifier la manière dont une installation Identity Manager modifie ces processus, les personnes affectées par ces changements, ainsi que la manière dont ces derniers sont mis en place.

La phase de découverte permet de bien comprendre les problèmes et les solutions pour toutes les parties prenantes. Elle crée un plan ou une feuille de route contenant les informations clé de l'entreprise et des systèmes touchées par la solution Identity Manager. Elle permet également aux parties prenantes de participer à la création de la solution Identity Manager, pour leur permettre de comprendre en quoi elle touche leur domaine d'activité.

La liste suivante énumère les étapes nécessaires pour réussir la phase de découverte. Vous aurez peut-être besoin d'y ajouter des éléments en avançant dans les phases de découverte et de conception.

- ♦ [Section 2.1.1, « Définition des processus d'entreprise actuels », page 16](#)
- ♦ [Section 2.1.2, « Définition de l'action de la solution Identity Manager sur les processus d'entreprise actuels », page 17](#)
- ♦ [Section 2.1.3, « Identification des principales parties prenantes professionnelles et techniques », page 18](#)

- ♦ [Section 2.1.4, « Interrogation de toutes les parties prenantes », page 18](#)
- ♦ [Section 2.1.5, « Création d'une stratégie de haut niveau et d'un chemin d'exécution conforme », page 19](#)

2.1.1 Définition des processus d'entreprise actuels

Identity Manager automatise les processus d'entreprise, afin de gérer aisément les identités de votre environnement. Vous ne pourrez pas concevoir de solution Identity Manager qui automatise ces processus si vous ne connaissez pas les processus d'entreprise actuels. Vous pouvez profiter du mode Architecture de Designer pour recueillir vos processus d'entreprise actuels et les afficher sous forme graphique. Pour plus d'informations, reportez-vous à la section « [Architect Mode](#) » (Mode architecte) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

Votre organisation peut, par exemple, identifier les processus d'entreprise suivants :

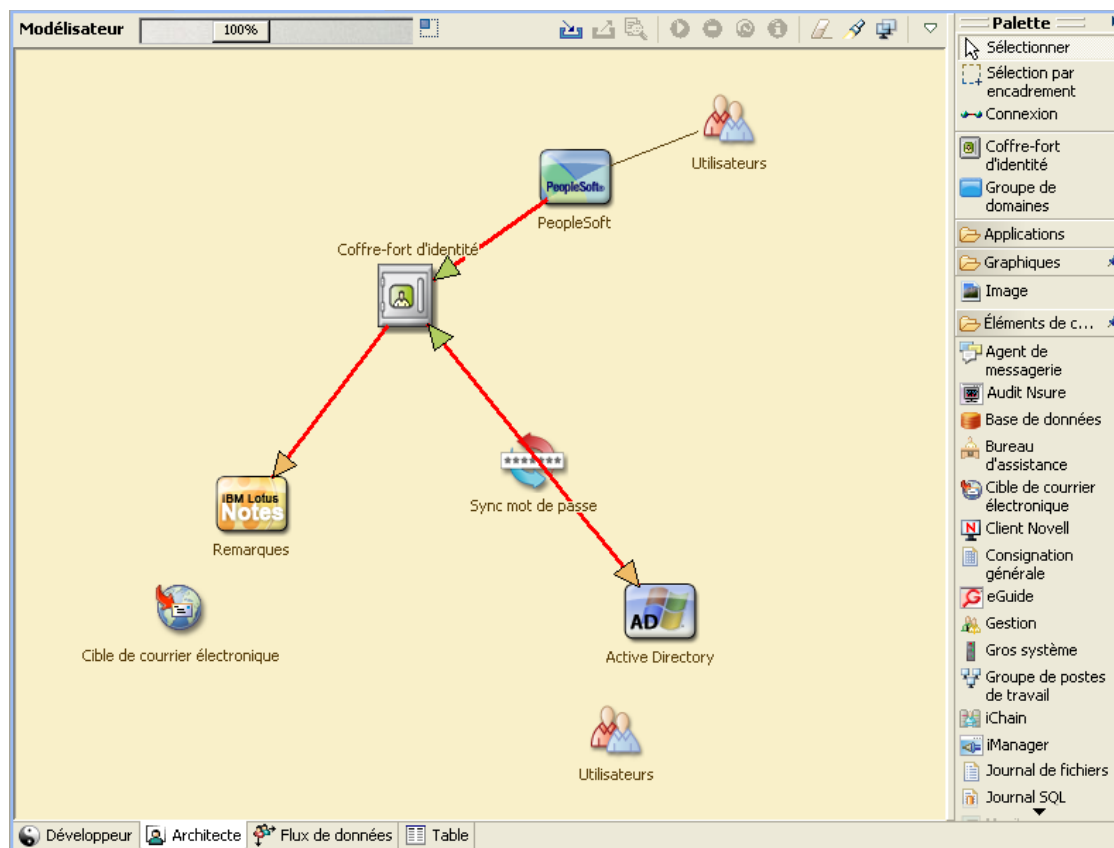
- ♦ Lorsqu'un employé est renvoyé, son compte utilisateur dans le système de messagerie est supprimé. Toutefois, dans tous les autres systèmes, il est désactivé et non supprimé.
- ♦ Le format d'une adresse de courrier électronique d'un utilisateur.
- ♦ Les systèmes ou ressources accessibles aux commerciaux.
- ♦ Les systèmes ou ressources accessibles aux responsables.
- ♦ Les systèmes qui génèrent les nouveaux comptes, plus spécifiquement le système des ressources humaines ou une requête de workflow.
- ♦ Une stratégie de mot de passe pour la société qui définit la fréquence à laquelle modifier le mot de passe, sa complexité et les systèmes qui le synchronisent.

Pour définir vos processus d'entreprise, reportez-vous à la liste ci-dessous, qui vous aidera à comprendre l'ensemble des processus.

- ♦ Définissez ou précisez les problèmes d'activité actuels.
- ♦ Déterminez les initiatives requises pour traiter ces problèmes.
- ♦ Déterminez les services et les systèmes concernés par ces initiatives.

Cette étape vous permet d'obtenir un aperçu de haut niveau des pratiques actuelles au sein de votre entreprise et des processus à améliorer. Par exemple, la [Figure 2-1](#) montre, à l'aide de Designer, comment les nouveaux comptes utilisateur sont générés depuis le système PeopleSoft. Ils sont synchronisés dans le coffre-fort d'identité, puis dans Lotus Notes et Active Directory. Les mots de passe sont synchronisés entre Active Directory et le coffre-fort d'identité. Les comptes se synchronisent dans le système Notes. En revanche, aucun compte n'est à nouveau synchronisé avec le coffre-fort d'identité.

Figure 2-1 Exemples de processus d'entreprise



Une fois les processus déterminés, vous devez définir les modalités de mise en œuvre d'Identity Manager. Passez à la [Section 2.1.2, « Définition de l'action de la solution Identity Manager sur les processus d'entreprise actuels »](#), page 17.

2.1.2 Définition de l'action de la solution Identity Manager sur les processus d'entreprise actuels

Après avoir défini vos processus d'entreprise actuels, vous devez choisir les processus à inclure dans une solution Identity Manager.

Mieux vaut étudier l'ensemble de la solution, puis établir les priorités pour la mise en place des procédures. Identity Manager traite tant d'aspects de votre entreprise qu'il est plus simple de planifier toute la solution, plutôt que de proposer une solution indépendante pour chaque processus.

Créez une liste des processus d'entreprise à automatiser en priorité, puis identifiez les systèmes qui seront affectés par ces changements. Passez ensuite à la [Section 2.1.3, « Identification des principales parties prenantes professionnelles et techniques »](#), page 18.

2.1.3 Identification des principales parties prenantes professionnelles et techniques

L'identification de tous les acteurs impliqués dans la solution Identity Manager compte pour le succès de la solution. Dans la plupart des sociétés, il est rare qu'une seule personne centralise la connaissance et la compréhension de tous les aspects professionnels et techniques des processus de l'entreprise. Vous devez identifier les services et les systèmes qui seront touchés par la solution Identity Manager, mais aussi la personne en charge de chacun.

Par exemple, si vous intégrez dans votre solution un système de messagerie électronique, vous devez lister le système de messagerie, son administrateur et ses coordonnées. Vous pouvez ajouter toutes ces informations dans le projet Designer. À chaque icône d'application correspond un espace où il est possible d'enregistrer les informations sur le système et son administrateur. Pour plus d'informations, reportez-vous à la section « [Configuring Application Properties](#) » (Configuration des propriétés d'application) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

Lorsque vous avez identifié toutes les personnes impliquées dans chaque procédure d'activité, vous pouvez passer à l'étape suivante qui se trouve à la [Section 2.1.4, « Interrogation de toutes les parties prenantes », page 18](#).

2.1.4 Interrogation de toutes les parties prenantes

Interroger les principaux acteurs professionnels et techniques vous permet de rassembler des informations nécessaires à la conception complète de la solution Identity Manager. Ces entretiens vous permettent également de former chaque personne sur la solution Identity Manager et de leur montrer en quoi la solution les concerne. Voici une liste des éléments à traiter lors des entretiens.

- ♦ Définissez ou précisez les processus d'entreprise traités par la solution Identity Manager. La personne que vous interrogez pourrait disposer d'informations susceptibles de modifier le plan en cours.
- ♦ Déterminez en quoi la solution concernera les différents acteurs et répondra à leurs préoccupations. Demandez également le temps que pourrait prendre leur partie de la solution. Il se peut qu'ils aient déjà procédé à une estimation mais le recueil de ces informations aide à déterminer l'ampleur de la solution.
- ♦ Rassemblez les principales informations sur les systèmes et l'activité auprès des parties prenantes. Une proposition de plan peut parfois avoir un impact négatif sur un processus ou un système. En recueillant ces informations, vous prendrez des décisions adaptées sur la solution Identity Manager.

Dès que vous avez interrogé les principaux intervenants, passez à l'étape suivante dans la [Section 2.1.5, « Création d'une stratégie de haut niveau et d'un chemin d'exécution conforme », page 19](#).

2.1.5 Création d'une stratégie de haut niveau et d'un chemin d'exécution conforme

Une fois toutes les informations rassemblées, vous devez créer une stratégie de haut niveau ou une feuille de route pour la solution Identity Manager. Ajoutez toutes les caractéristiques à inclure dans la solution Identity Manager. Ainsi, par exemple, les nouveaux comptes utilisateur sont générés à partir d'une requête via un workflow, mais le type d'utilisateur dépend des ressources auxquelles l'utilisateur a accès.

Présentez cette stratégie de haut niveau à tous les intervenants, si possible lors de la même réunion. Vous pouvez ainsi :

- ♦ Vérifier que toutes les initiatives incluses sont les plus correctes possible et identifier celles présentant la plus forte priorité.
- ♦ Identifier les activités de planification pour la préparation d'une phase de besoins et de conception.
- ♦ Déterminer les ressources nécessaires pour mener une ou plusieurs de ces initiatives.
- ♦ Créer un chemin d'exécution conforme pour la solution Identity Manager.
- ♦ Définir une formation supplémentaire pour les intervenants.

La procédure de découverte offre à tous les participants une vue claire des problèmes et solutions. Elle constitue une excellente base pour la phase d'analyse, qui nécessite que les participants aient une connaissance de base des annuaires, de Novell eDirectory et Novell Identity Manager ainsi que de l'intégration XML en général.

Une fois la phase de découverte terminée, passez à la [Section 2.2, « Phase d'analyse des besoins et de la conception »](#), page 19.

2.2 Phase d'analyse des besoins et de la conception

Pour cette phase d'analyse, prenez pour démarrer la feuille de route de haut niveau, qui a été créé lors de la phase de découverte. Le document et le projet Designer ont tous deux besoin des informations techniques et professionnelles. Le résultat en est le modèle de données et la conception d'architecture Identity Manager de haut niveau servant à mettre en place la solution.

La conception aura pour principal objectif la gestion des informations d'identité ; cependant, de nombreux éléments généralement associés à un annuaire de gestion des ressources tels que les fichiers et les imprimantes, peuvent également être traités. Identity Manager synchronise les comptes utilisateur et les annuaires n'ayant pas d'accès direct au système de fichiers du système d'exploitation. Ainsi, vous pouvez disposer d'un compte utilisateur dans Active Directory qui ne vous donne pourtant pas accès au système de fichiers sur le serveur Active Directory.

En vous servant des informations rassemblées pendant la phase de découverte, répondez aux exemples de questions pour constater les autres informations collectées. Ceci peut nécessiter de nouveaux entretiens avec les intervenants.

- ♦ Quelles sont les versions de logiciels utilisées ?
- ♦ La conception de eDirectory est-elle adaptée ? Le serveur Identity Manager contient-il, par exemple, une réplique maîtresse ou lecture-écriture des objets utilisateurs qui se synchronisent ? Dans la négative, la conception eDirectory n'est pas adaptée.

- ♦ La qualité des données dans tous les systèmes est-elle suffisante ? (Si les données ne sont pas exploitables, la stratégie d'activité pourrait ne pas être mise en place comme on le souhaite). Par exemple, il pourrait y avoir des doublons des comptes utilisateur pour les systèmes qui se synchronisent ou le format des données pourrait ne pas être cohérent dans tous les systèmes. Les données de chaque système doivent être évaluées avant que les informations ne soient synchronisées.
- ♦ La manipulation des données est-elle requise pour votre environnement ? Par exemple, le format de la date d'embauche d'un utilisateur dans le système des ressources humaines peut être 2008/02/23 et 02-23-2008 dans le coffre-fort d'identité. Il faudra donc modifier la date pour permettre la synchronisation.

Identity Manager intègre un outil qui vous permet de simplifier le processus d'analyse et de nettoyage de vos données. Pour plus d'informations, reportez-vous au manuel [Analyzer 1.2 for Identity Manager Administration Guide](#) (Guide d'administration d'Analyzer 1.2 pour Identity Manager).

Reprenez les informations du [Chapitre 3, « Directives techniques », page 27](#) pour prendre la bonne décision en ce qui concerne votre environnement.

Après analyse des besoins, vous pouvez établir la portée et le plan de projet pour la mise en place, puis déterminer s'il faut engager des activités préalables. Pour éviter des erreurs coûteuses, soyez aussi méticuleux que possible lors de la collecte des informations et de la description des besoins. Voici une liste des besoins possibles :

- ♦ Un modèle de données présentant tous les systèmes, les sources de données faisant autorité, les événements, les flux d'informations, les normes du format de données et les relations d'assignation entre les systèmes connectés et les attributs dans Identity Manager.
- ♦ Architecture Identity Manager appropriée pour la solution.
- ♦ Les détails des besoins supplémentaires pour le raccordement du système.
- ♦ Stratégies de validation des données et de concordance des enregistrements.
- ♦ Conception de l'annuaire pour la prise en charge de l'infrastructure Identity Manager.

Les tâches suivantes doivent être réalisées pendant l'évaluation des besoins et de la conception :

- ♦ [« Définition des besoins de votre entreprise » page 20](#)
- ♦ [« Analyse de vos processus d'entreprise » page 22](#)
- ♦ [« Conception d'un modèle de données d'entreprise » page 22](#)

2.2.1 Définition des besoins de votre entreprise

Lors de la phase de découverte, vous avez rassemblé les processus d'entreprise de votre organisation et les besoins qui les définissent. Créez une liste des besoins de votre entreprise, puis démarrez l'assignation de ces procédures dans Designer en procédant comme suit :

- ♦ Créer une liste des besoins de votre entreprise et déterminer les systèmes concernés par cette procédure. Par exemple, un besoin pour supprimer un employé peut définir que les comptes de messagerie et réseau de ce dernier doivent être supprimés ou archivés le jour même de son départ. Cette procédure de résiliation concerne le système de messagerie et le coffre-fort d'identité.
- ♦ Établir les flux de processus, les déclencheurs de processus et les relations d'assignation de données.

Par exemple, si un événement se produit au niveau d'un certain processus, quels sont les autres processus déclenchés ?

- ♦ Assigner des flux de données entre les applications. Designer vous permet d'afficher ces informations. Pour plus d'informations, reportez-vous à la section « [Managing the Flow of Data](#) » (Gestion du flux de données) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).
- ♦ Identifier les données dont le format doit être modifié (p. ex. remplacement de 25/02/2007 par 25 février 2007), puis utiliser Analyzer pour effectuer les modifications. Pour plus d'informations, reportez-vous au manuel *Analyzer 1.2 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 1.2 pour Identity Manager).
- ♦ Décrire les dépendances qui existent entre les données.

Si une valeur particulière a changé, il est important de savoir s'il existe une dépendance au niveau de cette valeur. Si un processus particulier a changé, il est important de savoir s'il existe une dépendance au niveau de ce processus.

Par exemple, la sélection de la valeur d'état d'employé « temporaire » dans un système de ressources humaines signifie que le service informatique doit créer, dans eDirectory, un objet Utilisateur doté de droits restreints et d'un accès réseau à certaines heures seulement.

- ♦ Répertorier les priorités.

Il n'est pas possible de répondre immédiatement à chaque exigence, souhait ou désir de toutes les parties. Les priorités pour la conception et le déploiement du système de provisioning aideront à planifier la feuille de route.

Il peut se révéler utile de diviser le déploiement en plusieurs phases, qui permettent de mettre en œuvre une partie du déploiement dans un premier temps et le reste ultérieurement, ou d'utiliser une méthode de déploiement progressive basée sur des groupes d'employés au sein de l'organisation.

- ♦ Définir la configuration requise.

Vous devez décrire la configuration requise pour la mise en œuvre d'une phase donnée du déploiement. Cela comprend l'accès aux systèmes connectés qui doivent interagir avec Identity Manager.

- ♦ Identifier les sources de données expertes.

En identifiant le plus tôt possible les éléments d'information qui relèvent de la responsabilité des gestionnaires et administrateurs système, vous pourrez obtenir et maintenir la coopération de chaque partie.

Par exemple, l'administrateur de comptes peut vouloir la propriété sur l'octroi des droits d'accès à des fichiers et des répertoires spécifiques pour un employé. Pour cela, vous pouvez mettre en œuvre des assignations d'ayants droit locales dans le système de comptes.

Après avoir défini les besoins de votre entreprise, passez à la [Section 2.2.2, « Analyse de vos processus d'entreprise »](#), page 22.

2.2.2 Analyse de vos processus d'entreprise

Une fois l'analyse des besoins de votre entreprise terminée, vous devez collecter d'autres informations pour bien cibler la solution Identity Manager. Vous devez interroger les personnes essentielles comme les responsables, les administrateurs et les employés qui utilisent véritablement l'application ou le système. Les problèmes à résoudre comprennent les points suivants :

- ♦ D'où proviennent les données ?
- ♦ Où sont acheminées les données ?
- ♦ Qui est responsable des données ?
- ♦ Qui est propriétaire de la fonction à laquelle appartiennent les données ?
- ♦ Qui faut-il contacter pour modifier les données ?
- ♦ Quelles sont les conséquences de la modification des données ?
- ♦ Quelles pratiques existent en matière de gestion (collecte et/ou modification) des données ?
- ♦ Quels types d'opérations ont lieu ?
- ♦ Quelles méthodes sont utilisées pour garantir la qualité et l'intégrité des données ?
- ♦ Où résident les systèmes (sur quels serveurs, dans quels services) ?
- ♦ Quels processus ne sont pas adaptés à la gestion automatisée ?

Vous pouvez, par exemple, poser les questions suivantes à l'administrateur d'un système PeopleSoft travaillant pour le département des ressources humaines :

- ♦ Quelles données sont stockées dans la base PeopleSoft ?
- ♦ Quelles informations apparaissent dans les divers volets d'un compte d'employé ?
- ♦ Quelles opérations doivent être reflétées dans le système de provisioning (p. ex. ajout, modification ou suppression) ?
- ♦ Lesquelles sont obligatoires ? Lesquelles sont facultatives ?
- ♦ Quelles opérations doivent être déclenchées en fonction d'opérations effectuées dans PeopleSoft ?
- ♦ Quels événements, opérations et actions doivent être ignorés ?
- ♦ Comment les données doivent-elles être transformées et assignées à Identity Manager ?

Les entrevues avec les personnes clés peuvent conduire vers d'autres parties de l'organisation et permettre d'obtenir une idée plus précise du processus complet.

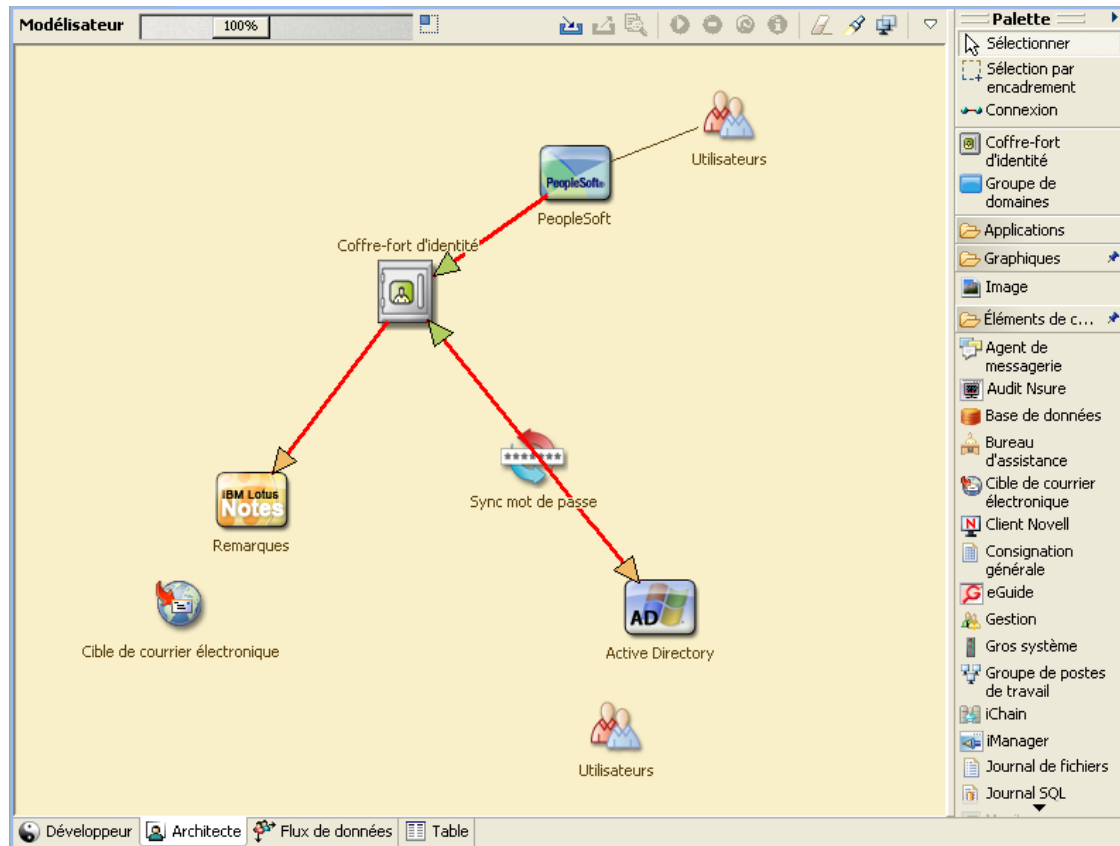
Après avoir rassemblé toutes ces informations, vous pouvez concevoir un modèle de données d'entreprise adapté à votre environnement. Passez à la [Section 2.2.3, « Conception d'un modèle de données d'entreprise »](#), page 22 pour démarrer la conception.

2.2.3 Conception d'un modèle de données d'entreprise

Une fois vos processus d'entreprise définis, vous pouvez utiliser Designer pour commencer à concevoir un modèle de données reflétant vos processus d'entreprise actuelles.

Le modèle de Designer montre d'où viennent les données, où elles se déplacent et où elles ne peuvent pas aller. Il peut aussi prendre en compte la manière dont les données essentielles affectent le flux des données. Par exemple, la [Figure 2-2](#) montre que les données proviennent de PeopleSoft mais qu'aucune donnée n'est à nouveau synchronisée dans PeopleSoft.

Figure 2-2 Flux de données dans Designer



Vous pourriez aussi vouloir développer un diagramme illustrant le processus d'entreprise proposé et les avantages de la mise en place d'un provisioning automatisé dans ce processus.

Pour développer ce modèle, commencez par répondre aux questions suivantes :

- ◆ Quels sont les types d'objets (utilisateurs, groupes, etc.) déplacés ?
- ◆ Quels sont les événements intéressants ?
- ◆ Quels attributs doivent être synchronisés ?
- ◆ Quelles sont les données stockées dans votre entreprise pour les différents types d'objets gérés ?
- ◆ S'agit-il d'une synchronisation unidirectionnelle ou bidirectionnelle ?
- ◆ Quel système représente la source experte et pour quels attributs ?

Il est également important de considérer les relations entre différentes valeurs sur les différents systèmes.

Par exemple, un champ d'état d'employé dans PeopleSoft peut avoir trois valeurs définies : employé, contractuel et stagiaire. Cependant, dans le système Active Directory, il ne peut exister que deux valeurs : permanent et temporaire. En l'occurrence, vous devez définir la relation entre l'état contractuel de PeopleSoft et les valeurs permanent et d'Active Directory.

L'objectif de ce travail est de comprendre chaque système d'annuaire, la manière dont les annuaires sont liés et de connaître les objets et les attributs à synchroniser dans ces systèmes. Une fois la conception achevée, vous pouvez créer une preuve de concept. Passez à la [Section 2.3, « Démonstration de faisabilité »](#), page 24.

2.3 Démonstration de faisabilité

Créez et testez votre démonstration de faisabilité en utilisant un exemple de mise en œuvre dans un environnement de laboratoire, afin de refléter le flux de données et la stratégie métier de votre entreprise. La mise en œuvre s'appuie sur le modèle de données développé au cours des phases de conception et d'analyse des besoins, et constitue l'étape finale avant l'introduction du pilote de production. Exécutez les tests dans l'environnement de laboratoire que vous avez créé comme indiqué au [Chapitre 1, « Mise en place d'un environnement de développement »](#), page 13.

Remarque : cette étape permet souvent d'améliorer la gestion en prévision de la mise en œuvre finale.

Le [Chapitre 3, « Directives techniques »](#), page 27 contient des informations pouvant vous aider à valider votre preuve de conception. Il contient des directives techniques pour vous aider à réussir votre déploiement Identity Manager.

En créant la preuve de conception, vous devez également créer un plan pour valider les données présentes dans vos systèmes. Cette étape vous permet de vous assurer de l'absence de conflits entre les systèmes. Passez à la [Section 2.4, « Validation et préparation des données »](#), page 24 pour vérifier que ces conflits n'existent pas.

2.4 Validation et préparation des données

La qualité et la cohérence des données présentes dans les systèmes de production peuvent varier et entraîner par conséquent des erreurs lors de la synchronisation des systèmes. Cette phase constitue une séparation nette entre l'équipe de mise en œuvre Ressources et les unités ou groupes au sein de l'entreprise, qui « possèdent » ou gèrent les données dans les systèmes à intégrer. Il arrive parfois que les facteurs combinés de risque et de coût n'entrent pas dans le projet de provisioning.

Vous devez utiliser le modèle de données développé lors des phases d'analyse et de conception. Pour préparer correctement les données, vous devez également définir une stratégie potentielle pour le format des données et la concordance des enregistrements. Une fois le modèle de données et la stratégie de format définis, vous pouvez accomplir deux étapes majeures :

- ♦ Créer des ensembles de données de production adaptés au chargement dans le coffre-fort d'identité (comme identifié dans les activités d'analyse et de conception). Cela comprend la définition de la méthode de chargement potentielle (chargement en bloc ou via des connecteurs). Les conditions requises pour les données validées ou formatées sont également identifiées.
- ♦ Identifier les facteurs de performances et valider ces facteurs par rapport à l'équipement utilisé et à l'architecture distribuée générale du déploiement d'Identity Manager.

Une fois les données préparées, passez à la [Section 2.5, « Pilote de production », page 25](#).

2.5 Pilote de production

L'introduction du pilote de production constitue la première étape de la migration dans un environnement de production. Pendant cette phase, des opérations de personnalisation supplémentaires peuvent être effectuées. Dans cette introduction limitée, les résultats voulus des activités précédentes peuvent être confirmés et l'accord obtenu pour le déploiement de la production. Le pilote valide le plan créé jusqu'à présent dans la procédure.

Remarque : cette phase peut fournir les critères d'acceptation de la solution et constituer le jalon nécessaire en vue de la pleine mise en production.

La solution pilote propose une preuve de conception et une validation en direct pour le modèle de données et les résultats souhaités de la procédure. Une fois que le pilote est terminé, passez à la [Section 2.6, « Planification du déploiement vers la production », page 25](#).

2.6 Planification du déploiement vers la production

Il s'agit de la phase de planification du déploiement vers la production. Le plan doit :

- ♦ Confirmer les plates-formes de serveur, les versions logicielles et les service packs
- ♦ Confirmer l'environnement général
- ♦ Confirmer la conception du coffre-fort d'identité dans une coexistence mixte
- ♦ Confirmer l'exactitude de la logique d'activité
- ♦ Confirmer le bon déroulement de la synchronisation des données
- ♦ Planifier le passage au nouveau processus
- ♦ Planifier une stratégie de retour à l'état initial en cas d'incident

Le plan doit contenir les dates de mise en place et de réalisation pour chaque étape du déploiement. Chaque intervenant propose sa contribution pour ces dates et confirme qu'elles lui conviennent. Ceci permet à chaque personne concernée par le déploiement de connaître le moment où interviennent les changements et le moment prévu pour leur achèvement.

Une fois le plan de déploiement de production terminé, passez à la [Section 2.7, « Déploiement vers la production », page 25](#).

2.7 Déploiement vers la production

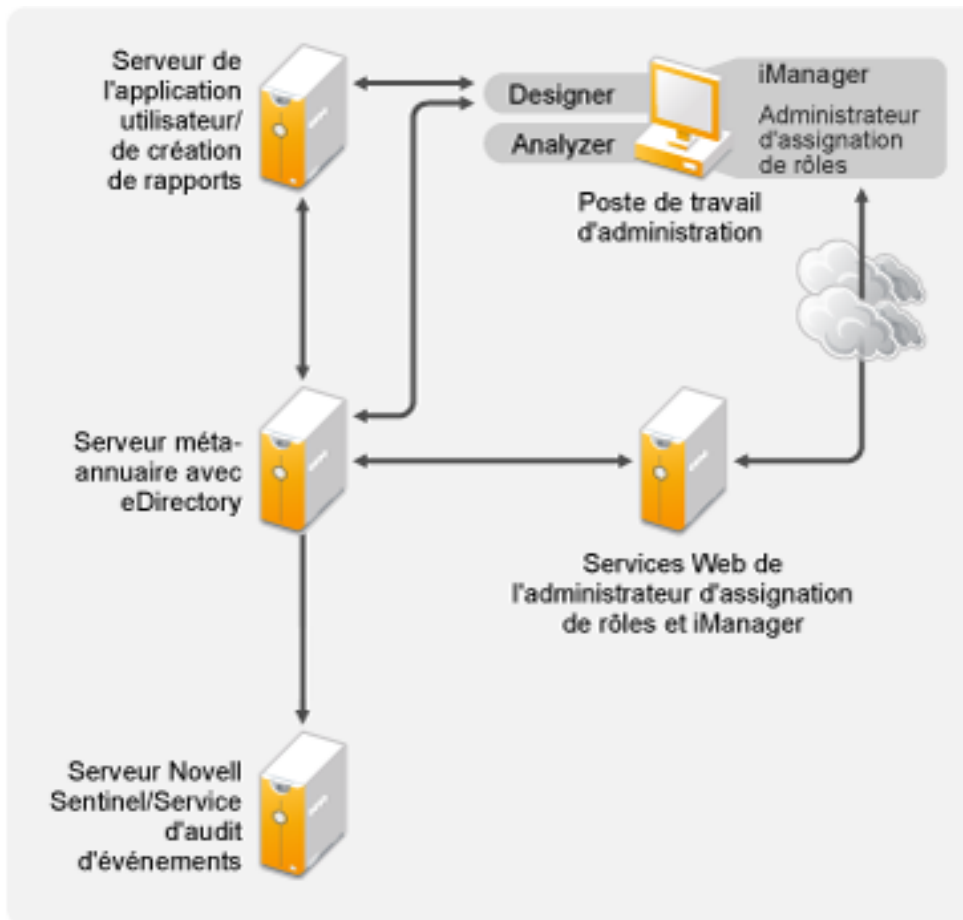
La phase de déploiement en production consiste à mettre à exécution l'ensemble des plans, de manière à créer la solution Identity Manager dans l'environnement réel. Utilisez le plan de déploiement en production pour mettre en place les différents éléments de la solution Identity Manager. En fonction de la complexité du plan, cette phase peut être rapide ou durer un certain temps.

Directives techniques

3

Les informations collectées dans Designer permettent de prendre des décisions d'ordre technique, telles que la définition de l'emplacement d'installation et des options de configuration de chaque composant d'Identity Manager. Pour obtenir une présentation de chaque composant, reportez-vous au guide *Présentation d'Identity Manager 4.0*. La *Figure 3-1* représente une configuration possible d'une solution Identity Manager.

Figure 3-1 Composants Identity Manager



Identity Manager est hautement personnalisable. Les sections suivantes contiennent les bonnes pratiques techniques qui vous aideront à paramétrer et configurer la solution Identity Manager qui conviendra le mieux à votre environnement. L'application de ces instructions à votre environnement est fonction du type de matériel dont vous disposez pour vos serveurs, de la configuration de votre réseau WAN et du nombre d'objets synchronisés.

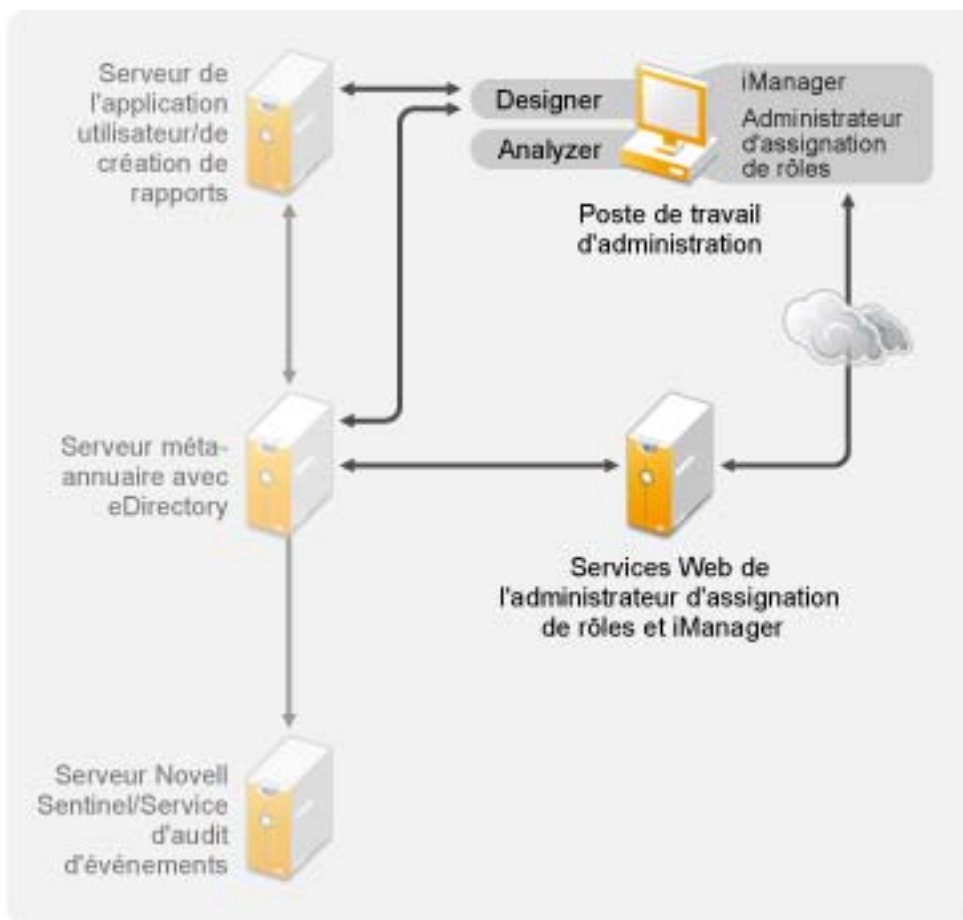
- ♦ [Section 3.1, « Instructions pour les outils de gestion », page 28](#)
- ♦ [Section 3.2, « Instructions pour le serveur méta-annuaire », page 30](#)
- ♦ [Section 3.3, « Instructions pour eDirectory », page 31](#)

- ♦ [Section 3.4, « Application utilisateur », page 36](#)
- ♦ [Section 3.5, « Instructions pour l'audit et la création de rapport », page 37](#)

3.1 Instructions pour les outils de gestion

Les deux principaux outils de gestion pour la solution Identity Manager sont Designer et iManager, comme vous le voyez à la [Figure 3-2](#). Designer est utilisé lors de la planification et de la création de la solution Identity Manager. iManager est utilisé pour sa gestion quotidienne.

Figure 3-2 Outils de gestion Identity Manager



L'application utilisateur utilise une page d'administration Web. Pour plus d'informations sur l'application utilisateur, reportez-vous à la section « [Administering the User Application](#) » (Administration de l'application utilisateur) du manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Administration Guide* (Guide d'administration de l'application utilisateur du module de provisioning basé sur les rôles d'Identity Manager version 4.0).

- ♦ [Section 3.1.1, « Instructions pour Analyser », page 29](#)
- ♦ [Section 3.1.2, « Instructions pour Designer », page 29](#)
- ♦ [Section 3.1.3, « Instructions pour iManager », page 29](#)
- ♦ [Section 3.1.4, « Instructions pour l'administrateur d'assignation de rôles », page 29](#)

3.1.1 Instructions pour Analyzer

Analyser est un client lourd installé sur un poste de travail. Il permet de contrôler et de nettoyer les données des systèmes que vous souhaitez ajouter à votre solution Identity Manager. Pendant la phase de planification, il vous aide à déterminer les modifications à apporter et le meilleur moyen de le faire.

Il n'existe pas de considérations particulières concernant l'utilisation d'Analyser. Pour plus d'informations, reportez-vous au manuel *Analyser 1.2 for Identity Manager Administration Guide* (Guide d'administration d'Analyser 1.2 pour Identity Manager).

3.1.2 Instructions pour Designer

Designer est un client lourd installé sur un poste de travail. Il sert à concevoir, tester, documenter puis déployer votre solution Identity Manager. Son utilisation dans toute la phase de planification vous aide à rassembler toutes les informations en un même lieu. Il vous aide également à pointer les problèmes dont vous pourriez ne pas être averti en regardant ensemble tous les composants de la solution.

Il n'existe pas de considérations particulières concernant l'utilisation de Designer, sauf si plusieurs personnes travaillent sur un même projet. Designer permet le contrôle des versions du projet. Pour plus d'informations, reportez-vous à la section « [Version Control](#) » (Contrôle des versions) du manuel *Designer 4.0 for Identity Manager 4.0 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

3.1.3 Instructions pour iManager

iManager est une application Web qui permet d'administrer Identity Manager. Lorsque vous installez Identity Manager, le programme suppose qu'un serveur iManager est déjà installé dans votre arborescence eDirectory.

Si plus de 10 administrateurs travaillent en continu et simultanément sur iManager, vous devez disposer d'un serveur n'hébergeant que iManager. La [Figure 3-2 page 28](#) montre cette configuration de votre solution Identity Manager. Si vous ne disposez que d'un administrateur, vous pouvez exécuter facilement iManager sur votre serveur méta-annuaire.

3.1.4 Instructions pour l'administrateur d'assignation de rôles

L'administrateur d'assignation de rôles est une application Web qui découvre les autorisations pouvant être octroyées au sein de vos principaux systèmes informatiques. Il permet aux administrateurs informatiques, mais aussi aux analystes d'entreprise, de définir et de gérer les autorisations associées aux différents rôles métier.

Il n'existe pas de considérations particulières concernant l'utilisation de l'administrateur d'assignation de rôles. Vous pouvez l'exécuter sur un serveur distinct, comme le montre la [Figure 3-2 page 28](#), ou sur le serveur méta-annuaire. Pour plus d'informations, reportez-vous au manuel *Identity Manager Role Mapping Administrator 2.0 Installation and Configuration Guide* (Guide d'installation et de configuration de la version 2.0 de l'administrateur d'assignation de rôles d'Identity Manager).

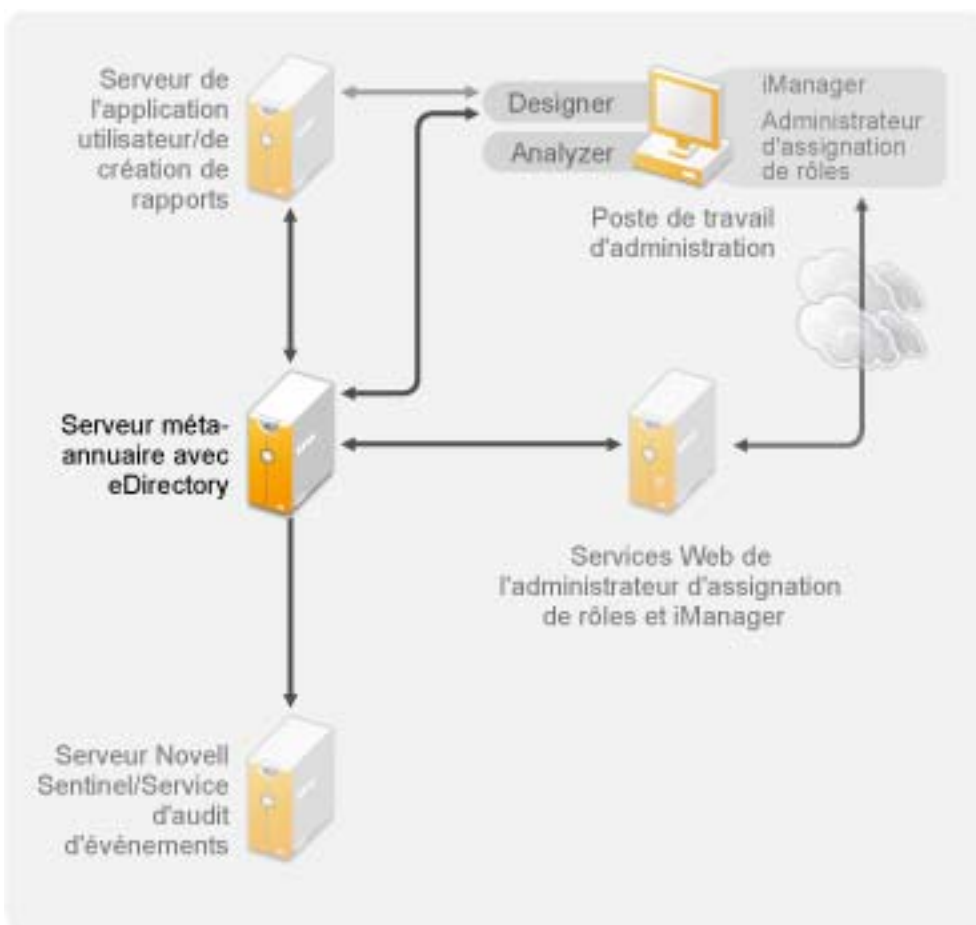
3.2 Instructions pour le serveur méta-annuaire

Votre solution Identity Manager peut être dotée d'un ou plusieurs serveurs méta-annuaires, ceci dépendant de la charge du serveur. Le serveur méta-annuaire nécessite l'installation de eDirectory, comme indiqué dans la [Figure 3-3](#). Pour faciliter la charge ou la configuration de votre environnement, vous pouvez ajouter un serveur de chargeur distant, qui n'est pas représenté dans la figure.

Les pilotes doivent s'exécuter sur le même serveur que l'application connectée. Ainsi, pour pouvoir configurer le pilote Active Directory, le serveur de la [Figure 3-3](#) doit être un serveur membre ou un contrôleur de domaine. Si vous ne souhaitez pas installer eDirectory et Identity Manager sur un serveur membre ou un contrôleur de domaine, vous pouvez installer le chargeur distant sur un serveur membre ou un contrôleur de domaine. Le chargeur distant envoie tous les événements d'Active Directory au serveur méta-annuaire. Le chargeur distant reçoit les informations du serveur méta-annuaire et les transmet à l'application connectée.

Il améliore la flexibilité de votre solution Identity Manager. Pour plus d'informations, reportez-vous au manuel [Identity Manager 4.0 Remote Loader Guide](#) (Guide du chargeur distant d'Identity Manager 4.0).

Figure 3-3 Serveur méta-annuaire



De nombreuses variables agissent sur les performances du serveur. Il est généralement recommandé de limiter à dix le nombre de pilotes exécutés sur un serveur méta-annuaire. Toutefois, si vous synchronisez des millions d'objets sur chaque pilote, vous ne pourrez peut-être pas exécuter dix pilotes sur un serveur. En revanche, si vous synchronisez 100 objets par pilote, vous pourrez probablement exécuter plus de dix pilotes sur un serveur.

La configuration de la solution Identity Manager dans un environnement de laboratoire vous permet de tester les futures performances des serveurs. Vous pouvez utiliser les outils de contrôle de l'état de santé dans iManager pour obtenir une ligne de base, puis prendre les meilleures décisions pour votre environnement. Pour plus d'informations sur les outils de contrôle de l'état de santé, reportez-vous à la section « [Monitoring Driver Health](#) » (Contrôle de l'état de santé des pilotes) du manuel *Identity Manager 4.0 Common Driver Administration Guide* (Guide d'administration des pilotes communs d'Identity Manager 4.0).

Pour des informations sur chaque pilote, reportez-vous au [site Web de la documentation des pilotes d'Identity Manager \(http://www.novell.com/documentation/idm36drivers/index.html\)](http://www.novell.com/documentation/idm36drivers/index.html). Chaque guide contient des informations spécifiques au pilote.

3.3 Instructions pour eDirectory

eDirectory correspond au coffre-fort d'identité qui conserve les objets synchronisés via la solution Identity Manager. Les sections suivantes contiennent des instructions pour vous aider à planifier votre déploiement eDirectory.

- ♦ [Section 3.3.1, « Objets Identity Manager dans eDirectory », page 31](#)
- ♦ [Section 3.3.2, « Réplication des objets nécessaires à Identity Manager sur le serveur », page 32](#)
- ♦ [Section 3.3.3, « Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents », page 33](#)

3.3.1 Objets Identity Manager dans eDirectory

La liste suivante répertorie les principaux objets Identity Manager stockés dans eDirectory et les relations qui les unissent. L'installation d'Identity Manager ne crée aucun objet. Les objets Identity Manager sont créés pendant la configuration de la solution Identity Manager.

- ♦ **Ensemble de pilotes** : un ensemble de pilotes est un conteneur pour les pilotes Identity Manager et les objets de bibliothèque. Vous ne pouvez activer qu'un seul ensemble de pilotes à la fois sur un serveur. Cependant, plusieurs serveurs peuvent être associés à un même ensemble de pilotes. De plus, un pilote peut être associé à plus d'un serveur à la fois. Toutefois, le pilote ne doit être exécuté que sur un serveur à la fois. Il doit être à l'état désactivé sur les autres serveurs. Le serveur méta-annuaire doit être installé sur tous les serveurs associés à un ensemble de pilotes.
- ♦ **Bibliothèque** : l'objet de bibliothèque est un espace de stockage des stratégies souvent utilisées et pouvant être référencées depuis plusieurs sites. La bibliothèque est stockée dans l'ensemble de pilotes. Vous pouvez placer une stratégie dans la bibliothèque, de façon à ce qu'elle puisse être référencée par chaque pilote de l'ensemble.
- ♦ **Pilote** : un pilote assure la connexion entre une application et le coffre-fort d'identité. Il permet également de synchroniser et de partager des données entre différents systèmes. Le pilote est conservé dans l'ensemble de pilotes.

- ♦ **Travail** : un travail permet d'automatiser une tâche récurrente. Par exemple, un travail peut configurer un système afin qu'il désactive un compte un jour donné ou qu'il initie un workflow pour demander l'extension de l'accès d'une personne à une ressource de l'entreprise. Le travail est stocké dans l'ensemble de pilotes.

3.3.2 Réplication des objets nécessaires à Identity Manager sur le serveur

Si votre environnement Identity Manager nécessite plusieurs serveurs afin d'exécuter plusieurs pilotes Identity Manager, votre plan doit garantir que certains objets eDirectory sont répliqués sur les serveurs sur lesquels vous voulez exécuter ces pilotes.

Vous pouvez utiliser des répliques filtrées, à condition que tous les objets et attributs dont le pilote a besoin pour lire ou synchroniser soient inclus dans la réplique filtrée.

N'oubliez pas que vous devez donner à l'objet du pilote Identity Manager des droits eDirectory suffisants sur tout objet qu'il doit synchroniser, soit en lui accordant explicitement des droits soit en rendant la sécurité de l'objet du pilote équivalente à un objet qui dispose des droits souhaités.

Un serveur eDirectory exécutant un pilote Identity Manager (ou auquel le pilote fait référence si vous utilisez le chargeur distant) doit contenir une réplique maîtresse ou lecture-écriture des éléments suivants :

- ♦ L'objet Ensemble des pilotes de ce serveur.

Vous devez avoir un objet Ensemble des pilotes pour chaque serveur qui exécute Identity Manager. À moins d'avoir des besoins particuliers, n'associez pas plusieurs serveurs au même objet Ensemble des pilotes.

Remarque : lorsque vous créez un objet Ensemble de pilotes, une partition distincte est créée par défaut. Novell recommande la création d'une partition séparée sur l'objet Ensemble des pilotes. Pour que Identity Manager fonctionne, le serveur doit comporter une réplique complète de l'objet Ensemble des pilotes. La partition n'est pas obligatoire si le serveur dispose d'une réplique complète de l'emplacement d'installation de l'objet Ensemble des pilotes.

- ♦ L'objet Serveur de ce serveur.

L'objet Serveur est nécessaire car il permet au pilote de générer des paires clés pour les objets. Il est également important pour l'authentification du chargeur distant.

- ♦ Les objets que vous souhaitez que cette instance du pilote synchronise.

Le pilote ne peut pas synchroniser des objets à moins qu'une réplique de ces objets se trouve sur le même serveur que le pilote. En fait, un pilote Identity Manager synchronise les objets dans *tous* les conteneurs qui sont répliqués sur le serveur à moins que vous ne créiez des règles pour le filtrage des étendues indiquant autre chose.

Ainsi, si vous souhaitez qu'un pilote synchronise tous les objets utilisateur, la manière la plus simple consiste à utiliser une instance du pilote sur un serveur détenant une réplique maîtresse ou lecture-écriture de tous vos utilisateurs.

Cependant, de nombreux environnements n'ont pas de serveur avec une réplique de tous les utilisateurs. L'ensemble des utilisateurs est plutôt réparti sur plusieurs serveurs. Dans ce cas, vous disposez de trois options :

- ♦ **Regrouper les utilisateurs sur un seul serveur.** Pour créer un seul serveur avec tous les utilisateurs, ajoutez des répliques sur un serveur existant. Les répliques filtrées peuvent être utilisées pour réduire la taille de la base de données eDirectory si nécessaire, à condition que les objets et attributs utilisateur nécessaires fassent partie de la réplique filtrée.
- ♦ **Utilisez plusieurs instances du pilote sur plusieurs serveurs, avec un filtrage des étendues.** Si vous ne voulez pas regrouper les utilisateurs sur un seul serveur, vous devez déterminer l'ensemble de serveurs qui contiendra tous les utilisateurs et configurer une instance du pilote Identity Manager sur chacun de ces serveurs.

Pour éviter que les instances séparées d'un pilote tentent de synchroniser les mêmes utilisateurs, vous devez utiliser le filtrage des étendues pour définir les utilisateurs que chaque instance du pilote doit synchroniser. Le filtrage des étendues signifie que vous ajoutez des règles à chaque pilote pour limiter l'étendue de la gestion du pilote à des conteneurs spécifiques. Reportez-vous à la section « [Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents](#) » page 33.

- ♦ **Utilisez plusieurs instances du pilote sur plusieurs serveurs, sans filtrage des étendues.** Si vous voulez exécuter plusieurs instances d'un pilote sur différents serveurs sans utiliser de répliques filtrées, vous devez définir des stratégies sur les différentes instances du pilote qui permettent au pilote de traiter différents ensembles d'objets au sein du même coffre-fort d'identité.
- ♦ Les objets Modèle que vous voulez que le pilote utilise lors de la création d'utilisateurs, si vous choisissez d'utiliser des modèles.

Les pilotes Identity Manager n'exigent pas que vous indiquiez des objets Modèle eDirectory pour créer des utilisateurs. Cependant, si vous indiquez qu'un pilote doit utiliser un modèle lors de la création d'utilisateurs dans eDirectory, l'objet Modèle doit être répliqué sur le serveur sur lequel le pilote est exécuté.

- ♦ Tout conteneur que vous voulez que le pilote Identity Manager utilise pour la gestion des utilisateurs.
Par exemple, si vous avez créé un conteneur nommé Utilisateurs inactifs qui contient les comptes utilisateur désactivés, vous devez avoir une réplique maîtresse ou lisible/inscriptible (de préférence une réplique maîtresse) de ce conteneur sur le serveur sur lequel le pilote est exécuté.
- ♦ Tout autre objet auquel le pilote doit se rapporter (par exemple, les objets Bon de travail pour le pilote Avaya PBX).
Si les autres objets ne doivent être que lus par le pilote, la réplique de ces objets sur le serveur peut être une réplique en lecture seule.

3.3.3 Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents

Le filtrage des étendues signifie l'ajout de règles à chaque pilote pour limiter l'étendue des actions du pilote à des conteneurs spécifiques. Voici deux situations dans lesquelles vous devez utiliser le filtrage des étendues :

- ♦ Vous voulez que le pilote ne synchronise que les utilisateurs d'un conteneur particulier.

Par défaut, un pilote Identity Manager synchronise les objets de tous les conteneurs répliqués sur le serveur sur lequel il est exécuté. Pour limiter cette étendue, vous devez créer des règles de filtrage des étendues.

- ♦ Vous voulez qu'un pilote Identity Manager synchronise tous les utilisateurs, mais vous ne voulez pas que tous les utilisateurs soient répliqués sur le même serveur.

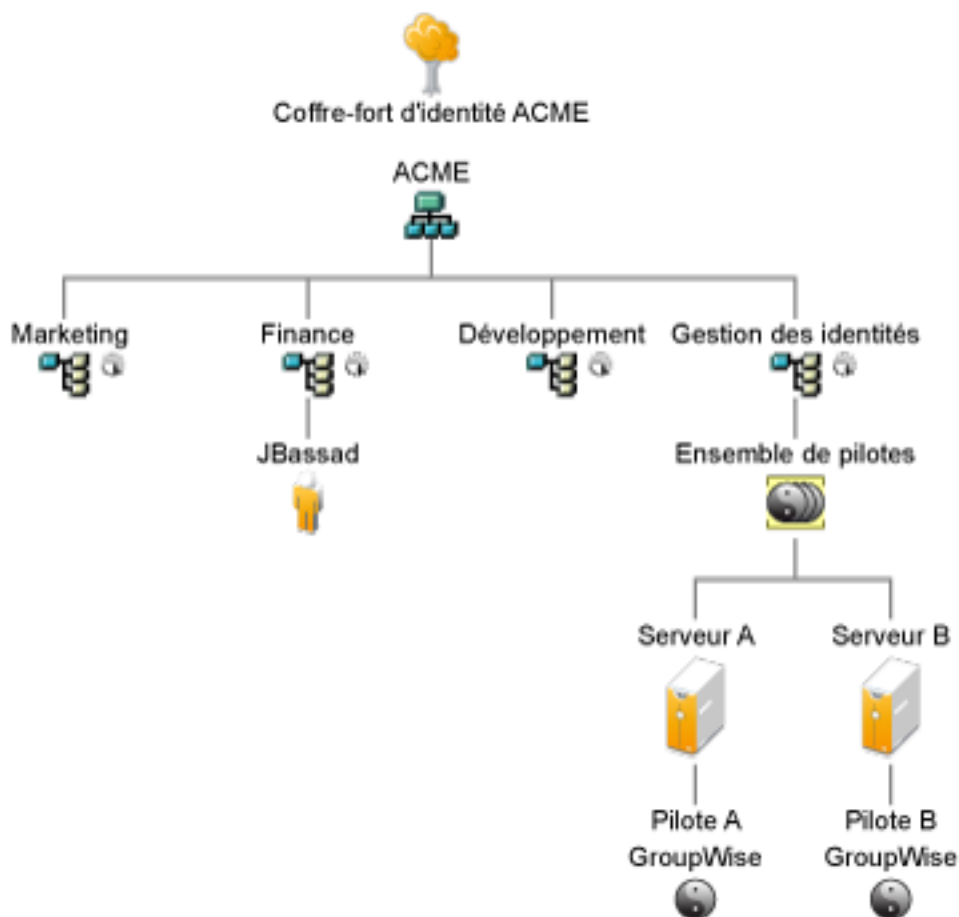
Pour synchroniser tous les utilisateurs sans les répliquer sur un seul serveur, vous devez déterminer l'ensemble de serveurs qui contient tous les utilisateurs, puis créer une instance du pilote Identity Manager sur chacun de ces serveurs. Pour éviter que deux instances du pilote tentent de synchroniser les mêmes utilisateurs, vous devez utiliser le filtrage des étendues pour définir les utilisateurs que chaque instance du pilote doit synchroniser.

Remarque : vous devez utiliser le filtrage des étendues même si les répliques de votre serveur ne sont pas en chevauchement pour l'instant. À l'avenir, des répliques peuvent être ajoutées à vos serveurs et un chevauchement peut être créé involontairement. Si le filtrage des étendues est en place, vos pilotes Identity Manager ne tentent pas de synchroniser les mêmes utilisateurs, même si des répliques sont ajoutées à vos serveurs à l'avenir.

Voici un exemple d'utilisation du filtrage des étendues :

L'illustration suivante montre un coffre-fort d'identité avec trois conteneurs d'utilisateurs : Marketing, Finance et Développement. Elle montre également un conteneur Identity Manager conservant les ensembles des pilotes. Chacun de ces conteneurs constitue une partition distincte.

Figure 3-4 Exemple d'arborescence de filtrage des étendues



Dans cet exemple, l'administrateur Identity Manager a deux serveurs de coffre-fort d'identité, le serveur A et le serveur B, tel qu'illustré dans la [Figure 3-5 page 36](#). Aucun des serveurs ne contient une copie de tous les utilisateurs. Chaque serveur contient deux des trois partitions, l'étendue de ce que les serveurs peuvent contenir est donc en chevauchement.

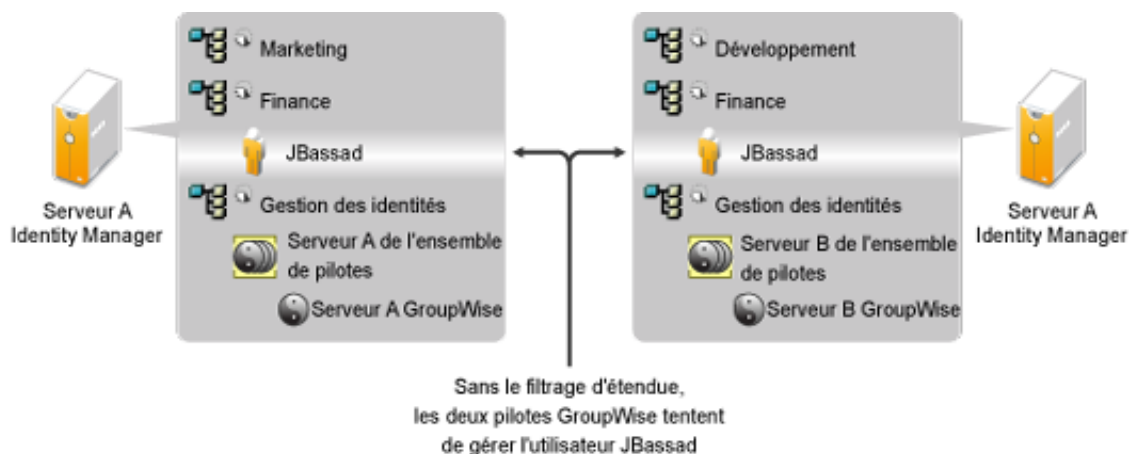
L'administrateur souhaite que tous les utilisateurs de l'arborescence soient synchronisés par le pilote GroupWise, mais ne veut pas regrouper les répliques des utilisateurs sur un seul serveur. Il choisit plutôt d'utiliser deux instances du pilote GroupWise, une sur chaque serveur. Il installe Identity Manager et configure le pilote GroupWise sur chaque serveur Identity Manager.

Le serveur A contient des répliques des conteneurs Marketing et Finance. Le serveur contient également une réplique du conteneur Identity Manager, qui stocke l'ensemble des pilotes pour le serveur A et l'objet de pilote GroupWise pour le serveur A.

Le serveur B contient des répliques des conteneurs Développement et Finance et le conteneur Gestion des identités conservant l'ensemble des pilotes pour le Serveur B et l'objet pilote GroupWise pour le serveur B.

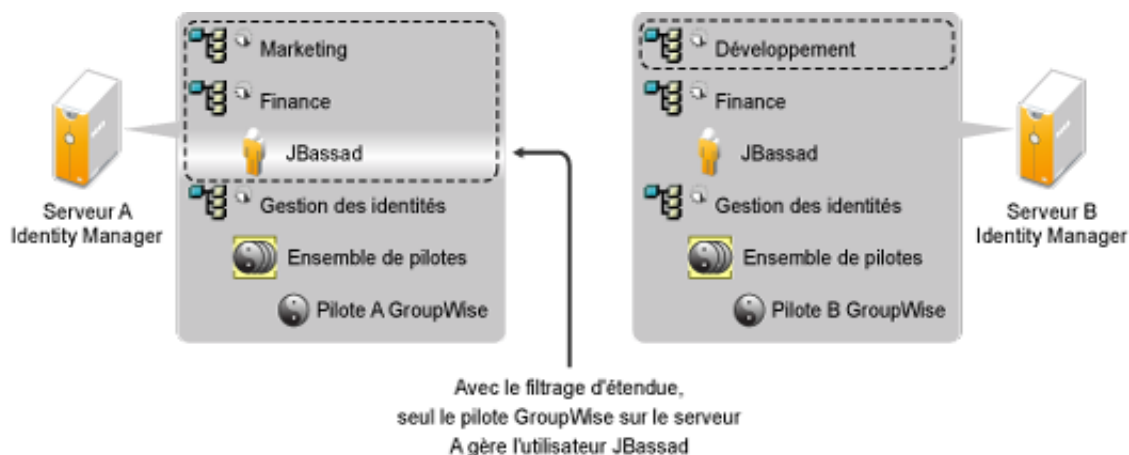
Comme le serveur A et le serveur B contiennent une réplique du conteneur Finance, ils contiennent tous deux l'utilisateur JBassad, qui est dans le conteneur Finance. Sans filtrage des étendues, le pilote GroupWise A et le pilote GroupWise B synchroniseraient JBassad.

Figure 3-5 Deux serveurs avec des répliques qui se chevauchent, sans filtrage des étendues



L'illustration suivante montre que le filtrage des étendues empêche les deux instances du pilote de gérer le même utilisateur, car il définit les pilotes qui synchronisent chaque conteneur.

Figure 3-6 Le filtrage des étendues définit les pilotes qui synchronisent chaque conteneur



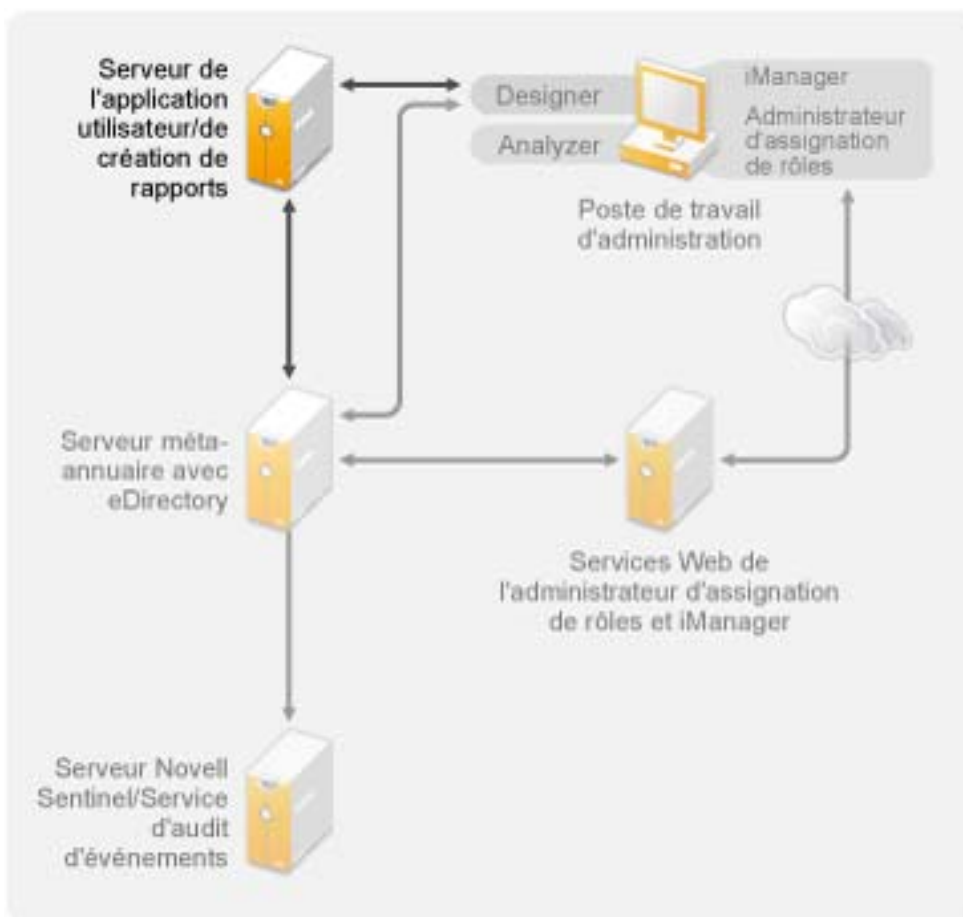
Identity Manager comporte des règles prédéfinies. Deux règles permettent de filtrer les étendues. Les stratégies « Transformation de l'événement - Filtrage de l'étendue - Inclure les sous-arborescences » et « Transformation de l'événement - Filtrage de l'étendue - Exclure les sous-arborescences » sont documentées dans la section [Understanding Policies for Identity Manager 4.0](#) (Présentation des stratégies d'Identity Manager 4.0).

Dans cet exemple, vous utiliseriez la règle prédéfinie Inclure les sous-arborescences pour le serveur A et le serveur B. Vous définiriez l'étendue de chaque pilote différemment de façon à ce qu'ils ne synchronisent que les utilisateurs des conteneurs indiqués. Le serveur A synchroniserait le conteneur Marketing et Finance. Le serveur B synchroniserait le conteneur Développement.

3.4 Application utilisateur

L'application utilisateur devrait s'exécuter sur son propre serveur, comme illustré dans la [Figure 3-7](#). Vous pourriez avoir besoin de plusieurs serveurs d'application utilisateur.

Figure 3-7 Application utilisateur



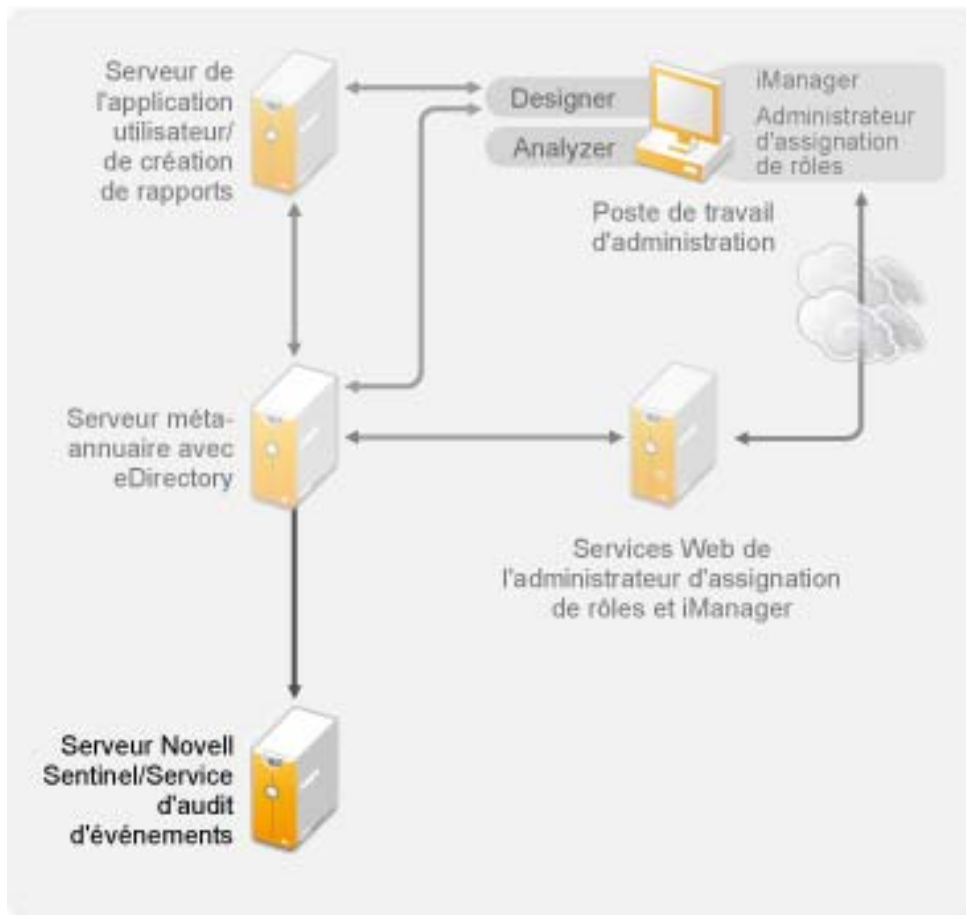
Utilisez les informations de la section [Affinage des performances](http://www.novell.com/documentation/idmr/bpm40/agpro/data/b2gx735.html) (<http://www.novell.com/documentation/idmr/bpm40/agpro/data/b2gx735.html>) du *Guide d'administration de l'application utilisateur* pour déterminer la meilleure manière de configurer le serveur de l'application utilisateur.

Si le serveur de l'application utilisateur doit être occupé, vous pourriez envisager d'utiliser la mise en grappe. La mise en grappe améliore la disponibilité, l'évolutivité et l'équilibrage des charges. Pour plus d'informations, reportez-vous à la section [Mise en grappe](http://www.novell.com/documentation/idmr/bpm40/agpro/data/b2gx73a.html) (<http://www.novell.com/documentation/idmr/bpm40/agpro/data/b2gx73a.html>) du *Guide d'administration de l'application utilisateur*.

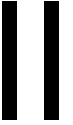
3.5 Instructions pour l'audit et la création de rapport

Pour utiliser l'audit et la création de rapports dans le cadre de la solution Identity Manager, vous devez exécuter Novell Identity Audit ou Novell Sentinel. Vous devez exécuter le service d'audit d'événements ou Sentinel sur son propre serveur, comme le montre la [Figure 3-8](#). Le nombre de serveurs nécessaires à votre solution dépend du nombre de pilotes de votre environnement et du nombre d'événements définis pour l'audit.

Figure 3-8 Sentinel



Installation



Les sections suivantes contiennent les informations nécessaires pour installer un système Identity Manager sans utiliser le programme d'installation intégré. Pour une installation et une configuration simples, utilisez le nouveau programme d'installation intégré au lieu d'installer les composants séparément. Pour plus d'informations sur le programme d'installation intégré, reportez-vous au *Guide du programme d'installation intégré d'Identity Manager 4.0*.

Toutefois, si vous devez installer séparément un ou plusieurs composants d'Identity Manager, reportez-vous aux instructions contenues dans les sections suivantes.

- ♦ [Chapitre 4, « Liste de vérification pour un système Identity Manager de base », page 41](#)
- ♦ [Chapitre 5, « Où se procurer Identity Manager », page 45](#)
- ♦ [Chapitre 6, « Configuration système requise », page 49](#)
- ♦ [Chapitre 7, « Installation d'Identity Manager », page 59](#)
- ♦ [Chapitre 8, « Activation des produits Novell Identity Manager », page 75](#)
- ♦ [Chapitre 9, « Dépannage d'Identity Manager », page 79](#)

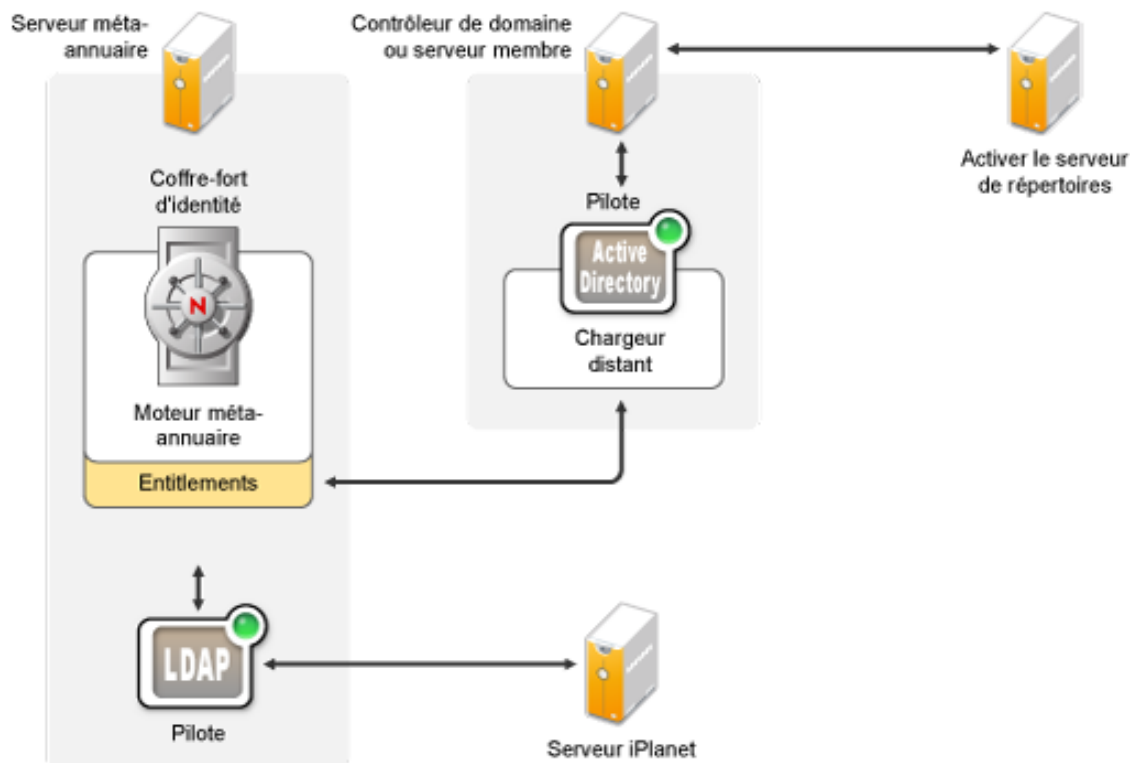
Liste de vérification pour un système Identity Manager de base

4

Il existe différentes méthodes pour configurer Identity Manager afin de profiter de toutes ses caractéristiques. La [Figure 4-1](#) représente une configuration de base d'Identity Manager. Cette configuration assure le provisioning des utilisateurs en synchronisant des données. Peu importe la configuration d'Identity Manager, vous commencez toujours par un système de base.

Pour configurer votre système Identity Manager, utilisez cette liste : vous vous assurez ainsi que toutes les étapes ont été réalisées.

Figure 4-1 Système Identity Manager de base



- ♦ [Section 4.1, « Conditions préalables », page 42](#)
- ♦ [Section 4.2, « Planification », page 42](#)
- ♦ [Section 4.3, « Installation », page 42](#)
- ♦ [Section 4.4, « Configuration du pilote avec le chargeur distant », page 43](#)
- ♦ [Section 4.5, « Configuration de pilotes sans chargeur distant », page 43](#)
- ♦ [Section 4.6, « Configuration supplémentaire », page 44](#)

4.1 Conditions préalables

- ❑ Vérifiez que votre système répond à la configuration système requise définie au [Chapitre 6](#), « Configuration système requise », page 49.

4.2 Planification

La planification est essentielle pour réussir la mise en place et le déploiement d'Identity Manager.

- ❑ Créez un environnement de développement. Il est important d'avoir accès à un système Identity Manager pour valider votre solution Identity Manager. Vous devrez réaliser l'ensemble des tests et des développements dans l'environnement de développement avant de changer d'environnement de production. Pour plus d'informations, reportez-vous au [Chapitre 1](#), « Mise en place d'un environnement de développement », page 13.
- ❑ Créez un plan de projet pour déployer Identity Manager. Le plan de projet passe par la définition de vos principaux processus d'entreprise, la création d'une solution Identity Manager qui automatise ces processus et l'établissement d'un plan de mise en œuvre technique. Pour réussir le déploiement d'Identity Manager, vous devez appliquer un plan de projet. Pour plus d'informations, reportez-vous au [Chapitre 2](#), « Création d'un plan de projet », page 15.
- ❑ Une fois le plan de projet créé, utilisez Analyzer pour nettoyer et préparer vos données en vue de leur synchronisation. Pour plus d'informations, reportez-vous au manuel *Analyzer 1.2 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 1.2 pour Identity Manager).

4.3 Installation

- ❑ Installez Analyzer. Pour plus d'informations, reportez-vous à la [Section 7.1](#), « Installation d'Analyzer », page 59.
- ❑ Installez Designer. Pour plus d'informations, reportez-vous à la [Section 7.2](#), « Installation de Designer », page 60.
- ❑ Installez eDirectory. Pour plus d'informations, reportez-vous à la [Section 7.3](#), « Installation d'eDirectory », page 60.
- ❑ Installez iManager. Pour plus d'informations, reportez-vous à la [Section 7.4](#), « Installation d'iManager », page 61.
- ❑ Installez le serveur et les pilotes méta-annuaire. Pour plus d'informations, reportez-vous au [Chapitre 7](#), « Installation d'Identity Manager », page 59.
- ❑ Activez Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 8](#), « Activation des produits Novell Identity Manager », page 75.
- ❑ (Facultatif) Concevez et créez les droits pour votre système Identity Manager.

Les droits représentent un ensemble de critères définis pour une personne ou un groupe, pouvant être appliqués à plusieurs pilotes. Une fois les critères réalisés, les droits lancent un événement pour accorder ou révoquer l'accès à des ressources d'activité. Les droits ajoutent un niveau supplémentaire de contrôle et d'automatisation, pour accorder ou révoquer des ressources.

Le principal avantage des droits est qu'ils permettent de créer et de définir une logique métier, puis de l'appliquer à plusieurs pilotes. Pour apporter un changement, vous procédez dans le droit plutôt que dans chaque pilote.

Les droits sont mis en place grâce à trois agents :

- ♦ Les droits basés sur les rôles utilisant le pilote de service des Droits
- ♦ Workflow
- ♦ Module de provisioning basé sur les rôles

Pour plus d'informations sur les droits, reportez-vous au manuel *Identity Manager 4.0 Entitlements Guide* (Guide des droits d'Identity Manager 4.0).

4.4 Configuration du pilote avec le chargeur distant

Le chargeur distant permet de synchroniser des informations avec un système connecté, sans installer eDirectory sur le système connecté. Le chargeur distant synchronise les informations sur le serveur méta-annuaire, qui conserve les données dans le coffre-fort d'identité. Identity Manager utilise eDirectory comme coffre-fort d'identité.

- Installez le chargeur distant sur une machine qui communique avec le système connecté. Le chargeur distant assure la communication entre le système connecté et le serveur méta-annuaire, et permet à Identity Manager de communiquer avec une machine sur laquelle eDirectory n'est pas installé. Pour plus d'informations, reportez-vous à la section « [Installing the Remote Loader](#) » (Installation du chargeur distant) du manuel *Identity Manager 4.0 Remote Loader Guide* (Guide du chargeur distant d'Identity Manager 4.0).
- Configurez le chargeur distant pour un pilote. Vous définissez une instance spécifique du chargeur distant pour communiquer avec un pilote spécifique. Pour plus d'informations, reportez-vous à la section « [Configuring the Remote Loader](#) » (Configuration du chargeur distant) du manuel *Identity Manager 4.0 Remote Loader Guide* (Guide du chargeur distant d'Identity Manager 4.0).
- Configurez le pilote pour qu'il communique avec le chargeur distant. Il existe un guide pour chaque pilote. Pour obtenir des informations spécifiques sur votre pilote, reportez-vous au [site Web de documentation des pilotes Identity Manager 4.0](http://www.novell.com/documentation/idm40drivers/) (<http://www.novell.com/documentation/idm40drivers/>).
- (Facultatif) Activez les droits sur le pilote. Vérifiez que vous disposez des bonnes stratégies pour exécuter le droit. Pour plus d'informations, reportez-vous au manuel *Identity Manager 4.0 Entitlements Guide* (Guide des droits d'Identity Manager 4.0).
- Répétez ces étapes pour chaque pilote de votre environnement.

4.5 Configuration de pilotes sans chargeur distant

- Créez et configurez votre pilote. Il existe un guide pour chaque pilote. Pour obtenir des informations spécifiques sur votre pilote, reportez-vous au [site Web de documentation des pilotes Identity Manager 4.0](http://www.novell.com/documentation/idm40drivers/) (<http://www.novell.com/documentation/idm40drivers/>).
- (Facultatif) Activez les droits sur le pilote. Vérifiez que vous disposez des bonnes stratégies pour exécuter le droit. Pour plus d'informations, reportez-vous au manuel *Identity Manager 4.0 Entitlements Guide* (Guide des droits d'Identity Manager 4.0).
- Répétez ces étapes pour chaque pilote de votre environnement.

4.6 Configuration supplémentaire

Lorsque le système Identity Manager est installé et configuré, vous pouvez ajouter les fonctions suivantes :

- ❑ **Gestion des mots de passe** : si vous souhaitez gérer des mots de passe avec Identity Manager, la procédure de configuration est un peu plus longue. Utilisez la « [Password Management Checklist](#) » (Liste de vérification de gestion des mots de passe) du manuel *Identity Manager 4.0 Password Management Guide* (Guide de gestion des mots de passe d'Identity Manager 4.0) pour vérifier que toutes les étapes de configuration sont réalisées.
- ❑ **Gestion des rôles** : si vous souhaitez gérer des rôles dans différents systèmes depuis un seul et même emplacement, utilisez l'administrateur d'assignation de rôles, un outil intégré à Identity Manager. Ce dernier permet d'assigner des rôles métier d'un système à un autre, sans devoir comprendre l'infrastructure informatique. Pour plus d'informations, reportez-vous au manuel *Identity Manager Role Mapping Administrator 2.0 Installation and Configuration Guide* (Guide d'installation et de configuration de la version 2.0 de l'administrateur d'assignation de rôles d'Identity Manager).
- ❑ **Provisioning basé sur les rôles** : pour ajouter la fonction de provisioning basé sur les rôles à votre solution Identity Manager, utilisez la « [Liste de contrôle de l'installation](#) » du *Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0* afin de vérifier que toutes les étapes de configuration sont réalisées.
- ❑ **Audit et création de rapports** : l'ajout de la fonction d'audit et de création de rapports à votre solution Identity Manager vous permet de vérifier que vos stratégies métier sont conformes aux stratégies de l'entreprise. Vous pouvez ajouter le module Identity Reporting ou Novell Sentinel à votre solution Identity Manager pour l'audit et la création de rapports. Pour plus d'informations sur le module Identity Reporting, reportez-vous au manuel *Identity Reporting Module Guide* (Guide du module Identity Reporting). Pour plus d'informations sur Novell Sentinel, reportez-vous au manuel *Identity Manager 4.0 Reporting Guide for Novell Sentinel* (Guide de création de rapports Identity Manager 4.0 pour Novell Sentinel).

Où se procurer Identity Manager

5

Vous pouvez télécharger une version d'évaluation d'Identity Manager et l'utiliser gratuitement pendant 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. Vous pouvez acquérir une licence produit et activer Identity Manager à tout moment, que ce soit pendant ou après cette période de 90 jours. Pour plus d'informations, reportez-vous au [Chapitre 8, « Activation des produits Novell Identity Manager », page 75](#).

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 de téléchargements Novell Identity Manager, cliquez sur le bouton *Télécharger* en regard du fichier souhaité. Le [Tableau 5-1](#) contient une description de chaque fichier.
Sélectionnez l'image ISO adaptée à vos besoins. Chaque image ISO contient les versions 32 et 64 bits du produit.
- 4 Suivez les instructions à l'écran pour télécharger le fichier vers un répertoire de votre ordinateur.
- 5 Répétez l'[Étape 3](#) jusqu'à ce que vous ayez téléchargé tous les fichiers dont vous avez besoin.
- 6 Montez ensuite le fichier `.iso` téléchargé en tant que volume ou utilisez le fichier `.iso` pour créer un DVD du logiciel. Si vous n'avez pas encore vérifié que le support gravé est valide, vous pouvez le faire à l'aide de l'option *Vérification du support*.

Tableau 5-1 Images ISO d'Identity Manager

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

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

- ♦ **Pilotes de service** : la liste suivante répertorie les pilotes de service qui 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 tâches manuelles
 - ♦ Service nul
 - ♦ Service de rôles et de ressources
 - ♦ Application utilisateur
 - ♦ Bon de travail
- ♦ **Pilotes communs** : la liste suivante répertorie les pilotes communs qui sont activés en même temps que le serveur méta-annuaire :
 - ♦ Active Directory
 - ♦ ADAM
 - ♦ eDirectory
 - ♦ GroupWise
 - ♦ LDAP
 - ♦ Lotus Notes

Les références d'activation de tous les autres pilotes Identity Manager doivent être achetées séparément. Les références d'activation des pilotes sont vendues en tant que modules d'intégration d'Identity Manager. Ces derniers peuvent contenir un ou plusieurs pilotes. Pour chaque module d'intégration d'Identity Manager acheté, vous recevez une référence d'activation du produit. Pour plus d'informations, reportez-vous à la [page Web des pilotes Identity Manager \(http://www.novell.com/products/identitymanager/drivers/\)](http://www.novell.com/products/identitymanager/drivers/).

Le module de provisioning basé sur les rôles de l'application utilisateur est inclus avec le produit Identity Manager que vous achetez. Il ajoute un puissant workflow d'approbation basé sur les rôles qui vous aide à gérer les identités de vos utilisateurs.

Votre produit Identity Manager inclut également plusieurs outils vous permettant de concevoir, de créer et de gérer votre solution Identity Manager :

- ♦ Analyzer
- ♦ Designer
- ♦ iManager
- ♦ Administrateur d'assignation de rôles

Le module Identity Reporting est un autre composant d'Identity Manager qui vous permet d'auditer et de générer des rapports sur votre solution Identity Manager. Vous pouvez utiliser ces rapports pour aider votre entreprise à respecter les normes de conformité qu'elle doit observer.

Pour plus d'informations sur les composants d'Identity Manager, reportez-vous au guide *Présentation d'Identity Manager 4.0*.

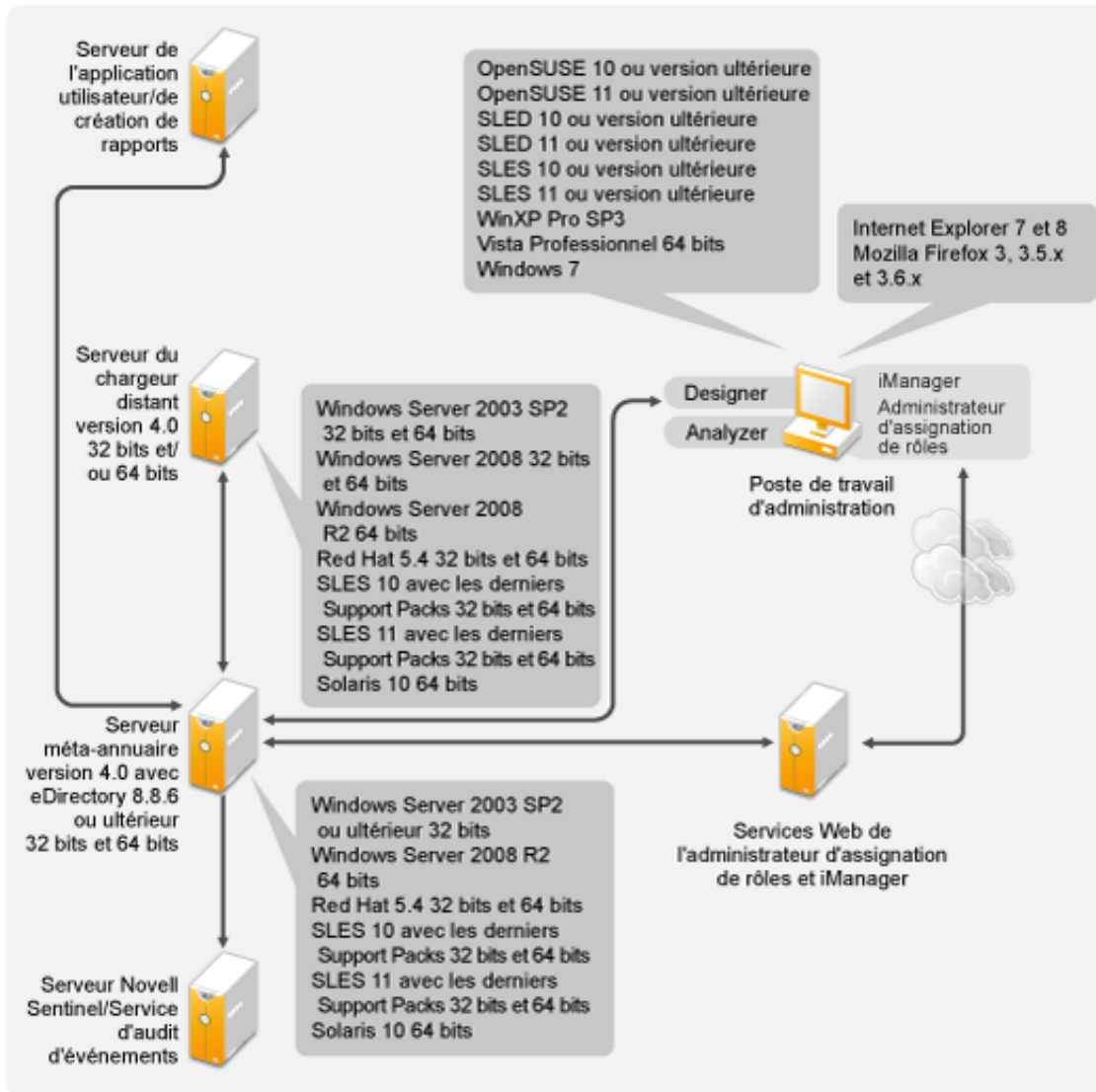
Configuration système requise

6

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

La [Figure 6-1](#) montre les plates-formes et les systèmes pris en charge.

Figure 6-1 Configuration système pour les composants Identity Manager



Selon la configuration de votre système, vous devrez peut-être exécuter le programme d'installation Identity Manager plusieurs fois pour installer les composants d'Identity Manager sur les systèmes adéquats.

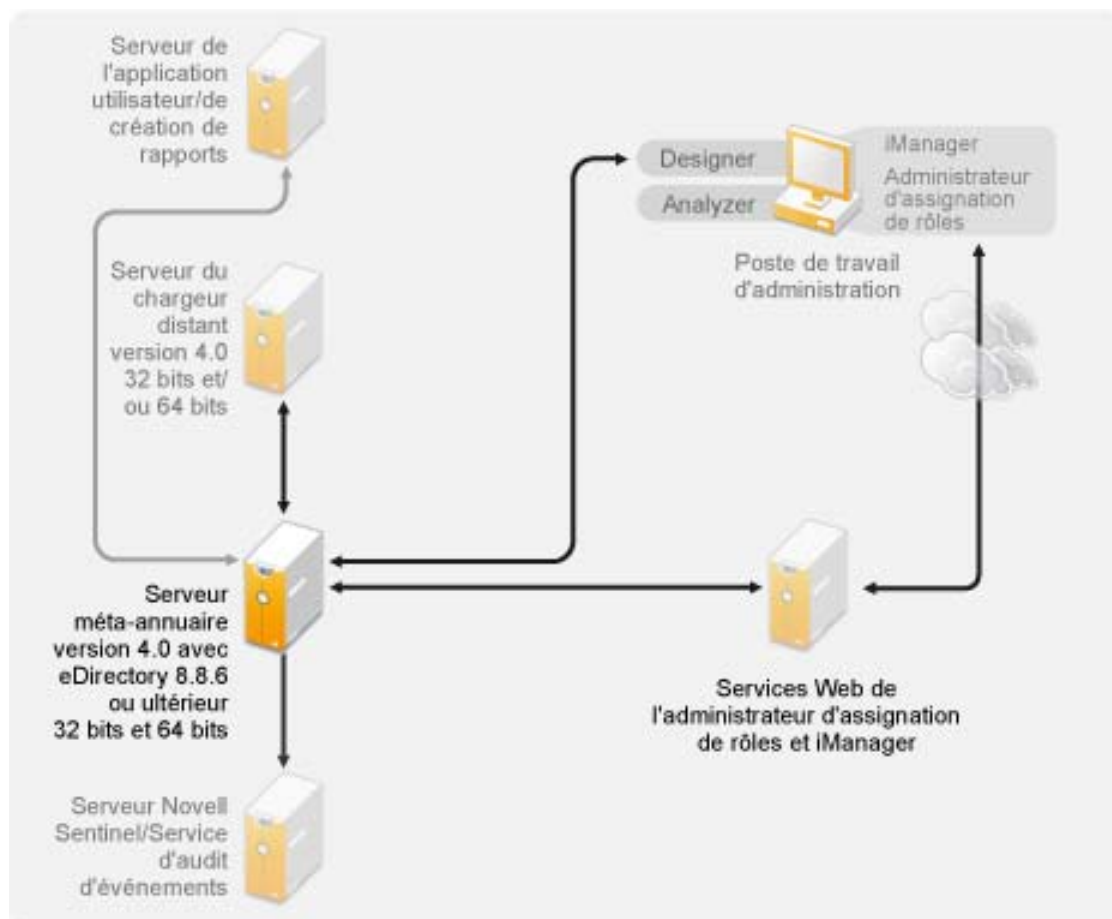
- ♦ [Section 6.1, « eDirectory et iManager », page 50](#)
- ♦ [Section 6.2, « Serveur méta-annuaire », page 51](#)

- ♦ Section 6.3, « Chargeur distant », page 53
- ♦ Section 6.4, « Application utilisateur », page 55
- ♦ Section 6.5, « Audit et création de rapports », page 56
- ♦ Section 6.6, « Postes de travail », page 57

6.1 eDirectory et iManager

Identity Manager nécessite l'installation d'eDirectory et d'iManager. Ces produits constituent la base d'Identity Manager et sont inclus dans l'image ISO d'Identity Manager Advanced Edition. La [Figure 6-2](#) illustre ces composants.

Figure 6-2 Produits de base pour Identity Manager



Vous devez disposer des versions suivantes de ces produits :

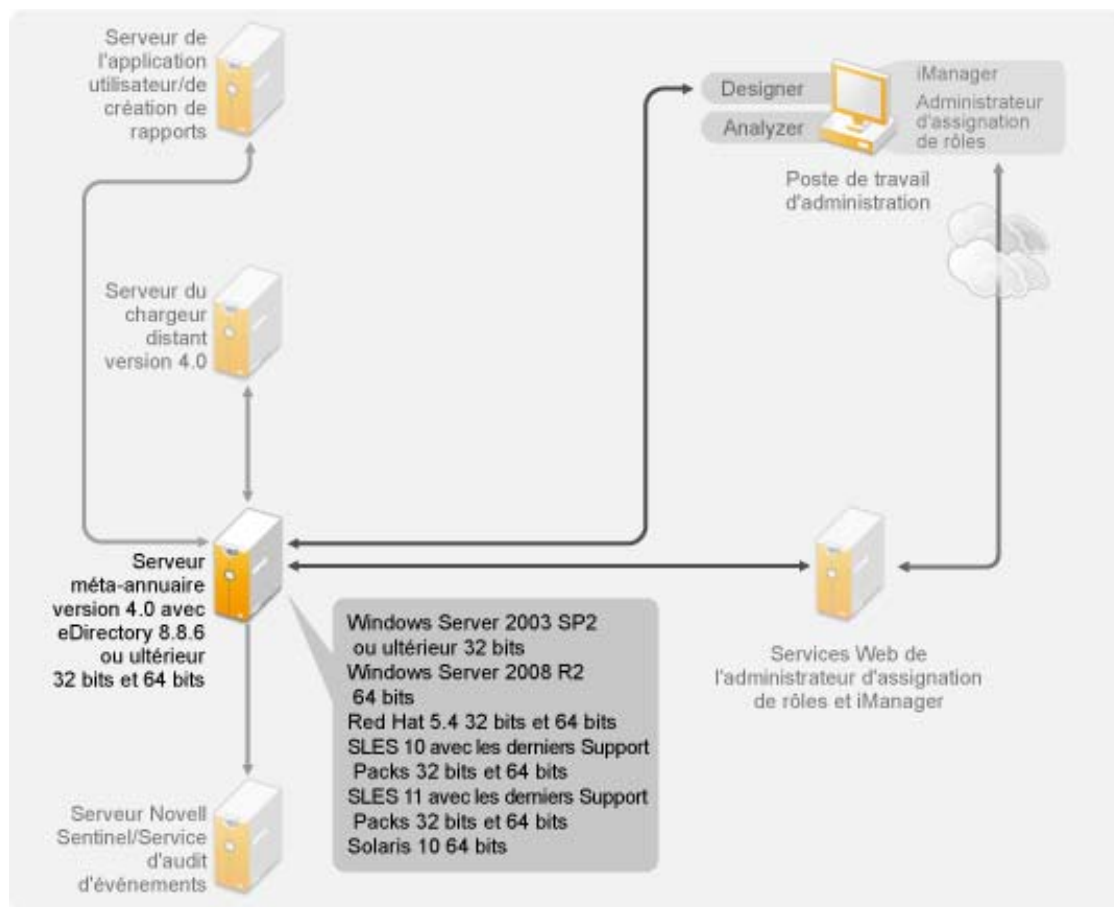
- ♦ eDirectory 8.8.6 ou version ultérieure (32 ou 64 bits)
- ♦ iManager 2.7.4

Pour plus d'informations sur la configuration système requise pour eDirectory, reportez-vous au *Guide d'installation de Novell eDirectory 8.8* (<http://www.novell.com/documentation/edir88/index.html>). Pour plus d'informations sur la configuration système d'iManager, reportez-vous au *Guide d'installation d'iManager 2.7* (<http://www.novell.com/documentation/imanager27/index.html>).

6.2 Serveur méta-annuaire

Le serveur méta-annuaire traite les événements des lecteurs, qu'ils soient configurés avec le chargeur distant ou non. Pour obtenir la liste des systèmes d'exploitation pris en charge, reportez-vous à la [Figure 6-3](#).

Figure 6-3 Systèmes d'exploitation pris en charge pour le serveur méta-annuaire



Pendant l'installation du serveur méta-annuaire, le programme d'installation détecte la version d'eDirectory installée.

Remarque : si eDirectory 8.8.6 ou version ultérieure (32 ou 64 bits) n'est pas installé, le programme d'installation s'interrompt.

- ♦ [Section 6.2.1, « Processeurs pris en charge », page 52](#)
- ♦ [Section 6.2.2, « Systèmes d'exploitation du serveur », page 52](#)

6.2.1 Processeurs pris en charge

Les processeurs listés ici sont utilisés pour le test d'Identity Manager. Le processeur SPARC est utilisé pour les tests de Solaris.

Les processeurs 32 bits pris en charge pour les systèmes d'exploitation Linux (Red Hat et SUSE Linux Enterprise Server) et Windows sont les suivants :

- ◆ Intel x86-32
- ◆ AMD x86-32

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

- ◆ Intel EM64T
- ◆ AMD Athlon64
- ◆ AMD Opteron

Les Support Packs les plus récents doivent être installés sur tous les systèmes d'exploitation.

6.2.2 Systèmes d'exploitation du serveur

Vous pouvez installer le serveur méta-annuaire en tant qu'application 32 bits sur un système d'exploitation 64 bits. Le [Tableau 6-1](#) contient une liste des systèmes d'exploitation du serveur pris en charge sur lesquels le serveur méta-annuaire peut s'exécuter.

Tableau 6-1 *Systèmes d'exploitation pris en charge pour le serveur*

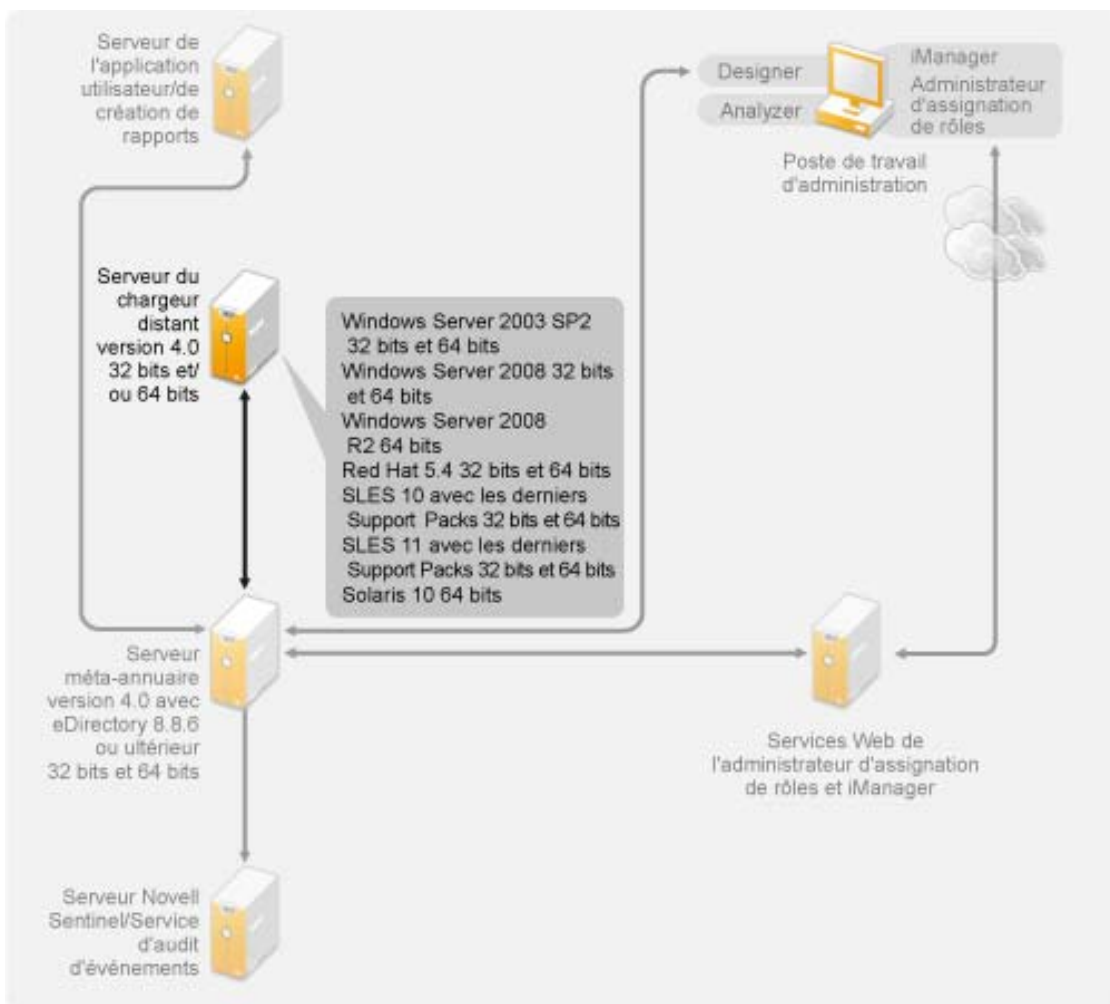
Version du système d'exploitation du serveur	Notes
Windows Server 2003 SP2 ou version ultérieure (32 bits)	Le serveur méta-annuaire s'exécute uniquement en mode 32 bits.
Windows Server 2008 R2 (64 bits)	Le serveur méta-annuaire s'exécute uniquement en mode 64 bits.
Red Hat 5.4 (32 et 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits. Novell vous recommande d'appliquer les derniers correctifs de système d'exploitation en passant par le service des mises à jour automatisé avant d'installer Identity Manager.
SUSE Linux Enterprise Server 10 SP3 ou Support Packs ultérieurs (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.

Version du système d'exploitation du serveur	Notes
SUSE Linux Enterprise Server 11 ou Support Packs ultérieurs (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.
Zones Solaris 10	Le serveur méta-annuaire s'exécute uniquement en mode 64 bits.
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.
VMware ESX	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.
Virtualisation de Red Hat Enterprise Linux 5	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.
Virtualisation avec Hyper-V de Windows Server 2008 R2	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.

6.3 Chargeur distant

Le chargeur distant vous apporte de la flexibilité pour la configuration de votre solution Identity Manager. Il offre une prise en charge 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.

Figure 6-4 Systèmes d'exploitation pris en charge pour le chargeur distant



Si vous installez le serveur méta-annuaire en tant qu'application 32 bits sur un système d'exploitation 64 bits, vous pouvez installer un chargeur distant 32 bits et un chargeur distant 64 bits sur la même machine.

Le [Tableau 6-2](#) liste les systèmes d'exploitation pris en charge pour le chargeur distant.

Tableau 6-2 Systèmes d'exploitation pris en charge pour le chargeur distant

Version du système d'exploitation du serveur	Notes
Windows Server 2003 SP2 ou version ultérieure (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
Windows Server 2008 SP1 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
Windows Server 2008 R2 (64 bits)	Le chargeur distant s'exécute uniquement en mode 64 bits.

Version du système d'exploitation du serveur	Notes
Red Hat 5.4 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits. Avant d'installer Identity Manager, Novell recommande d'appliquer les derniers correctifs de système d'exploitation à l'aide du service de mise à jour automatique du fabricant.
SUSE Linux Enterprise Server 10 SP3 ou Support Packs ultérieurs (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits. Avant d'installer Identity Manager, Novell recommande d'appliquer les derniers correctifs de système d'exploitation à l'aide du service de mise à jour automatique du fabricant.
SUSE Linux Enterprise Server 11 ou Support Packs ultérieurs (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits. Avant d'installer Identity Manager, Novell recommande d'appliquer les derniers correctifs de système d'exploitation à l'aide du service de mise à jour automatique du fabricant.
Solaris 10 (64 bits)	Le chargeur distant s'exécute uniquement en mode 64 bits.
Zones Solaris 10	Le chargeur distant s'exécute uniquement en mode 64 bits.
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.
VMware ESX (64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
Virtualisation de Red Hat Enterprise Linux 5 (64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
Virtualisation avec Hyper-V de Windows Server 2008 R2	Le chargeur distant s'exécute en mode 32 et 64 bits.

Le chargeur distant Java est pris en charge sur les plates-formes sur lesquelles le chargeur distant natif n'est pas disponible. Le chargeur distant .NET est pris en charge sur la plate-forme .NET version 2.

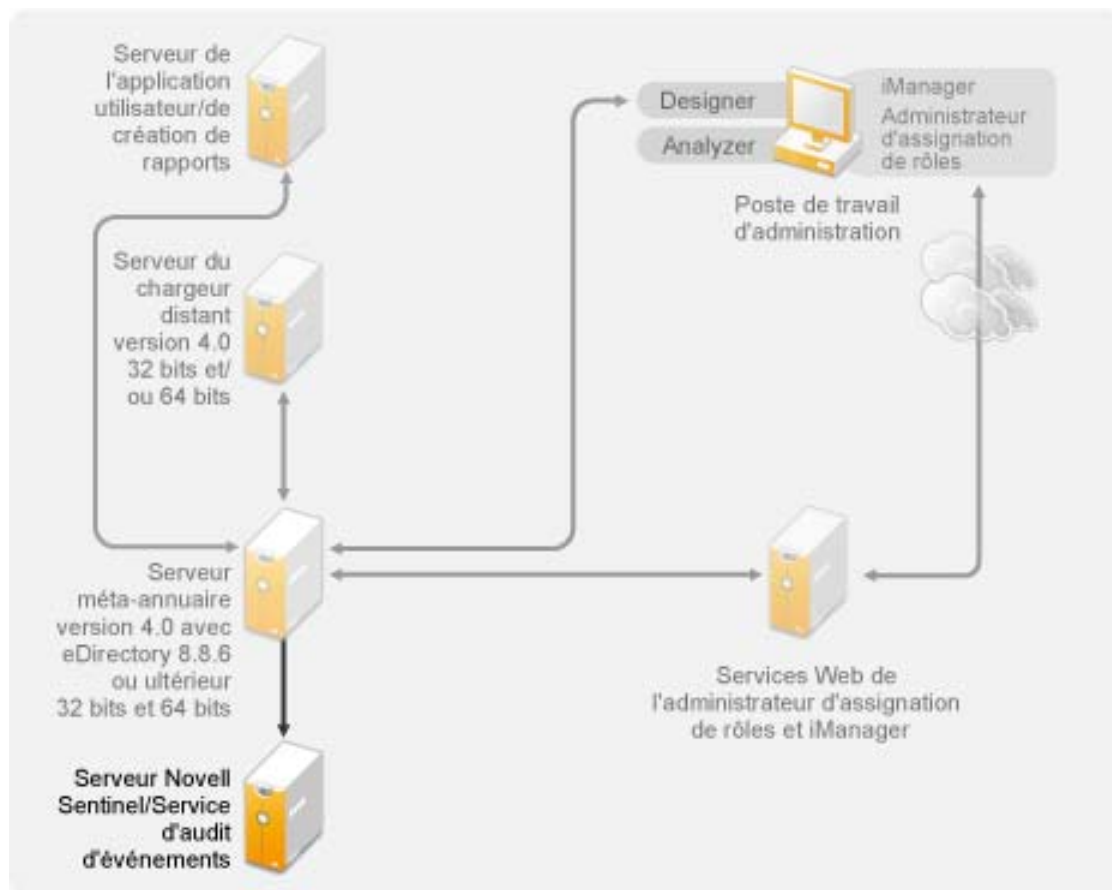
6.4 Application utilisateur

Pour connaître la configuration système requise pour l'application utilisateur, reportez-vous au [Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0](#).

6.5 Audit et création de rapports

Le module Identity Reporting et Novell Sentinel sont deux outils qui permettent de rassembler des informations d'audit et de création de rapports sur Identity Manager. La [Figure 6-5](#) montre la version de Sentinel prise en charge avec Identity Manager 4.0.

Figure 6-5 Sentinel



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

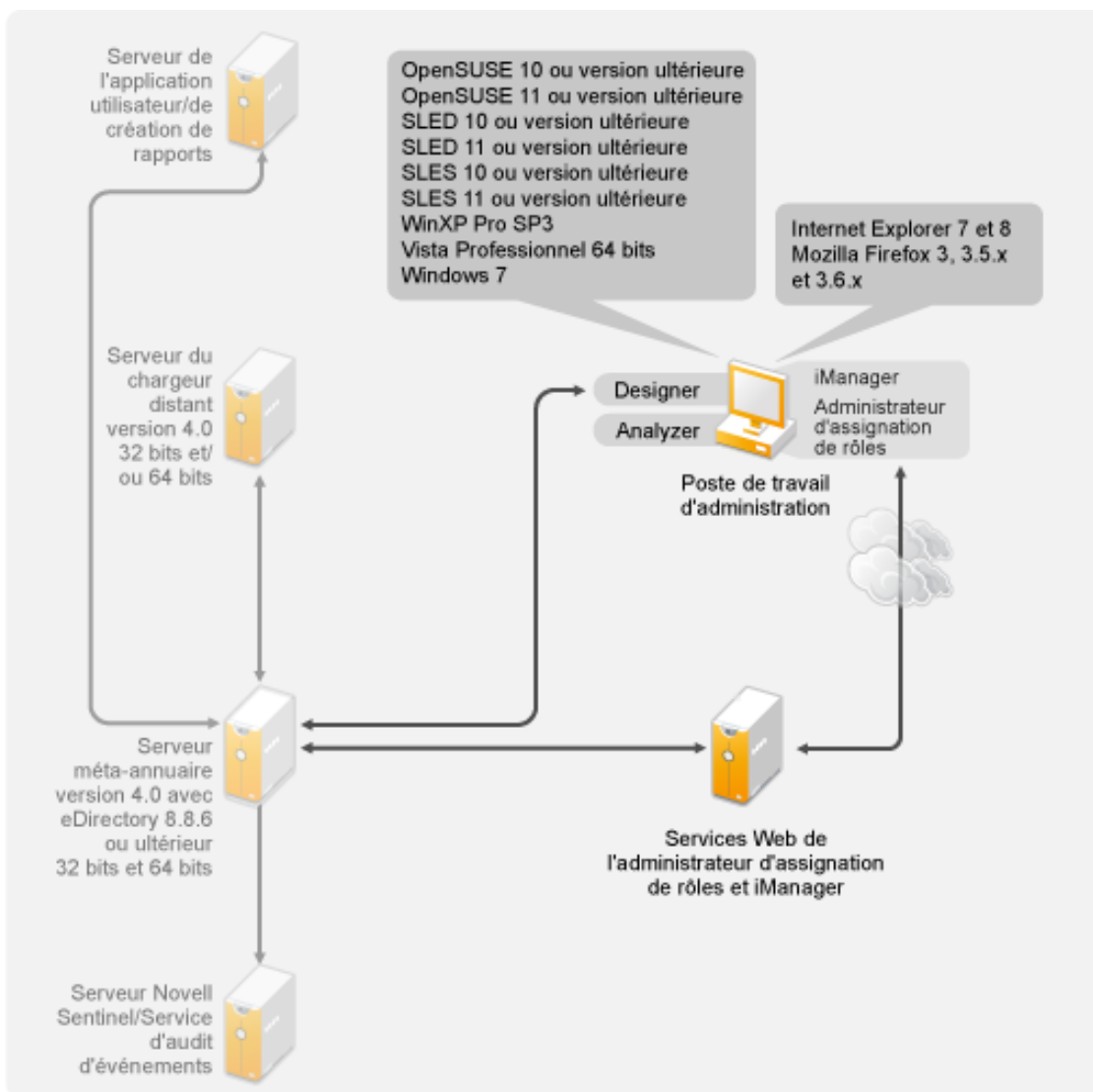
L'ajout des fonctions d'audit et de création de rapports permet de respecter les normes de conformité que de nombreuses sociétés doivent observer. Vous pouvez créer des suivis d'audit pour les événements que vous devez suivre, ainsi que générer des rapports pour respecter les normes d'audit de votre société.

Pour plus d'informations sur la configuration système requise et la configuration du module Identity Reporting, reportez-vous au manuel [Identity Reporting Module Guide](#) (Guide du module Identity Reporting). Pour plus d'informations sur la configuration de Sentinel avec Identity Manager, reportez-vous au manuel [Identity Manager 4.0 Reporting Guide for Novell Sentinel](#) (Guide de création de rapports Identity Manager 4.0 pour Novell Sentinel). Pour plus d'informations sur la configuration système de 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>).

6.6 Postes de travail

Les postes de travail permettent d'accéder à Designer, à iManager, à l'administrateur d'assignation de rôles ou à la page Web d'administration de l'application utilisateur. La [Figure 6-6](#) montre les différents composants des postes de travail qui sont pris en charge avec Identity Manager 4.0.

Figure 6-6 Composants pris en charge pour les postes de travail



Trois éléments différents affectent les postes de travail :

- ♦ [Section 6.6.1, « Plates-formes des postes de travail », page 58](#)
- ♦ [Section 6.6.2, « Navigateurs Web », page 58](#)
- ♦ [Section 6.6.3, « Ressources requises », page 58](#)

6.6.1 Plates-formes des postes de travail

Le [Tableau 6-3](#) contient une liste des plates-formes de postes de travail prises en charge pour Designer et iManager.

Tableau 6-3 *Plates-formes de poste de travail prises en charge*

Plates-formes	Détails
Windows 7	
Windows Vista	Seule l'Édition Professionnelle 64 bits est prise en charge.
Windows XP Professionnel SP3	
openSUSE 10 et 11	Appliquez les derniers correctifs à l'aide du système de mise à jour automatique.
SUSE Linux Enterprise Desktop 10 SP1 et SP2	Appliquez les derniers correctifs à l'aide du système de mise à jour automatique.
SUSE Linux Enterprise Server 10 SP1 et SP2	Appliquez les derniers correctifs à l'aide du système de mise à jour automatique.

6.6.2 Navigateurs Web

iManager exécute tous les plug-ins nécessaires à l'administration d'Identity Manager.

L'administrateur d'assignation de rôles permet d'assigner des rôles métier dans différents systèmes, sans devoir comprendre l'infrastructure informatique. Vous pouvez accéder à ces deux applications via un navigateur Web.

Les navigateurs Web pris en charge pour iManager et l'administrateur d'assignation de rôles sont les suivants :

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

6.6.3 Ressources requises

- ♦ 2048 Mo de RAM au minimum.
- ♦ 3 Go d'espace disque disponible pour pouvoir installer tous les composants.
- ♦ 20 Go supplémentaires pour configurer et charger les données. La quantité nécessaire peut varier en fonction de vos systèmes connectés.
- ♦ De préférence un serveur multiprocesseur avec un processeur de 2 GHz.
- ♦ 64 Mo de mémoire de tas au minimum.

Installation d'Identity Manager

7

Identity Manager inclut un programme d'installation intégré qui simplifie le processus d'installation en installant et configurant tous les composants en même temps. Si c'est la première fois que vous installez un système Identity Manager, utilisez le programme d'installation intégré. Pour plus d'informations, reportez-vous au [Guide du programme d'installation intégré d'Identity Manager 4.0](#).

Si vous êtes familiarisé à Identity Manager et souhaitez installer chaque élément séparément, Identity Manager propose des programmes d'installation distincts pour les différents composants.

Il importe d'installer et d'utiliser Analyzer et Designer pendant la phase de planification de la mise en œuvre d'Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 2, « Création d'un plan de projet », page 15](#).

Installez les composants dans l'ordre indiqué ci-après. Pour obtenir des explications sur les différents composants, reportez-vous au manuel [Présentation d'Identity Manager 4.0](#).

- ♦ [Section 7.1, « Installation d'Analyzer », page 59](#)
- ♦ [Section 7.2, « Installation de Designer », page 60](#)
- ♦ [Section 7.3, « Installation d'eDirectory », page 60](#)
- ♦ [Section 7.4, « Installation d'iManager », page 61](#)
- ♦ [Section 7.5, « Installation du serveur méta-annuaire », page 61](#)
- ♦ [Section 7.6, « Installation du chargeur distant », page 66](#)
- ♦ [Section 7.7, « Installation du module de provisioning basé sur les rôles », page 71](#)
- ♦ [Section 7.8, « Installation d'un pilote personnalisé », page 71](#)
- ♦ [Section 7.9, « Installation de l'administrateur d'assignation de rôles », page 71](#)
- ♦ [Section 7.10, « Installation du module Identity Reporting ou de Sentinel », page 72](#)
- ♦ [Section 7.11, « Installation d'Identity Manager dans un environnement en grappe », page 73](#)

7.1 Installation d'Analyzer

Outil basé sur le poste de travail, Analyzer vous permet d'analyser, de nettoyer et de préparer vos données en vue de leur synchronisation avec Identity Manager. Installez Analyzer et utilisez-le durant toute la phase de planification de la mise en œuvre de votre solution Identity Manager. Pour plus d'informations sur la planification, reportez-vous à la [Partie I, « Planification », page 11](#).

- 1** Vérifiez que le système d'exploitation de votre poste de travail est bien pris en charge.
Pour plus d'informations, reportez-vous à la [Section 6.6, « Postes de travail », page 57](#).
- 2** Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager », page 45](#).
- 3** Lancez l'installation en exécutant le programme adapté à la plate-forme de votre poste de travail.
 - ♦ **Linux :** `IDM4.0_Lin/products/Analyzer/install`
Pour exécuter le fichier binaire, saisissez `./install`.

- ♦ **Windows** : IDM4.0_Win:/products/Analyzer/install.exe
- 4 Complétez les informations suivantes pour terminer l'installation :
- ♦ **Emplacement d'installation** : indiquez l'emplacement d'installation d'Analyzer sur le poste de travail.
 - ♦ **Créer des raccourcis et sélectionner une langue** : indiquez si vous souhaitez créer des raccourcis pour Analyzer sur le bureau et sélectionnez la langue d'installation d'Analyzer.

Analyzer est maintenant installé. La première fois que vous le lancez, vous êtes invité à l'activer. Tant que vous ne l'avez pas activé, vous ne pouvez pas l'utiliser. Pour plus d'informations, reportez-vous au [Chapitre 8, « Activation des produits Novell Identity Manager », page 75](#).

7.2 Installation de Designer

Outil basé sur le poste de travail, Designer vous permet de concevoir votre solution Identity Manager. Installez Designer et utilisez-le durant toute la phase de planification de la mise en œuvre de votre solution Identity Manager. Pour plus d'informations sur la planification, reportez-vous à la [Partie I, « Planification », page 11](#).

- 1 Vérifiez que le système d'exploitation de votre poste de travail est bien pris en charge. Pour plus d'informations, reportez-vous à la [Section 6.6, « Postes de travail », page 57](#).
- 2 Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager », page 45](#).
- 3 Lancez l'installation en exécutant le programme adapté à la plate-forme de votre poste de travail.
 - ♦ **Linux** : IDM4.0_Lin/products/Designer/install
Pour exécuter le fichier binaire, saisissez ./install.
 - ♦ **Windows** : IDM4.0_Win:\products\Designer\install.exe
- 4 Les informations suivantes permettent de terminer l'installation :
 - ♦ **Dossier d'installation** : indiquez l'emplacement d'installation de Designer sur le poste de travail.
 - ♦ **Créer les raccourcis** : choisissez les raccourcis placés sur votre bureau et dans le menu du bureau.

Pour en savoir plus, reportez-vous au manuel [Designer 4.0 for Identity Manager 4.0 Administration Guide](#) (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

7.3 Installation d'eDirectory

Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager », page 45](#).

eDirectory 8.8.6 est inclus sur le support d'Identity Manager. Des programmes d'installation sont disponibles pour les plates-formes 32 et 64 bits. L'emplacement du programme d'installation dépend de la plate-forme :

- ♦ **Linux 32 bits** : IDM4.0_Lin/products/eDirectory/x86/setup/nds-install

- ♦ **Linux 64 bits** : `IDM4.0_Lin/products/eDirectory/x64/setup/nds-install`
- ♦ **Solaris 32 bits** : `IDM4.0_Solaris/products/eDirectory/x86/setup/nds-install`
- ♦ **Solaris 64 bits** : `IDM4.0_Solaris/products/eDirectory/x64/setup/nds-install`
Pour exécuter le fichier binaire, saisissez `./nds-install`.
- ♦ **Windows 32 bits** : `IDM4.0_Win:\products\eDirectory\x86\nt\Setup.exe`
- ♦ **Windows 64 bits** : `IDM4.0_Win:\products\eDirectory\x64\windows\Setup.exe`

La procédure d'installation d'eDirectory varie d'une plate-forme à l'autre. Pour connaître la procédure d'installation adaptée à votre plate-forme, reportez-vous à la section correspondante du [Guide d'installation de Novell eDirectory 8.8](http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html) (<http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html>).

Remarque : sur les plates-formes Linux et Solaris, vous devez installer et configurer eDirectory avant de pouvoir installer le serveur méta-annuaire. Pour connaître la procédure de configuration, reportez-vous à la section « [Configuration de Novell eDirectory sur les systèmes Linux, Solaris ou AIX](http://www.novell.com/documentation/edir88/edirin88/data/bnn8z89.html) » (<http://www.novell.com/documentation/edir88/edirin88/data/bnn8z89.html>) du *Guide d'installation de Novell eDirectory 8.8*.

7.4 Installation d'iManager

Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager », page 45](#).

iManager 2.7.4 est inclus sur le support d'Identity Manager. Des programmes d'installation sont disponibles pour les plates-formes Windows et Linux. iManager n'est pas pris en charge sur les plates-formes Solaris. L'emplacement du programme d'installation dépend de la plate-forme :

- ♦ **Linux** : `IDM4.0_Lin/products/iManager/installs/linux/iManagerInstallLinux.bin`
Pour exécuter le fichier binaire, saisissez `./iManagerInstallLinux.bin`.
- ♦ **Windows** : `IDM4.0_Win:\products\iManager\installs\win\iManagerInstall.exe`

La procédure d'installation d'iManager varie d'une plate-forme à l'autre. Pour connaître la procédure d'installation, reportez-vous à la section correspondante du [Guide d'installation d'iManager](http://www.novell.com/documentation/imanager27/imanager_install_27/data/hk42s9ot.html) (http://www.novell.com/documentation/imanager27/imanager_install_27/data/hk42s9ot.html).

7.5 Installation du serveur méta-annuaire

Sur les plates-formes Linux/UNIX, vous pouvez installer le serveur méta-annuaire en tant qu'utilisateur `root` ou `non-root`. Si vous utilisez l'installation `non-root`, la procédure est différente. Pour connaître la procédure d'installation, reportez-vous à la [Section 7.5.1, « Installation non-root du serveur méta-annuaire », page 63](#).

Cette procédure englobe l'installation du serveur méta-annuaire, des composants Web et des utilitaires pour les différentes plates-formes prises en charge par Identity Manager à l'aide de l'interface graphique. Si vous souhaitez installer ces composants en mode silencieux, reportez-vous à la [Section 7.5.2, « Installation en mode silencieux du serveur méta-annuaire », page 65](#).

- 1 Vérifiez que vous disposez de la configuration système requise indiquée au [Chapitre 6, « Configuration système requise », page 49](#).
- 2 Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager », page 45](#).
- 3 (Linux/UNIX uniquement) Pour vérifier que les variables d'environnement pour eDirectory sont exportées avant le début de l'installation sur Linux/UNIX, accédez à une invite de commande et saisissez :

```
set | grep PATH
```

Les variables d'environnement définissent le chemin pour l'installation eDirectory. Le chemin d'installation d'eDirectory est listé si les variables d'environnement sont définies. Si les variables d'environnement ne sont pas définies, l'installation d'Identity Manager échoue.

Pour définir les variables d'environnement pour votre shell actuel, saisissez :

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

Vous devez respecter l'espace entre le point (.) et la barre oblique (/) pour que la commande fonctionne. Pour davantage d'informations, reportez-vous à la page [Using the nds-install Utility to Install eDirectory Components \(http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#ai39feq\)](http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#ai39feq) (Utilisation de l'utilitaire nds-install pour installer les composants eDirectory).

- 4 Lancez l'installation à l'aide du programme adapté à votre plate-forme.
 - ♦ **Linux - installation à partir de l'interface graphique :** IDM4.0_Lin/products/IDM/install.bin [-i gui]
 - ♦ **Linux - installation à partir de la ligne de commande :** IDM4.0_Lin/products/IDM/install.bin -i console
 - ♦ **Solaris - installation à partir de l'interface graphique :** IDM4.0_Solaris/products/IDM/install.bin [-i gui]
 - ♦ **Solaris - installation à partir de la ligne de commande :** IDM4.0_Solaris/products/IDM/install.bin -i console

Pour exécuter les fichiers binaires sous Linux ou Solaris, saisissez ./install.bin [-i {gui | console}].

 - ♦ **Windows :** IDM4.0_Win:\products\IDM\windows\setup\idm_install.exe

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

- ♦ **Sélectionner les composants :** sélectionnez le serveur méta-annuaire, les plug-ins iManager et les utilitaires pour installer le serveur méta-annuaire.
 - ♦ **Serveur méta-annuaire de Novell Identity Manager :** cette option nécessite l'installation du coffre-fort d'identité sur ce serveur et installe la version 64 bits d'Identity Manager. Elle étend le schéma d'Identity Manager et installe le serveur méta-annuaire, les pilotes Identity Manager ainsi que Novell Audit Agent.

- ♦ **Serveur méta-annuaire de Novell Identity Manager (32 bits)** : cette option nécessite l'installation du coffre-fort d'identité sur ce serveur et installe la version 32 bits d'Identity Manager. Elle étend le schéma d'Identity Manager et installe le serveur méta-annuaire, les pilotes Identity Manager ainsi que Novell Audit Agent.
 - ♦ **Serveur de système connecté Novell Identity Manager (64 bits)** : cette option ne nécessite pas l'installation du coffre-fort d'identité sur ce serveur. Ne choisissez cette option que si vous installez le chargeur distant 64 bits. Pour plus d'informations, reportez-vous à la [Section 7.6, « Installation du chargeur distant », page 66](#).
 - ♦ **Serveur de système connecté Novell Identity Manager (.NET)** : cette option (Windows uniquement) installe le service de chargeur distant .NET et le pilote SharePoint sur ce serveur.
 - ♦ **Plug-ins Novell Identity Manager pour Identity Manager** : sélectionnez cette option si vous avez installé iManager sur ce serveur. Elle installe les plug-ins iManager pour Identity Manager.
 - ♦ **Utilitaires** : cette option installe les utilitaires servant à configurer les pilotes pour les systèmes connectés. Tous les pilotes n'ont pas d'utilitaires. Si vous n'êtes pas certain d'en avoir besoin, sélectionnez-les tout de même. Ils n'occupent pas beaucoup d'espace disque.
 - ♦ **Personnaliser les composants sélectionnés** : cette option permet de personnaliser les composants que vous avez choisi d'installer. Avant de la sélectionner, vous devez choisir les composants à installer.
 - ♦ **Authentification** : spécifiez un utilisateur et un mot de passe disposant de droits suffisants dans eDirectory pour prolonger le schéma. Indiquez le nom d'utilisateur au format LDAP. Par exemple, `cn=idmadmin,o=company`
- 6** Activez Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 8, « Activation des produits Novell Identity Manager », page 75](#).
- 7** Créez et configurez vos objets de pilotes. Ces informations figurent dans le guide de chaque pilote. Pour plus d'informations, reportez-vous à la [documentation des pilotes Identity Manager \(http://www.novell.com/documentation/idm40drivers/\)](#).

7.5.1 Installation non-root du serveur méta-annuaire

Vous pouvez installer Identity Manager en tant qu'utilisateur non-root afin d'améliorer la sécurité de votre serveur UNIX/Linux. Vous ne pouvez pas installer Identity Manager en tant qu'utilisateur non-root si eDirectory est installé par un utilisateur root.

Si vous optez pour l'installation non-root, les éléments suivants ne sont pas installés :

- ♦ **Chargeur distant** : utilisez le chargeur distant Java si vous devez installer le chargeur distant en tant qu'utilisateur non-root. Pour plus d'informations, reportez-vous à la [Section 7.6.5, « Installation du chargeur distant Java sous UNIX ou Linux », page 70](#).
- ♦ **Pilote du compte UNIX/Linux** : nécessite des privilèges root pour fonctionner.
- ♦ **Agent de la plate-forme Novell Sentinel** : vous devez installer l'agent de la plate-forme Novell Sentinel en tant qu'utilisateur root. Créez le fichier `Dirxml.properties` dans le répertoire `/etc/opt/novell/sentinelpa/conf`. Le répertoire dans lequel le fichier journal des événements est généré (`/var/opt/novell/sentinelpa/data/AuditEvents.log` est l'emplacement par défaut) doit être accessible en écriture à l'utilisateur non-root.

Pour exécuter l'installation non-root du serveur méta-annuaire, procédez comme suit :

- 1 Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager », page 45](#).
- 2 Installez eDirectory 8.8.6 ou version ultérieure en tant qu'utilisateur non-root. Pour plus d'informations, reportez-vous à la section « [Installation d'eDirectory 8.8.6 par un utilisateur non-root](http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs) » (<http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs>).
- 3 Loguez-vous sous l'identité de l'utilisateur non-root employé pour installer eDirectory.
Vous devez installer Identity Manager avec la même identité que celle employée pour installer la version non-root d'eDirectory. L'utilisateur qui installe Identity Manager doit disposer d'un accès en écriture aux répertoires et aux fichiers de l'installation non-root d'eDirectory.
- 4 Exécutez le programme d'installation pour votre plate-forme.
 - ♦ **Linux** : `IDM4.0_Lin/products/IDM/linux/setup/idm-nonroot-install`
 - ♦ **Solaris** : `IDM4.0_Solaris/products/IDM/solaris/setup/idm-nonroot-install`
Pour exécuter les fichiers de script, saisissez `./idm-nonroot-install`
- 5 Les informations suivantes permettent de terminer l'installation :
 - ♦ **Répertoire de base de l'installation non-root d'eDirectory** : indiquez le répertoire dans lequel se trouve l'installation non-root d'eDirectory. Par exemple, `/home/user/install/eDirectory`.
 - ♦ **Étendre le schéma eDirectory** : s'il s'agit du premier serveur Identity Manager installé dans cette instance d'eDirectory, entrez `y` pour étendre le schéma. Si le schéma ne peut pas être étendu, Identity Manager ne fonctionnera pas.

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

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

Exécutez le programme `/opt/novell/eDirectory/bin/idm-install-schema` pour étendre le schéma sur d'autres instances d'eDirectory une fois l'installation terminée.
 - ♦ **Utilitaires** : (facultatif) si vous avez besoin d'un utilitaire de pilote Identity Manager, vous devez copier les utilitaires du support d'installation d'Identity Manager sur le serveur Identity Manager. Tous les utilitaires se trouvent dans le répertoire `IDM4.0_platform/product/IDM/platform/setup/utilities`.
- 6 Activez Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 8, « Activation des produits Novell Identity Manager », page 75](#).
- 7 Créez et configurez les objets de pilote. Ces informations figurent dans le guide de chaque pilote. Pour plus d'informations, reportez-vous à la [documentation des pilotes Identity Manager](http://www.novell.com/documentation/idm40drivers/) (<http://www.novell.com/documentation/idm40drivers/>).

7.5.2 Installation en mode silencieux du serveur méta-annuaire

Pour installer Identity Manager en mode silencieux, vous devez créer un fichier de propriétés contenant les paramètres nécessaires à l'installation. Un exemple de fichier est inclus sur le support d'Identity Manager :

- ♦ **Linux** : `IDM4.0_Lin/products/IDM/linux/setup/silent.properties`
- ♦ **Solaris** : `IDM4.0_Solaris/products/IDM/solaris/setup/silent.properties`
- ♦ **Windows** : `IDM4.0_Win:\products\IDM\windows\setup\silent.properties`

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

- ♦ **Linux** : `IDM4.0_Lin/products/IDM/install.bin -i silent -f <nom_fichier>.properties`
- ♦ **Solaris** : `IDM4.0_Solaris/products/IDM/install.bin -i silent -f <nom_fichier>.properties`
- ♦ **Windows** : `IDM4.0_Win:\products\IDM\windows\setup\idm_install.exe -i silent -f <nom_fichier>.properties`

Créez un fichier de propriétés `<nom_fichier>.properties` avec les attributs suivants, à l'emplacement à partir duquel vous exécutez le programme d'installation d'Identity Manager :

```
EDIR_USER_NAME=cn=admin,o=test
EDIR_USER_PASSWORD=test
METADIRECTORY_SERVER_SELECTED=true
CONNECTED_SYSTEM_SELECTED=false
X64_CONNECTED_SYSTEM_SELECTED=false
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

Pour les emplacements d'installation par défaut, reportez-vous au fichier `/tmp/idmInstall.log`.

Si vous avez installé iManager et souhaitez installer les plug-ins iManager ultérieurement, vous devez définir la valeur `WEB_ADMIN_SELECTED` sur `true`.

Si vous souhaitez procéder à une installation silencieuse d'Identity Manager sur plusieurs instances, vous devez vous assurer que le fichier `<nom_fichier>.properties` comporte les lignes suivantes :

```
EDIR_NCP_PORT=524
EDIR_NDS_CONF=/etc/opt/novell/eDirectory/conf
EDIR_IP_ADDRESS=<xxx.xx.xx.xx>
```

Le mot de passe est enregistré dans un fichier en vue de l'installation en mode silencieux du méta-annuaire. Au lieu de l'écrire dans un fichier, vous pouvez aussi spécifier le mot de passe en utilisant la variable d'environnement `EDIR_USER_PASSWORD`. Si la variable `EDIR_USER_PASSWORD` n'est pas définie dans le fichier de propriétés, le programme d'installation lit la valeur de la variable d'environnement `EDIR_USER_PASSWORD`.

7.6 Installation du chargeur distant

Le chargeur distant élargit les possibilités d'Identity Manager en permettant au pilote d'accéder au système connecté sans que le coffre-fort d'identité et le serveur méta-annuaire soient installés sur le même serveur que le système connecté. Dans le cadre de la planification, vous devez décider si vous voulez ou non utiliser le chargeur distant. Pour plus d'informations sur la procédure de planification, reportez-vous au [Chapitre 3, « Directives techniques », page 27](#).

- ♦ [Section 7.6.1, « Configuration requise », page 66](#)
- ♦ [Section 7.6.2, « Pilotes pris en charge », page 66](#)
- ♦ [Section 7.6.3, « Procédure d'installation », page 67](#)
- ♦ [Section 7.6.4, « Installation silencieuse du chargeur distant », page 69](#)
- ♦ [Section 7.6.5, « Installation du chargeur distant Java sous UNIX ou Linux », page 70](#)
- ♦ [Section 7.6.6, « Coexistence de chargeurs distants 32 et 64 bits », page 71](#)

Si vous souhaitez installer le chargeur distant à l'aide d'un utilisateur non-root, utilisez le chargeur distant Java. Ce dernier peut également être utilisé lorsque vous personnalisez votre environnement et installez le chargeur distant Java sur une plate-forme non prise en charge, telle que HP-UX. Pour plus d'informations, reportez-vous à la [Section 7.6.5, « Installation du chargeur distant Java sous UNIX ou Linux », page 70](#).

7.6.1 Configuration requise

Le chargeur distant nécessite la disponibilité du système connecté de chaque pilote et la fourniture des API pertinentes. Reportez-vous à la [documentation des pilotes d'Identity Manager \(http://www.novell.com/documentation/idm40drivers\)](http://www.novell.com/documentation/idm40drivers) pour connaître la configuration requise du système d'exploitation et du système connecté spécifiques à chaque pilote.

7.6.2 Pilotes pris en charge

Tous les pilotes Identity Manager ne sont pas pris en charge par le chargeur distant. La liste ci-dessous répertorie les pilotes pris en charge par le chargeur distant.

- ♦ Active Directory
- ♦ Avaya PBX
- ♦ Services de collecte de données
- ♦ Texte délimité
- ♦ GroupWise (disponible uniquement pour le chargeur distant 32 bits)
- ♦ JDBC
- ♦ JMS
- ♦ LDAP
- ♦ Pilote pour Linux et UNIX
- ♦ Boucle
- ♦ Lotus Notes
- ♦ Passerelle système gérée
- ♦ Services de tâches manuelles

- ♦ Services nuls
- ♦ PeopleSoft 5.2
- ♦ Remedy ARS
- ♦ RACF
- ♦ Salesforce.com
- ♦ SAP Business Logic
- ♦ SAP GRC (CMP uniquement)
- ♦ SAP HR
- ♦ Portail SAP
- ♦ SAP User Management
- ♦ Script
- ♦ SharePoint
- ♦ SOAP
- ♦ Bon de travail

Les pilotes listés ci-dessous ne peuvent pas utiliser le chargeur distant.

- ♦ eDirectory
- ♦ Services de droits
- ♦ Service de rôle
- ♦ Application utilisateur

7.6.3 Procédure d'installation

Le chargeur distant dispose de différents programmes pour les différentes plates-formes, ce qui lui permet de communiquer avec le serveur méta-annuaire.

- ♦ **Linux/UNIX** : `rdxml` est un exécutable qui permet au serveur méta-annuaire de communiquer avec les pilotes Identity Manager s'exécutant dans des environnements Solaris ou Linux.
- ♦ **Windows** : la console du chargeur distant utilise `rlconsole.exe` pour interagir avec `dirxml_remote.exe`, un exécutable qui permet au serveur méta-annuaire de communiquer avec les pilotes Identity Manager s'exécutant sous Windows.

Pour installer le chargeur distant :

- 1 Vérifiez que vous respectez la configuration système listée dans le [Chapitre 6, « Configuration système requise »](#), page 49.
- 2 Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager »](#), page 45.
- 3 Lancez l'installation à l'aide du programme adapté à votre plate-forme.
 - ♦ **Linux - installation à partir de l'interface graphique** : `IDM4.0_Lin/products/IDM/install.bin [-i gui]`
 - ♦ **Linux - installation à partir de la ligne de commande** : `IDM4.0_Lin/products/IDM/install.bin -i console`

- ♦ **Solaris - installation à partir de l'interface graphique** : `IDM4.0_Solaris/products/IDM/install.bin [-i gui]`
- ♦ **Solaris - installation à partir de la ligne de commande** : `IDM4.0_Solaris/products/IDM/install.bin -i console`
- ♦ **Windows** : `IDM4.0_Win:\products\IDM\windows\setup\idm_install.exe`

Pour exécuter les fichiers binaires sous Linux ou Solaris, saisissez `./install.bin [-i {gui | console}]`.

4 Utilisez les informations suivantes prévues pour terminer l'installation :

- ♦ **Sélectionner les composants** : choisissez le serveur et les utilitaires du système connecté pour installer le chargeur distant.
 - ♦ **Serveur méta-annuaire de Novell Identity Manager** : ne choisissez cette option que si vous installez le serveur méta-annuaire. cette option nécessite que le coffre-fort d'identité soit installé sur ce serveur. Pour plus d'informations, reportez-vous à la [Section 7.5, « Installation du serveur méta-annuaire », page 61](#).
 - ♦ **Serveur de système connecté Novell Identity Manager 32 bits** : cette option ne nécessite pas l'installation du coffre-fort d'identité sur ce serveur. Elle installe la version 32 bits du service de chargeur distant sur votre serveur d'applications.
 - ♦ **Serveur de système connecté Novell Identity Manager 64 bits** : cette option ne nécessite pas l'installation du coffre-fort d'identité sur ce serveur. Elle installe la version 64 bits du service de chargeur distant sur votre serveur d'applications.
 - ♦ **Serveur de système connecté Novell Identity Manager (.NET)** : cette option (Windows uniquement) installe le service de chargeur distant .NET et le pilote SharePoint sur ce serveur.
 - ♦ **Plug-ins Novell Identity Manager pour Identity Manager** : sélectionnez cette option si vous avez installé iManager sur ce serveur. Elle installe les plug-ins iManager pour Identity Manager.
 - ♦ **Utilitaires** : installe les utilitaires servant à configurer les pilotes pour les systèmes connectés. Tous les pilotes n'ont pas d'utilitaires. Si vous n'êtes pas certain d'en avoir besoin, sélectionnez-les tout de même. Ils n'occupent pas beaucoup d'espace disque.
 - ♦ **Personnalisé** : sélectionnez cette option pour personnaliser les fonctions installées. Vous pouvez alors sélectionner les options listées ci-dessous. Avant de sélectionner cette option, vous devez choisir les composants à installer.
 - ♦ **Service de chargeur distant 32 bits** : service qui communique avec le serveur méta-annuaire.
 - ♦ **Service de chargeur distant 64 bits** : service qui communique avec le serveur méta-annuaire.
 - ♦ **Pilotes** : sélectionnez les fichiers de pilotes à installer. Il est recommandé d'installer tous les fichiers de pilote. Vous n'avez pas besoin d'exécuter à nouveau l'installation pour ajouter une autre instance du chargeur distant.
 - ♦ **Serveur de système connecté Novell Identity Manager (.NET)** : (Windows uniquement) installe le service de chargeur distant .NET et le pilote SharePoint.
- Les autres options doivent être sélectionnées lorsque vous sélectionnez la personnalisation pour que l'installation se poursuive.
- ♦ **(Windows uniquement) Emplacement d'installation pour le serveur du système connecté** : indiquez le répertoire dans lequel est installé le serveur du système connecté.

- ♦ **(Windows uniquement) Emplacement d'installation du chargeur distant .NET :**
indiquez le répertoire dans lequel est installé le chargeur distant .NET.
 - ♦ **(Windows seulement) Emplacement d'installation pour les utilitaires :** indiquez le répertoire dans lequel sont installés les utilitaires.
- 5 Créez et configurez vos objets de pilote pour utiliser le chargeur distant. Ces informations figurent dans le guide de chaque pilote. Pour plus d'informations, reportez-vous à la [documentation des pilotes Identity Manager \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).
 - 6 Créez un fichier de configuration de chargeur distant pour travailler avec votre système connecté. Pour plus d'informations, reportez-vous à la section « [Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File](#) » (Configuration du chargeur distant pour Linux/UNIX en créant un fichier de configuration) du manuel *Identity Manager 4.0 Remote Loader Guide* (Guide du chargeur distant d'Identity Manager 4.0).

7.6.4 Installation silencieuse du chargeur distant

Pour installer le chargeur distant en mode silencieux, vous devez créer un fichier de propriétés contenant les paramètres nécessaires à l'installation. Un exemple de fichier est inclus sur le support d'Identity Manager :

- ♦ **Linux :** IDM4.0_Lin/products/IDM/linux/setup/silent.properties
- ♦ **Solaris :** IDM4.0_Solaris/products/IDM/solaris/setup/silent.properties
- ♦ **Windows :** IDM4.0_Win:\products\IDM\windows\setup\silent.properties

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

- ♦ **Linux :** IDM4.0_Lin/products/IDM/install.bin -i silent -f <nom_fichier>.properties
- ♦ **Solaris :** IDM4.0_Solaris/products/IDM/install.bin -i silent -f <nom_fichier>.properties
- ♦ **Windows :** IDM4.0_Win:\products\IDM\windows\setup\idm_install.exe -i silent -f <nom_fichier>.properties

Créez un fichier de propriétés <nom_fichier>.properties avec les attributs suivants, à l'emplacement à partir duquel vous exécutez le programme d'installation d'Identity Manager :

```
METADIRECTORY_SERVER_SELECTED=false
CONNECTED_SYSTEM_SELECTED=true
X64_CONNECTED_SYSTEM_SELECTED=true
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

Pour les emplacements d'installation par défaut, reportez-vous au fichier /tmp/idmInstall.log.

Si vous avez installé iManager et souhaitez installer les plug-ins iManager ultérieurement, vous devez définir la valeur WEB_ADMIN_SELECTED sur true.

7.6.5 Installation du chargeur distant Java sous UNIX ou Linux

`dirxml_jremote` est un chargeur distant Java pur. Il permet d'échanger des données entre le serveur méta-annuaire qui s'exécute sur un serveur et les pilotes Identity Manager s'exécutant à un autre emplacement, où `rdxml` ne s'exécute pas. Il devrait pouvoir s'exécuter sur tout système doté d'un JRE compatible (1.5.0 minimum) et de Java Sockets. Il est pris en charge sur les plates-formes Linux/UNIX compatibles avec Identity Manager.

- 1 Vérifiez que le JDK/JRE 1.5.x de Java est disponible sur le système hôte.
- 2 Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager »](#), page 45.
- 3 Recherchez les fichiers d'installation du chargeur distant Java sur le support d'Identity Manager :

- ♦ **Linux** : `IDM4.0_Lin/products/IDM/java_remoteloader`
- ♦ **Solaris** : `IDM4.0_Solaris/products/IDM/java_remoteloader`

- 4 Copiez le fichier `dirxml_jremote_dev.tar.gz` à l'emplacement souhaité sur le serveur distant.
- 5 Copiez le fichier `dirxml_jremote.tar.gz` ou `dirxml_jremote_mvs.tar` à l'emplacement souhaité sur le serveur distant.

Par exemple : `/usr/idm`

Pour plus d'informations sur `mvs`, décompressez le fichier `dirxml_jremote_mvs.tar`, puis reportez-vous au document `usage.html`.

- 6 Décompressez et extrayez les fichiers `dirxml_jremote.tar.gz` et `dirxml_jremote_dev.tar.gz`.

Par exemple : `gunzip dirxml_jremote.tar.gz` ou `tar -xvf dirxml_jremote_dev.tar`

- 7 Copiez les fichiers `.jar` du module d'interface d'application dans le sous-répertoire `lib` créé lors de l'extraction du fichier `dirxml_jremote.tar`.

Étant donné que le fichier `.tar` ne contient pas les fichiers `.jar`, vous devez copier manuellement ces fichiers `.jar` depuis le serveur méta-annuaire vers le répertoire `lib`. Le répertoire `lib` se trouve sous le répertoire de décompression.

Le répertoire d'installation par défaut des fichiers `.jar` sur le serveur méta-annuaire est `/opt/novell/eDirectory/lib/dirxml/classes`.

- 8 Personnalisez le script `dirxml_jremote` en effectuant l'une des opérations suivantes :
- Vérifiez que l'exécutable Java peut être atteint via la variable d'environnement `PATH` en définissant la variable d'environnement `RDXML_PATH`. Saisissez les commandes suivantes pour définir la variable d'environnement :
 1. `set RDXML_PATH=path`
 2. `export RDXML_PATH`
 - Modifiez le script `dirxml_jremote` et préfixez la ligne de script exécutant Java avec le chemin vers l'exécutable Java.
- 9 Configurez le fichier d'exemple `config8000.txt` à utiliser avec votre module d'interface d'application. Pour plus d'informations, reportez-vous à la section « [Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File](#) » (Configuration du chargeur distant pour Linux/UNIX en créant un fichier de configuration) du manuel *Identity Manager 4.0 Remote Loader Guide* (Guide du chargeur distant d'Identity Manager 4.0).

7.6.6 Coexistence de chargeurs distants 32 et 64 bits

Identity Manager 4.0 permet à des chargeurs distants 32 et 64 bits de coexister 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, il est mis à niveau et un chargeur distant 64 bits est également installé. Vous pouvez avoir un chargeur distant 32 bits et un chargeur distant 64 bits sur la même machine.

7.7 Installation du module de provisioning basé sur les rôles

Pour installer le module de provisioning basé sur les rôles, reportez-vous au [Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0](#).

7.8 Installation d'un pilote personnalisé

Vous pouvez créer un pilote personnalisé à utiliser dans le votre environnement. Pour plus d'informations sur la création d'un pilote personnalisé ou son installation, reportez-vous au [Novell Developer Kit](#) (<http://developer.novell.com/wiki/index.php/Dirxml>) (Kit du développeur Novell).

7.9 Installation de l'administrateur d'assignation de rôles

L'administrateur d'assignation de rôles est un service Web qui découvre les autorisations pouvant être octroyées au sein de vos principaux systèmes informatiques. Pour installer l'administrateur d'assignation de rôles :

- 1 Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager », page 45](#).
- 2 Recherchez le fichier d'installation de l'administrateur d'assignation de rôles sur le support d'Identity Manager situé ici :
 - **Linux** : `IDM4.0_Lin/products/RMA/IDMRMAP.jar`
 - **Windows** : `IDM4.0_Win:\products\RMA\IDMRMAP.jar`

- 3 Accédez au répertoire d'installation de l'administrateur d'assignation de rôles à partir d'une ligne de commande, puis saisissez `java -jar IDMRMAP.jar`.

Remarque : si vous utilisez Linux, vous devez, pour des raisons de sécurité, installer l'administrateur d'assignation de rôles en tant qu'utilisateur `non-root`.

- 4 Entrez `Oui` pour accepter l'accord de licence.
- 5 Indiquez le répertoire d'installation de l'administrateur d'assignation de rôles. Le chemin par défaut est l'emplacement actuel.
- 6 Spécifiez la partie de l'URL correspondant au nom de l'administrateur d'assignation de rôles. La valeur par défaut est `IDMRMAP`.
- 7 Spécifiez le port HTTP. La valeur par défaut est `8081`.
- 8 Indiquez un mot de passe pour l'administrateur de la configuration.

L'administrateur d'assignation de rôles est maintenant installé. L'application ne démarre pas automatiquement une fois l'installation terminée. Utilisez les scripts suivants, situés dans le répertoire d'installation, pour démarrer et arrêter l'application.

- ♦ **Linux :** le script de démarrage est `start.sh` et le script d'arrêt, `stop.sh`.
- ♦ **Windows :** le script de démarrage est `start.bat` et le script d'arrêt, `stop.bat`.

Une fois l'administrateur d'assignation de rôles installé et démarré, vous devez le configurer. Pour plus d'informations sur la configuration, reportez-vous à la section « [Configuring the Application](#) » (Configuration de l'application) du manuel *Identity Manager Role Mapping Administrator 2.0 Installation and Configuration Guide* (Guide d'installation et de configuration de la version 2.0 de l'administrateur d'assignation de rôles).

7.10 Installation du module Identity Reporting ou de Sentinel

Le module Identity Reporting et Sentinel sont deux composants facultatifs qui peuvent être ajoutés à la solution Identity Manager. L'ajout des fonctions d'audit et de création de rapports permet de respecter les normes de conformité que de nombreuses sociétés doivent observer. Vous pouvez créer des suivis d'audit pour les événements que vous devez suivre, ainsi que générer des rapports pour vous assurer que vous respectez les normes d'audit de votre société.

Pour plus d'informations sur l'installation et la configuration du module Identity Reporting, reportez-vous au manuel *Identity Reporting Module Guide* (Guide du module Identity Reporting). Pour plus d'informations sur la configuration de Sentinel avec Identity Manager, reportez-vous au manuel *Identity Manager 4.0 Reporting Guide for Novell Sentinel* (Guide de création de rapports Identity Manager 4.0 pour Novell Sentinel). Pour plus d'informations sur la configuration système requise pour Sentinel, reportez-vous au *Guide d'installation de Novell Sentinel* (<http://www.novell.com/documentation/sentinel6/index.html>).

7.11 Installation d'Identity Manager dans un environnement en grappe

Si vous déployez Identity Manager dans un environnement en grappe, Novell prend en charge Identity Manager s'exécutant dans la grappe, même si, la plupart du temps, la grappe proprement dite n'est pas prise en charge. Les deux scénarios suivants décrivent la portée de la prise en charge :

- ♦ Si vous exécutez le serveur méta-annuaire ou le chargeur distant sous SUSE Linux Enterprise Server (SLES) et utilisez Heartbeat pour gérer la haute disponibilité, tous les éléments sont pris en charge.
- ♦ Si vous exécutez le serveur méta-annuaire ou le chargeur distant dans un environnement en grappe sur toute autre plate-forme prise en charge, la prise en charge est étendue à tous les éléments, à l'exception du système de gestion de grappe.

Remarque : SLES est la seule plate-forme pleinement prise en charge dans un environnement en grappe.

Pour plus d'informations sur la configuration d'une grappe avec Identity Manager, reportez-vous à ces ressources :

- ♦ Configuring a Linux High Availability Cluster for IDM 3 and eDirectory 8.8 (Configuration d'une grappe haute disponibilité Linux pour IDM 3 et eDirectory 8.8), sur le [site Web Novell Cool Solutions \(http://www.novell.com/coolsolutions/appnote/18591.html\)](http://www.novell.com/coolsolutions/appnote/18591.html).
- ♦ Clustering eDirectory and IDM on Windows 2003 (Mise en grappe d'eDirectory et IDM sous Windows 2003), sur le [site Web Novell Cool Solutions \(http://www.novell.com/coolsolutions/appnote/14856.html\)](http://www.novell.com/coolsolutions/appnote/14856.html).
- ♦ Novell Identity Manager High Availability on PolyServe Clusters (Haute disponibilité de Novell Identity Manager sur les grappes PolyServe), sur le [site Web Novell Cool Solutions \(http://www.novell.com/coolsolutions/appnote/16131.html\)](http://www.novell.com/coolsolutions/appnote/16131.html).
- ♦ Setting Up an Identity Manager Cluster on Windows (Configuration d'une grappe Identity Manager sous Windows), sur le [site Web de support Novell \(http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3575742&sliceId=SAL_Public&dialogID=310596&stateId=1%200%20308676\)](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3575742&sliceId=SAL_Public&dialogID=310596&stateId=1%200%20308676). Le document porte le numéro 3575742.

Activation des produits Novell Identity Manager

8

Les sections suivantes expliquent comment activer les produits Novell Identity Manager. Identity Manager, les modules d'intégration et le module de provisioning doivent être activés dans un délai de 90 jours suivant l'installation, sinon ils ne fonctionneront plus. À n'importe quel moment au cours de ces 90 jours, ou plus tard, vous pouvez choisir d'activer les produits Identity Manager.

Vous pouvez activer Identity Manager et les pilotes en effectuant les tâches suivantes :

- ♦ Section 8.1, « Achat d'une licence de produit Identity Manager », page 75
- ♦ Section 8.2, « Installation d'une référence d'activation de produit », page 75
- ♦ Section 8.3, « Affichage des activations de produits pour Identity Manager et les pilotes », page 76
- ♦ Section 8.4, « Activation des pilotes Identity Manager », page 77
- ♦ Section 8.5, « Activation d'Analyzer », page 77
- ♦ Section 8.6, « Activation de Designer et de l'administrateur d'assignation de rôles », page 78

8.1 Achat d'une licence de produit Identity Manager

Pour acquérir une licence de produit Identity Manager afin de pouvoir l'activer, reportez-vous à la page [Web Novell Identity Manager - Guide d'achat \(http://www.novell.com/products/identitymanager/howtobuy.html\)](http://www.novell.com/products/identitymanager/howtobuy.html).


Une fois la licence de produit achetée, Novell vous envoie votre ID client par courrier électronique. Le courrier électronique contient également une URL vers le site Novell sur lequel vous pouvez obtenir une référence d'activation de produit. Si vous oubliez votre ID client ou si vous ne le recevez pas, appelez le centre d'activation Novell (Novell Activation Center) au 1-800-418-8373 si vous résidez aux États-Unis. Pour tout autre pays, composez le 1-801-861-8373. (Les appels effectués avec l'indicatif 801 vous seront facturés.) Vous pouvez aussi [communiquer avec nous en ligne \(http://support.novell.com/chat/activation\)](http://support.novell.com/chat/activation).

8.2 Installation d'une référence d'activation de produit

Vous devez installer la référence d'activation du produit via iManager.

- 1 Une fois la licence achetée, Novell vous envoie un courrier électronique avec votre ID client. Ce courrier électronique contient également un lien sous la section Détail de la commande vers le site sur lequel vous pouvez obtenir votre référence. Cliquez sur le lien pour aller sur le site.
- 2 Cliquez sur le lien de téléchargement de licence et effectuez l'une des opérations suivantes :
 - ♦ Enregistrez le fichier de référence d'activation du produit.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.

8.3 Affichage des activations de produits pour Identity Manager et les pilotes

Pour chaque ensemble de pilotes, vous pouvez afficher les références d'activation de produit installées pour le serveur 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 l'arborescence, puis sur  pour exécuter 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.

8.4 Activation des pilotes Identity Manager

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

- ♦ **Pilotes de service :** les pilotes de service suivants sont activés en même temps que le serveur méta-annuaire :
 - ♦ Service de collecte de données
 - ♦ Services de droits
 - ♦ Fournisseur d'ID
 - ♦ Service de boucle
 - ♦ Passerelle système gérée
 - ♦ Service de tâches manuelles
 - ♦ Service nul
 - ♦ Service de rôles
 - ♦ Application utilisateur
 - ♦ Bon de travail
- ♦ **Pilotes communs :** les pilotes communs suivants sont activés en même temps que le serveur méta-annuaire :
 - ♦ Active Directory
 - ♦ ADAM
 - ♦ eDirectory
 - ♦ GroupWise
 - ♦ LDAP
 - ♦ Lotus Notes

Les références d'activation de tous les autres pilotes Identity Manager doivent être achetées séparément. Les références d'activation des pilotes sont vendues en tant que modules d'intégration d'Identity Manager. Ces derniers peuvent contenir un ou plusieurs pilotes. Pour chaque module d'intégration d'Identity Manager acheté, vous recevez une référence d'activation du produit.

Pour activer les pilotes, vous devez réaliser la procédure décrite à la [Section 8.2, « Installation d'une référence d'activation de produit »](#), page 75 pour chaque module d'intégration d'Identity Manager.

8.5 Activation d'Analyzer

La première fois que vous lancez Analyzer, vous êtes invité à l'activer. Si vous ne l'activez pas, vous ne pouvez pas l'utiliser. Pour plus d'informations, reportez-vous à la section « [Activating Analyzer](#) » (Activation d'Analyzer) du manuel *Analyzer 1.2 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 1.2 pour Identity Manager).

8.6 Activation de Designer et de l'administrateur d'assignation de rôles

Pour activer Designer et l'administrateur d'assignation de rôles, il suffit d'activer le serveur méta-annuaire ou les pilotes.

Dépannage d'Identity Manager

9

Les informations suivantes sont utiles lorsque vous installez Identity Manager :

- ♦ « [Problème lié au pilote Lotus Notes lors de l'installation d'Identity Manager](#) » page 79
- ♦ « [L'installation d'Identity Manager peut parfois échouer sur la plate-forme Windows 2008 SP2 32 bits](#) » page 79

Problème lié au pilote Lotus Notes lors de l'installation d'Identity Manager

Source : Sous Solaris 10, le message d'erreur de pilote Lotus Notes suivant peut s'afficher lors de l'installation d'Identity Manager 4.0 en tant qu'utilisateur non-root :

```
ln: cannot create /usr/lib/locale/ja/wnn//ndsrep: File exists
ln: cannot create
cp: cannot create /usr/lib/locale/ja/wnn//
libnotesdrvjni.so.1.0.0: Permission
denied
ln: cannot create /usr/lib/locale/ja/wnn//
libnotesdrvjni.so.1: File exists
ln: cannot create /usr/lib/locale/ja/wnn//libnotesdrvjni.so:
File exists
```

Action : Créez manuellement les liens symboliques. Pour plus d'informations sur la vérification et la recréation des liens symboliques, reportez-vous à la section « [Troubleshooting Installation Problems](#) » (Dépannage des problèmes d'installation) du manuel *Identity Manager 4.0 Driver for Lotus Notes Implementation Guide* (Guide de mise en oeuvre du pilote Identity Manager 4.0 pour Lotus Notes).

L'installation d'Identity Manager peut parfois échouer sur la plate-forme Windows 2008 SP2 32 bits

Source : Le programme d'installation de la structure affiche le message d'erreur suivant :

```
Java Platform SE binary has stopped working.
```

Action : Pour contourner ce problème :

- 1 Exécutez le programme d'installation d'Identity Manager avec l'option - *DCLUSTER_INSTALL="true"*. Seuls les fichiers Identity Manager sont alors installés, sans le schéma eDirectory ni les autres fichiers.

```
<install_drive>:\windows\setup\idm_install.exe -
DCLUSTER_INSTALL="true"
```

- 2 Étendez le schéma Identity Manager à l'aide d'iManager en utilisant l'assistant *Importation/Conversion/Exportation* sous *Maintenance d'eDirectory*.
- 3 Créez les objets par défaut à l'aide du fichier LDIF.
 - ♦ Fichier LDIF de stratégie de mot de passe par défaut

```
dn: cn=Password Policies,cn=Security
objectClass: nspmPasswordPolicyContainer
objectClass: Top
cn: Password Policies
ACL: 1#subtree#[Public]#[Entry Rights]
ACL: 3#subtree#[Public]#[All Attributes Rights]
```

```
dn: cn=Sample Challenge Set,cn=Password
Policies,cn=Security
objectClass: nsimChallengeSet
objectClass: Top
cn: Sample Challenge Set
```

```
dn: cn=Sample Password Policy,cn=Password
Policies,cn=Security
objectClass: nspmPasswordPolicy
objectClass: Top
cn: Sample Password Policy
```

◆ Fichier LDIF de stratégie de collection de notification par défaut

```
dn: cn=Default Notification Collection,cn=Security
objectClass: notifTemplateCollection
objectClass: Top
cn: Default Notification Collection
ACL: 1#subtree#[Public]#[Entry Rights]
ACL: 3#subtree#[Public]#[All Attributes Rights]
```

```
dn: cn=Password Expiration Notification,cn=Default
Notification Collection,cn=Security
notifMergeTemplateSubject: Password Expiration
Notification
notifMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9yYT0iaHR0cDovL3d3dy5ub3ZlbgwY29tL
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4gDQo8Zm9ybTp0b2t1bi1kZX
NjcmlwdGlvbnM+IA0KPGZvcM06dG9rZW4tZGVzY3JpcHRpb24gZGV
zY3JpcHRpb249IkZ1bGwgbmFtZSBieSB3aGljaCB0byBhZGRyZXNz
IHVzZXIiIGl0ZW0tbnFtZT0iVXNlckZ1bGxvYm11Ii8+IA0KPGZvc
m06dG9rZW4tZGVzY3JpcHRpb24gZGVzY3JpcHRpb249Ik51bWJlci
BvZiBkYXlzIHVudGlsIHBhc3N3b3JkIGV4cGlyZXMiIGl0ZW0tbnF
tZT0iRXhwRGF5cyIvPiANCjwvZm9ybTp0b2t1bi1kZXNjcmlwdGlv
bnM+IA0KPGhlYWQ+IA0KPHRpdGx1PlBhc3N3b3JkIEV4cGlyYXRpb
24gTm90aWZpY2F0aW9uPC90aXR5ZT4gDQo8c3R5bGU+IA0KPCeTlS
Bib2R5IHsgZm9udC1mYW1pbHk6IFRyZWJlY2hldCBNUyB9IC0tPiA
NCjwvc3R5bGU+IA0KPC9oZWFKPiANCjxib2R5IEJHQ09MT1I9IiNG
RkZGRkYiPiANCjxwPkRlYXlIgJFVzZXJGdWxsTmFtZS0sPC9wPiANC
jxwPlRoaxMgbWVzc2FnZSBpcyB0byBpbmZvcM0geW91IHRoYXQgeW
91ciBwYXNzd29yZCB3aWxsIGV4cGlyZSBpbjwvcD4gDQo8YnIvPiA
NCiAgJEV4cERheXMkIGRheXM8YnIvPiANCjxici8+IA0KPHA+UGxl
YXNlIHBSYW4gdG8gY2hhbmdlIHlvdXIgcGFzc3dvcmQgYmVmb3JlI
Gl0IGV4cGlyZXMuPC9wPiANCjxwPiAtIEF1dG9tYXRlZCBTZW51cm
l0eSAtIDwvcD4gDQo8cD4gDQo8aW1nIEFMDV0iUG93ZXJlZCBieSB
Ob3Z1bGwiIFNSQz0iY2lkOnBvd2VyZWRFYnlfbm92ZWxsLmdpZiIg
aGVpZ2h0PSiYOSIGd2lkDgG9IjgwIi8+IA0KPC9wPiANCjwvYm9keS
T4gDQo8L2h0bWw+IA0K
objectClass: notifMergeTemplate
objectClass: Top
cn: Password Expiration Notification
```

```
dn: cn=Password Reset Fail,cn=Default Notification
```


Collection, cn=Security
notifMergeTemplateSubject: Notice of Password Reset
Failure
notifMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbgWuY29tL
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvcM06dG9rZW4tZG
VzY3JpcHRpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9
uIGl0ZW0tbmFtZT0iVXNlckZlbgxOYW11IiBkZXNjcmlwdGlvbj0i
VGhlIHVzZXIncyBmdWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2t1b
i1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVzZXJHaXZlbnk5hbWUiIG
Rlc2NyaXB0aW9uPSJUaGUgdXNlckZlIGdpdmVzIG5hbWdDT0xPUj0
iI0ZGRkZGRiI+DQogIDxwPkRlYXJgJFVzZXJGdWxsTmFtZSQsPC9w
Pg0KICA8cD5UaGlzIGlzIGegbm90aWNlIHROYYQgeW91ciBwYXNzd
29yZCBjb3VsZCBub3QgYmUgcmlvZmVzZXQgaW4gdGhlICRDb25uZWN0ZW
RTeXN0ZW10YW11JCBzeXN0ZW0uLiAgVGhlIHJlYXNvbiBmb3IgzMf
pbHVyZSBpcyBpbmRyY2F0ZWQgYmVsb3c6PC9wPg0KICA8cD5SZWFz
b246ICRGYwlsdXJlUmVhc29uJDwvcD4NCiAgPHA+SWYgeW91IGhhd
mUgYw55IGZlcnRoZXIgcXVlc3Rpb25zLA0KICAgICBwbGVhc2UgY2
9udGJfdCB0aGUgaGVscCBkZXNrIGF0ICGwMTIpIDM0NS02Nzg5IG9
yIGVtYWlsDQogICAgIGF0IDxhIGhyZWY9Im1haWx0b2ZpoZWxwLmRl
c2tAbXljb21wYW55LmNvbSI+DQogICAgIGhlbHhAuZGVza0BteWVnb
XBhbnkuY29tIDwvYT48L3A+DQogIDxwPiAtIEF1dG9tYXRlZCBTZW
N1cm10eTwvcD4NCiAgPHA+PglzYyBTUkM9ImNpZDpwb3dlcmVxZ2J
5X25vdmVsbC5naWYiIEFMVD0iUG93ZXJlZCBieSB0b3ZlbgwiIHDp
ZHRoPSI4MCIgaGVpZ2h0PSIyOSIvPjwvcD4NCjwvYm9keT4NCjwva
HRtbD4NCg==
objectClass: notifMergeTemplate
objectClass: Top
cn: Password Reset Fail

dn: cn=Password Set Fail,cn=Default Notification
Collection, cn=Security
notifMergeTemplateSubject: Notice of Password Set
Failure
notifMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbgWuY29tL
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvcM06dG9rZW4tZG
VzY3JpcHRpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9
uIGl0ZW0tbmFtZT0iVXNlckZlbgxOYW11IiBkZXNjcmlwdGlvbj0i
VGhlIHVzZXIncyBmdWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2t1b
i1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVzZXJHaXZlbnk5hbWUiIG
Rlc2NyaXB0aW9uPSJUaGUgdXNlckZlIGdpdmVzIG5hbWU9IlVz
ZXJMYXN0TmFtZSIgZGVzY3JpcHRpb249IlRoZSB1c2VyJ3MgbGFzd
CBuYW11Ii8+DQogICAgPGZvcM06dG9rZW4tZGVzY3JpcHRpb24gaX
RlbS1uYW11PSJDb25uZWN0ZWRTeXN0ZW10YW11IiBkZXNjcmlwdG1
vb3IiVGhlIGV4dGVybmFsIGFwcGxpY2F0b24gcmFtZSIvPg0KICAg
IDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmFtZT0iRmFpb
HVyZVJlYXNvbiIgzGVzY3JpcHRpb249IlRoZSBmYwlsdXJlIHJlYX
NvbiIvPg0KICA8L2ZvcM06dG9rZW4tZGVzY3JpcHRpb25zPg0KPGh
lYWQ+DQogIDx0aXRzT50b3RyY2Ugb2YgUGFzc3dvcM06dG9rZW4tZG
VzY3JpcHRpb25zPg0KICA8c3R5bGU+IDwhLS0gYm9keSB7IGZvb
nQtZmFtaWx50iBUcmVidWNoZXQgTVMgfSAatLT4gPC9zdHlsZT4NCj
wvaGVhZD4NCjxib2R5IEJHQ09MT1I9IiINGRkZGRkYiPg0KPHA+RGV
hciAkVXNlckZlbgxOYW11JlJlYXNlZC5hbWU9IlVzZXJHaXZlbnk5
hbWUiIGRlc2NyaXB0aW9uPSJUaGUgdXNlckZlIGdpdmVzIG5hbWdD
T0xPUj0iI0ZGRkZGRiI+DQogIDxwPkRlYXJgJFVzZXJGdWxsTmFtZ
SQsPC9wPg0KICA8cD5SZWFzb246ICRGYwlsdXJlUmVhc29uJDwv
sb3c6PC9wPg0KICA8cD5SZWFzb246ICRGYwlsdXJlUmVhc29uJDwv

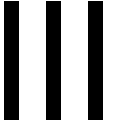
cD4NCiAgPHA+SWYgeW91IGhhdMUGYw55IGZ1cnRoZXIgcXVlc3Rpb
25zLA0KICAgICBwbGVhc2UgY29udGFjdCB0aGUgaGVscCBkZXNRIG
F0ICgWMTIpIDMONS02Nzg5IG9yIGVtYWlscDQogICAgIGF0IDxhIGh
yZWY9Im1haWx0bzpoZWxwLmRlc2tAbXlj21wYw55LmNvbSI+DQog
ICAgIGh1bHAuZGVza0BteWNvbXBhbnkuY29tIDwvYT48L3A+DQogI
DxwPiAtIEF1dG9tYXRlZCBTZWN1cm10eTwvcD4NCiAgPHA+PglTzY
BTUkM9ImNpZDpw3dlcmVhX2J5X25vdmVsbC5naWYiIEFMVD0iUG9
3ZXJlZCBieSB0b3ZlbGwiIHdpZHRoPSI4MCIgaGVzP2h0PSIyOSIv
PjwvcD4NCjwvYm9keT4NCjwvaHRtdD4NCg==
objectClass: notfMergeTemplate
objectClass: Top
cn: Password Set Fail

dn: cn=Password Sync Fail,cn=Default Notification
Collection,cn=Security
notfMergeTemplateSubject: Notice of Password
Synchronization Failure
notfMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbGwvY29tL
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvc06dG9rZW4tZG
VzY3JpcHRpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9
uIGl0ZW0tbmFtZT0iVXNlckZ1bGxvOYW11IiBkZXNjcmlwdGlvbj0i
VGhlIHVzZXIncyBmdWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2t1b
i1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9I1VzZXJHaXZ1b2t1bWUiIG
Rlc2NyaXB0aW9uPSJUaGUgdXNlcidzIGdpdmVuIG5hbWUiLz4NCiAg
gICA8Zm9ybTp0b2t1b2t1b2t1b2t1b2t1b2t1b2t1b2t1b2t1b2t1b
249I1RoZSB1c2VyJ3MgbGFzd
CBuYw11Ii8+DQogICAgPGZvc06dG9rZW4tZGVzY3JpcHRpb24gaX
RlbS1uYw11PSJDb25uZWN0ZWRTeXN0ZW10YW11IiBkZXNjcmlwdG1
vbj0iVGhlIGV4dGVybmFsIGFwcGxpY2F0b24gbmFtZSIvPg0KICAg
IDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmFtZT0iRmFpb
HVyZVJlYXNvbiIgcGVzY3JpcHRpb249I1RoZSBmYwlsdXJlIHJlYX
NvbiIvPg0KICA8L2Zvc06dG9rZW4tZGVzY3JpcHRpb25zPg0KPGh
lYwQ+DQogIDx0aXRzZT5Ob3RpY2Ugb2YgUGFzc3dvc0gU3luY2hy
b25pemF0aW9uIEZhaWx1cmU8L3RpdGx1Pg0KICA8c3R5bGU+IDwhL
S0gYm9keSB7IGZvbnQtZmFtaWx5OibUcmVidWNoZXQgTVMgfSAtLT
4gPC9zdHlsZT4NCjwvaGVhZD4NCjxi2R5IEJHQ09MT1I9IiInGRkZ
GRkYiPg0KICA8cD5EZWFyICRvc2VyRnVsbE5hbWUKLDwvcD4NCiAg
PHA+VGhpcyBpcyBhIG5vdG1jZSB0aGF0IHlvdXlIgcGFzc3dvc0gZ
nJvbSB0aGUgJENvbm51Y3RlZFN5c3R1bU5hbWUKIHdhcyB1bmFibG
UgdG8gc3luY2hyb25pemUgdG8gb3RoZXIgcY29ubmVjdGVkIHN5c3R
lbXMuICBUaGUgcVhc29uIGZvciBmYwlsdXJlIGlzcGluc2luc2luc2l
ZCBiZWxvdzo8L3A+DQogIDxwPlJlYXNvbjogJEZhaWx1cmVZSWFzb
24kPC9wPg0KICA8cD5JZiB5b3UgaGF2ZSBhbnkgZnVydGh1ciBxdW
VzdGlvbnMsIHBSZWFzZSBjb250YWN0IHRoZSB0ZWxwIGRlc2sgYXQ
gKDAxMikNCiAgICAgMzQ1LT53ODkqb3IgcW1haWwgcYXQgPGEgaHJl
Zj0ibWFpbHRvOmhlbHAuZGVza0BteWNvbXBhbnkuY29tIj4NCiAgI
CAgaGVscC5kZXNRQG15Y29tcGFueS5jb20gPC9hPjwvcD4NCiAgPH
A+IC0gQXV0b21hdGVkIFNlY3VyaXR5PC9wPg0KICA8cD48aW1nIFN
SQz0iY2lkOnBvd2VyZWRfYnlfbm92ZWxsLmdpZiIgQUxUPSJQb3dl
cmVhIGJ5IE5vdmVsbCIgd2lkdGg9IjgwIiBoZWlnaHQ9IjI5Ii8+P
C9wPg0KPC9ib2R5Pg0KPC9odGlsPg0K
objectClass: notfMergeTemplate
objectClass: Top
cn: Password Sync Fail

- 4 Installez les méthodes NMAS.
- 5 Une fois les plug-ins NMAS installés sur iManager, accédez à *NMAS > NMAS Login (Login NMAS) > Methods (Méthodes) > New (Nouveau)*. Recherchez et installez les fichiers de configuration des méthodes NMAS souhaitées.

Remarque : veuillez à référencer le fichier journal avant d'appliquer la solution de contournement. Par exemple, le schéma du module de provisioning basé sur les rôles est déjà étendu. Vous ne devez donc pas l'étendre lors de l'installation du pilote RBPM.

Mise à niveau ou migration



Les sections suivantes contiennent des informations sur la mise à niveau ou la migration de votre solution Identity Manager existante :

- ♦ [Chapitre 10, « Nouveautés », page 87](#)
- ♦ [Chapitre 11, « Mise à niveau et migration », page 91](#)
- ♦ [Chapitre 12, « Versions prises en charge et configuration système requise pour les mises à niveau et migrations », page 93](#)
- ♦ [Chapitre 13, « Réalisation d'une mise à niveau », page 95](#)
- ♦ [Chapitre 14, « Exécution d'une migration », page 113](#)

Identity Manager 4.0 comporte plusieurs améliorations et nouvelles fonctions :

- ♦ [Section 10.1, « Module Identity Reporting », page 87](#)
- ♦ [Section 10.2, « Nouveaux pilotes », page 87](#)
- ♦ [Section 10.3, « Prise en charge de l'audit XDAS », page 88](#)
- ♦ [Section 10.4, « Remplacement des fichiers de configuration de pilote par des paquets », page 88](#)
- ♦ [Section 10.5, « Administrateur d'assignation de rôles », page 88](#)
- ♦ [Section 10.6, « Analyzer », page 88](#)
- ♦ [Section 10.7, « Programme d'installation intégré », page 89](#)

10.1 Module Identity Reporting

Le module Identity Reporting vous permet de générer des rapports contenant des informations sur différentes caractéristiques de votre configuration Identity Manager, notamment des informations provenant d'un ou de plusieurs systèmes gérés ou coffres-forts d'identité. Le module de création de rapports comprend un ensemble de définitions de rapport prédéfinies que vous pouvez utiliser pour générer des rapports. En outre, il permet d'importer des rapports personnalisés définis dans un outil tiers.

Le module Identity Reporting nécessite deux nouveaux pilotes de service :

- ♦ Pilote de service de collecte de données
- ♦ Pilote de passerelle système gérée

Pour plus d'informations sur le module et les deux pilotes de création de rapports, reportez-vous au manuel [Identity Reporting Module Guide](#) (Guide du module Identity Reporting). Pour plus d'informations sur les rapports prédéfinis, reportez-vous à la section [Utilisation des rapports Identity Manager 4.0](#).

10.2 Nouveaux pilotes

Les nouveaux pilotes suivants sont fournis avec Identity Manager 4.0 :

- ♦ [Section 10.2.1, « Pilote SharePoint \(chargeur distant .NET\) », page 87](#)
- ♦ [Section 10.2.2, « Pilote Salesforce.com », page 88](#)

10.2.1 Pilote SharePoint (chargeur distant .NET)

Le pilote SharePoint pour Novell Identity Manager permet de synchroniser les événements d'adhésion utilisateur et à un groupe entre le coffre-fort d'identité et un ensemble de sites SharePoint 2007 ou 2010. Un seul pilote peut traiter ces événements pour un seul ensemble de sites, qui gère les informations d'adhésion utilisateur et à un groupe d'un ou plusieurs sites SharePoint. Pour plus d'informations, reportez-vous au manuel [Identity Manager Driver for Lotus Notes Implementation Guide](#) (Guide de mise en oeuvre du pilote Identity Manager 4.0 pour SharePoint).

10.2.2 Pilote Salesforce.com

Identity Manager 4.0 permet de provisionner et de synchroniser automatiquement des utilisateurs avec des applications nuage. Le nouveau pilote Salesforce.com pour Novell Identity Manager permet de provisionner et de déprovisionner, de façon transparente, des utilisateurs avec une application nuage Salesforce.com, ce qui garantit la cohérence des informations d'identité utilisateur entre le coffre-fort d'identité et l'application nuage. Il prend également en charge la synchronisation sécurisée des mots de passe entre le coffre-fort d'identité et le nuage Salesforce.com, de même qu'un serveur proxy authentifié et un profil utilisateur configurable pour le provisioning automatique des utilisateurs. Pour plus d'informations, reportez-vous au manuel [Identity Manager 4.0 Driver for Salesforce.com Implementation Guide](#) (Guide de mise en oeuvre du pilote Identity Manager 4.0 pour Salesforce.com).

10.3 Prise en charge de l'audit XDAS

Identity Manager 4.0 prend en charge l'audit XDAS, ce qui permet d'accroître les capacités d'audit de l'agent de la plate-forme d'audit Novell. Il utilise le schéma XDAS commun pour Identity Manager, NMAS, eDirectory et l'administrateur d'assignation de rôles. Le nouveau service d'audit prend également en charge les appenders Syslog et fichier. Pour plus d'informations, reportez-vous aux manuels [Identity Reporting Module Guide](#) (Guide du module Identity Reporting) et [Identity Manager 4.0 Reporting Guide for Novell Sentinel](#) (Guide de création de rapports Identity Manager 4.0 pour Novell Sentinel).

10.4 Remplacement des fichiers de configuration de pilote par des paquetages

Identity Manager 4.0 introduit des paquetages qui contiennent des blocs de construction de qualité supérieure du contenu de stratégie d'Identity Manager. Désormais, les pilotes ne sont plus créés à l'aide de fichiers de configuration de pilote, mais au moyen de paquetages. Pour plus d'informations, 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).

10.5 Administrateur d'assignation de rôles

L'administrateur d'assignation de rôles est un nouvel outil qui vous permet d'analyser les autorisations pouvant être octroyées au sein de vos systèmes informatiques et de les accorder. Les autorisations peuvent être octroyées non seulement par des consultants ou le personnel informatique, mais également par un analyste d'entreprise. Pour plus d'informations, reportez-vous au manuel [Novell Identity Manager Role Mapping Administrator 2.0 User Guide](#) (Guide de l'utilisateur de la version 2.0 de l'administrateur d'assignation de rôles de Novell Identity Manager).

10.6 Analyser

Analyser vous permet de diagnostiquer, de nettoyer et de préparer des données d'identité en vue de les gérer avec Identity Manager. Pour plus d'informations, reportez-vous au manuel [Analyzer 1.2 for Identity Manager Administration Guide](#) (Guide d'administration d'Analyzer 1.2 pour Identity Manager).

10.7 Programme d'installation intégré

Identity Manager 4.0 est fourni avec un programme d'installation intégré qui installe et configure tous les composants Identity Manager en une seule fois. Le programme d'installation est utilisé pour les nouvelles installations dans des environnements de taille petite à moyenne. Pour plus d'informations, reportez-vous au [Guide du programme d'installation intégré d'Identity Manager 4.0](#).

Vous pouvez mettre à jour votre logiciel Identity Manager par le biais d'une mise à niveau ou d'une migration. On parle de mise à niveau lorsque le logiciel est mis à jour sur le matériel existant. On parle de migration lorsque du nouveau matériel et une nouvelle version du logiciel sont installés. Chacune de ces méthodes possède ses avantages et ses inconvénients ; dans certains cas, une seule méthode peut être utilisée.

- ♦ [Section 11.1, « Mise à niveau », page 91](#)
- ♦ [Section 11.2, « Migration », page 92](#)
- ♦ [Section 11.3, « Plusieurs serveurs associés à un seul ensemble de pilotes », page 92](#)

11.1 Mise à niveau

L'installation de la nouvelle version d'Identity Manager sur le serveur existant constitue une mise à niveau. Pour installer Identity Manager, vous devez mettre à niveau les versions actuelles du système d'exploitation et d'eDirectory vers les versions prises en charge pour Identity Manager 4.0. Pour obtenir la liste des plates-formes prises en charge, reportez-vous au [Chapitre 6, « Configuration système requise », page 49](#).

La réalisation d'une mise à niveau présente plusieurs avantages :

- ♦ Pas de nouveau matériel
- ♦ Pas de migration des données

Elle présente également des inconvénients :

- ♦ Temps hors service lors de la mise à niveau du système d'exploitation et lors du redémarrage du serveur
- ♦ Temps hors service lors de la mise à niveau et du redémarrage d'eDirectory

Dans certains cas, une mise à niveau n'est pas possible ou plusieurs mises à niveau doivent être effectuées. Étant donné qu'Identity Manager 3.5.x et ses versions ultérieures sont les seuls chemins de migration pris en charge, seules ces versions sont concernées par les cas suivants :

Une mise à niveau n'est possible que si Identity Manager 3.5.x est installé sur un système d'exploitation pris en charge. Il existe cependant des situations dans lesquelles il n'est pas possible d'effectuer une mise à niveau. Voici quelques exemples de cas dans lesquels une mise à niveau ne peut pas être réalisée :

- ♦ **Système d'exploitation non pris en charge** : si la version actuelle du système d'exploitation n'est pas prise en charge par Identity Manager 4.0, le seul chemin de mise à niveau possible consiste à migrer vers un nouveau serveur.
- ♦ **Identity Manager 3.0.x** : si la version actuelle d'Identity Manager est 3.0.x, vous ne pouvez pas effectuer une mise à niveau directe. Vous avez alors le choix entre les deux options suivantes :
 - ♦ effectuer une mise à niveau vers Identity Manager 3.5.x et eDirectory 8.8.6, puis vers Identity Manager 4.0. ;
 - ♦ effectuer une migration vers un nouveau serveur.

- ♦ **Module de provisioning basé sur les rôles** : si le module de provisioning basé sur les rôles est installé, vous ne pouvez pas effectuer de mise à niveau. Vous devez réaliser une migration. Pour plus d'informations, reportez-vous au manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide* (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager 4.0).

Si vous effectuez une mise à niveau, passez au [Chapitre 13, « Réalisation d'une mise à niveau »](#), page 95.

11.2 Migration

Une migration installe Identity Manager 4.0 sur un nouveau serveur, puis migre les données existantes vers ce nouveau serveur. Pour vérifier que l'installation est terminée, suivez les instructions du [Chapitre 4, « Liste de vérification pour un système Identity Manager de base »](#), page 41.

L'avantage de la migration réside dans le temps hors service minimal des pilotes. L'inconvénient est qu'elle nécessite du nouveau matériel.

Si vous effectuez une migration, passez au [Chapitre 14, « Exécution d'une migration »](#), page 113.

11.3 Plusieurs serveurs associés à un seul ensemble de pilotes

Si plusieurs serveurs sont associés à un ensemble de pilotes, vous ne pouvez effectuer une mise à niveau ou une migration que sur un serveur à la fois. Si vous n'avez pas le temps de mettre à niveau les serveurs en même temps, les pilotes continuent de fonctionner avec les différentes versions d'Identity Manager jusqu'à ce que chaque serveur soit mis à niveau.

Le moteur d'Identity Manager est compatible avec les versions précédentes ; ainsi, le moteur d'Identity Manager 4.0 peut exécuter sans difficulté les pilotes d'Identity Manager 3.6.x.

Important : si vous activez des fonctions pour des pilotes qui ne sont pris en charge que par Identity Manager 4.0, les pilotes cessent de fonctionner sur les serveurs comportant plusieurs versions d'Identity Manager. Les moteurs plus anciens ne prennent pas en charge les nouvelles fonctions. Les pilotes sont arrêtés jusqu'à ce que tous les serveurs soient mis au niveau vers Identity Manager 4.0.

Versions prises en charge et configuration système requise pour les mises à niveau et migrations

Cette section vous permet de vérifier si votre version d'Identity Manager est prise en charge pour une mise à niveau ou une migration. On parle de mise à niveau lorsque le logiciel est mis à jour sur le matériel existant. On parle de migration lorsque du nouveau matériel et une nouvelle version du logiciel sont installés.

- ♦ [Section 12.1, « Mises à niveau », page 93](#)
- ♦ [Section 12.2, « Migrations », page 94](#)

12.1 Mises à niveau

- ♦ [Section 12.1.1, « Versions prises en charge pour les mises à niveau », page 93](#)
- ♦ [Section 12.1.2, « Configuration système requise », page 94](#)

12.1.1 Versions prises en charge pour les mises à niveau

Le tableau suivant indique les mises à niveau prises en charge pour les versions précédentes d'Identity Manager.

Tableau 12-1 Versions prises en charge pour les mises à niveau

Version installée	Version la plus récente	Mise à niveau prise en charge
DirXML 1.1a	Identity Manager 4.0	Non
Identity Manager 2.x	Identity Manager 4.0	Non
Identity Manager 3.0.x	Identity Manager 4.0	Non
Identity Manager 3.5.x*	Identity Manager 4.0	Oui
Identity Manager 3.6.x*	Identity Manager 4.0	Oui

*Si vous exécutez le module de provisioning basé sur les rôles, vous ne pouvez pas effectuer de mise à niveau. Vous devez réaliser une migration. Pour plus d'informations, reportez-vous au manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide* (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager 4.0).

12.1.2 Configuration système requise

Pour pouvoir effectuer une mise à niveau vers Identity Manager 4.0, les serveurs qui exécutent les services d'Identity Manager doivent répondre à la configuration minimale requise. Reportez-vous au [Chapitre 6, « Configuration système requise », page 49](#) pour connaître la configuration minimale requise pour chaque plate-forme.

12.2 Migrations

- ♦ [Section 12.2.1, « Versions prises en charge pour les migrations », page 94](#)
- ♦ [Section 12.2.2, « Configuration système requise », page 94](#)

12.2.1 Versions prises en charge pour les migrations

Le tableau suivant indique les chemins de migration pris en charge pour les versions précédentes d'Identity Manager.

Tableau 12-2 Versions prises en charge pour les migrations

Version installée	Version la plus récente	Mise à niveau prise en charge
DirXML 1.1a*	Identity Manager 4.0	Non
Identity Manager 2.x*	Identity Manager 4.0	Non
Identity Manager 3.0.x*	Identity Manager 4.0	Non
Identity Manager 3.5.x	Identity Manager 4.0	Oui
Identity Manager 3.6.x	Identity Manager 4.0	Oui

*Vous pouvez effectuer des migrations depuis des versions d'Identity Manager antérieures à la version 3.5.x. Toutefois, elles n'ont pas été testées. Il se peut donc que vous deviez suivre une procédure supplémentaire, qui n'est pas documentée, pour convertir les données de ces anciennes versions dans la version actuelle.

12.2.2 Configuration système requise

Pour pouvoir effectuer une migration vers Identity Manager 4.0, les serveurs qui exécutent les services d'Identity Manager doivent répondre à la configuration minimale requise. Reportez-vous au [Chapitre 6, « Configuration système requise », page 49](#) pour connaître la configuration minimale requise pour chaque plate-forme.

Avant de commencer, assurez-vous d'avoir examiné les différences entre une mise à niveau et une migration. Reportez-vous au [Chapitre 11, « Mise à niveau et migration »](#), page 91.

- ♦ [Section 13.1, « Liste de contrôle de mise à niveau »](#), page 95
- ♦ [Section 13.2, « Création d'une sauvegarde de la configuration actuelle »](#), page 97
- ♦ [Section 13.3, « Mise à niveau d'iManager »](#), page 100
- ♦ [Section 13.4, « Arrêt des pilotes »](#), page 101
- ♦ [Section 13.5, « Mise à niveau d'Analyzer »](#), page 102
- ♦ [Section 13.6, « Mise à niveau de Designer »](#), page 102
- ♦ [Section 13.7, « Mise à niveau du serveur méta-annuaire et des fichiers de module d'interface pilote »](#), page 103
- ♦ [Section 13.8, « Mise à niveau du chargeur distant »](#), page 104
- ♦ [Section 13.9, « Mise à niveau des pilotes vers des paquetages »](#), page 104
- ♦ [Section 13.10, « Restauration de stratégies et de règles personnalisées sur le pilote »](#), page 107
- ♦ [Section 13.11, « Superposition du nouveau pilote sur le fichier de configuration de pilote existant \(obsolète\) »](#), page 109
- ♦ [Section 13.12, « Déploiement du projet converti »](#), page 110
- ♦ [Section 13.13, « Lancement des pilotes »](#), page 110

13.1 Liste de contrôle de mise à niveau

Utilisez la liste de contrôle suivante pour vérifier que toutes les étapes sont exécutées dans le bon ordre afin de garantir la réussite de la mise à niveau du système Identity Manager. Suivez la procédure ci-dessous pour chaque serveur Identity Manager de votre environnement.

- Vérifiez que vous avez téléchargé les fichiers ISO d'Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager »](#), page 45.
- Créez une sauvegarde de la configuration actuelle de votre solution Identity Manager. Créez pour cela des exportations de vos pilotes ou un projet Designer de votre solution Identity Manager. Pour plus d'informations, reportez-vous à la [Section 13.2, « Création d'une sauvegarde de la configuration actuelle »](#), page 97.
- Vérifiez que le système d'exploitation sur les serveurs exécutant Identity Manager soit bien une version prise en charge. Pour obtenir la liste des systèmes d'exploitation pris en charge, reportez-vous au [Chapitre 6, « Configuration système requise »](#), page 49. Si le système d'exploitation ne nécessite qu'un Service Pack pour répondre à la configuration système requise, procédez à la mise à niveau.

Si votre système d'exploitation figure dans la liste ci-dessous, vous ne pouvez pas utiliser cette procédure. Vous devez effectuer une migration au lieu d'une mise à niveau.

- ♦ NetWare
- ♦ Windows NT
- ♦ Windows 2000

- ♦ Red Hat Linux 3
 - ♦ SLES 8
 - ♦ Solaris 8 ou 9
- ❑ Mettez à niveau votre serveur iManager vers iManager 2.7.3. Pour plus d'informations, reportez-vous à la [Section 13.3, « Mise à niveau d'iManager », page 100](#).
 - ❑ Arrêtez les pilotes associés au serveur que vous mettez à niveau. Pour plus d'informations, reportez-vous à la [Section 13.4, « Arrêt des pilotes », page 101](#).
 - ❑ Sur le serveur exécutant Identity Manager, mettez eDirectory à niveau vers la version 8.8.6 ou une version ultérieure. Pour plus d'informations, reportez-vous au [Guide d'installation de Novell eDirectory 8.8 \(<http://www.novell.com/documentation/edir88/>\)](#).
 - ❑ Lancez les pilotes et vérifiez qu'ils démarrent. La réussite de la mise à niveau vers eDirectory 8.8.6 est aussi contrôlée. Pour plus d'informations, reportez-vous à la [Section 13.13, « Lancement des pilotes », page 110](#).
 - ❑ (Conditionnel) Si vous utilisez Analyzer, effectuez une mise à niveau vers Analyzer 1.2. Pour plus d'informations, reportez-vous à la [Section 13.5, « Mise à niveau d'Analyzer », page 102](#).
 - ❑ Effectuez une mise à niveau vers Designer 4.0. Pour plus d'informations, reportez-vous à la [Section 13.6, « Mise à niveau de Designer », page 102](#).
 - ❑ Convertissez le projet Designer. Pour plus d'informations, reportez-vous à la section « [Converting Earlier Projects](#) » (Conversion de projet antérieurs) du manuel [Designer 4.0 for Identity Manager 4.0 Administration Guide](#) (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).
 - ❑ Arrêtez les pilotes associés au serveur que vous mettez à niveau. Pour plus d'informations, reportez-vous à la [Section 13.4, « Arrêt des pilotes », page 101](#).
 - ❑ Mettez le serveur méta-annuaire à niveau. Pour plus d'informations, reportez-vous à la [Section 13.7, « Mise à niveau du serveur méta-annuaire et des fichiers de module d'interface pilote », page 103](#).
 - ❑ (Facultatif) Si l'un des pilotes dans l'ensemble de pilotes de ce serveur est un pilote de chargeur distant, mettez à niveau les serveurs de chargeur distant pour chaque pilote. Pour plus d'informations, reportez-vous à la [Section 13.8, « Mise à niveau du chargeur distant », page 104](#).
 - ❑ (Facultatif) Si ce serveur est votre serveur d'application utilisateur, exécutez les étapes supplémentaires suivantes :
 - ❑ Le pilote de l'application utilisateur doit être migré dans Designer. Pour plus d'informations, reportez-vous au manuel [Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide](#) (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager 4.0).
 - ❑ Créez un nouveau pilote de service de rôles et de ressources. Le pilote de service de rôles et de ressources n'est pas migré. Si vous avez déjà un pilote de service de rôles et de ressources, vous devez créer un nouveau pilote pour Identity Manager 4.0. Pour plus d'informations, reportez-vous au manuel [Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide](#) (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager 4.0).

- ❑ Déployez le pilote d'application utilisateur migré dans le coffre-fort d'identité. Pour plus d'informations, reportez-vous au manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide* (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager 4.0).
- ❑ Mettez à niveau l'application utilisateur. Pour plus d'informations, reportez-vous au manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide* (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager 4.0).
- ❑ (Facultatif) Superposez les pilotes existants aux fichiers de configuration du nouveau pilote pour obtenir de nouvelles stratégies. Cette action n'est requise que si une nouvelle fonction est incluse dans les stratégies pour un pilote que vous voulez ajouter à votre pilote existant. Pour plus d'informations, reportez-vous à la [Section 13.11, « Superposition du nouveau pilote sur le fichier de configuration de pilote existant \(obsolète\) », page 109](#).
- ❑ (Facultatif) Restaurez les règles et stratégies personnalisées vers les pilotes. Quand vous superposez les nouveaux fichiers de configuration du pilote, les stratégies sont écrasées. La restauration des stratégies n'est donc requise que si vous avez superposé le nouveau fichier de configuration du pilote. Pour plus d'informations, reportez-vous à la [Section 13.10, « Restauration de stratégies et de règles personnalisées sur le pilote », page 107](#).
- ❑ 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).
- ❑ Démarrez les pilotes associés à ce serveur. Pour plus d'informations, reportez-vous à la [Section 13.13, « Lancement des pilotes », page 110](#).
- ❑ (Conditionnel) Si vous utilisez Novell Sentinel, vous devez effectuer une mise à jour vers Novell Sentinel 6.1. Pour plus d'informations sur la mise à niveau de Sentinel, reportez-vous au [Guide d'installation de Sentinel](http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel6_installationguide.pdf) (http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel6_installationguide.pdf).
- ❑ Activez le serveur méta-annuaire et tout pilote mis à niveau. Pour plus d'informations, reportez-vous au [Chapitre 8, « Activation des produits Novell Identity Manager », page 75](#).

13.2 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. Aucune étape supplémentaire n'est requise si vous utilisez l'application utilisateur. Toute la configuration de l'application utilisateur est stockée dans le pilote de cette application. Il existe deux façons de créer une sauvegarde :

- ♦ [Section 13.2.1, « Vérification de l'actualité de votre projet Designer », page 98](#)
- ♦ [Section 13.2.2, « Création d'une exportation des pilotes », page 99](#)

13.2.1 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 de votre solution Identity Manager vous permet d'exporter tous les pilotes en une seule fois au lieu de devoir créer un fichier d'exportation pour chaque pilote.

- ♦ [« Exportation du projet actuel » page 98](#)
- ♦ [« Création d'un nouveau projet à partir du coffre-fort d'identité » page 98](#)

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*.
Sauvegardez le projet à n'importe quel emplacement, sauf sur l'espace de travail actuel. Lorsque vous effectuez une mise à niveau vers Designer, vous devez créer un nouvel emplacement d'espace de travail. Pour plus d'informations, reportez-vous à la section [« Exporting a Project »](#) (Exportation d'un projet) du manuel *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, utilisez la procédure suivante :

- 1 Installez Designer 3.5.
Avec Designer 3.5, vous pouvez créer un projet Identity Manager 3.6.x. Pour plus d'informations, reportez-vous à la [Section 7.2, « Installation de Designer », page 60](#).
- 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'outil, 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 du 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, passez à l'[Étape 16](#).
- 16 Dans la barre d'outils, cliquez sur *Activité en direct > Importer*.
- 17 Répétez la procédure de l'[Étape 8](#) à l'[Étape 14](#) pour chaque coffre-fort d'identité supplémentaire.

13.2.2 Création d'une exportation des pilotes


Lorsque vous créez une exportation des pilotes, votre configuration actuelle est sauvegardée.

- ♦ [« Utilisation de Designer pour créer une exportation du pilote » page 99](#)
- ♦ [« Utilisation d'iManager pour créer une exportation du pilote » page 100](#)

Utilisation de Designer pour créer une exportation du pilote

- 1 Vérifiez que votre projet dans Designer dispose de la dernière version en date de votre pilote. Pour connaître la procédure, reportez-vous à la section [« Importing a Library, a Driver Set, or a Driver from the Identity Vault »](#) (Importation d'une bibliothèque, d'un ensemble de pilotes ou d'un pilote depuis le coffre-fort d'identité) du manuel *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.

13.3 Mise à niveau d'iManager

Pour pouvoir utiliser les fonctionnalités mises à jour des plug-ins Identity Manager, vous devez mettre à niveau iManager.

iManager ne peut être installé que sous Windows ou Linux. Si votre serveur méta-annuaire est installé sous Solaris, vous devez installer iManager sur un serveur distinct.

Si iManager version 2.6 ou antérieure est installé, vous ne pouvez pas utiliser cette procédure pour mettre à niveau iManager. Utilisez la procédure de mise à niveau adéquate décrite dans le [Guide d'installation de Novell iManager 2.7](http://www.novell.com/documentation/imanager27/imanager_install_27/data/bhxda4r.html) (http://www.novell.com/documentation/imanager27/imanager_install_27/data/bhxda4r.html).

Pour mettre à niveau iManager :

- 1 (Conditionnel) Si vous effectuez l'installation sous Linux, loguez-vous en tant qu'utilisateur `root` avant de lancer l'installation.
- 2 Accédez au support d'installation d'Identity Manager sur votre plate-forme.
- 3 Lancez le programme d'installation d'iManager adapté à votre plate-forme :
 - ♦ **Linux** : `IDM4.0_Lin/products/iManager/installs/linux/iManagerInstallLinux.bin`
Pour exécuter le fichier binaire, saisissez `./iManagerInstallLinux.bin` à partir du répertoire d'installation.
 - ♦ **Windows** :
`IDM4.0_Win:\product\iManager\installs\win\iManagerinstall.exe`
- 4 Sélectionnez la langue dans laquelle vous souhaitez installer iManager.
- 5 Lisez et acceptez l'accord de licence.
- 6 Sélectionnez les éléments à installer suivants : iManager 2.7, Tomcat et la JVM.
- 7 Cliquez sur OK pour supprimer l'ancienne version de Tomcat installée avec l'ancienne version d'iManager.
- 8 Cliquez sur Oui pour télécharger les plug-ins.
- 9 Accédez à l'emplacement par défaut pour télécharger les plug-ins.




- 10 Choisissez d'installer les plug-ins sélectionnés par défaut.
- 11 Cliquez sur Non lorsque vous êtes invité à installer les plug-ins à partir d'un répertoire local.
- 12 Indiquez le port HTTP sur lequel Tomcat doit s'exécuter. Le port par défaut est 8080.
- 13 Indiquez le port SSL sur lequel Tomcat doit s'exécuter. Le port par défaut est 8443.
- 14 Passez en revue les éléments sélectionnés, puis cliquez sur *OK* pour exécuter la mise à niveau.
- 15 Une fois l'installation terminée, redémarrez Tomcat pour appliquer les modifications.

13.4 Arrêt des pilotes



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

- ♦ [Section 13.4.1, « Utilisation de Designer pour arrêter les pilotes », page 101](#)
- ♦ [Section 13.4.2, « Utilisation d'iManager pour arrêter les pilotes », page 101](#)

13.4.1 Utilisation de Designer pour arrêter les pilotes

- 1 Dans Designer, 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.

13.4.2 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.

13.5 Mise à niveau d'Analyzer

Si Analyzer est installé, vous devez le mettre à niveau pour qu'il fonctionne avec Identity Manager 4.0. S'il n'est pas installé, ignorez cette section et passez à la [Section 13.6, « Mise à niveau de Designer », page 102](#).

Analyzer ne peut être installé que sous Windows ou Linux. Si votre serveur méta-annuaire est installé sous Solaris, vous devez installer Analyzer sur un serveur distinct.

Pour mettre à niveau Analyzer :

- 1** Lancez le programme d'installation d'Analyzer à partir du support d'Identity Manager :
 - ♦ **Linux** : `IDM4.0_Lin/products/Analyzer/install`
Pour exécuter le fichier binaire, saisissez `./install`.
 - ♦ **Windows** : `IDM4.0_Win:\products\ANALZYER\install.exe`
- 2** Sélectionnez la langue dans laquelle vous souhaitez exécuter Analyzer, puis lisez et acceptez l'accord de licence.
- 3** Indiquez le répertoire d'installation d'Analyzer, puis cliquez sur *Oui* dans le message indiquant qu'Analyzer est déjà installé.
- 4** Indiquez si vous souhaitez créer des raccourcis sur votre bureau ou dans le menu du bureau.
- 5** Lisez le résumé, puis cliquez sur *Installer*.
- 6** Passez en revue le résumé de l'installation, puis cliquez sur *Terminé*.

13.6 Mise à niveau de Designer

Avant de mettre Designer à niveau, vérifiez de bien exporter vos projets afin d'en générer une sauvegarde. Pour savoir comment exporter 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 serveur méta-annuaire est installé sous Solaris, vous devez installer Designer sur un serveur distinct.

Pour mettre à niveau Designer :

- 1** Lancez le programme d'installation de Designer à partir du support d'Identity Manager :
 - ♦ **Linux** : `IDM4.0_Lin/products/Designer/install`
Pour exécuter le fichier binaire, saisissez `./install`.
 - ♦ **Windows** : `IDM4.0_Win:\products\Designer\install.exe`
- 2** Sélectionnez la langue dans laquelle vous souhaitez installer Designer, puis lisez et acceptez l'accord de licence.
- 3** Indiquez le répertoire d'installation de Designer, puis cliquez sur *Oui* dans le message indiquant que Designer est déjà installé.

- 4 Indiquez si vous souhaitez créer des raccourcis sur votre 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 Choisissez de lancer Designer, puis cliquez sur *Terminé*.
- 8 Spécifiez l'emplacement de votre espace de travail Designer, puis cliquez sur *OK*.
- 9 Cliquez sur *OK* dans le message d'avertissement indiquant que votre projet doit être fermé et converti.
- 10 Dans la vue Projet, étendez le projet, puis double-cliquez sur *Le projet doit être converti*.
- 11 Passez en revue les étapes effectuées par l'assistant de conversion de projet, puis cliquez sur *Suivant*.
- 12 Attribuez un nom à la sauvegarde de votre projet, puis cliquez sur *Suivant*.
- 13 Passez en revue le résumé de la procédure de conversion, puis cliquez sur *Convertir*.
- 14 Passez en revue le résumé une fois la conversion terminée, puis cliquez sur *Ouvrir*.

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

13.7 Mise à niveau du serveur méta-annuaire et des fichiers de module d'interface pilote

Une fois les composants de prise en charge mis à niveau, vous devez mettre à niveau le serveur méta-annuaire. Lors de la procédure de mise à niveau, les fichiers de 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 13.4, « Arrêt des pilotes », page 101](#).
- 2 Lancez le programme d'installation du serveur méta-annuaire à partir du support d'Identity Manager :
 - ♦ **Linux** : `IDM4.0_Lin/products/IDM/install.bin`
 - ♦ **Solaris** : `IDM4.0_Solaris/products/IDM/install.bin`
Pour exécuter le fichier binaire, saisissez `./install.bin`.
 - ♦ **Windows** : `IDM4.0_Win:\products\IDM\Windows\setup\idm_install.exe`
- 3 Sélectionnez la langue d'installation, puis lisez et acceptez l'accord de licence.
- 4 Sélectionnez les options *Serveur méta-annuaire de Novell Identity Manager, Plug-ins Novell iManager pour Identity Manager* et *Utilitaires* pour mettre à jour le serveur méta-annuaire et les fichiers de module d'interface pilote.
- 5 Spécifiez un utilisateur et le mot de passe utilisateur avec droits d'administrateur sur eDirectory au format LDAP.
- 6 Lisez le résumé, puis cliquez sur *Installer*.
- 7 Lisez le résumé de l'installation, puis cliquez sur *Terminé*.

Remarque : après la mise à niveau d'Identity Manager 32 bits vers la version 64 bits, le pilote GroupWise et les pilotes personnalisés natifs ne fonctionnent plus.

13.8 Mise à niveau du chargeur distant

Si vous exécutez le chargeur distant, vous devez aussi mettre à niveau les fichiers du chargeur distant.

- 1 Créez une sauvegarde des fichiers de configuration du chargeur distant. L'emplacement par défaut des fichiers est :
 - ♦ **Windows** : `C:\Novell\RemoteLoader\ nomchargeurdistant-config.txt`
 - ♦ **Linux** : créez votre fichier de configuration dans le chemin de `rdxml`.
- 2 Vérifiez que les pilotes sont bien arrêtés. Pour connaître les instructions, reportez-vous à la [Section 13.4, « Arrêt des pilotes », page 101](#).
- 3 Arrêtez le service ou le daemon du chargeur distant pour chaque pilote.
 - ♦ **Windows** : dans la console du chargeur distant, sélectionnez l'instance du chargeur distant, puis cliquez sur *Arrêter*.
 - ♦ **Linux** : `rdxml -config chemin_vers_fichier_config -u`
 - ♦ **Chargeur distant Java** : `dirxml_jremote -config chemin_vers_fichier_config -u`
- 4 Exécutez les programmes d'installation du chargeur distant.

La procédure d'installation met à jour les fichiers et les binaires avec la version actuelle. Pour plus d'informations, reportez-vous à la [Section 7.6, « Installation du chargeur distant », page 66](#).
- 5 Une fois l'installation terminée, vérifiez que vos fichiers de configuration contiennent bien les informations de votre environnement.
- 6 (Conditionnel) Si vous rencontrez un problème avec le fichier de configuration, copiez le fichier de sauvegarde créé à l'[Étape 1](#). Sinon, passez à l'[Étape 7](#).
- 7 Lancez le service ou le daemon du chargeur distant pour chaque pilote.
 - ♦ **Windows** : dans la console du chargeur distant, sélectionnez l'instance du chargeur distant, puis cliquez sur *Démarrer*.
 - ♦ **Linux** : `rdxml -config chemin_vers_fichier_config -sp password password`
 - ♦ **Chargeur distant Java** : `dirxml_jremote -config chemin_vers_fichier_config -sp password password`

Remarque : après la mise à niveau du chargeur distant 32 bits vers la version 64 bits, le pilote GroupWise et les pilotes personnalisés natifs ne fonctionnent plus.

13.9 Mise à niveau des pilotes vers des paquetages

Les paquetages sont une nouvelle fonction de gestion de contenu proposée par Identity Manager 4.0. Tout le nouveau contenu de pilote est désormais fourni via des paquetages et non plus via des fichiers de configuration de pilote.

Les paquetages sont gérés, actualisés et créés à l'aide de Designer. iManager est compatible avec les paquetages. Toutefois, les modifications apportées au contenu de pilote via iManager ne sont pas conservées 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 façons de mettre à niveau vos pilotes vers des paquetages :

- ♦ [Section 13.9.1, « Création d'un nouveau pilote », page 105](#)
- ♦ [Section 13.9.2, « Remplacement du contenu existant par le contenu des paquetages », page 105](#)
- ♦ [Section 13.9.3, « Conservation du contenu existant et ajout de nouveau contenu à l'aide des paquetages », page 106](#)

13.9.1 Création d'un nouveau pilote

La manière la plus simple et la plus propre de mettre à niveau un pilote vers un paquetage consiste à supprimer le pilote existant et à en créer un nouveau à l'aide d'un paquetage. Ajoutez toutes les fonctionnalités que vous souhaitez au nouveau pilote. La procédure est différente pour chaque pilote. Pour connaître la procédure, reportez-vous aux guides des différents pilotes sur le [site Web de documentation des pilotes Identity Manager](http://www.novell.com/documentation/idm40drivers/) (<http://www.novell.com/documentation/idm40drivers/>).

13.9.2 Remplacement du contenu existant par le contenu des paquetages

Si vous devez conserver les associations créées par le pilote, vous ne pouvez pas le supprimer et le recréer. Cette option vous permet de conserver les associations tout en créant le contenu du pilote à l'aide de paquetages.

Pour remplacer le contenu existant par le contenu des paquetages :

- 1** Créez une sauvegarde du pilote et de tout son contenu personnalisé.
Pour connaître la procédure, reportez-vous à la [Section 13.2.2, « Création d'une exportation des pilotes », page 99](#).
- 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 connaître les 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 connaître la procédure, reportez-vous au 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 obligatoires, optionnels et de base au pilote afin d'obtenir les fonctionnalités souhaitées. Cette procédure varie d'un pilote à l'autre.

Pour connaître la procédure, reportez-vous au 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 toutes les stratégies et règles personnalisées sur le pilote. Pour connaître la procédure, reportez-vous à la [Section 13.10, « Restauration de stratégies et de règles personnalisées sur le pilote », page 107.](#)

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

13.9.3 Conservation du contenu existant et ajout de nouveau contenu à l'aide paquetages

Vous pouvez conserver le pilote tel quel et lui ajouter de nouvelles fonctionnalités à l'aide de paquetages, tant que les fonctionnalités des paquetages n'empiètent pas sur les fonctionnalités actuelles du pilote. Lorsque vous installez un paquetage, celui-ci peut écraser les stratégies existantes et empêcher le pilote de fonctionner.

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

- 1 Créez une sauvegarde du pilote et de tout son contenu personnalisé.
Pour connaître la procédure, reportez-vous à la [Section 13.2.2, « Création d'une exportation des pilotes », page 99.](#)
- 2 Importez les paquetages de pilotes dans le catalogue de paquetages.
Pour connaître les 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 connaître la procédure, reportez-vous au 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. Cette procédure varie d'un pilote à l'autre.
Pour connaître la procédure, 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 les nouvelles fonctionnalités ajoutées par les paquetages.

13.10 Restauration de stratégies et de règles personnalisées sur le pilote

Si vous disposez de stratégies ou de règles personnalisées, elles doivent être restaurées sur le pilote une fois que vous avez superposé 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 13.10.1, « Utilisation de Designer pour restaurer les stratégies et les règles personnalisées sur le pilote », page 107](#)
- ♦ [Section 13.10.2, « Utilisation d'iManager pour restaurer les stratégies et les règles personnalisées sur le pilote », page 108](#)


13.10.1 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 107](#)
- ♦ [« Ajout d'une stratégie personnalisée via la vue Afficher le flux de stratégie » page 108](#)

Ajout d'une stratégie personnalisée via la vue Aperçu

Exécutez cette procédure dans un environnement de test avant de déplacer le pilote mis à niveau dans votre environnement de production.


- 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 13.13, « Lancement des pilotes », page 110](#). Pour plus d'informations sur le test du pilote, reportez-vous au point « [Testing Policies with Policy Simulator](#) » (Test des stratégies avec le simulateur de stratégies) de la section *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**

Exécutez cette procédure dans un environnement de test avant de déplacer le pilote mis à niveau dans votre environnement de production.

- 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 13.13](#), « [Lancement des pilotes](#) », page 110. Pour plus d'informations sur le test du pilote, reportez-vous au point « [Testing Policies with Policy Simulator](#) » (Test des stratégies avec le simulateur de stratégies) de la section *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.

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

Exécutez cette procédure dans un environnement de test avant de déplacer le pilote mis à niveau dans votre environnement de production.

- 1 Dans iManager, sélectionnez *Identity Manager > Présentation d'Identity Manager*.
- 2 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 13.13, « Lancement des pilotes », page 110](#). 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.

13.11 Superposition du nouveau pilote sur le fichier de configuration de pilote existant (obsolète)

Identity Manager 4.0 n'utilise plus de fichiers de configuration de pilote, mais des paquets. Il n'existe aucun nouveau fichier de configuration pour cette version. Tout le nouveau contenu de pilote est désormais fourni dans des paquets.

Avant de commencer, assurez-vous que les stratégies personnalisées disposent de noms différents de ceux des stratégies par défaut. Quand une configuration de pilote est déposée avec un nouveau fichier de pilote, les stratégies existantes sont écrasées. Si vos stratégies personnalisées n'ont pas un nom unique, vous les perdrez.

Le fait de superposer le nouveau fichier de configuration de pilote sur votre pilote existant permet de mettre à jour le pilote avec les nouvelles stratégies ou fonctionnalités qui figurent dans le fichier de configuration de pilote.

- ♦ [Section 13.11.1, « Utilisation de Designer pour superposer le nouveau pilote sur le fichier de configuration de pilote existant », page 109](#)
- ♦ [Section 13.11.2, « Utilisation d'iManager pour superposer le nouveau pilote sur le fichier de configuration de pilote existant », page 110](#)

13.11.1 Utilisation de Designer pour superposer le nouveau pilote sur le fichier de configuration de pilote existant


Important : vérifiez que vos stratégies personnalisées n'ont pas le même nom que les stratégies par défaut, de manière à ne perdre aucune donnée.

- 1 Dans Modeler, cliquez avec le bouton droit de la souris sur la ligne du pilote que vous mettez à niveau.
- 2 Sélectionnez *Exécuter l'assistant de configuration*.
- 3 Cliquez sur *Oui* dans la page d'avertissement.
Le message d'avertissement vous informe que tous les paramètres et stratégies de pilote vont être réinitialisés.
- 4 Naviguez jusqu'à la configuration du pilote que vous mettez à niveau, puis cliquez sur *Exécuter*.
- 5 Indiquez les informations du pilote, puis cliquez sur *Suivant*.
Il est possible de devoir préciser plusieurs pages d'informations.
- 6 Cliquez sur *OK* sur la page des résultats.

- 7 Examinez les paramètres et stratégies du pilote pour vous assurer que tout soit défini de la façon désirée.
- 8 Si vous disposez de stratégies personnalisées, passez à la [Section 13.10, « Restauration de stratégies et de règles personnalisées sur le pilote », page 107](#). Sinon, passez à la [Section 13.13, « Lancement des pilotes », page 110](#).

13.11.2 Utilisation d'iManager pour superposer le nouveau pilote sur le fichier de configuration de pilote existant

Important : vérifiez que vos stratégies personnalisées n'ont pas le même nom que les stratégies par défaut, de manière à ne perdre aucune donnée.

- 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 > Ajouter un pilote*, puis sur *Suivant* dans la page Assistant Nouveau pilote.
- 5 Sélectionnez la configuration de pilote à superposer, puis cliquez sur *Suivant*.
- 6 Dans le champ *Pilotes existants*, naviguez jusqu'au pilote à mettre à niveau et sélectionnez-le.
- 7 Indiquez les informations du pilote, puis cliquez sur *Suivant*.
- 8 Sur la page de résumé, sélectionnez *Mettre à jour tout ce qui concerne ce pilote et ces bibliothèques de stratégies*.
- 9 Cliquez sur *Suivant*, puis sur *Terminer* dans la page de résumé.
- 10 Examinez les paramètres et stratégies du pilote pour vous assurer que tout soit défini de la façon désirée.
- 11 Si vous disposez de stratégies personnalisées, passez à la [Section 13.10, « Restauration de stratégies et de règles personnalisées sur le pilote », page 107](#). Sinon, passez à la [Section 13.13, « Lancement des pilotes », page 110](#).

13.12 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).

13.13 Lancement des pilotes



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

- ♦ [Section 13.13.1, « Utilisation de Designer pour lancer les pilotes », page 111](#)
- ♦ [Section 13.13.2, « Utilisation d'iManager pour démarrer les pilotes », page 111](#)

13.13.1 Utilisation de Designer pour lancer les pilotes

- 1 Dans Designer, sélectionnez l'objet Coffre-fort d'identité  sous 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 au point « [Testing Policies with Policy Simulator](#) » (Test des stratégies avec le simulateur de stratégies) de la section *Policies in Designer 4.0* (Stratégies dans Designer 4.0).

13.13.2 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.

Avant de commencer, assurez-vous d'avoir examiné les différences entre une mise à niveau et une migration. Reportez-vous au [Chapitre 11, « Mise à niveau et migration »](#), page 91.

- ♦ [Section 14.1, « Liste de contrôle de migration »](#), page 113
- ♦ [Section 14.2, « Ajout du nouveau serveur à l'ensemble de pilotes »](#), page 115
- ♦ [Section 14.3, « Modification des informations spécifiques du serveur »](#), page 115
- ♦ [Section 14.4, « Suppression de l'ancien serveur de l'ensemble de pilotes »](#), page 117

14.1 Liste de contrôle de migration


Utilisez la liste de contrôle suivante pour vérifier que toutes les étapes ont été exécutées dans le bon ordre et assurer la réussite de la migration du système Identity Manager. Suivez ces étapes pour chaque serveur d'Identity Manager de votre environnement.

- Vérifiez que vous avez téléchargé les fichiers ISO d'Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager »](#), page 45.
- Créez une sauvegarde de la configuration actuelle de votre solution Identity Manager. Pour ce faire, créez des exportations de vos pilotes ou un projet Designer de votre solution Identity Manager. Pour plus d'informations, reportez-vous à la [Section 13.2, « Création d'une sauvegarde de la configuration actuelle »](#), page 97.
- Installez le système d'exploitation désiré. Pour obtenir la liste des plates-formes prises en charge, reportez-vous au [Chapitre 6, « Configuration système requise »](#), page 49.
- Installez eDirectory 8.8.6 sur le serveur. Pour plus d'informations, reportez-vous au [Guide d'installation de Novell eDirectory 8.8 \(http://www.novell.com/documentation/edir88/index.html\)](#).
- Ajoutez à ce nouveau serveur les mêmes répliques que celles qui figurent sur le serveur d'Identity Manager actuel. Pour plus d'informations, reportez-vous à la section [Administration de répliques \(http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html\)](#) dans le [Guide d'administration d'eDirectory \(http://www.novell.com/documentation/edir88/pdfdoc/edir88/edir88.pdf\)](#).
- Installez Identity Manager 4.0. Reportez-vous au [Chapitre 4, « Liste de vérification pour un système Identity Manager de base »](#), page 41 pour vérifier que toutes les étapes sont réalisées.
- Si l'un des pilotes dans l'ensemble de pilotes est un pilote de chargeur distant, mettez à niveau le serveur de chargeur distant pour chaque pilote. Pour plus d'informations, reportez-vous à la [Section 13.8, « Mise à niveau du chargeur distant »](#), page 104.
- (Facultatif) Si l'ancien serveur est votre serveur d'application utilisateur, exécutez les étapes supplémentaires suivantes :
 - Exécutez l'utilitaire NrfCaseUpdate. Pour plus d'informations, 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](#).

- ❑ Le pilote de l'application utilisateur doit être migré dans Designer. Pour plus d'informations, reportez-vous au manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide* (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager 4.0).
- ❑ Créez un nouveau pilote de service de rôles et de ressources. Le pilote de service de rôles et de ressources n'est pas migré. Si vous avez déjà un pilote de service de rôles et de ressources, vous devez créer un nouveau pilote pour Identity Manager 4.0. Pour plus d'informations, reportez-vous au manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide* (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager 4.0).
- ❑ Déployez le pilote d'application utilisateur migré dans le coffre-fort d'identité. Pour plus d'informations, reportez-vous au manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide* (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager 4.0).
- ❑ Installez l'application utilisateur sur ce nouveau serveur. Pour plus d'informations, reportez-vous au manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide* (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager 4.0).
- ❑ Ajoutez le nouveau serveur à l'ensemble de pilotes. Pour plus d'informations, reportez-vous à la [Section 14.2, « Ajout du nouveau serveur à l'ensemble de pilotes », page 115](#).
- ❑ Modifiez les informations spécifiques du serveur pour chaque pilote. Si vous utilisez iManager, vous devez le faire manuellement. Si vous migrez d'un serveur Identity Manager antérieur à la version 3.5 vers un serveur Identity Manager 3.5 ou ultérieur, vous devez utiliser iManager. Pour tous les autres chemins de migration pris en charge, vous pouvez utiliser Designer. Pour plus d'informations, reportez-vous à la [Section 14.3, « Modification des informations spécifiques du serveur », page 115](#).
- ❑ (Facultatif) Exécutez `configupdate.sh` ou `configupdate.bat` pour déplacer les informations spécifiques du serveur de l'ancien serveur vers le nouveau pour la configuration de l'application utilisateur. Pour plus d'informations, reportez-vous à la section « [Référence de configuration de l'application utilisateur IDM](#) » du *Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0*.
- ❑ (Facultatif) Mettez à niveau vos pilotes pour utiliser des paquetages. Tout le contenu des pilotes est fourni via des paquetages, et non plus au moyen d'un fichier de configuration de pilote. Pour plus d'informations, reportez-vous à la [Section 13.9, « Mise à niveau des pilotes vers des paquetages », page 104](#).
- ❑ (Facultatif) Restaurez les règles et stratégies personnalisées vers les pilotes. Lorsque vous mettez à jour vos pilotes vers des paquetages, les stratégies sont écrasées. Par conséquent, vous ne devez les restaurer que si vous avez mis à niveau vos pilotes pour utiliser des paquetages. Pour plus d'informations, reportez-vous à la [Section 13.10, « Restauration de stratégies et de règles personnalisées sur le pilote », page 107](#).
- ❑ Supprimez l'ancien serveur de l'ensemble de pilotes. Pour plus d'informations, reportez-vous à la [Section 14.4, « Suppression de l'ancien serveur de l'ensemble de pilotes », page 117](#).
- ❑ Si vous utilisez Novell Sentinel, vous devez effectuer une mise à jour vers Novell Sentinel 6.1. Pour plus d'informations sur la mise à niveau de Sentinel, reportez-vous au *Guide d'installation de Sentinel* (http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel60_installationguide.pdf).
- ❑ Activez le serveur méta-annuaire et tout pilote mis à niveau. Pour plus d'informations, reportez-vous au [Chapitre 8, « Activation des produits Novell Identity Manager », page 75](#).

14.2 Ajout du nouveau serveur à l'ensemble de pilotes

Si vous utilisez iManager, vous devez ajouter le nouveau serveur à l'ensemble de pilotes. Designer contient un assistant de migration de serveur qui accomplit cette tâche pour vous. Si vous utilisez Designer, ignorez cette étape et allez à la [Section 14.3, « Modification des informations spécifiques du serveur », page 115](#). Si vous utilisez iManager, exécutez la procédure suivante :

- 1 Dans iManager, cliquez sur  pour afficher la page d'administration d'Identity Manager.
- 2 Cliquez sur *Présentation d'Identity Manager*.
- 3 Naviguez jusqu'au conteneur dans lequel se trouve l'ensemble de pilotes et sélectionnez-le.
- 4 Cliquez sur le nom de l'ensemble de pilotes pour accéder à la page Présentation de l'ensemble de pilotes.
- 5 Cliquez sur *Serveurs > Ajouter un serveur*.
- 6 Recherchez et sélectionnez le nouveau serveur Identity Manager 4.0, puis cliquez sur *OK*.

14.3 Modification des informations spécifiques du serveur

Vous devez modifier toutes les informations spécifiques du serveur stockées dans chaque pilote en fonction des informations du nouveau serveur. Les informations spécifiques du serveur sont contenues dans :

- ♦ Les valeurs de configuration globale
- ♦ Les valeurs de contrôle du moteur
- ♦ Les mots de passe nommés
- ♦ Les informations d'authentification de pilote
- ♦ Les options de démarrage de pilote
- ♦ Les paramètres de pilote
- ♦ Les données d'ensemble de pilotes

Cela peut être fait dans Designer ou dans iManager. Si vous utilisez Designer, le processus est automatisé. Si vous utilisez iManager, vous devez le faire manuellement. Si vous migrez d'un serveur Identity Manager antérieur à la version 3.5 vers un serveur Identity Manager 3.5 ou ultérieur, vous devez utiliser iManager. Pour tous les autres chemins de migration pris en charge, vous pouvez utiliser Designer.


- ♦ [Section 14.3.1, « Modification des informations spécifiques du serveur dans Designer », page 116](#)
- ♦ [Section 14.3.2, « Modification des informations spécifiques du serveur dans iManager », page 116](#)

14.3.1 Modification des informations spécifiques du serveur dans Designer

La procédure a une incidence sur tous les pilotes stockés dans l'ensemble de pilotes.

- 1 Dans Designer, ouvrez votre projet.
- 2 Dans l'onglet *Aperçu*, cliquez avec le bouton droit sur le serveur, puis sélectionnez *Migrer*.
- 3 Lisez la présentation pour savoir quels éléments sont migrés vers le nouveau serveur, puis cliquez sur *Suivant*.
- 4 Sélectionnez le serveur cible dans la liste des serveurs disponibles, puis cliquez sur *Suivant*.
Les serveurs répertoriés sont ceux qui ne sont actuellement pas associés à un ensemble de pilotes et qui sont équivalents à la version d'Identity Manager du serveur source ou plus récents que celle-ci.
- 5 Sélectionnez *Activer le serveur cible*.
Parmi les trois options proposées, *Activer le serveur cible* est l'option recommandée.
 - ♦ **Activer le serveur cible** : les paramètres du serveur source sont copiés vers le serveur cible et les pilotes désactivés sur le serveur source.
 - ♦ **Garder le serveur source actif** : les paramètres ne sont pas copiés et tous les pilotes sont désactivés sur le serveur cible.
 - ♦ **Les serveurs source et cible sont tous deux activés** : les paramètres du serveur source sont copiés vers le serveur cible sans désactiver les pilotes sur les serveurs source et cible. Cette option n'est pas recommandée. En cas de démarrage des deux pilotes, les mêmes informations sont écrites dans deux files d'attente, ce qui peut provoquer des altérations.
- 6 Cliquez sur *Migrer*.
- 7 Déployer les pilotes modifiés vers le coffre-fort d'identité.
Pour plus d'informations, reportez-vous à la section « [Deploying a Driver to an Identity Vault](#) » (Déploiement d'un pilote vers le 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).
- 8 Démarrez les pilotes.
Pour plus d'informations, reportez-vous à la [Section 13.13, « Lancement des pilotes », page 110](#).

14.3.2 Modification des informations spécifiques du serveur dans iManager

- 1 Dans iManager, cliquez sur  pour afficher la page d'administration d'Identity Manager.
- 2 Cliquez sur *Présentation d'Identity Manager*.
- 3 Naviguez jusqu'au conteneur dans lequel se trouve l'ensemble de pilotes et sélectionnez-le.
- 4 Cliquez sur le nom de l'ensemble de pilotes pour accéder à la page Présentation de l'ensemble de pilotes.
- 5 Cliquez dans l'angle supérieur droit, puis cliquez sur *Arrêter le pilote*.
- 6 Cliquez dans l'angle supérieur droit, puis cliquez sur *Modifier les propriétés*.

- 7 Copiez ou migrez l'ensemble des paramètres de pilote spécifiques au serveur, valeurs de configuration globale, valeurs de contrôle du moteur, mots de passe nommés, données d'authentification de pilote et options de démarrage de pilote qui contiennent les informations de l'ancien serveur vers les informations du nouveau serveur. Les valeurs de configuration globale et autres paramètres de l'ensemble de pilotes, tels que la taille maximale de tas, les paramètres Java, etc., doivent être identiques à ceux de l'ancien serveur.
- 8 Cliquez sur *OK* pour sauvegarder toutes les modifications.
- 9 Cliquez dans l'angle supérieur droit du pilote pour le démarrer.
- 10 Répétez la procédure de l'[Étape 5](#) à l'[Étape 9](#) pour chaque pilote dans l'ensemble de pilotes.

14.4 Suppression de l'ancien serveur de l'ensemble de pilotes

Une fois que le nouveau serveur exécute tous les pilotes, il faut retirer l'ancien serveur de l'ensemble de pilotes.


- ♦ [Section 14.4.1, « Utilisation de Designer pour retirer l'ancien serveur de l'ensemble de pilotes », page 117](#)
- ♦ [Section 14.4.2, « Utilisation d'iManager pour retirer l'ancien serveur de l'ensemble de pilotes », page 117](#)
- ♦ [Section 14.4.3, « Déclassement de l'ancien serveur », page 118](#)

14.4.1 Utilisation de Designer pour retirer l'ancien serveur de l'ensemble de pilotes

- 1 Dans Designer, ouvrez votre projet.
- 2 Dans Modeler, cliquez avec le bouton droit sur l'ensemble de pilotes, puis sélectionnez *Propriétés*.
- 3 Sélectionnez *Liste de serveurs*.
- 4 Sélectionnez l'ancien serveur d'Identity Manager dans la liste de *Serveurs sélectionnés*, puis cliquez sur le signe < pour retirer le serveur de la liste des *Serveurs sélectionnés*.
- 5 Cliquez sur *OK* pour enregistrer les modifications.
- 6 Déployez les modifications vers le coffre-fort d'identité.

Pour plus d'informations, reportez-vous à la section « [Deploying a Driver Set to an Identity Vault](#) » (Déploiement d'un ensemble de pilotes vers un 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).

14.4.2 Utilisation d'iManager pour retirer l'ancien serveur de l'ensemble de pilotes

- 1 Dans iManager, cliquez sur  pour afficher la page d'administration d'Identity Manager.
- 2 Cliquez sur *Présentation d'Identity Manager*.
- 3 Naviguez jusqu'au conteneur dans lequel se trouve l'ensemble de pilotes et sélectionnez-le.

- 4 Cliquez sur le nom de l'ensemble de pilotes pour accéder à la page Présentation de l'ensemble de pilotes.
- 5 Cliquez sur *Serveurs > Supprimer le serveur*.
- 6 Sélectionnez l'ancien serveur d'Identity Manager, puis cliquez sur *OK*.

14.4.3 Déclassement de l'ancien serveur

À ce stade, le serveur n'héberge aucun pilote. Si vous n'avez plus besoin de ce serveur, vous devez suivre des étapes supplémentaires pour le déclasser :

- 1 Supprimez les répliques d'eDirectory de ce serveur.

Pour plus d'informations, reportez-vous à la section [Suppression d'une réplique \(http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html\)](http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html) du *Guide d'administration d'eDirectory* (<http://www.novell.com/documentation/edir88/pdfdoc/edir88/edir88.pdf>).

- 2 Supprimez eDirectory de ce serveur.

Pour plus d'informations, reportez-vous au document [TID 10056593, Removing a Server From an NDS Tree Permanently \(Suppression définitive d'un serveur dans une arborescence NDS\)](#) (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=10056593&sliceId=&docTypeID=DT_TID_1_1&dialogID=35218849&stateId=0%20%2035214815).

Désinstallation d'Identity Manager

IV

Pour désinstaller Identity Manager, vous devez désinstaller chacun de ses composants.

- ♦ [Chapitre 15, « Désinstallation des composants d'Identity Manager », page 121](#)

Désinstallation des composants d'Identity Manager

15

Désinstallez les composants d'Identity Manager dans l'ordre indiqué ci-dessous.

- ♦ Section 15.1, « Suppression d'objets dans eDirectory », page 121
- ♦ Section 15.2, « Désinstallation du serveur méta-annuaire », page 122
- ♦ Section 15.3, « Désinstallation du chargeur distant », page 122
- ♦ Section 15.4, « Désinstallation du module de provisioning basé sur les rôles », page 123
- ♦ Section 15.5, « Désinstallation des composants du module Identity Reporting », page 125
- ♦ Section 15.6, « Désinstallation d'iManager », page 126
- ♦ Section 15.7, « Désinstallation d'eDirectory », page 126
- ♦ Section 15.8, « Désinstallation d'Analyzer », page 127
- ♦ Section 15.9, « Désinstallation de Designer », page 127
- ♦ Section 15.10, « Désinstallation de l'administrateur d'assignation de rôles », page 128

15.1 Suppression d'objets dans eDirectory

La première étape de la désinstallation d'Identity Manager consiste à effacer tous les objets Identity Manager du coffre-fort d'identité. Si des objets Ensemble de pilotes sont des objets Racine de partition dans eDirectory, la partition doit être fusionnée avec la partition parente avant que l'objet Ensemble de pilotes puisse être supprimé. Lorsque l'ensemble de pilotes est créé, l'assistant vous invite à convertir l'ensemble de pilotes en partition.

- 1** Contrôlez l'état de santé de la base de données eDirectory. En cas d'erreurs, corrigez-les avant de continuer.

Pour plus d'informations, reportez-vous à la section [Keeping eDirectory Healthy \(Conserver la bonne santé d'eDirectory\)](http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html) (<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>) du *Guide d'administration de Novell eDirectory 8.8*.

- 2** Connectez-vous à iManager en tant qu'administrateur avec tous les droits dans l'arborescence eDirectory.
- 3** Sélectionnez *Partitions et répliques > Fusionner la partition*.
- 4** Naviguez jusqu'à l'objet Ensemble des pilotes qui soit l'objet racine de partition et sélectionnez-le, puis cliquez sur *OK*.
- 5** Attendez que la procédure de fusion soit terminée, puis cliquez sur *OK*.
- 6** Effacez l'objet Ensemble des pilotes.

Lorsque vous effacez l'objet Ensemble des pilotes, cela efface tous les objets de pilotes associés à cet ensemble des pilotes.

- 7 Répétez l'[Étape 3](#) à l'[Étape 6](#) pour chaque objet Ensemble des pilotes se trouvant dans la base de données eDirectory, jusqu'à ce qu'ils soient supprimés.
- 8 Répétez l'[Étape 1](#) pour vérifier que toutes les fusions ont été réalisées et que tous les objets ont été supprimés.

15.2 Désinstallation du serveur méta-annuaire

Lors de l'installation d'Identity Manager, un script de désinstallation est placé sur le serveur Identity Manager. Il permet de supprimer tous les services, les paquetages et les répertoires créés lors de l'installation d'Identity Manager.

- ♦ [Section 15.2.1, « Désinstallation sous Linux/UNIX », page 122](#)
- ♦ [Section 15.2.2, « Désinstallation sous Windows », page 122](#)

15.2.1 Désinstallation sous Linux/UNIX

Pour désinstaller Identity Manager sous Linux/UNIX, exécutez le script de désinstallation situé à l'emplacement `/root/idm/Uninstall_Identity_Manager/Uninstall_Identity_Manager`. Pour exécuter le script, saisissez `./Uninstall_Identity_Manager`.

Si vous avez installé Identity Manager en tant qu'utilisateur non-`root`, le répertoire `idm` est placé dans le répertoire de l'utilisateur qui a installé Identity Manager.

15.2.2 Désinstallation sous Windows

La procédure de désinstallation du serveur méta-annuaire est différente pour chacune des plateformes Windows prises en charge.

- ♦ **Windows 2003 SP2 (32 et 64 bits) :** dans le Panneau de configuration, sélectionnez *Ajouter ou supprimer des programmes > Identity Manager*, puis cliquez sur *Modifier/Supprimer*.
- ♦ **Windows 2008 SP1 (32 et 64 bits) :** cliquez sur *Programmes et fonctionnalités > Identity Manager*, puis cliquez avec le bouton droit et sélectionnez *Désinstaller*.

15.3 Désinstallation du chargeur distant

Lorsque le chargeur distant est installé, un script de désinstallation est placé sur le serveur du chargeur distant. Il vous permet de supprimer tous les services, paquetages et répertoires créés lors de l'installation du chargeur distant.

- ♦ [Section 15.3.1, « Désinstallation sous Linux/UNIX », page 122](#)
- ♦ [Section 15.3.2, « Désinstallation sous Windows », page 123](#)

15.3.1 Désinstallation sous Linux/UNIX

Pour désinstaller le chargeur distant sous Linux/UNIX, exécutez le script de désinstallation situé à l'emplacement `/root/idm/Uninstall_Identity_Manager/Uninstall_Identity_Manager`. Pour exécuter le script, saisissez `./Uninstall_Identity_Manager`.

Si vous avez installé le chargeur distant en tant qu'utilisateur non-`root`, le répertoire `idm` est placé dans le répertoire de l'utilisateur qui a installé le chargeur distant.

15.3.2 Désinstallation sous Windows

La procédure de désinstallation du chargeur distant est différente pour chacune des plates-formes Windows prises en charge.

- ♦ **Windows 2003 SP2 (32 et 64 bits)** : dans le Panneau de configuration, sélectionnez *Ajouter ou supprimer des programmes* > *Identity Manager*, puis cliquez sur *Modifier/Supprimer*.
- ♦ **Windows 2008 SP1 (32 et 64 bits)** : cliquez sur *Programmes et fonctionnalités* > *Identity Manager*, puis cliquez avec le bouton droit et sélectionnez *Désinstaller*.

15.4 Désinstallation du module de provisioning basé sur les rôles

Le module de provisioning basé sur les rôles comporte plusieurs composants qui doivent tous être désinstallés.

- ♦ [Section 15.4.1, « Suppression des pilotes », page 123](#)
- ♦ [Section 15.4.2, « Désinstallation de l'application utilisateur », page 123](#)
- ♦ [Section 15.4.3, « Désinstallation du serveur d'applications et de la base de données », page 124](#)

15.4.1 Suppression des pilotes

Vous devez supprimer les pilotes de l'application utilisateur et du service de rôles et de ressources.

- 1 Arrêtez les pilotes de l'application utilisateur et du service de rôles et de ressources.
 - ♦ **Designer** : cliquez avec le bouton droit sur la ligne du pilote, puis cliquez sur *En direct* > *Arrêter le pilote*.
 - ♦ **iManager** : sur la page Présentation de l'ensemble de pilotes, cliquez sur le coin supérieur droit du pilote, puis sur *Arrêter le pilote*.
- 2 Supprimez les pilotes de l'application utilisateur et du service de rôles et de ressources.
 - ♦ **Designer** : cliquez avec le bouton droit sur la ligne du pilote, puis cliquez sur *Supprimer*.
 - ♦ **iManager** : sur la page Présentation de l'ensemble de pilotes, cliquez sur *Pilotes* > *Supprimer des pilotes*, puis sur le pilote à supprimer.

15.4.2 Désinstallation de l'application utilisateur

- ♦ **Linux/UNIX** : exécutez le script de désinstallation situé à l'emplacement `/root/Roles_Based_Provisioning_Module_for_Novell_Identity_Manager/Uninstall Roles Based Provisioning Module for Novell Identity Manager`.

Pour exécuter le script, saisissez `./Uninstall\ Roles\ Based\ Provisioning\ Module\ for\ Novell\ Identity\ Manager`.

- ♦ **Windows** : la procédure de désinstallation de l'application utilisateur est différente pour chacune des plates-formes Windows prises en charge.
 - ♦ **Windows 2003 SP2 (32 et 64 bits)** : dans le Panneau de configuration, sélectionnez *Ajouter ou supprimer des programmes* > *Module de provisioning basé sur les rôles*, puis cliquez sur *Modifier/Supprimer*.

- ♦ **Windows 2008 SP1 (32 et 64 bits)** : cliquez sur *Programmes et fonctionnalités > Module de provisioning basé sur les rôles*, puis cliquez avec le bouton droit et sélectionnez *Désinstaller*.

15.4.3 Désinstallation du serveur d'applications et de la base de données

L'application utilisateur s'exécute sur les serveurs d'applications et bases de données suivants.

Tableau 15-1 *Serveurs d'applications et bases de données pris en charge*

Serveur d'applications	Base de données
JBoss 5.1.0	♦ MS SQL 2008
	♦ MySQL version 5.1
	♦ Oracle 11gR2
	♦ PostgreSQL 8.4.3
WebSphere 7.0	♦ DB2 9.5b
	♦ MS SQL 2008
	♦ Oracle 11gR2
	♦ PostgreSQL 8.4.3
WebLogic 10.3	♦ MS SQL 2008
	♦ Oracle 11gR2
	♦ PostgreSQL 8.4.3

La procédure suivante permet de désinstaller un serveur d'applications JBoss et une base de données PostgreSQL. Si vous utilisez une base de données et un serveur d'applications différents, reportez-vous à la documentation de ces produits pour connaître la procédure à suivre.

- ♦ **Linux/UNIX** : exécutez le script de désinstallation situé à l'emplacement `/opt/novell/idm/Postgres/JBossPostgreSQL_Uninstaller/Uninstall_JBossPostgreSQL`.

Pour exécuter le script, saisissez `./Uninstall_JBossPostgreSQL`.

- ♦ **Windows** : la procédure de désinstallation de JBoss et PostgreSQL est différente pour chacune des plates-formes Windows prises en charge.
 - ♦ **Windows 2003 SP2 (32 et 64 bits)** : dans le Panneau de configuration, sélectionnez *Ajouter ou supprimer des programmes > JBossPostgreSQL*, puis cliquez sur *Modifier/Supprimer*.
 - ♦ **Windows 2008 SP1 (32 et 64 bits)** : cliquez sur *Programmes et fonctionnalités > JBossPostgreSQL*, puis cliquez avec le bouton droit et sélectionnez *Désinstaller*.

15.5 Désinstallation des composants du module Identity Reporting

Le module Identity Reporting comporte plusieurs composants. Pour le désinstaller, chacun de ses composants doit être désinstallé.

- ♦ [Section 15.5.1, « Suppression des pilotes de création de rapports », page 125](#)
- ♦ [Section 15.5.2, « Désinstallation du module Identity Reporting », page 125](#)
- ♦ [Section 15.5.3, « Désinstallation du service d'audit d'événements », page 125](#)

15.5.1 Suppression des pilotes de création de rapports

Vous devez supprimer les pilotes de collecte de données et de passerelle système gérée.

- 1 Arrêtez les pilotes de collecte de données et de passerelle système gérée.
 - ♦ **Designer** : cliquez avec le bouton droit sur la ligne du pilote, puis cliquez sur *En direct > Arrêter le pilote*.
 - ♦ **iManager** : sur la page Présentation de l'ensemble de pilotes, cliquez sur le coin supérieur droit du pilote, puis sur *Arrêter le pilote*.
- 2 Supprimez les pilotes de collecte de données et de passerelle système gérée.
 - ♦ **Designer** : cliquez avec le bouton droit sur la ligne du pilote, puis cliquez sur *Supprimer*.
 - ♦ **iManager** : sur la page Présentation de l'ensemble de pilotes, cliquez sur *Pilotes > Supprimer des pilotes*, puis sur le pilote à supprimer.

15.5.2 Désinstallation du module Identity Reporting

- ♦ **Linux** : exécutez le script de désinstallation situé à l'emplacement `/opt/novell/IdentityReporting/Uninstall_Identity Reporting`.
Pour exécuter le script, saisissez `./Uninstall\ Identity\ Reporting`.
- ♦ **Windows** : la procédure de désinstallation du module Identity Reporting est différente pour chacune des plates-formes Windows prises en charge.
 - ♦ **Windows 2003 SP2 (32 et 64 bits)** : dans le Panneau de configuration, sélectionnez *Ajouter ou supprimer des programmes > Identity Reporting*, puis cliquez sur *Modifier/Supprimer*.
 - ♦ **Windows 2008 SP1 (32 et 64 bits)** : cliquez sur *Programmes et fonctionnalités > Identity Reporting*, puis cliquez avec le bouton droit et sélectionnez *Désinstaller*.

15.5.3 Désinstallation du service d'audit d'événements

Le service d'audit d'événements (EAS) n'est pris en charge que sous Linux. Exécutez le script de désinstallation situé à l'emplacement `/opt/novell/sentinel_eas/Uninstall_Event Auditing Service/Uninstall Event Auditing Service`. Pour exécuter le script, saisissez `./Uninstall\ Event\ Auditing\ Service`.

15.6 Désinstallation d'iManager

- ♦ **Linux** : exécutez, en tant qu'utilisateur `root`, le script de désinstallation situé à l'emplacement `/var/opt/novell/iManager/nps/UninstallerData/UninstalliManager`.

Pour exécuter le script, saisissez `./UninstalliManager`.

- ♦ **Windows** : la procédure de désinstallation d'iManager est différente pour chacune des plates-formes Windows prises en charge.
 - ♦ **Windows 2003 SP2 (32 et 64 bits)** : dans le Panneau de configuration, sélectionnez *Ajouter ou supprimer des programmes* > *Novell iManager*, puis cliquez sur *Modifier/Supprimer*.
 - ♦ **Windows 2008 SP1 (32 et 64 bits)** : cliquez sur *Programmes et fonctionnalités* > *Novell iManager*, puis cliquez avec le bouton droit et sélectionnez *Désinstaller*.

Dans le Panneau de configuration, Tomcat et NICI sont listés en tant qu'entrées distinctes. Si vous n'utilisez plus ces programmes, vous pouvez les désinstaller. Si eDirectory est installé sur ce même serveur, NICI est nécessaire pour qu'eDirectory continue de fonctionner. Si vous ne désinstallez pas eDirectory, ne désinstallez pas NICI.

15.7 Désinstallation d'eDirectory

Avant de désinstaller eDirectory, assurez-vous que vous connaissez bien votre arborescence eDirectory et les emplacements de vos répliques, afin d'éviter d'éventuels problèmes au niveau de l'arborescence eDirectory.

Avant de désinstaller eDirectory, répondez aux questions suivantes :

- Votre arborescence comporte-t-elle plusieurs serveurs ?

Si la réponse est oui, répondez aux autres questions de cette liste. Si la réponse est non, vous pouvez supprimer eDirectory.

- Ce serveur contient-il des répliques maîtresses ?

Si la réponse est oui, vous devez promouvoir un autre serveur de l'anneau de répliques en tant que maître avant de supprimer eDirectory. Pour plus d'informations, reportez-vous à la section « [Gestion des partitions et des répliques](http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiiik.html) » (<http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiiik.html>) du *Guide d'administration d'eDirectory 8.8*.

- Ce serveur contient-il l'unique copie d'une partition ?

Si la réponse est oui, vous devez fusionner cette partition avec la partition parente ou ajouter une réplique de cette partition à un autre serveur et faire de ce dernier le détenteur de la réplique maîtresse. Pour plus d'informations, reportez-vous à la section « [Gestion des partitions et des répliques](http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiiik.html) » (<http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiiik.html>) du *Guide d'administration d'eDirectory 8.8*.

Après vous être assuré que votre arborescence eDirectory est prête, utilisez la procédure suivante pour désinstaller eDirectory :

- 1 Si votre arborescence ne comporte qu'un seul serveur, passez à l'**Étape 2**. Sinon, contrôlez l'état de santé de la base de données eDirectory. En cas d'erreurs, corrigez-les avant de continuer. Pour plus d'informations, reportez-vous à la section « [Vérification de l'état de santé d'eDirectory](http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html) » (<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>) du *Guide d'administration de Novell eDirectory 8.8*.

2 Désinstallez eDirectory.

- ♦ **Linux/UNIX** : exécutez le script de désinstallation situé à l'emplacement `/opt/novell/eDirectory/sbin/nds-uninstall`.

Pour exécuter le script, saisissez `./nds-uninstall`.

- ♦ **Windows** : la procédure de désinstallation d'eDirectory est différente pour chacune des plates-formes Windows prises en charge.
 - ♦ **Windows 2003 SP2 (32 et 64 bits)** : dans le Panneau de configuration, sélectionnez *Ajouter ou supprimer des programmes* > *Novell eDirectory*, puis cliquez sur *Modifier/Supprimer*.
 - ♦ **Windows 2008 SP1 (32 et 64 bits)** : cliquez sur *Programmes et fonctionnalités* > *Novell eDirectory*, puis cliquez avec le bouton droit et sélectionnez *Désinstaller*.

3 (Conditionnel) Si votre arborescence comporte plusieurs serveurs, supprimez tous les objets spécifiques au serveur restés dans l'arborescence, puis effectuez un autre contrôle de l'état de santé pour vérifier que le serveur a bien été supprimé de l'arborescence.

Pour plus d'informations, reportez-vous à la section « [Vérification de l'état de santé d'eDirectory](http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html) » (<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>) du *Guide d'administration de Novell eDirectory 8.8*.

15.8 Désinstallation d'Analyzer

1 Assurez-vous qu'Analyzer est fermé.

2 Désinstallez Analyzer :

- ♦ **Linux** : exécutez le script de désinstallation situé à l'emplacement `<répertoire_installation>/analyzer/UninstallAnalyzer/UninstallAnalyzer for Identity Manager`.
Pour exécuter le script, saisissez `./Uninstall\ Analyzer\ for\ Identity\ Manager`.
- ♦ **Windows** : la procédure de désinstallation d'Analyzer est différente pour chacune des plates-formes Windows prises en charge.
 - ♦ **Windows 2003 SP2 (32 et 64 bits)** : dans le Panneau de configuration, sélectionnez *Ajouter ou supprimer des programmes* > *Analyzer pour Identity Manager*, puis cliquez sur *Modifier/Supprimer*.
 - ♦ **Windows 2008 SP1 (32 et 64 bits)** : cliquez sur *Programmes et fonctionnalités* > *Analyzer pour Identity Manager*, puis cliquez avec le bouton droit et sélectionnez *Désinstaller*.

15.9 Désinstallation de Designer

1 Assurez-vous que Designer est fermé.

2 Désinstallez Designer.:

- ♦ **Linux/UNIX** : exécutez le script de désinstallation situé à l'emplacement `<répertoire_installation>/designer/UninstallDesigner/UninstallDesigner for Identity Manager`.
Pour exécuter le script, saisissez `./Uninstall\ Designer\ for\ Identity\ Manager`.

- ♦ **Windows** : la procédure de désinstallation de Designer est différente pour chacune des plates-formes Windows prises en charge.
 - ♦ **Windows 2003 SP2 (32 et 64 bits)** : dans le Panneau de configuration, sélectionnez *Ajouter ou supprimer des programmes > Designer pour Identity Manager*, puis cliquez sur *Modifier/Supprimer*.
 - ♦ **Windows 2008 SP1 (32 et 64 bits)** : cliquez sur *Programmes et fonctionnalités > Designer pour Identity Manager*, puis cliquez avec le bouton droit et sélectionnez *Désinstaller*.

15.10 Désinstallation de l'administrateur d'assignation de rôles

- 1 Accédez au répertoire d'installation de l'administrateur d'assignation de rôles.
Étant donné que ce répertoire est défini lors de l'installation, il peut être différent pour chaque installation.
- 2 Arrêtez l'administrateur d'assignation de rôles à partir de la ligne de commande en exécutant le script `stop`
 - ♦ **Linux** : `stop.sh`
Pour exécuter le script, saisissez `./stop.sh`
 - ♦ **Windows** : `stop.bat`
- 3 Exécutez le script de désinstallation à partir de la ligne de commande.
 - ♦ **Linux** : `rma-uninstall.sh [-h] [-s]`
 - ♦ `[-h]` : correspond à l'aide.
 - ♦ `[-s]` : correspond au mode silencieux.
 Pour exécuter le script, saisissez `./rma-uninstall.sh`.
 - ♦ **Windows** : `rma-uninstall.bat [-h] [-s]`
- 4 Supprimez le répertoire d'installation.