

Guide d'installation

Novell® Identity Manager

3.6.1

15 mai 2009

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 acceptez de vous conformer à toutes les réglementations de contrôle des exportations et à vous procurer les licences requises ou la classification permettant d'exporter, de réexporter ou d'importer des biens de consommation. Vous acceptez de ne pas procéder à des exportations ou à des réexportations vers des entités figurant sur les listes d'exclusion 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 aux [Services de commerce international \(http://www.novell.com/company/policies/trade_services\)](http://www.novell.com/company/policies/trade_services) pour plus d'informations sur l'exploration des logiciels Novell. Novell décline toute responsabilité dans le cas où vous n'obtiendriez pas les autorisations d'exportation nécessaires.

Copyright © 2007-2009 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. est titulaire des droits de propriété intellectuelle relatifs à la technologie intégrée au produit décrit dans ce document. En particulier et sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains mentionnés sur le [site Web de Novell relatif aux mentions légales \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) (en anglais) et un ou plusieurs brevets supplémentaires ou en cours d'homologation aux États-Unis et dans d'autres pays.

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	17
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	18
2.2 Phase d'analyse des besoins et de la conception	19
2.2.1 Définir les besoins de votre entreprise	20
2.2.2 Analyser vos processus d'entreprise	21
2.2.3 Conception d'un modèle de données d'entreprise	22
2.3 Preuve de conception	23
2.4 Validation et préparation des données	23
2.5 Pilote de production	24
2.6 Planification du déploiement vers la production	24
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 Designer	28
3.1.2 Instructions pour iManager	29
3.2 Instructions pour le serveur méta-annuaire	29
3.3 Instructions pour eDirectory	30
3.3.1 Objets Identity Manager dans eDirectory	31
3.3.2 Réplication des objets dont Identity Manager a besoin sur le serveur	31
3.3.3 Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents	33
3.4 Application utilisateur	35
3.5 Instructions pour l'audit et la création de rapport	36
Partie II Installation	39
4 Liste de vérification pour un système Identity Manager de base	41
4.1 Conditions préalables	41
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	43
5	Où se procurer Identity Manager	45
6	Configuration système requise	47
6.1	eDirectory et iManager	47
6.2	Serveur méta-annuaire	48
6.2.1	Processeurs pris en charge	49
6.2.2	Systèmes d'exploitation du serveur	50
6.3	Chargeur distant	51
6.4	Application utilisateur	52
6.5	Audit et création de rapport	52
6.6	Postes de travail	53
6.6.1	Plates-formes des postes de travail	54
6.6.2	iManager et navigateurs Web	55
7	Installation d'Identity Manager	57
7.1	Installation de Designer	57
7.2	Installation du serveur méta-annuaire	58
7.2.1	Installation non-root du serveur méta-annuaire	59
7.2.2	Installation en mode silencieux du serveur méta-annuaire	61
7.3	Installation du chargeur distant	61
7.3.1	Configuration requise	62
7.3.2	Pilotes pris en charge	62
7.3.3	Procédure d'installation	63
7.3.4	Installation en mode silencieux du chargeur distant	65
7.3.5	Installation du chargeur distant Java sous UNIX, Linux ou AIX	66
7.4	Installation du module de provisioning basé sur les rôles	66
7.5	Installation d'un pilote personnalisé	67
7.6	Installation d'Identity Audit ou de Sentinel	67
7.7	Installation d'Identity Manager dans un environnement en grappe	67
8	Activation des produits Novell Identity Manager	69
8.1	Achat d'une licence de produit Identity Manager	69
8.2	Installation d'une référence d'activation de produit	69
8.3	Affichage des activations de produits pour Identity Manager et les pilotes	70
9	Dépannage d'Identity Manager	73
Partie III Mise à niveau		75
10	Nouveautés	77
10.1	Prise en charge des systèmes d'exploitation 64 bits	77
10.2	Prise en charge de l'installation du chargeur distant 32 bits sur les systèmes d'exploitation 64 bits	77

11 Versions prises en charge pour les mises à niveau et configuration système requise	79
11.1 Versions prises en charge pour les mises à niveau	79
11.2 Configuration système requise	79
12 Mise à niveau directe (in-place) et migration	81
12.1 Mise à niveau directe	81
12.2 Migration	82
12.3 Plusieurs serveurs associés à un seul ensemble de pilotes	82
13 Mise à niveau directe	83
13.1 Création d'une sauvegarde de la configuration actuelle	85
13.1.1 Vérification de l'actualité de votre projet Designer	85
13.1.2 Création d'une exportation des pilotes	87
13.2 Arrêt des pilotes	87
13.2.1 Utilisation de Designer pour arrêter les pilotes	88
13.2.2 Utilisation d'iManager pour arrêter les pilotes	88
13.3 Ajout de fichiers à l'emplacement correct sur les plates-formes Linux/UNIX	88
13.4 Mise à niveau de Designer	89
13.5 Mise à niveau du moteur méta-annuaire et des fichiers de configuration des pilotes	89
13.6 Mise à niveau du chargeur distant	90
13.7 Superposition du nouveau fichier de configuration du pilote sur le pilote existant	91
13.7.1 Utilisation d'iManager pour superposer le nouveau fichier de configuration de pilote sur le pilote existant	91
13.7.2 Utilisation d'iManager pour superposer le nouveau fichier de configuration de pilote sur le pilote existant	91
13.8 Restauration de stratégies et de règles personnalisées pour le pilote	92
13.8.1 Utilisation de Designer pour restaurer les stratégies et les règles personnalisées sur le pilote	92
13.8.2 Utilisation d'iManager pour restaurer les stratégies et les règles personnalisées sur le pilote	93
13.9 Déploiement du projet converti	94
13.10 Lancement des pilotes	94
13.10.1 Utilisation de Designer pour lancer les pilotes	94
13.10.2 Utilisation d'iManager pour démarrer les pilotes	95
14 Exécution d'une migration	97
14.1 Ajout du nouveau serveur à l'ensemble de pilotes	98
14.2 Modification des informations spécifiques du serveur	99
14.2.1 Modification des informations spécifiques du serveur dans Designer	99
14.2.2 Modification des informations spécifiques du serveur dans iManager	100
14.3 Suppression de l'ancien serveur de l'ensemble de pilotes	100
14.3.1 Utilisation de Designer pour retirer l'ancien serveur de l'ensemble de pilotes	100
14.3.2 Utilisation d'iManager pour retirer l'ancien serveur de l'ensemble de pilotes	101
14.3.3 Déclassement de l'ancien serveur	101

Partie IV Désinstallation d'Identity Manager	103
15 Suppression d'objets dans eDirectory	105
16 Désinstallation du serveur et des pilotes méta-annuaire	107
16.1 Désinstallation sous Windows	107
16.2 Désinstallation sous Linux/UNIX	107
17 Désinstallation de Designer	109

À propos de ce guide

Novell® Identity Manager est un service de partage et de synchronisation des 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 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 47**
 - ♦ **Chapitre 7, « Installation d'Identity Manager », page 57**
 - ♦ **Chapitre 8, « Activation des produits Novell Identity Manager », page 69**
- ♦ **Partie III, « Mise à niveau », page 75**
 - ♦ **Chapitre 10, « Nouveautés », page 77**
 - ♦ **Chapitre 11, « Versions prises en charge pour les mises à niveau et configuration système requise », page 79**
 - ♦ **Chapitre 12, « Mise à niveau directe (in-place) et migration », page 81**
 - ♦ **Chapitre 13, « Mise à niveau directe », page 83**
 - ♦ **Chapitre 14, « Exécution d'une migration », page 97**
- ♦ **Partie IV, « Désinstallation d'Identity Manager », page 103**
 - ♦ **Chapitre 15, « Suppression d'objets dans eDirectory », page 105**
 - ♦ **Chapitre 16, « Désinstallation du serveur et des pilotes méta-annuaire », page 107**

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 \(http://www.novell.com/documentation/idm361/index.html\)](http://www.novell.com/documentation/idm361/index.html).

Documentation complémentaire

Pour obtenir une documentation supplémentaire sur Identity Manager, reportez-vous au [site Web de documentation d'Identity Manager \(http://www.novell.com/documentation/idm361/index.html\)](http://www.novell.com/documentation/idm361/index.html).

Pour obtenir la documentation de l'application utilisateur, reportez-vous au [site Web de la documentation du module de provisioning basé sur les rôles Identity Manager \(http://www.novell.com/documentation/idmrbpm361/index.html\)](http://www.novell.com/documentation/idmrbpm361/index.html).

Conventions relatives à la documentation

Dans la documentation Novell, le symbole « supérieur à » (>) est utilisé pour séparer deux opérations dans une étape de procédure, ainsi que deux éléments dans un chemin de références croisées.

Un symbole de marque déposée (® , ™ , etc.) indique qu'il s'agit d'une marque de Novell. L'astérisque (*) indique une marque de fabricant tiers.

Lorsqu'un nom de chemin peut s'écrire avec une barre oblique pour certaines plates-formes et une barre oblique inverse pour d'autres, il sera toujours présenté avec une barre oblique inverse. Les utilisateurs de plates-formes qui utilisent une barre oblique, telles que Linux* ou UNIX*, doivent utiliser des barres obliques lorsque le logiciel l'exige.

Planification

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

Pour toute question sur les différents composants d'une solution Identity Manager, reportez-vous au guide *Présentation d'Identity Manager 3.6.1*, qui détaille chaque composant.

Pour créer une solution Identity Manager efficace pour votre environnement, prenez le temps de la planifier et de 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.

Nous recommandons fortement d'engager un expert Identity Manager pour vous aider dans chaque phase de la mise en oeuvre. 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 mise en place d'un environnement de développement dans lequel vous pouvez tester, analyser et développer votre solution Identity Manager vous permet de découvrir chaque composant, ainsi que des problèmes et des complications imprévus qui peuvent survenir.

Ainsi, par exemple, lorsque vous synchronisez des informations entre les différents systèmes, celles-ci sont présentées différemment sur chacun d'entre eux. La modification des données à synchroniser entre ces deux systèmes vous permet de constater si ces changements affectent d'autres systèmes faisant appel à ces informations.

L'autre raison essentielle pour configurer un environnement de développement est de s'assurer que la solution fonctionne, sans compromettre les données existantes. Identity Manager gère des données, et notamment leur suppression. 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 pour tous les aspects de la planification, afin de recueillir l'ensemble des données. Designer simplifie la création d'un plan de projet comprenant les informations d'activité, ainsi que les données techniques. Pour en savoir plus sur Designer, reportez-vous au *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.

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 permet de s'assurer que vous avez installé et configuré tous les composants d'Identity Manager que vous pouvez utiliser pour développer un plan de projet. Exploitez les informations fournies dans le [Chapitre 3, « Directives techniques », page 27](#) pour configurer votre environnement de développement et vous documenter sur les aspects techniques 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 propose une présentation du type d'activités qui fait généralement partie d'un projet Identity Manager, de son origine à son déploiement de production complet. 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, « Preuve de conception », page 23](#)
- ♦ [Section 2.4, « Validation et préparation des données », page 23](#)
- ♦ [Section 2.5, « Pilote de production », page 24](#)
- ♦ [Section 2.6, « Planification du déploiement vers la production », page 24](#)
- ♦ [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 17](#)

- ♦ [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 18](#)

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 « [Mode architecte](#) » dans le [Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6](#).

Voici quelques exemples de processus d'entreprise.

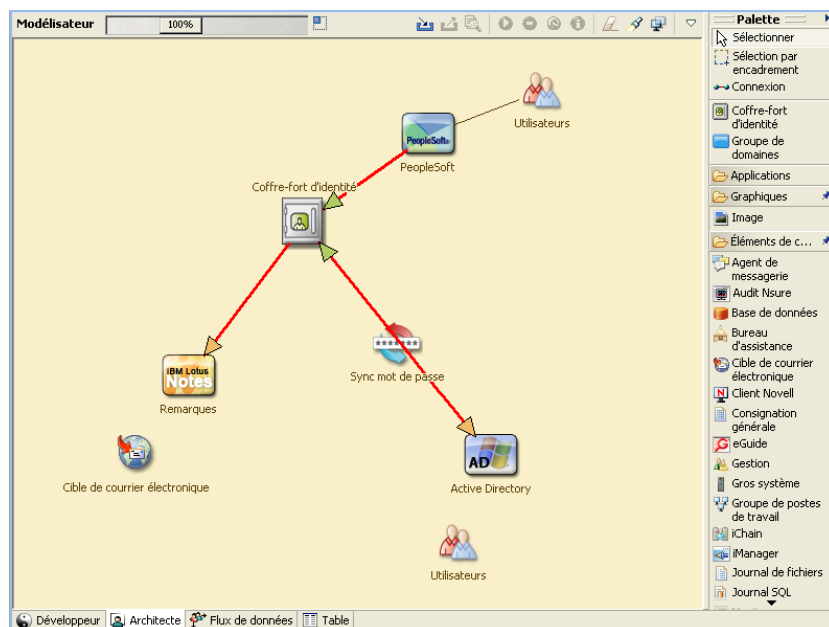
- ♦ Lorsqu'un employé est renvoyé, son compte utilisateur dans le système de messagerie est supprimé. Toutefois, dans tous les autres systèmes, il est désactivé et non supprimé.
- ♦ Le format d'une adresse de courrier électronique d'un utilisateur.
- ♦ Les systèmes ou les ressources accessibles aux commerciaux.
- ♦ Les systèmes ou les ressources accessibles aux responsables.
- ♦ Quels sont les systèmes qui génèrent les nouveaux comptes ? Est-ce 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. Ainsi, par exemple, la [Figure 2-1](#) est tirée de Designer et montre que de nouveaux comptes utilisateur sont créés à partir du 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



La prochaine étape est décrite 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. La prochaine étape est décrite à la [Section 2.1.3, « Identification des principales parties prenantes professionnelles et techniques », page 17.](#)

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 « [Configuration des propriétés d'application](#) » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.

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 18.

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. Ceci vous permet de :

- ◆ 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 assure une excellente amorce à la phase d'analyse, qui nécessite des intervenants une connaissance de base des annuaires, de Novell® eDirectory™, de Novell Identity Manager, et de l'intégration XML en général.

Une fois la phase de découverte achevée, 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.

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 :

- ♦ « Définir les besoins de votre entreprise » page 20
- ♦ « Analyser vos processus d'entreprise » page 21
- ♦ « Conception d'un modèle de données d'entreprise » page 22

2.2.1 Définir les 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 va survenir dans un processus donné, quelles seront les conséquences de ce 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 « [Gestion du flux de données](#) » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.
- ♦ Identifier les transformations de données devant être effectuées d'un format à un autre (par exemple de 2/25/2007 à 25 Fév 2007).
- ♦ 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 s'avérer nécessaire de diviser le déploiement en phases qui permettront de mettre en oeuvre une première partie de la solution, puis les autres parties ultérieurement. Vous pouvez également adopter une approche de déploiement par phases. Celle-ci doit être basée sur des groupes de personnes de votre organisation.

- ◆ Définir la configuration requise.

Vous devez décrire la configuration requise pour la mise en oeuvre d'une phase donnée du déploiement. Cela comprend l'accès aux systèmes connectés que vous voulez mettre en contact avec Identity Manager.

- ◆ Identifier les sources de données expertes.

En identifiant le plus tôt possible les éléments qui relèvent de la responsabilité des administrateurs système et des directeurs, 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 oeuvre 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, « Analyser vos processus d'entreprise »](#), page 21.

2.2.2 Analyser vos processus d'entreprise

Au terme de l'analyse des besoins de votre entreprise, 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 ?

Les questions qui pourraient être posées à un administrateur d'un système PeopleSoft aux ressources humaines pourraient inclure :

- ◆ 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 sur le système de provisioning (telles qu'ajouts, modifications ou suppressions) ?
- ◆ 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 entretiens avec les personnes clés peuvent conduire vers d'autres parties de l'organisation et permettre d'obtenir une idée plus précise du processus complet.

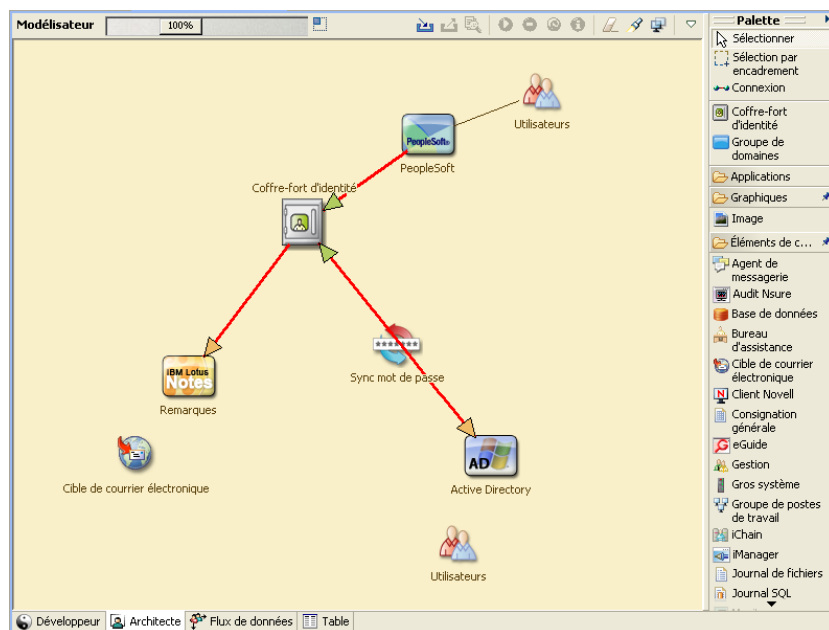
Après avoir rassemblé toutes ces informations, vous pouvez concevoir un modèle de données d'entreprise adapté à votre environnement. Passez à la [Section 2.2.3, « Conception d'un modèle de données d'entreprise »](#), page 22 pour démarrer la conception.

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, « Preuve de conception », page 23](#).

2.3 Preuve de conception

L'objectif de cette activité est d'obtenir un exemple de mise en oeuvre dans un environnement de test qui reflète la stratégie d'entreprise et le flux de données de votre société. Elle s'appuie sur la conception du modèle de données développé au cours de l'analyse des besoins et constitue l'étape finale avant d'introduire le pilote dans l'environnement de production.

Remarque : cette étape permet souvent d'améliorer la gestion en prévision de la mise en oeuvre 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 23](#) 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 oeuvre 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.

Il vous faut le modèle de données réalisé dans les phases d'analyse et de conception. Pour préparer correctement les données, vous devez également définir une stratégie proposée pour le format des données et la concordance des enregistrements. Une fois le modèle de données et la stratégie du format définis, vous pouvez :

- ♦ Créer des ensembles de données de production adaptés au chargement dans le coffre-fort d'identité (tel que cela est identifié dans les activités d'analyse et de conception). Cela comprend la méthode de chargement (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 24](#).

2.5 Pilote de production

L'objectif de cette activité est de commencer la migration vers l'environnement de production. Pendant cette phase, des opérations de personnalisation supplémentaires peuvent avoir lieu. 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 le jalon nécessaire en vue de la pleine 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 24](#).

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

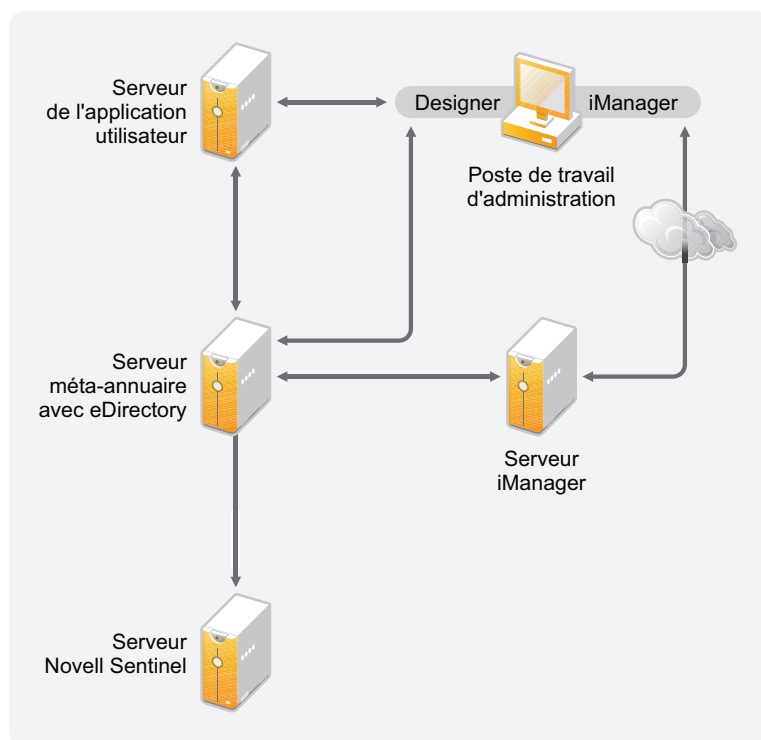
La phase de déploiement de la production met en marche l'ensemble des plans, puis la solution Identity Manager est créée dans l'environnement en direct. Utilisez le plan de déploiement de production pour mettre en place les différents éléments de la solution Identity Manager. Cela peut demander une nuit ou se dérouler pendant une période prolongée : tout dépend du contenu du plan.

Directives techniques

3

Les informations collectées dans Designer permettent de prendre des décisions techniques, comme les options de configuration et de localisation de l'installation, et ce pour chaque composant d'Identity Manager. Pour une présentation de chaque composant, reportez-vous au guide *Présentation d'Identity Manager 3.6.1*. La **Figure 3-1** représente une configuration possible d'une solution Identity Manager.

Figure 3-1 Composants Identity Manager



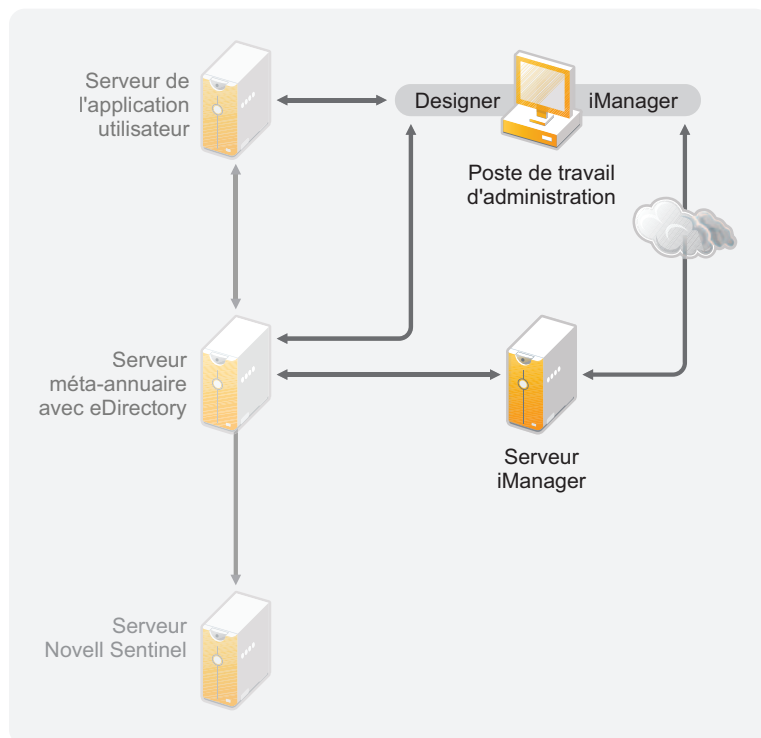
Identity Manager est hautement personnalisable. Les sections suivantes contiennent les bonnes pratiques techniques qui vous aideront à paramétrer et configurer la solution Identity Manager qui conviendra le mieux à votre environnement. L'application de ces instructions à votre environnement est fonction 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 29](#)
- ♦ [Section 3.3, « Instructions pour eDirectory », page 30](#)
- ♦ [Section 3.4, « Application utilisateur », page 35](#)
- ♦ [Section 3.5, « Instructions pour l'audit et la création de rapport », page 36](#)

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



Les informations contenues dans ce document concernent uniquement Designer et iManager. L'application utilisateur fait appel à une page d'administration sur le Web qui n'est pas traitée ici. Pour en savoir plus sur l'application utilisateur, reportez-vous à [Administration de l'application utilisateur \(http://www.novell.com/documentation/idmrpbpm361/agpro/data/agpropartadminapp.html\)](http://www.novell.com/documentation/idmrpbpm361/agpro/data/agpropartadminapp.html) dans le *Guide d'administration de l'application utilisateur*.

- ♦ [Section 3.1.1, « Instructions pour Designer », page 28](#)
- ♦ [Section 3.1.2, « Instructions pour iManager », page 29](#)

3.1.1 Instructions pour Designer

Designer est un client épais 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 d'instruction particulière pour utiliser 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 « [Contrôle des versions](#) » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.

3.1.2 Instructions pour iManager

iManager est l'outil d'administration d'Identity Manager. Lorsque vous installez Identity Manager, le programme nécessite que le serveur iManager soit 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](#) 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.

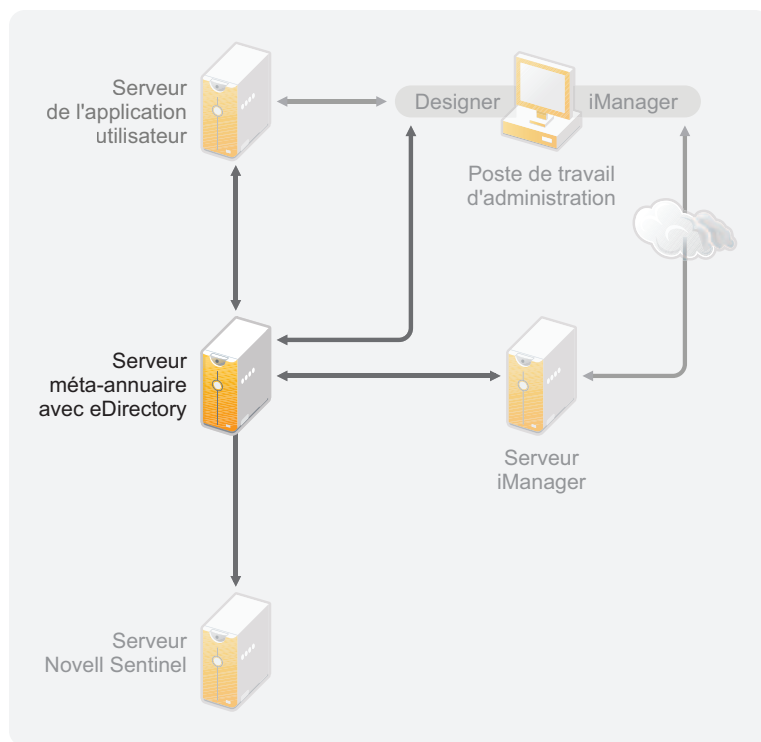
3.2 Instructions pour le serveur méta-annuaire

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 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, installez 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 [Guide du chargeur distant d'Identity Manager 3.6.1](#).

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 « *Contrôle de l'état de santé du pilote* » dans le *Guide d'administration du pilote commun d'Identity Manager 3.6.1*.

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 dont Identity Manager a besoin sur le serveur », page 31](#)
- ♦ [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. Tout serveur associé à un ensemble de pilotes doit disposer du moteur méta-annuaire.
- ♦ **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 pouvant être référencée par chaque pilote de l'ensemble de pilotes.
- ♦ **Pilote** : un pilote assure la connexion entre une application et le coffre-fort d'identité. Il est le connecteur qui permet la synchronisation des données et le partage entre les systèmes. Le pilote est conservé dans l'ensemble de pilotes.
- ♦ **Travail** : l'objectif d'un travail est la réalisation d'une tâche survenant à plusieurs reprises. Par exemple, un travail peut configurer le 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 dont Identity Manager a besoin sur le serveur

Si votre environnement Identity Manager demande plusieurs serveurs afin d'exécuter plusieurs pilotes Identity Manager, votre plan doit veiller à ce que certains objets eDirectory soient répliqués sur les serveurs sur lesquels vous voulez exécuter ces pilotes Identity Manager.

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 : lors de la création d'un objet Ensemble des pilotes, le paramètre par défaut est la création d'une partition séparée. Novell® conseille de créer 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 « [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.

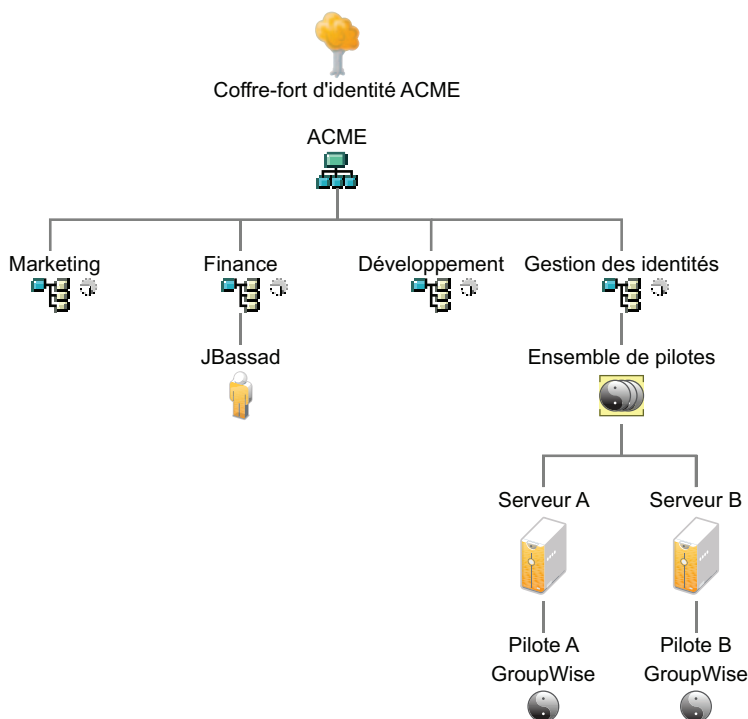
Pour synchroniser tous les utilisateurs sans les répliquer sur un seul serveur, vous devez déterminer l'ensemble de serveurs qui contient tous les utilisateurs, puis créer une instance du pilote Identity Manager sur chacun de ces serveurs. Pour éviter que deux instances du pilote tentent de synchroniser 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 35](#). 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.

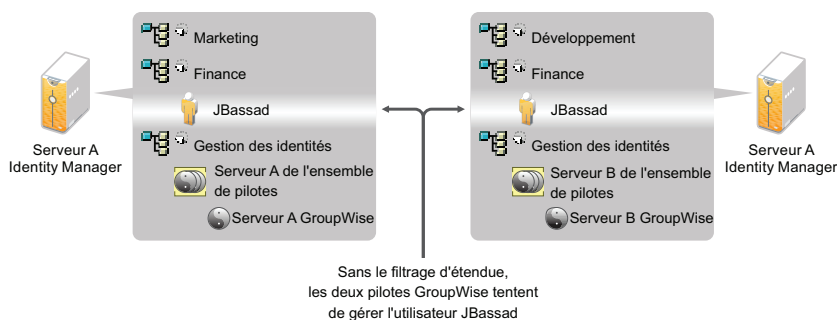
L'administrateur souhaite que tous les utilisateurs de l'arborescence soient synchronisés par le pilote GroupWise®, mais ne souhaite pas regrouper les répliques des utilisateurs sur un seul serveur. Il choisit plutôt d'utiliser deux instances du pilote GroupWise, une sur chaque serveur. Il installe Identity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

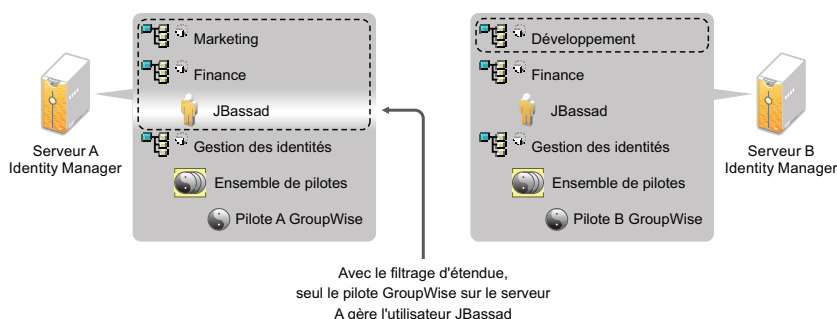
Comme le serveur A et le serveur B contiennent une réplique du conteneur Finance, ils contiennent tous deux l'utilisateur JBassad, qui est dans le conteneur Finance. Sans filtrage des étendues, le pilote GroupWise A et le pilote GroupWise B synchroniseraient JBassad.

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



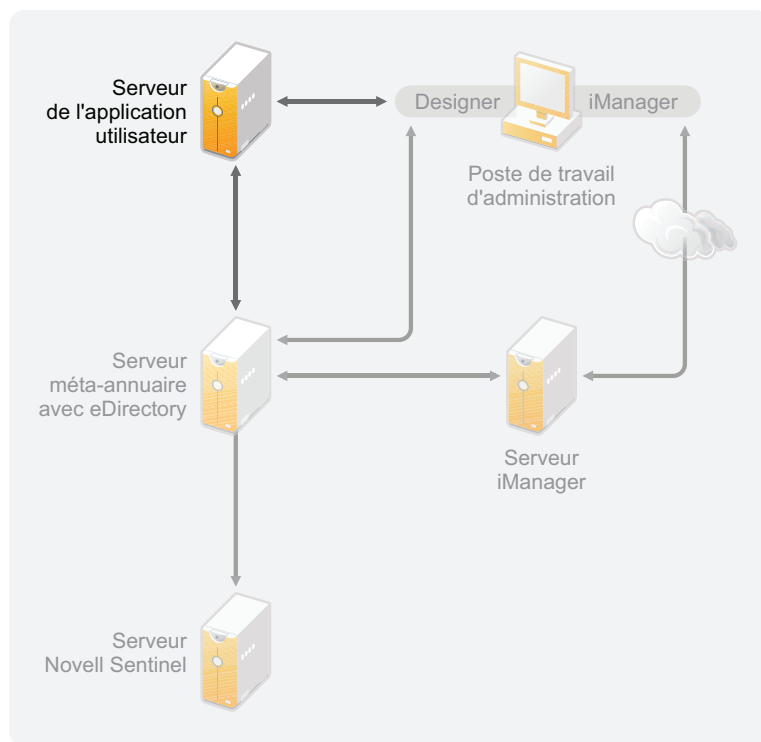
Identity Manager 3.6.1 comporte des règles prédéfinies. Deux règles aident au filtrage des étendues. « Transformation de l'événement - Filtrage de l'étendue - Inclure les sous-arborescences » et « Transformation de l'événement - Filtrage de l'étendue - Exclure les sous-arborescences » sont documentés dans *Understanding Policies for Identity Manager 3.6* (Comprendre les stratégies pour Identity Manager 3.6).

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



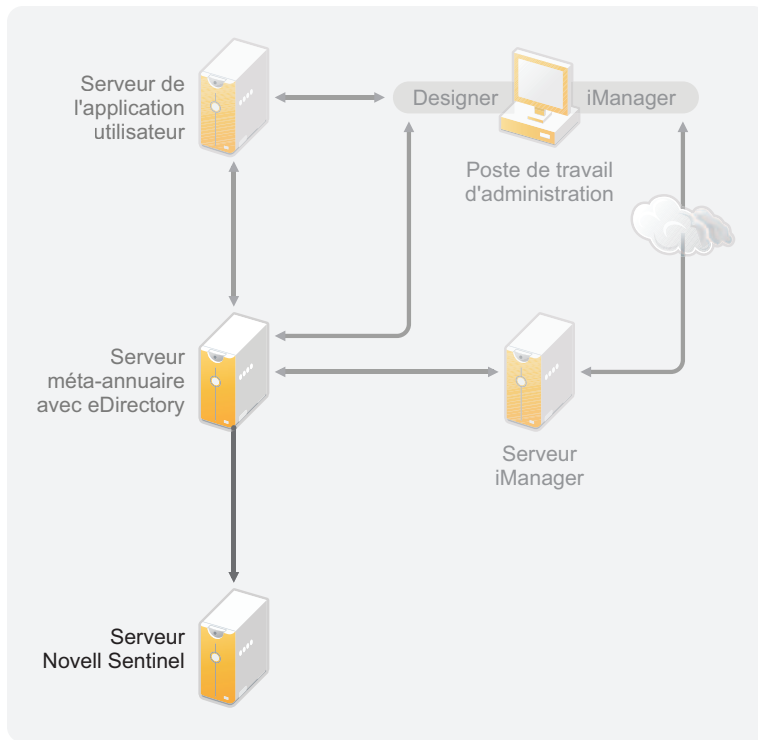
Utilisez les informations de la section [Affinage des performances](http://www.novell.com/documentation/idmrpbm361/agpro/data/b2gx735.html) (<http://www.novell.com/documentation/idmrpbm361/agpro/data/b2gx735.html>) du *Guide d'administration de l'application utilisateur* pour déterminer la meilleure 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 [Mise en grappe](http://www.novell.com/documentation/idmrpbm361/agpro/data/b2gx73a.html) (<http://www.novell.com/documentation/idmrpbm361/agpro/data/b2gx73a.html>) dans le *Guide d'administration de l'application utilisateur*.

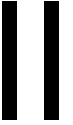
3.5 Instructions pour l'audit et la création de rapport

Pour utiliser l'audit et la création de rapport dans le cadre de la solution Identity Manager, vous devez installer Identity Audit ou Novell Sentinel™. Nous recommandons d'exécuter Identity Audit ou Sentinel sur son propre serveur, comme illustré à 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 requises pour l'installation d'un système Identity Manager.

- ♦ [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 47](#)
- ♦ [Chapitre 7, « Installation d'Identity Manager », page 57](#)
- ♦ [Chapitre 8, « Activation des produits Novell Identity Manager », page 69](#)
- ♦ [Chapitre 9, « Dépannage d'Identity Manager », page 73](#)

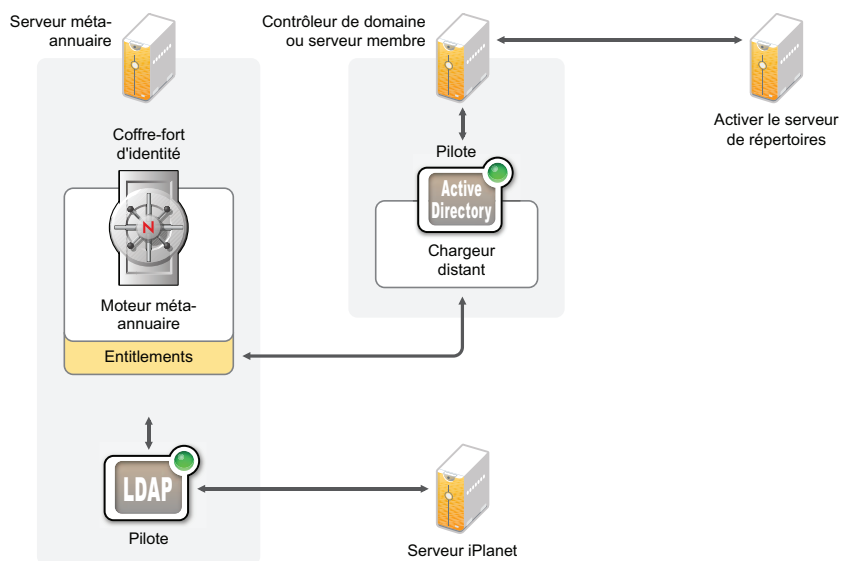
Liste de vérification pour un système Identity Manager de base

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, qui provisionne les utilisateurs en synchronisant les 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 41**
- ♦ **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 43**

4.1 Conditions préalables

- ❑ Installez Novell® eDirectory™ 8.8.5 ou une version ultérieure sur le serveur qui doit exécuter Identity Manager. Vérifiez que NMAS™ s'installe pendant l'installation d'eDirectory. Pour plus d'informations, reportez-vous au **site Web de la documentation d'eDirectory 8.8** (<http://www.novell.com/documentation/edir88/index.html>).

- ❑ Installez Novell iManager 2.7.3 sur le même serveur. Pour plus d'informations, reportez-vous au [site Web de la documentation d'iManager \(http://www.novell.com/documentation/imanager27/index.html\)](http://www.novell.com/documentation/imanager27/index.html).
- ❑ Téléchargez le produit Identity Manager. Pour savoir comment accéder au logiciel Identity Manager, reportez-vous au [Chapitre 5, « Où se procurer Identity Manager », page 45](#).
- ❑ Installez Designer 3.0.1 sur un poste de travail. Pour plus d'informations, reportez-vous à [Section 7.1, « Installation de Designer », page 57](#).

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, ainsi que par un plan de mise en place 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](#).

4.3 Installation

- ❑ Installez le serveur et les pilotes méta-annuaire. Pour plus d'informations, reportez-vous au [Chapitre 7, « Installation d'Identity Manager », page 57](#).
- ❑ Activez Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 8, « Activation des produits Novell Identity Manager », page 69](#).
- ❑ (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 de créer et de définir une logique d'activité dans les droits, 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 [Guide des droits d'Identity Manager 3.6.1](#).

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 moteur 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 « [Installation du chargeur distant](#) » dans le *Guide du chargeur distant d'Identity Manager 3.6.1*.
- ❑ 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 « [Configuration du chargeur distant](#) » dans le *Guide du chargeur distant d'Identity Manager 3.6.1*.
- ❑ 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 la documentation des pilotes pour Identity Manager 3.6.1](http://www.novell.com/documentation/idm36drivers/) (<http://www.novell.com/documentation/idm36drivers/>).
- ❑ (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 *Guide des droits d'Identity Manager 3.6.1*.
- ❑ 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 la documentation des pilotes pour Identity Manager 3.6.1](http://www.novell.com/documentation/idm36drivers/) (<http://www.novell.com/documentation/idm36drivers/>).
- ❑ (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 *Guide des droits d'Identity Manager 3.6.1*.
- ❑ 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** : pour gérer des mots de passe avec Identity Manager, vous devez procéder à une configuration supplémentaire. Utilisez la « [Liste de vérification de gestion des mots de passe](#) » dans le *Guide de gestion des mots de passe d'Identity Manager 3.6.1* pour vérifier que toutes les étapes de configuration sont réalisées.

- ❑ **Provisioning basé sur les rôles :** pour ajouter le provisioning basé sur les rôles à votre solution Identity Manager, utilisez la liste de vérification du *Guide d'installation de l'application utilisateur* (<http://www.novell.com/documentation/idmrbpm361/install/data/bookinfo.html>) pour vérifier que toutes les étapes de configuration sont réalisées.
- ❑ **Audit et création de rapport :** l'ajout de l'audit et de la création de rapport à votre solution Identity Manager vous permet de montrer que vos stratégies d'activité respectent les stratégies de la société. Vous pouvez ajouter Identity Audit ou Novell Sentinel à votre solution Identity Manager pour l'audit et la création de rapport. Pour plus d'informations sur Identity Audit, reportez-vous au *Guide d'intégration Identity Manager 3.6.1 pour Identity Audit*. Pour plus d'informations sur Novell Sentinel, reportez-vous au *Guide de création de rapports d'Identity Manager 3.6.1 pour Novell Sentinel*.

Où se procurer Identity Manager

5

Pour télécharger Identity Manager et ses services :

- 1 Allez sur le [site Web de téléchargements Novell \(http://download.novell.com\)](http://download.novell.com).
- 2 Dans le menu *Produit (Product) ou Technologie (Technologie)*, sélectionnez *Novell Identity Manager*, puis cliquez sur *Search (Rechercher)*.
- 3 Sur la page des téléchargements Novell Identity Manager, cliquez sur le bouton *Télécharger* à côté du fichier souhaité.
- 4 Suivez les invites à l'écran pour télécharger le fichier vers un répertoire de votre ordinateur.
- 5 Recommencez à partir de l'étape 2 jusqu'à ce que vous ayez téléchargé tous les fichiers dont vous avez besoin. La plupart des installations requièrent plusieurs images ISO.

Tableau 5-1 Fonctionnement des images ISO

Composants Identity Manager	Plates-formes	ISO
DVD Identity Manager	Identity Manager : Linux, Windows* et UNIX Designer : Linux et Windows	Identity_Manager_3_6_1_DVD.iso
CD Identity Manager et pilotes	Windows :	Identity_Manager_3_6_1_Win.iso
CD Identity Manager et pilotes	Linux	Identity_Manager_3_6_1_Linux.iso
CD Identity Manager et pilotes	Solaris	Identity_Manager_3_6_1_Solaris.iso
Identity Manager et pilotes	AIX	Identity_Manager_3_6_1_AIX.iso
CD Designer pour Identity Manager	Windows :	Identity_Manager_3_6_1_Designer_Win.iso
CD Designer pour Identity Manager	Linux	Identity_Manager_3_6_1_Designer_Linux.iso
Application utilisateur		Pour plus d'informations, reportez-vous au Guide d'installation de l'application utilisateur (http://www.novell.com/documentation/idmr/bpm361/index.html) .

Votre acquisition d'Identity Manager comprend des modules d'intégration pour plusieurs systèmes communs pour lesquels vous pourriez déjà avoir des licences : Novell® eDirectory™, Microsoft* Active Directory, LDAP v3 Directories, Novell GroupWise® et Lotus* Notes*. Tous les autres modules d'intégration d'Identity Manager doivent être achetés séparément.

L'image ISO de l'application utilisateur correspond à la version standard comprise avec votre achat Identity Manager 3.6.1. Le module de provisioning basé sur les rôles de l'application utilisateur est un produit complémentaire qui ajoute un workflow d'approbation puissant, basé sur les rôles, pour gérer les identités de vos utilisateurs. Le module de provisioning basé sur les rôles est livré sur une image ISO séparée et il est acheté séparément. Pour plus d'informations, reportez-vous au *Guide d'installation de l'application utilisateur* (<http://www.novell.com/documentation/idmrpbm361/index.html>).

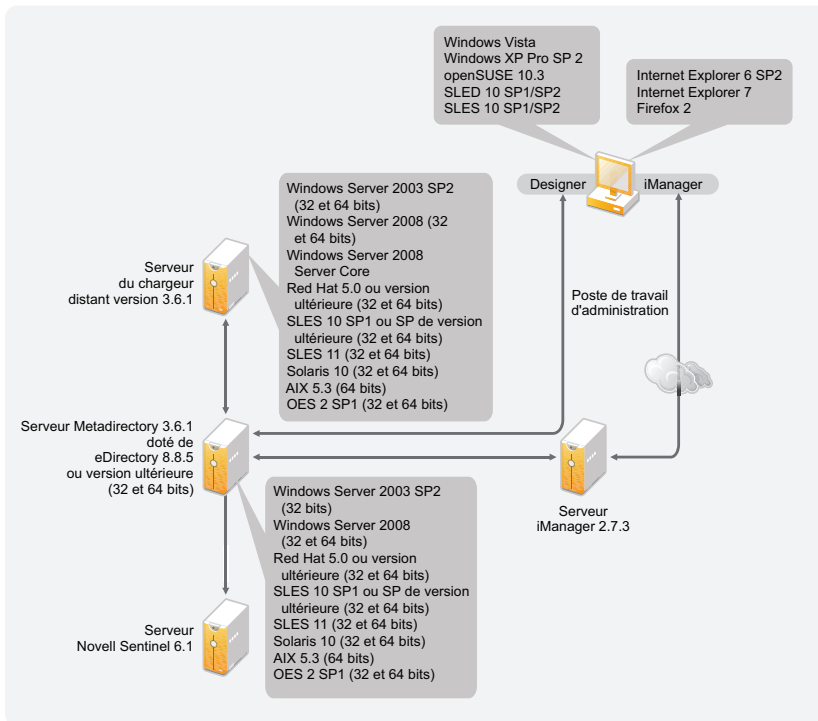
Votre achat d'Identity Manager comprend également Designer pour Identity Manager, un outil d'administration puissant et souple qui simplifie considérablement la configuration et le déploiement.

Configuration système requise

6

Les composants de Novell® Identity Manager peuvent être installés sur plusieurs systèmes et plusieurs 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



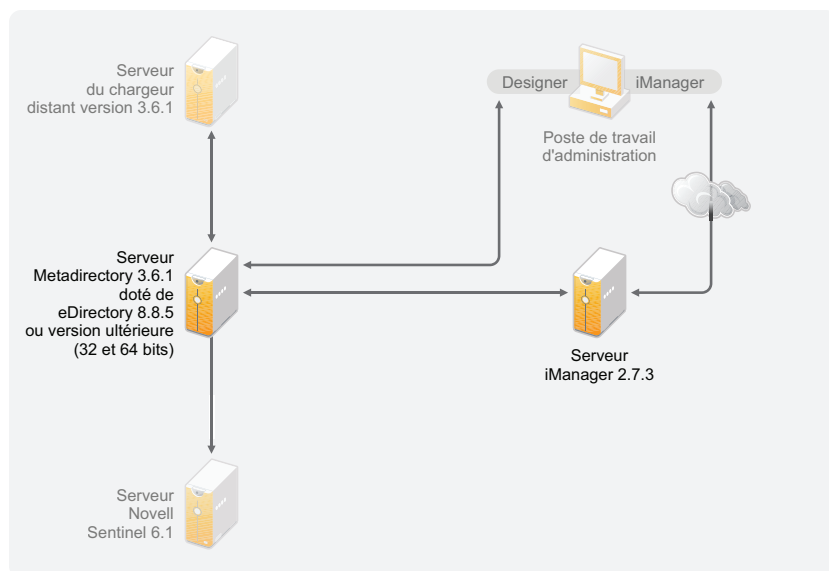
Selon la configuration de votre système, vous devrez peut-être exécuter le programme d'installation Identity Manager plusieurs fois pour installer les composants d'Identity Manager sur les systèmes adéquats.

- ♦ [Section 6.1, « eDirectory et iManager », page 47](#)
- ♦ [Section 6.2, « Serveur méta-annuaire », page 48](#)
- ♦ [Section 6.3, « Chargeur distant », page 51](#)
- ♦ [Section 6.4, « Application utilisateur », page 52](#)
- ♦ [Section 6.5, « Audit et création de rapport », page 52](#)
- ♦ [Section 6.6, « Postes de travail », page 53](#)

6.1 eDirectory et iManager

Identity Manager nécessite l'installation d'eDirectory™ et d'iManager. Ces produits forment la base d'Identity Manager. La **Figure 6-2** illustre ces composants.

Figure 6-2 Produits de base pour Identity Manager



La liste suivante répertorie les versions requises de ces produits :

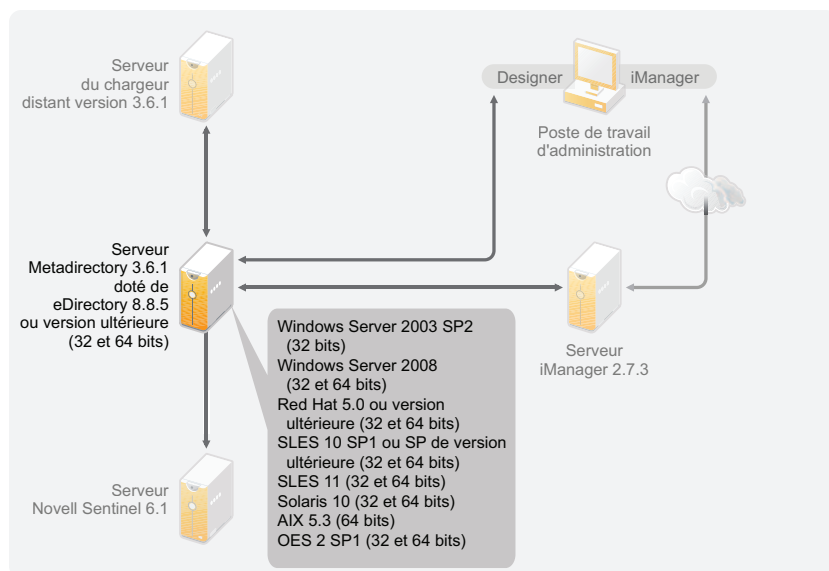
- ♦ eDirectory 8.8.5 ou une version ultérieure (32 ou 64 bits)
- ♦ iManager 2.7.3

Pour plus d'informations sur la configuration système d'eDirectory, reportez-vous au [Guide d'installation pour Novell eDirectory 8.8 SP5](http://www.novell.com/documentation/edir88/index.html) (<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) (<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 : eDirectory 8.8.5 ou une version ultérieure (32 ou 64 bits) doit être installé, sinon le programme d'installation s'interrompt.

- ♦ [Section 6.2.1, « Processeurs pris en charge », page 49](#)
- ♦ [Section 6.2.2, « Systèmes d'exploitation du serveur », page 50](#)

6.2.1 Processeurs pris en charge

Les processeurs listés ici sont utilisés pour le test d'Identity Manager. Le processeur SPARC* sert pour le test de Solaris*.

Les processeurs 32 bits pris en charge pour Linux (Red Hat* et SUSE® Linux Enterprise Server) et Windows sont :

- ♦ 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*

6.2.2 Systèmes d'exploitation du serveur

Vous pouvez installer le moteur méta-annuaire comme une 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.

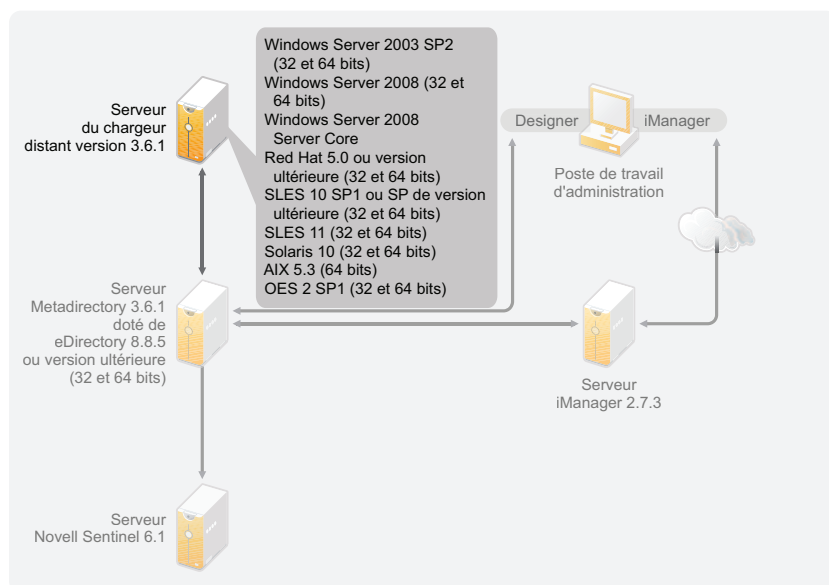
Tableau 6-1 *Systèmes d'exploitation pris en charge pour le serveur*

Version du système d'exploitation du serveur	Notes
Windows Server* 2003 SP2 (32 bits)	Le serveur méta-annuaire s'exécute uniquement en mode 32 bits.
Windows Server 2008 (32 ou 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.
Red Hat 5.0 ou version ultérieure (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.
Support Packs pour SUSE Linux Enterprise Server 10 SP1 ou 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.
SUSE Linux Enterprise Server 11 (32 et 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits. Novell conseille d'appliquer les derniers correctifs pour les systèmes d'exploitation en passant par le système de mises à jour automatisées du fabricant avant d'installer Identity Manager.
Solaris 10 (32 bits et 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.
Zones Solaris (32 et 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.
AIX* 5L v5.3 (64 bits)	Le serveur méta-annuaire s'exécute uniquement en mode 32 bits.
Xen*	Xen est pris en charge lorsque la machine virtuelle Xen exécute SLES 10/OES 2/OES 2 SP1 comme système d'exploitation invité en mode paravirtualisé.
VMware*	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.
Open Enterprise Server 2 SP1 (32 et 64 bits)	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 propose une prise en charge de 32 ou 64 bits. Par défaut, le programme d'installation détecte la version du système d'exploitation, puis installe la version correspondante du chargeur distant. Pour installer le chargeur distant 32 bits sur un système d'exploitation 64 bits, reportez-vous à « [Installation du chargeur distant 32 bits sur un système d'exploitation 64 bits](#) » page 64. La [Figure 6-4](#) liste les systèmes d'exploitation pris en charge pour le chargeur distant.

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



Si vous avez installé le moteur méta-annuaire comme application 32 bits sur un système d'exploitation 64 bits, vous ne pouvez pas installer le chargeur distant 64 bits sur la même machine. Les bibliothèques pour le moteur méta-annuaire 32 bits et pour le chargeur distant 64 bits ont les mêmes noms. Si elles sont toutes les deux installées sur la même machine, cela génère des conflits.

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 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 ou 64 bits.
Windows Server 2008 (32 ou 64 bits)	Le chargeur distant s'exécute en mode 32 ou 64 bits.
Windows Server 2008 Server Core (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 ou 64 bits.

Version du système d'exploitation du serveur	Notes
Red Hat 5.0 ou version ultérieure (32 et 64 bits)	Le chargeur distant 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.
Support Packs pour SUSE Linux Enterprise Server 10 SP1 ou ultérieurs (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 ou 64 bits. Novell conseille d'appliquer les derniers correctifs pour les systèmes d'exploitation en passant par le système de mises à jour automatisées du fabricant avant d'installer Identity Manager.
SUSE Linux Enterprise Server 11 (32 et 64 bits)	Le chargeur distant 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 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 ou 64 bits.
Zones Solaris (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 ou 64 bits.
AIX* 5L v5.3 (64 bits)	Le chargeur distant s'exécute en mode 32 bits uniquement. Le chargeur distant 64 bits n'est pas pris en charge.
Open Enterprise Server 2 SP1 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 ou 64 bits.

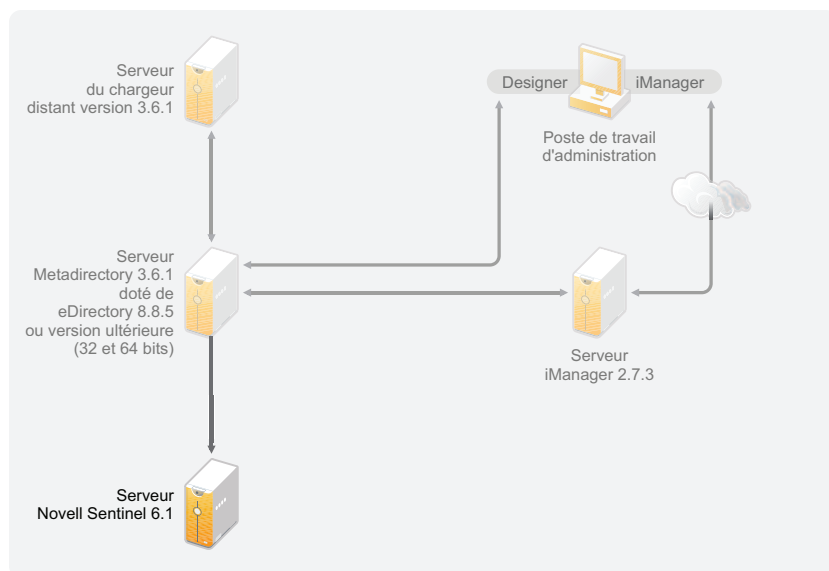
6.4 Application utilisateur

Pour plus d'informations sur la configuration système de l'application utilisateur, reportez-vous au *Guide d'installation de l'application utilisateur* (<http://www.novell.com/documentation/idmrbpm361/index.html>).

6.5 Audit et création de rapport

Identity Audit et Novell Sentinel™ sont deux outils qui permettent de rassembler des informations d'audit et de création de rapport sur Identity Manager. La **Figure 6-5** présente la version de Sentinel prise en charge avec Identity Manager 3.6.1.

Figure 6-5 Sentinel



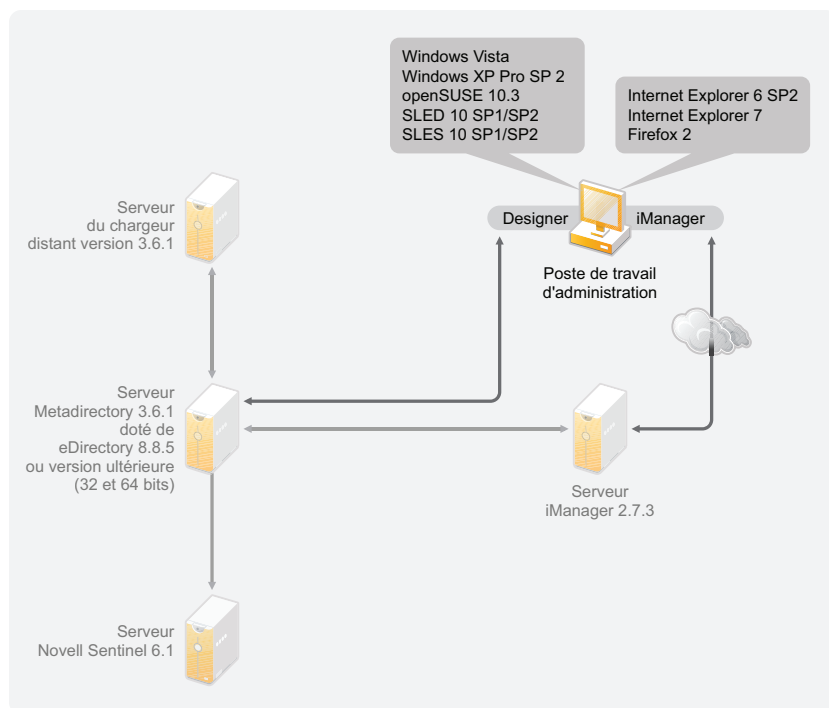
Il s'agit d'un ajout optionnel à la solution Identity Manager. L'ajout de l'audit et de la création de rapport permet de respecter les normes auxquelles de nombreuses sociétés doivent se conformer. Cela crée des suivis d'audit pour les événements que vous devez suivre et peut générer des rapports pour se conformer aux normes d'audit pour votre société.

Pour obtenir des informations de configuration sur Identity Audit avec Identity Manager, reportez-vous au *Guide d'intégration Identity Manager 3.6.1 pour Identity Audit*. Pour uniformiser la configuration à propos de Sentinel avec Identity Manager, reportez-vous au *Guide de création de rapports d'Identity Manager 3.6.1 pour Novell Sentinel*. Pour plus d'informations sur la configuration d'Identity Audit, reportez-vous au [Guide d'Identity Audit \(http://www.novell.com/documentation/identityaudit/index.html\)](http://www.novell.com/documentation/identityaudit/index.html). 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)*.

6.6 Postes de travail

Les postes de travail sont utilisés pour Designer, iManager ou la page Web d'administration de l'application utilisateur. La **Figure 6-6** montre les différents composants des postes de travail pris en charge avec Identity Manager 3.6.1.

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 54](#)
- ♦ [Section 6.6.2, « iManager et navigateurs Web », page 55](#)

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 Vista*	Les éditions Ultimate et Business sont prises en charge.
Windows XP Professionnel SP2	
openSUSE® 10.3	Appliquez les derniers correctifs en passant par le système de mise à jour automatisé.
SUSE Linux Enterprise Desktop 10 SP1/SP2	Appliquez les derniers correctifs en passant par le système de mise à jour automatisé.
SUSE Linux Enterprise Server 10 SP1/SP2	Appliquez les derniers correctifs en passant par le système de mise à jour automatisé.

6.6.2 iManager et navigateurs Web

La version de iManager prise en charge avec Identity Manager 3.6.1 est iManager 2.7.3. Elle exécute tous les plug-ins nécessaires à la configuration et à l'administration d'Identity Manager.

Voici les navigateurs Web pris en charge pour gérer Identity Manager :

- ◆ Internet Explorer* 6 SP2
- ◆ Internet Explorer 7
- ◆ Firefox* 2

Installation d'Identity Manager

7

Identity Manager propose des installations séparées pour les différents composants. Il est important d'installer et d'utiliser Designer pendant la phase de planification de la mise en place d'Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 2, « Création d'un plan de projet »](#), page 15.

Vous pouvez ensuite installer le serveur méta-annuaire ou le chargeur distant, dans l'ordre voulu. Les autres composants doivent être installés dans l'ordre indiqué. Pour obtenir une explication des différents composants, reportez-vous au guide *Présentation d'Identity Manager 3.6.1*.

- ♦ [Section 7.1, « Installation de Designer »](#), page 57
- ♦ [Section 7.2, « Installation du serveur méta-annuaire »](#), page 58
- ♦ [Section 7.3, « Installation du chargeur distant »](#), page 61
- ♦ [Section 7.4, « Installation du module de provisioning basé sur les rôles »](#), page 66
- ♦ [Section 7.5, « Installation d'un pilote personnalisé »](#), page 67
- ♦ [Section 7.6, « Installation d'Identity Audit ou de Sentinel »](#), page 67
- ♦ [Section 7.7, « Installation d'Identity Manager dans un environnement en grappe »](#), page 67

7.1 Installation de Designer

Designer 3.0.1 est un outil basé sur le poste de travail, permettant de concevoir votre solution Identity Manager. Installez d'abord Designer et utilisez-le dans toute la partie de planification de votre mise en place d'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 53.
- 2 Lancez l'installation en exécutant le programme adapté à la plate-forme de votre poste de travail.
 - ♦ **Windows** : `IDM3.6.1_Designer_Win:/windows/designer/install.exe`
 - ♦ **Linux** : `IDM3.6.1_Designer_Linux:/linux/designer/install`
Pour exécuter le fichier binaire, saisissez `./install`.
- 3 Les informations suivantes permettent de terminer l'installation :
 - ♦ **Dossier d'installation** : indiquez un emplacement sur le poste de travail sur lequel installer Designer.
 - ♦ **Créez les raccourcis** : choisissez les raccourcis placés sur votre bureau et dans le menu du bureau.
- 4 Pour en savoir plus, reportez-vous au [Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6](#).

7.2 Installation du serveur méta-annuaire

Pour les plates-formes Linux/UNIX, vous pouvez installer le serveur méta-annuaire en tant que `root` ou utilisateur non-root. Vous pouvez installer Identity Manager comme utilisateur non-root pour augmenter la sécurité sur le serveur. eDirectory doit être installé par un utilisateur non-root pour que l'installation non-root fonctionne. La procédure d'installation diffère si vous passez par l'installation non-root. Reportez-vous à la [Section 7.2.1, « Installation non-root du serveur méta-annuaire », page 59](#) pour obtenir des instructions d'installation.

Cette procédure traite de l'installation du serveur méta-annuaire, des composants Web et des utilitaires pour les différentes plates-formes prises en charge par Identity Manager.

- 1 Vérifiez de bien vous conformer à la configuration système du [Chapitre 6, « Configuration système requise », page 47](#).
- 2 (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 [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).

- 3 Lancez l'installation, à l'aide du programme convenant à votre plate-forme.
 - ♦ **Windows** : `IDM3.6.1_Win:windows\setup\idm_install.exe`
 - ♦ **Linux - Installation par la GUI** : `IDM3_6_1_Lin/install.bin [-i gui]`
 - ♦ **Linux - Installation par la ligne de commande** : `IDM3_6_1_Lin/install.bin -i console`
 - ♦ **Solaris - Installation par l'interface graphique** : `IDM3_6_1_Solaris/install.bin [-i gui]`
 - ♦ **Solaris - Installation par la ligne de commande** : `IDM3_6_1_Solaris/install.bin -i console`
 - ♦ **AIX - Installation par l'interface graphique** : `IDM3_6_1_AIX/install.bin [-i gui]`
 - ♦ **AIX - Installation par la ligne de commande** : `IDM3_6_1_AIX/install.bin -i console`

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

4 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 que le coffre-fort d'identité soit installé sur ce serveur. Elle prolonge le schéma pour Identity Manager, installe le moteur méta-annuaire, les pilotes Identity Manager et Novell® Audit Agent.
 - ♦ **Serveur système Novell Identity Manager connecté** : 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. Pour plus d'informations, reportez-vous à la [Section 7.3, « Installation du chargeur distant », page 61](#).
 - ♦ **Aucun** : sélectionnez cette option pour installer les plug-ins ou les utilitaires iManager sans installer le serveur méta-annuaire ni le serveur du système connecté sur ce serveur.
 - ♦ **Serveur d'administration Novell Identity Manager basé sur le Web** : 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.
 - ♦ **Personnaliser les composants sélectionnés** : cette option permet de personnaliser les composants que vous avez choisi d'installer. C'est pourquoi, avant de la sélectionner, vous devez sélectionner 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.

5 Activez Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 8, « Activation des produits Novell Identity Manager », page 69](#).

6 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 \(http://www.novell.com/documentation/idm36drivers/\)](#).

7.2.1 Installation non-root du serveur méta-annuaire

Vous pouvez installer Identity Manager en tant qu'utilisateur non-root pour 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`.

L'installation non-root n'installe pas les éléments suivants :

- ♦ **Chargeur distant** : utilisez le chargeur distant Java si vous voulez installer le chargeur distant en tant qu'utilisateur non-root. Pour plus d'informations, reportez-vous à la [Section 7.3.5, « Installation du chargeur distant Java sous UNIX, Linux ou AIX », page 66](#).
- ♦ **Pilote du compte UNIX/Linux** : nécessite des privilèges root pour fonctionner.

- ♦ **Agent de la plate-forme Novell Sentinel** : installez l'agent de la plate-forme Novell Sentinel en tant que root. Créez `Dirxml.properties` dans le répertoire `/etc/opt/novell/sentinelpa/conf`. L'emplacement dans lequel le fichier journal des événements est généré (`/var/opt/novell/sentinelpa/data/AuditEvents.log` est l'emplacement par défaut) doit disposer de l'autorisation en écriture pour un utilisateur non-root.

Procédez comme suit pour exécuter l'installation non-root du serveur méta-annuaire :

- 1 Installez eDirectory 8.8.5 ou une version ultérieure en tant qu'utilisateur non-root. Pour plus d'informations, reportez-vous à [Nonroot User Installing eDirectory 8.8 \(http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs\)](http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs) (Utilisateur non-root installant eDirectory 8.8).
- 2 Identifiez-vous sous l'identité de l'utilisateur non-root ayant installé eDirectory.
Il est conseillé d'installer Identity Manager avec la même identité que celle employée pour installer la version non-root d'eDirectory. L'utilisateur installant Identity Manager doit disposer d'un accès en écriture aux répertoires et aux fichiers de l'installation non-root d'eDirectory.
- 3 Exécutez le programme d'installation pour votre plate-forme.
 - ♦ **Linux** : `IDM3.6.1_Lin/linux/setup/idm-nonroot-install`
 - ♦ **AIX** : `IDM3.6.1_Unix/aix/setup/idm-nonroot-install`

Important : le seul niveau de maintenance AIX pris en charge est le niveau 5300-09. Les niveaux de maintenance plus récents ou plus anciens ne sont pas pris en charge.

 - ♦ **Solaris** : `IDM3.6.1_solaris/setup/idm-nonroot-install`

Pour exécuter les fichiers de script, saisissez `./idm-nonroot-install`
- 4 Les informations suivantes permettent de terminer l'installation :
 - ♦ **Répertoire de base pour l'installation eDirectory non-root** : 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 invités à étendre le schéma pour chaque instance d'eDirectory appartenant à l'utilisateur non-root hébergé par l'installation eDirectory non-root.
Si vous choisissez d'étendre le schéma, indiquez le nom distinctif (DN) complet pour l'utilisateur eDirectory ayant le droit d'étendre le schéma. L'utilisateur doit avoir reçu un droit de Superviseur sur la totalité de l'arborescence pour étendre le schéma. Pour plus d'informations sur le prolongement du schéma en tant qu'utilisateur non-root, reportez-vous au fichier `schema.log` placé dans le répertoire `data` pour chaque instance d'eDirectory.
Exécutez le programme `/opt/novell/eDirectory/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 `IDM3.6.1_platform/setup/utilities`.

- 5 Activez Identity Manager. Pour plus d'informations, reportez-vous au [Chapitre 8, « Activation des produits Novell Identity Manager », page 69](#).
- 6 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 \(http://www.novell.com/documentation/idm36drivers/\)](http://www.novell.com/documentation/idm36drivers/).

7.2.2 Installation en mode silencieux du serveur méta-annuaire

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

- ♦ **Linux** : `IDM3_6_1_Lin/install.bin -i silent -f <nom du fichier>.properties`
- ♦ **Solaris** : `IDM3_6_1_Solaris/install.bin -i silent -f <nom du fichier>.properties`
- ♦ **AIX** : `IDM3_6_1_AIX/install.bin -i silent -f <nom du fichier>.properties`

Créez un fichier de propriétés `<nom du 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
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

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

Remarque : si vous avez installé iManager et que vous souhaitez installer les plug-ins associés ultérieurement, vous devez définir la valeur `WEB_ADMIN_SELECTED` sur `true`.

Remarque : si vous souhaitez procéder à une installation silencieuse d'Identity Manager sur plusieurs instances, vous devez vous assurer que le fichier `<nom de fichier>.properties` comporte les éléments suivants :

```
EDIR_NCP_PORT=1524
EDIR_NDS_CONF=/etc/opt/novell/eDirectory/conf
EDIR_IP_ADDRESS=<xxx.xx.xx.xx>
```

7.3 Installation du chargeur distant

Le chargeur distant prolonge les fonctionnalités d'Identity Manager en permettant au pilote d'accéder au système connecté sans avoir installé le coffre-fort d'identité et le moteur méta-annuaire 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 7.3.1, « Configuration requise », page 62](#)
- ♦ [Section 7.3.2, « Pilotes pris en charge », page 62](#)
- ♦ [Section 7.3.3, « Procédure d'installation », page 63](#)

Pour installer le chargeur distant à l'aide d'un utilisateur non-root, utilisez le chargeur distant Java. Il peut aussi servir pour personnaliser votre environnement et l'installer sur une plate-forme non prise en charge, comme HP-UX*. Pour plus d'informations, reportez-vous à la [Section 7.3.5, « Installation du chargeur distant Java sous UNIX, Linux ou AIX »](#), page 66.

7.3.1 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 \(http://www.novell.com/documentation/idm36drivers\)](http://www.novell.com/documentation/idm36drivers) pour connaître la configuration requise du système d'exploitation et du système connecté spécifiques à chaque pilote.

7.3.2 Pilotes pris en charge

Tous les pilotes Identity Manager ne sont pas pris en charge par le chargeur distant. Le [Tableau 7-1](#) liste les pilotes compatibles avec le chargeur distant.

Tableau 7-1 Pilotes compatibles avec le chargeur distant

Active Directory	Avaya* PBX
Texte délimité	GroupWise®
JDBC*	JMS
LDAP	Pilote pour Linux et UNIX
Lotus Notes*	PeopleSoft* 5.2
Remedy* ARS	SAP* HR
SAP User Management	Scripting
SOAP	WorkOrder
Manual Task Services	Null Services
LoopBack	

Les pilotes listés dans le [Tableau 7-2](#) ne peuvent pas utiliser le chargeur distant.

Tableau 7-2 Non compatibles avec le chargeur distant

eDirectory	Service des droits
Service de rôle	Application utilisateur

7.3.3 Procédure d'installation

Le chargeur distant possède des programmes différents pour les différentes plates-formes lui permettant de communiquer avec le moteur méta-annuaire.

- ♦ **Windows** : la console du chargeur distant utilise `rlconsole.exe` pour s'interfacer avec `dirxml_remote.exe`, un exécutable permettant au moteur méta-annuaire de communiquer avec les pilotes Identity Manager s'exécutant sous Windows.
- ♦ **Linux/UNIX** : `rdxml` est un exécutable permettant au moteur méta-annuaire de communiquer avec les pilotes Identity Manager s'exécutant sous Solaris, Linux ou AIX.

Pour installer le chargeur distant :

- 1 Vérifiez que vous respectez la configuration système listée dans le [Chapitre 6, « Configuration système requise », page 47](#).
- 2 Lancez l'installation, à l'aide du programme convenant à votre plate-forme.
 - ♦ **Windows** : `IDM3.6.1_Win:windows\setup\idm_install.exe`
 - ♦ **Linux - Installation par la GUI** : `IDM3_6_1_Lin/install.bin [-i gui]`
 - ♦ **Linux - Installation par la ligne de commande** : `IDM3_6_1_Lin/install.bin -i console`
 - ♦ **Solaris - Installation par l'interface graphique** : `IDM3_6_1_Solaris/install.bin [-i gui]`
 - ♦ **Solaris - Installation par la ligne de commande** : `IDM3_6_1_Solaris/install.bin -i console`
 - ♦ **AIX - Installation par l'interface graphique** : `IDM3_6_1_AIX/install.bin [-i gui]`
 - ♦ **AIX - Installation par la ligne de commande** : `IDM3_6_1_AIX/install.bin -i console`

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

Important : le seul niveau de maintenance AIX pris en charge est le niveau 5300-09. Les niveaux de maintenance plus récents ou plus anciens ne sont pas pris en charge.

- 3 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 7.2, « Installation du serveur méta-annuaire », page 58](#).
 - ♦ **Serveur système Novell Identity Manager connecté** : cette option ne nécessite pas l'installation du coffre-fort d'identité sur ce serveur. Elle installe le service du chargeur distant sur votre serveur d'application.
 - ♦ **Aucun** : sélectionnez cette option pour installer les plug-ins ou les utilitaires iManager sans installer le serveur méta-annuaire ni le serveur du système connecté sur ce serveur.

- ♦ **Serveur d'administration Novell Identity Manager basé sur le Web :** 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.

Avvertissement : pour installer Identity Manager 3.6.1, ne sélectionnez pas le composant Utilitaires. Si vous sélectionnez le composant Utilitaires, l'installation ne pourra pas se poursuivre.

- ♦ **Personnalisé :** sélectionnez cette option pour personnaliser les fonctions installées. Cela vous permet de sélectionner les options suivantes :
 - ♦ **Service du chargeur distant :** le service qui communique avec le moteur 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.
 - ♦ **Enregistrer les composants du système Identity Audit pour Identity Manager :** choisissez cette option si vous avez installé Identity Audit ou Novell Sentinel.

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 seulement) Emplacement d'installation pour les utilitaires :** indiquez le répertoire dans lequel sont installés les utilitaires.
- 4 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 \(http://www.novell.com/documentation/idm36drivers/\)](http://www.novell.com/documentation/idm36drivers/).
 - 5 Créez un fichier de configuration de chargeur distant pour travailler avec votre système connecté. Pour plus d'informations, reportez-vous à « **Configuration du chargeur distant pour Linux/UNIX en créant un fichier de configuration** » dans le *Guide du chargeur distant d'Identity Manager 3.6.1*.

Installation du chargeur distant 32 bits sur un système d'exploitation 64 bits

Sous Windows :

- 1 Recherchez le fichier `32bit_RL_Install.properties` dans le dossier `..\Windows\setup\` et définissez les valeurs de la propriété `RL_32BIT_INSTALL_ON_64BIT` sur `true` de la façon suivante :


```
RL_32BIT_INSTALL_ON_64BIT=true
```
- 2 Dans l'invite de commande, remplacez le chemin du répertoire par le dossier d'installation d'IDM 3.6.1 (par exemple, `C:\IDM3.6.1\windows\setup`) et saisissez la commande suivante :


```
idm_install.exe - i gui[console] -f 32bit_RL_Install.properties
```

- 3 Poursuivez à partir de l'étape 3 de la Section 7.3.3, « Procédure d'installation », page 63 pour terminer l'installation.

Sous Linux :

- 1 Recherchez le fichier `32bit_RL_Install.properties` dans le dossier `../linux/setup` et définissez les valeurs de la propriété `RL_32BIT_INSTALL_ON_64BIT` sur `true` de la façon suivante :

```
RL_32BIT_INSTALL_ON_64BIT=true
```

- 2 Dans le terminal, remplacez le chemin du répertoire par le dossier d'installation d'IDM 3.6.1 (par exemple, `../linux/setup`) et saisissez la commande suivante :

```
idm_linux.bin - i gui[console] -f 32bit_RL_Install.properties
```

- 3 Poursuivez à partir de l'étape 3 de la Section 7.3.3, « Procédure d'installation », page 63 pour terminer l'installation.

7.3.4 installation en mode silencieux du chargeur distant

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

- ♦ **Linux** : `IDM3_6_1_Lin/install.bin -i silent -f <nom du fichier>.properties`
- ♦ **Solaris** : `IDM3_6_1_Solaris/install.bin -i silent -f <nom du fichier>.properties`
- ♦ **AIX** : `IDM3_6_1_AIX/install.bin -i silent -f <nom du fichier>.properties`

Créez un fichier de propriétés `<nom du 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=false  
CONNECTED_SYSTEM_SELECTED=true  
WEB_ADMIN_SELECTED=false  
UTILITIES_SELECTED=false
```

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

Remarque : si vous avez installé iManager et que vous souhaitez installer les plug-ins associés ultérieurement, vous devez définir la valeur `WEB_ADMIN_SELECTED` sur `true`

7.3.5 Installation du chargeur distant Java sous UNIX, Linux ou AIX

`dirxml_jremote` est un chargeur distant Java pur. Il sert à échanger des données entre le moteur méta-annuaire s'exécutant sur un serveur et les pilotes Identity Manager s'exécutant sur un autre emplacement, où ne s'exécute pas `rdxml`. 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 Java 1.5x JDK*/JRE est disponible sur le système hôte.
- 2 Copiez le fichier `dirxml_jremote_dev.tar.gz` à l'emplacement souhaité sur le serveur distant.
- 3 Copiez le fichier `dirxml_jremote.tar.gz` ou `dirxml_jremote_mvs.tar` à l'emplacement souhaité sur le serveur distant.

Par exemple : `/usr/idm`

Le fichier se trouve au même endroit sur les images ISO Linux ou UNIX. Les fichiers se trouvent dans le dossier `java_remoteloader` à la racine de l'image ISO. Pour plus d'informations sur `mvs`, décompressez le fichier `dirxml_jremote_mvs.tar`, puis reportez-vous au document `usage.html`.

- 4 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`

- 5 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`.

Le fichier compressé ne contenant pas de pilotes, vous devez copier manuellement les pilotes dans le répertoire `lib`. Le répertoire `lib` se trouve sous le répertoire de décompression.

- 6 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.

- 7 Configurez le fichier d'exemple `config8000.txt` à utiliser avec votre module d'interface d'application. Pour plus d'informations, reportez-vous à « [Configuration du chargeur distant pour Linux/UNIX en créant un fichier de configuration](#) » dans le *Guide du chargeur distant d'Identity Manager 3.6.1* [Guide du chargeur distant d'Identity Manager 3.6.1](#)

7.4 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](#) (<http://www.novell.com/documentation/idmrbpm361/index.html>) pour le module de provisioning basé sur les rôles.

7.5 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 \(http://developer.novell.com/wiki/index.php/Dirxml\)](http://developer.novell.com/wiki/index.php/Dirxml) (Kit du développeur Novell).

7.6 Installation d'Identity Audit ou de Sentinel

Il s'agit d'un ajout optionnel à la solution Identity Manager. L'ajout de l'audit et de la création de rapport permet de respecter les normes auxquelles de nombreuses sociétés doivent se conformer. Cela crée des suivis d'audit pour les événements que vous devez suivre et peut générer des rapports pour vérifier que vous vous conformez aux normes d'audit de votre société.

Pour obtenir des informations de configuration sur Identity Audit avec Identity Manager, reportez-vous au *Guide d'intégration Identity Manager 3.6.1 pour Identity Audit*. Pour obtenir des informations de configuration sur Sentinel avec Identity Manager, reportez-vous au *Guide de création de rapports d'Identity Manager 3.6.1 pour Novell Sentinel*. Pour plus d'informations sur la configuration d'Identity Audit, reportez-vous au [Guide d'Identity Audit \(http://www.novell.com/documentation/identityaudit/index.html\)](http://www.novell.com/documentation/identityaudit/index.html). 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)*.

7.7 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, le plus souvent, la grappe elle-même n'est pas prise en charge. Les deux scénarios suivants décrivent la portée de la prise en charge :

- ♦ Si vous exécutez le moteur Identity Manager ou le chargeur distant sur SUSE Linux Enterprise Server (SLES) et que vous utilisez Heartbeat pour gérer la haute disponibilité, tous les éléments sont pris en charge.
- ♦ Si vous exécutez le moteur Identity Manager 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 en 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 \(Configuration d'une grappe haute disponibilité Linux pour IDM 3 et eDirectory 8.8\)](http://www.novell.com/coolsolutions/appnote/18591.html), 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 \(Mise en grappe d'eDirectory et IDM sous Windows 2003\)](http://www.novell.com/coolsolutions/appnote/14856.html), sur le [site Web Novell Cool Solutions \(http://www.novell.com/coolsolutions/appnote/14856.html\)](http://www.novell.com/coolsolutions/appnote/14856.html).

- ♦ High Availability on PolyServe Clusters (Haute disponibilité sur des grappes PolyServe), sur le [site Web Novell Cool Solutions \(http://www.novell.com/cool solutions/appnote/16131.html\)](http://www.novell.com/cool solutions/appnote/16131.html).
- ♦ Setting Up an Identity Manager Cluster on Windows (Configuration d'une grappe Identity Manager sous Windows), sur le [site Web Novell Support \(http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3575742&sliceId=SAL_Public&dialogID=310596&stateId=1%20%20308676\)](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3575742&sliceId=SAL_Public&dialogID=310596&stateId=1%20%20308676). Le document porte le numéro 3575742.

Activation des produits Novell Identity Manager

8

Les informations suivantes expliquent comment fonctionne l'activation pour les produits basés sur 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 69](#)
- ♦ [Section 8.2, « Installation d'une référence d'activation de produit », page 69](#)
- ♦ [Section 8.3, « Affichage des activations de produits pour Identity Manager et les pilotes », page 70](#)

8.1 Achat d'une licence de produit Identity Manager

Pour acheter une licence de produit Identity Manager, reportez-vous à la [page Web Acheter Novell Identity Manager \(http://www.novell.com/products/identitymanager/howtobuy.html\)](http://www.novell.com/products/identitymanager/howtobuy.html)


Une fois la licence de produit achetée, Novell vous envoie votre ID client par courrier électronique. Le courrier électronique contient également une URL vers le site Novell sur lequel vous pouvez obtenir une référence. Si vous ne vous en souvenez pas ou si vous ne recevez pas votre ID client, appelez le centre d'activation Novell Activation au 1-800-418-8373 aux États-Unis. Dans les autres pays, appelez le 1-801-861-8373. (Les appels effectués avec l'indicatif 801 vous seront facturés.)

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 du produit installé pour le moteur méta-annuaire et les pilotes Identity Manager :

- 1 Ouvrez iManager.
- 2 Cliquez sur *Identity Manager > Présentation d'Identity Manager*.
- 3 Cliquez sur  pour naviguer jusqu'à un ensemble de pilotes dans l'arborescence et le sélectionner, puis cliquez sur  pour lancer la recherche.
- 4 Sur la page Présentation d'Identity Manager, cliquez sur l'ensemble de pilotes pour lequel afficher les informations d'activation.
- 5 Sur la page Présentation de l'ensemble des pilotes, cliquez sur *Activation > Information*.
Vous pouvez afficher le texte de la référence d'activation ou, si une erreur est signalée, vous pouvez supprimer une référence d'activation.

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

Dépannage d'Identity Manager

9

Les informations suivantes sont utiles lorsque vous installez Identity Manager :

- ♦ Sous AIX 5.3, l'installation d'IDM 3.6.1 se bloque si des montages NFS sont arrêtés. C'est également le cas lorsque le programme d'installation iso d'IDM se trouve sur la même machine (AIX) et qu'une partition montée quelconque est arrêtée.

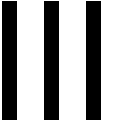
Solution : démontez/remontez les montages arrêtés et poursuivez l'installation.

- ♦ Sous Solaris 10, lors de l'installation d'IDM 3.6.1 en tant qu'utilisateur non-root, le message d'erreur de pilote de Lotus Notes suivant peut apparaître :

```
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
```

Solution : vous devez créer manuellement les liens symboliques. Pour plus d'informations sur la vérification et la recréation de liens symboliques, reportez-vous à « [Dépannage des problèmes d'installation](#) » dans le *Guide d'implémentation du pilote Identity Manager 3.6.1 pour Lotus Notes*.

Mise à niveau



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

- ♦ [Chapitre 10, « Nouveautés », page 77](#)
- ♦ [Chapitre 11, « Versions prises en charge pour les mises à niveau et configuration système requise », page 79](#)
- ♦ [Chapitre 12, « Mise à niveau directe \(in-place\) et migration », page 81](#)
- ♦ [Chapitre 13, « Mise à niveau directe », page 83](#)
- ♦ [Chapitre 14, « Exécution d'une migration », page 97](#)

- [Section 10.1, « Prise en charge des systèmes d'exploitation 64 bits », page 77](#)
- [Section 10.2, « Prise en charge de l'installation du chargeur distant 32 bits sur les systèmes d'exploitation 64 bits », page 77](#)

10.1 Prise en charge des systèmes d'exploitation 64 bits

Identity Manager prend désormais en charge les systèmes d'exploitation 64 bits. Pour obtenir une liste des systèmes d'exploitation pris en charge, reportez-vous à la [Section 6.2.2, « Systèmes d'exploitation du serveur », page 50](#).

10.2 Prise en charge de l'installation du chargeur distant 32 bits sur les systèmes d'exploitation 64 bits

Identity Manager prend en charge l'installation du chargeur distant 32 bits sur les systèmes d'exploitation 64 bits. Pour obtenir une liste des systèmes d'exploitation pris en charge, reportez-vous à la [Section 6.3, « Chargeur distant », page 51](#).

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

- [Section 11.1, « Versions prises en charge pour les mises à niveau », page 79](#)
- [Section 11.2, « Configuration système requise », page 79](#)

11.1 Versions prises en charge pour les mises à niveau

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

Tableau 11-1 Versions prises en charge pour les mises à niveau

Versions installées	Version la plus récente	Mise à niveau prise en charge
DirXML® 1.1a	Identity Manager 3.6.1	Non
Identity Manager 2.x	Identity Manager 3.6.1	Non
Identity Manager 3.0.x	Identity Manager 3.6.1	Non
Identity Manager 3.5.x	Identity Manager 3.6.1	Oui

Remarque : Identity Manager 3.5.x est compatible avec les plates-formes prises en charge par le chargeur distant 3.6 et 3.6.1.

11.2 Configuration système requise

Pour une mise à niveau vers Identity Manager 3.6.1, les serveurs qui exécutent les services d'Identity Manager doivent respecter les conditions minimum requises. Reportez-vous au [Chapitre 6, « Configuration système requise », page 47](#) pour connaître la configuration minimum requise pour chaque plate-forme.

Mise à niveau directe (in-place) et migration

12

Il existe deux manières de mettre à niveau : la mise à niveau directe ou la migration. Chacune de ces méthodes possède ses avantages et ses inconvénients ; dans certains cas, une seule méthode peut être utilisée.

- ♦ [Section 12.1, « Mise à niveau directe », page 81](#)
- ♦ [Section 12.2, « Migration », page 82](#)
- ♦ [Section 12.3, « Plusieurs serveurs associés à un seul ensemble de pilotes », page 82](#)

12.1 Mise à niveau directe

L'installation de la nouvelle version d'Identity Manager sur le serveur existant constitue une mise à niveau directe. Pour installer Identity Manager, vous devez mettre les versions actuelles du système d'exploitation et d'eDirectory™ au niveau des versions prises en charge pour Identity Manager 3.6.1. Pour obtenir la liste des plates-formes prises en charge, reportez-vous au [Chapitre 6, « Configuration système requise », page 47](#).

Les avantages sont les suivants :

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

Les inconvénients sont les suivants :

- ♦ 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 directe ne peut pas avoir lieu ; dans d'autres, plusieurs mises à niveau directes doivent être effectuées. Identity Manager 3.5x et les versions ultérieures, étant les seuls chemins de migration pris en charge, sont aussi les seules versions concernées par les cas suivants :

La mise à niveau directe n'est possible que si Identity Manager 3.5.x est exécuté sur un système d'exploitation pris en charge. Il existe cependant des situations dans lesquelles la mise à niveau directe n'est pas réalisable. Voici quelques exemples de cas dans lesquels la mise à niveau directe n'est pas réalisable :

- ♦ **Système d'exploitation non pris en charge** : si la version actuelle du système d'exploitation n'est pas prise en charge par Identity Manager 3.6.1, le seul chemin de mise à niveau possible consiste en une migration 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 (in-place). Les deux options sont :
 - ♦ Effectuez une mise à niveau directe (in-place) vers Identity Manager 3.5.1, installez eDirectory 8.8.5, puis effectuez une mise à niveau directe (in-place) vers Identity Manager 3.6.1.
 - ♦ Effectuez une migration vers un nouveau serveur.

Si vous effectuez une mise à niveau directe, passez au [Chapitre 13, « Mise à niveau directe », page 83](#).

12.2 Migration

Une migration installe Identity Manager 3.6.1 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](#).

Les avantages sont les suivants :

- ♦ Le temps hors service des pilotes est minime.

Les inconvénients sont les suivants :

- ♦ Nouveau matériel requis

Si vous effectuez une migration, passez au [Chapitre 14, « Exécution d'une migration », page 97](#).

12.3 Plusieurs serveurs associés à un seul ensemble de pilotes

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

Le moteur d'Identity Manager est compatible avec les versions précédentes ; ainsi, le moteur d'Identity Manager 3.6.1 peut exécuter sans difficulté les pilotes d'Identity Manager 3.5.x

Avertissement : si vous activez des fonctions pour des pilotes qui ne sont pris en charge que par Identity Manager 3.6.1, les pilotes cessent de fonctionner sur les serveurs à versions mixtes. Les moteurs plus anciens ne peuvent pas traiter les nouvelles fonctions. Les pilotes sont arrêtés jusqu'à ce que tous les serveurs soient mis au niveau d'Identity Manager 3.6.1.

Avant de commencer, assurez-vous d'avoir examiné les différences entre une mise à niveau directe et une migration. Reportez-vous au [Chapitre 12, « Mise à niveau directe \(in-place\) et migration »](#), page 81.

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 mise à niveau directe du système Identity Manager. Suivez ces étapes pour chaque serveur d'Identity Manager de votre environnement.

- ❑ 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 13.1, « Création d'une sauvegarde de la configuration actuelle »](#), page 85.
- ❑ 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 47. Si le système d'exploitation n'exige qu'un service pack pour remplir les exigences du système, passez à la mise à niveau directe. S'il exige plus, vous devez exécuter une migration au lieu d'une mise à niveau directe. Continuez avec le [Chapitre 14, « Exécution d'une migration »](#), page 97 si votre système d'exploitation est l'un des suivants :
 - ♦ NetWare®
 - ♦ Windows NT
 - ♦ Windows 2000
 - ♦ Red Hat Linux 3
 - ♦ SLES 8
 - ♦ Solaris 8 ou 9
- ❑ Mettez votre serveur iManager à niveau vers iManager 2.7.3. Pour plus d'informations, reportez-vous au [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).
- ❑ Arrêtez les pilotes associés au serveur que vous mettez à niveau. Pour plus d'informations, reportez-vous à la [Section 13.2, « Arrêt des pilotes »](#), page 87.
- ❑ Sur le serveur exécutant Identity Manager, mettez eDirectory™ à niveau vers la version 8.8.5 ou une version ultérieure. Pour plus d'informations, reportez-vous au [Guide d'installation d'eDirectory \(http://www.novell.com/documentation/edir88/index.html\)](http://www.novell.com/documentation/edir88/index.html).
- ❑ (Facultatif) Si votre plate-forme est Linux, UNIX ou Solaris, vous devez réaliser des étapes supplémentaires pour ajouter des fichiers à l'emplacement souhaité. Pour plus d'informations, reportez-vous à la [Section 13.3, « Ajout de fichiers à l'emplacement correct sur les plates-formes Linux/UNIX »](#), page 88.
- ❑ Lancez les pilotes et vérifiez qu'ils démarrent. La réussite de la mise à niveau vers eDirectory 8.8.5 est aussi contrôlée. Pour plus d'informations, reportez-vous à la [Section 13.10, « Lancement des pilotes »](#), page 94.
- ❑ Effectuez la mise à niveau vers Designer 3.0.1. Pour plus d'informations, reportez-vous à [« Mise à niveau de Designer »](#) dans le [Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6](#).

- ❑ Convertissez le projet Designer. Pour plus d'informations, reportez-vous à « [Conversion de projet antérieurs](#) » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.
- ❑ Arrêtez les pilotes associés au serveur que vous mettez à niveau. Pour plus d'informations, reportez-vous à la [Section 13.2, « Arrêt des pilotes »](#), page 87.
- ❑ Mettez le serveur méta-annuaire à niveau. Pour plus d'informations, reportez-vous à la [Section 13.5, « Mise à niveau du moteur méta-annuaire et des fichiers de configuration des pilotes »](#), page 89.
- ❑ (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 13.6, « Mise à niveau du chargeur distant »](#), page 90
- ❑ (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 *Guide de migration d'un module de provisioning basé sur les rôles* (<http://www.novell.com/documentation/idmrpbm361/index.html>).
 - ❑ Créez un nouveau pilote de service de rôle. Les pilotes de service de rôle ne sont pas migrés. Si vous avez un pilote de service de rôle pour la version 3.6.1, vous devez créer un nouveau pilote pour la version 3.6.1. Pour plus d'informations, reportez-vous au *Guide de migration d'un module de provisioning basé sur les rôles* (<http://www.novell.com/documentation/idmrpbm361/index.html>).
 - ❑ Déployez le pilote de l'application utilisateur migré dans le coffre-fort d'identité. Pour plus d'informations, reportez-vous au *Guide de migration d'un module de provisioning basé sur les rôles* (<http://www.novell.com/documentation/idmrpbm361/index.html>).
 - ❑ Mettez à niveau l'application utilisateur. Pour plus d'informations, reportez-vous au *Guide de migration d'un module de provisioning basé sur les rôles* (<http://www.novell.com/documentation/idmrpbm361/index.html>).
- ❑ (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 13.7, « Superposition du nouveau fichier de configuration du pilote sur le pilote existant »](#), page 91.
- ❑ (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 13.8, « Restauration de stratégies et de règles personnalisées pour le pilote »](#), page 92.
- ❑ Déployez le projet Designer converti dans le coffre-fort d'identité. Pour plus d'informations, reportez-vous à « [Déploiement et exportation](#) » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.
- ❑ Démarrez les pilotes associés à ce serveur. Pour plus d'informations, reportez-vous à la [Section 13.10, « Lancement des pilotes »](#), page 94

- ❑ Si vous utilisez Novell Sentinel™, vous devez effectuer la 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 moteur méta-annuaire et tout pilote mis à niveau. Pour plus d'informations, reportez-vous au **Chapitre 8, « Activation des produits Novell Identity Manager », page 69.**

13.1 Création d'une sauvegarde de la configuration actuelle

Avant de procéder à la mise à niveau, il est important de créer une sauvegarde de la configuration actuelle de votre système Identity Manager. 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 13.1.1, « Vérification de l'actualité de votre projet Designer », page 85**
- ♦ **Section 13.1.2, « Création d'une exportation des pilotes », page 87**

13.1.1 Vérification de l'actualité de votre projet Designer

Un projet Designer contient le schéma et toutes les informations de configuration du pilote, sauf celles du pilote de droits basés sur les rôles. La création d'un projet contenant votre solution Identity Manager permet d'exporter tous les pilotes en une seule étape au lieu de créer un fichier d'exportation pour chaque pilote.

- ♦ **« Exportation du projet actuel » page 85**
- ♦ **« Création d'un nouveau projet à partir du coffre-fort d'identité » page 86**

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 « **Utilisation de la fonction de comparaison lors du déploiement** » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.
- 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. Quand vous mettez Designer au niveau de la version 3.0.1, vous devez créer un nouvel emplacement d'espace de travail. Pour plus d'informations, reportez-vous à « **Exportation d'un projet** » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.

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** Téléchargez et installez Designer 3.0.1.
Avec Designer 3.0.1, vous pouvez créer un projet Identity Manager 3.6.x. Pour plus d'informations, reportez-vous à la [Section 7.1, « Installation de Designer », page 57](#).
- 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 de coffre-fort d'identité.
 - ♦ **Nom d'utilisateur** : indiquez le DN de l'utilisateur pour l'authentification au coffre-fort d'identité.
 - ♦ **Mot de passe** : indiquez le mot de passe de l'utilisateur d'authentification.
- 9** Cliquez sur *Suivant*.
- 10** Laissez le schéma de coffre-fort d'identité et la collection de notification par défaut cochés.
- 11** Développez la collection de notification par défaut et décochez les langues dont vous n'avez pas besoin.
Les collections de notification par défaut sont traduites vers beaucoup de langues différentes. Vous pouvez importer toutes les langues ou sélectionner seulement celles que vous utilisez.
- 12** Cliquez sur *Parcourir*, puis naviguez jusqu'à un ensemble de pilotes à importer et sélectionnez-le.
- 13** Répétez l'[Étape 12](#) pour chaque ensemble de pilotes dans ce coffre-fort d'identité, puis cliquez sur *Terminer*.
- 14** Une fois l'importation du projet terminée, cliquez sur *OK*.
- 15** Si vous n'avez qu'un seul coffre-fort d'identité, vous avez terminé. Si vous n'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.

13.1.2 Création d'une exportation des pilotes


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

- ♦ « [Utilisation de Designer pour créer une exportation du pilote](#) » page 87
- ♦ « [Utilisation d'iManager pour créer une exportation du pilote](#) » page 87

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 les instructions, reportez-vous à « [Importation d'une bibliothèque, d'un ensemble des pilotes ou d'un pilote à partir du coffre-fort d'identité](#) » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.
- 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.

13.2 Arrêt des pilotes



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

- ♦ [Section 13.2.1, « Utilisation de Designer pour arrêter les pilotes », page 88](#)
- ♦ [Section 13.2.2, « Utilisation d'iManager pour arrêter les pilotes », page 88](#)

13.2.1 Utilisation de Designer pour arrêter les pilotes

- 1 Sélectionnez l'objet Coffre-fort d'identité  dans 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 Paramétrez les pilotes sur un démarrage manuel pour vous assurer que les pilotes ne démarrent pas tant que la procédure de mise à niveau ne s'est pas achevée.
 - 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.

13.2.2 Utilisation d'iManager pour arrêter les pilotes

- 1 Dans iManager, sélectionnez *Identity Manager > Présentation d'Identity Manager*.
- 2 Naviguez jusqu'à l'emplacement de l'arborescence dans lequel rechercher les objets Ensemble des pilotes et sélectionnez-le, puis cliquez sur l'icône de recherche .
- 3 Cliquez sur l'objet Ensemble des pilotes.
- 4 Cliquez sur *Pilotes > Arrêter tous les pilotes*.
- 5 Répétez la procédure de l'**Étape 2** à l'**Étape 4** pour chaque objet Ensemble des pilotes.
- 6 Paramétrez les pilotes sur un démarrage manuel pour vous assurer que les pilotes ne démarrent pas tant que la procédure de mise à niveau ne s'est pas achevée.
 - 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.

13.3 Ajout de fichiers à l'emplacement correct sur les plates-formes Linux/UNIX

Lors d'une mise à niveau directe d'eDirectory 8.7.3 vers eDirectory 8.8.5, l'installation place les fichiers d'eDirectory à des emplacements distincts. Identity Manager étant installé, eDirectory ne démarre pas, sauf s'il existe des fichiers Identity Manager spécifiques. La procédure suivante permet de placer les fichiers au bon endroit :

- 1 Une fois la mise à niveau d'eDirectory vers la version 8.8.5 terminée, exécutez l'installation d'Identity Manager avec la commande suivante :

```
./install.bin -i console -DCLUSTER_INSTALL=true
```

Les bons fichiers sont ajoutés sans authentification vers eDirectory.

2 Saisissez `ndsconfig upgrade` pour mettre les fichiers eDirectory à niveau.

3 Vérifiez que l'entrée suivante est bien présente dans le fichier `nds.conf` :

```
n4u.server.interfaces=<adresse ip>@<port>
```

Par exemple : `n4u.server.interfaces=<adresse ip>@524`

Si l'entrée `n4u.server.interfaces` n'existe pas, vous devez la définir manuellement. Pour définir `n4u.server.interfaces`, procédez de la façon suivante :

1. Exécutez la commande suivante pour trouver le port *ncp* :

```
ndsconfig get "n4u.server.interfaces"
```

Cette commande renvoie le numéro du port *ncp*, par exemple,

```
n4u.server.interfaces=@524
```

2. Exécutez la commande suivante pour définir `ndsconfig` pour

```
n4u.server.interfaces :
```

```
ndsconfig set n4u.server.interfaces=<adresse ip>@<port>
```

Où

<adresse ip> est l'adresse ip de la machine sur laquelle réside eDirectory.

<port> est le numéro de port *ncp* obtenu à l'étape 1.

Par exemple :

```
ndsconfig set n4u.server.interfaces=<adresse ip>@524
```

4 Passez à la [Section 13.5, « Mise à niveau du moteur méta-annuaire et des fichiers de configuration des pilotes »](#), page 89.

13.4 Mise à niveau de Designer

Avant de mettre Designer à niveau, vérifiez de bien exporter vos projets afin d'en générer une sauvegarde. Pour connaître les instructions d'exportation de votre projet, reportez-vous à « [Exportation d'un projet](#) » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*. Pour plus d'informations sur la mise à niveau, reportez-vous à « [Conversion de projets précédents](#) » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.

13.5 Mise à niveau du moteur méta-annuaire et des fichiers de configuration des pilotes

Une fois les composants de prise en charge mis à niveau, c'est le moteur méta-annuaire qui est mis à niveau. Lors de la procédure de mise à niveau, les fichiers de configuration du 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 13.2, « Arrêt des pilotes »](#), page 87.

2 Installez Identity Manager 3.6.1.

Les étapes de mise à niveau vers Identity Manager 3.6.1 sont les mêmes que celles de l'installation d'Identity Manager 3.6.1. Reportez-vous au [Chapitre 7, « Installation d'Identity Manager »](#), page 57 pour connaître les instructions d'installation d'Identity Manager.

L'installation d'Identity Manager 3.6.1 écrase les versions précédentes d'Identity Manager, en mettant à jour les binaires, en étendant le schéma et en mettant à jour les fichiers de configuration des pilotes.

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

13.6 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\remoteloadername-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 13.2, « Arrêt des pilotes »](#), page 87.
- 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 7.3, « Installation du chargeur distant »](#), page 61.
- 5 Une fois l'installation terminée, vérifiez que vos fichiers de configuration contiennent bien les informations de votre environnement.
- 6 (Facultatif) Si vous rencontrez un problème avec le fichier de configuration, copiez le fichier de secours 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 de 32 bits vers 64 bits, le pilote GroupWise et les pilotes personnalisés natifs ne fonctionnent plus.

13.7 Superposition du nouveau fichier de configuration du pilote sur le pilote existant

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 13.7.1, « Utilisation d'iManager pour superposer le nouveau fichier de configuration de pilote sur le pilote existant », page 91](#)
- ♦ [Section 13.7.2, « Utilisation d'iManager pour superposer le nouveau fichier de configuration de pilote sur le pilote existant », page 91](#)

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


- 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.

L'avertissement vous informe que tous vos paramètres et toutes vos stratégies de pilotes sont réinitialisés.

Important : vérifiez que vos stratégies personnalisées disposent de noms différents de ceux des stratégies par défaut, de manière à ne perdre aucune donnée.

- 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 13.8, « Restauration de stratégies et de règles personnalisées pour le pilote », page 92](#). Sinon, passez à la [Section 13.10, « Lancement des pilotes », page 94](#).

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

- 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*.

Important : vérifiez que vos stratégies personnalisées disposent de noms différents de ceux des stratégies par défaut, de manière à ne perdre aucune donnée.

- 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 13.8, « Restauration de stratégies et de règles personnalisées pour le pilote », page 92](#). Sinon, passez à la [Section 13.10, « Lancement des pilotes », page 94](#).

13.8 Restauration de stratégies et de règles personnalisées pour le pilote

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


- ♦ [Section 13.8.1, « Utilisation de Designer pour restaurer les stratégies et les règles personnalisées sur le pilote », page 92](#)
- ♦ [Section 13.8.2, « Utilisation d'iManager pour restaurer les stratégies et les règles personnalisées sur le pilote », page 93](#)

13.8.1 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 92](#)
- ♦ [« Ajout d'une stratégie personnalisée via la vue Afficher le flux de stratégie » page 93](#)

Ajout d'une stratégie personnalisée via la vue Aperçu


- 1 Dans la vue *Aperçu*, choisissez le pilote mis à niveau pour afficher la vue *Ensemble de stratégies*.
- 2 Cliquez avec le bouton droit de la souris sur l'icône de l'ensemble de stratégie  là où vous devez restaurer la stratégie personnalisée sur le pilote, puis choisissez *Nouveau > À partir de la copie*.

- 3 Naviguez jusqu'à la stratégie personnalisée, puis sélectionnez-la et cliquez sur *OK*.
- 4 Indiquez le nom de la stratégie personnalisée, puis cliquez sur *OK*.
- 5 Cliquez sur *Oui* dans le message de conflit de fichier pour enregistrer votre projet.
- 6 Lorsque le Générateur de stratégies ouvre la stratégie, vérifiez que les informations sont correctes dans la stratégie copiée.
- 7 Répétez la procédure de l'**Étape 2** à l'**Étape 6** pour chaque stratégie personnalisée à restaurer pour le pilote.
- 8 Lancez le pilote et testez-le.
Pour plus d'informations sur le lancement du pilote, reportez-vous à la [Section 13.10, « Lancement des pilotes », page 94](#). Pour plus d'informations sur le test du pilote, reportez-vous à « [Testing Policies with Policy Simulator \(Test des stratégies avec le simulateur de stratégies\)](#) » dans *Policies in Designer 3.0 (Stratégies dans Designer 3.0)*.
- 9 Une fois que vous avez vérifié que les stratégies fonctionnent, déplacez le pilote vers l'environnement de production.

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

- 1 Dans la vue *Aperçu*, sélectionnez le pilote mis à niveau, puis cliquez sur l'icône *Afficher le flux de stratégie* .
- 2 Cliquez avec le bouton droit de la souris sur l'ensemble de stratégies dans lequel vous devez restaurer la stratégie personnalisée sur le pilote, puis choisissez *Ajouter une stratégie > Copier existant*.
- 3 Naviguez jusqu'à la stratégie personnalisée, puis sélectionnez-la et cliquez sur *OK*.
- 4 Indiquez le nom de la stratégie personnalisée, puis cliquez sur *OK*.
- 5 Cliquez sur *Oui* dans le message de conflit de fichier pour enregistrer votre projet.
- 6 Lorsque le Générateur de stratégies ouvre la stratégie, vérifiez que les informations sont correctes dans la stratégie copiée.
- 7 Répétez la procédure de l'**Étape 2** à l'**Étape 6** pour chaque stratégie personnalisée à restaurer pour le pilote.
- 8 Lancez le pilote et testez-le.
Pour plus d'informations sur le lancement du pilote, reportez-vous à la [Section 13.10, « Lancement des pilotes », page 94](#). Pour plus d'informations sur le test du pilote, reportez-vous à « [Testing Policies with Policy Simulator \(Test des stratégies avec le simulateur de stratégies\)](#) » dans *Policies in Designer 3.0 (Stratégies dans Designer 3.0)*.
- 9 Une fois que vous avez vérifié que les stratégies fonctionnent, déplacez le pilote vers l'environnement de production.

13.8.2 Utilisation d'iManager pour restaurer les stratégies et les règles personnalisées sur le 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 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 13.10**, « **Lancement des pilotes** », page 94. Il n'existe pas de simulateur de stratégie dans iManager. Pour tester les stratégies, faites intervenir des événements qui les exécutent. Vous pouvez, par exemple, créer un utilisateur, le modifier ou le supprimer.
- 10 Une fois que vous avez vérifié que les stratégies fonctionnent, déplacez le pilote vers l'environnement de production.

13.9 Déploiement du projet converti




Déployez le projet Designer converti dans le coffre-fort d'identité. Pour plus d'informations, reportez-vous à « **Déploiement et exportation** » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.

13.10 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 13.10.1**, « **Utilisation de Designer pour lancer les pilotes** », page 94
- ♦ **Section 13.10.2**, « **Utilisation d'iManager pour démarrer les pilotes** », page 95

13.10.1 Utilisation de Designer pour lancer les pilotes

- 1 Sélectionnez l'objet Coffre-fort d'identité  dans l'onglet *Aperçu*.
- 2 Cliquez sur l'icône *Démarrer tous les pilotes*  dans la barre d'outils Modeler. Ceci lance tous les pilotes du projet.
- 3 Définissez les options de démarrage des pilotes.
 - 3a Double-cliquez sur l'icône du pilote  dans l'onglet *Aperçu*.
 - 3b Sélectionnez *Configuration du pilote* > *Option de démarrage*.

- 3c** Sélectionnez *Démarrage auto* ou choisissez votre méthode préférée pour lancer le pilote, puis cliquez sur *OK*.
- 3d** Répétez la procédure de l'**Étape 3a** à l'**Étape 3c** pour chaque pilote.
- 4** Testez les pilotes pour vérifier que les stratégies fonctionnent comme prévu. Pour plus d'informations sur la manière de tester vos stratégies, reportez-vous à « **Testing Policies with Policy Simulator (Test des stratégies avec le simulateur de stratégies)** » dans *Policies in Designer 3.0 (Stratégies dans Designer 3.0)*.

13.10.2 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 directe et une migration. Reportez-vous au [Chapitre 12, « Mise à niveau directe \(in-place\) et migration »](#), page 81.


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.

- ❑ 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 13.1, « Création d'une sauvegarde de la configuration actuelle »](#), page 85.
- ❑ 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 47.
- ❑ Installez eDirectory™ 8.8.5 sur le serveur. Pour plus d'informations, reportez-vous au [Guide d'installation d'eDirectory \(http://www.novell.com/documentation/edir88/index.html\)](#).
- ❑ 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 [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 3.6.1. Reportez-vous au [Chapitre 4, « Liste de vérification pour un système Identity Manager de base »](#), page 41 pour vérifier que toutes les étapes sont terminées.
- ❑ 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 13.6, « Mise à niveau du chargeur distant »](#), page 90.
- ❑ (Facultatif) Si l'ancien 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 [Guide de migration d'un module de provisioning basé sur les rôles \(http://www.novell.com/documentation/idmrpbm361/index.html\)](#).
 - ❑ Créez un nouveau pilote de service de rôle . Les pilotes de service de rôle ne sont pas migrés. Si vous avez un pilote de service de rôle pour la version 3.6.1, vous devez créer un nouveau pilote pour la version 3.6.1. Pour plus d'informations, reportez-vous au [Guide de migration d'un module de provisioning basé sur les rôles \(http://www.novell.com/documentation/idmrpbm361/index.html\)](#).
 - ❑ Déployez le pilote de l'application utilisateur migré dans le coffre-fort d'identité. Pour plus d'informations, reportez-vous au [Guide de migration d'un module de provisioning basé sur les rôles \(http://www.novell.com/documentation/idmrpbm361/index.html\)](#).
 - ❑ Installez l'application utilisateur sur ce nouveau serveur. Pour plus d'informations, reportez-vous au [Guide d'installation d'un module de provisioning basé sur les rôles \(http://www.novell.com/documentation/idmrpbm361/install/data/bookinfo.html\)](#).

- ❑ Ajoutez le nouveau serveur à l'ensemble de pilotes. Pour plus d'informations, reportez-vous à la [Section 14.1, « Ajout du nouveau serveur à l'ensemble de pilotes », page 98](#).
- ❑ Modifiez les informations spécifiques du serveur pour chaque pilote. Pour plus d'informations, reportez-vous à la [Section 14.2, « Modification des informations spécifiques du serveur », page 99](#).
- ❑ (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 [Référence de la configuration de l'application utilisateur \(<http://www.novell.com/documentation/idmrpbm361/install/data/bb1zmw0.html>\)](#) dans le *Guide d'installation d'un module de provisioning basé sur les rôles* (<http://www.novell.com/documentation/idmrpbm361/install/data/bookinfo.html>).
- ❑ (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 13.7, « Superposition du nouveau fichier de configuration du pilote sur le pilote existant », page 91](#).
- ❑ (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 13.8, « Restauration de stratégies et de règles personnalisées pour le pilote », page 92](#).
- ❑ Supprimez l'ancien serveur de l'ensemble de pilotes. Pour plus d'informations, reportez-vous à la [Section 14.3, « Suppression de l'ancien serveur de l'ensemble de pilotes », page 100](#).
- ❑ Si vous utilisez Novell Sentinel™, vous devez effectuer la 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).
- ❑ Activez le moteur méta-annuaire et tout pilote mis à niveau. Pour plus d'informations, reportez-vous au [Chapitre 8, « Activation des produits Novell Identity Manager », page 69](#).

14.1 Ajout du nouveau serveur à l'ensemble de pilotes

Si vous utilisez iManager, vous devez ajouter le nouveau serveur à l'ensemble de pilotes. Designer contient un assistant de migration de serveur qui accomplit cette tâche pour vous. Si vous utilisez Designer, ignorez cette étape et allez à la [Section 14.2, « Modification des informations spécifiques du serveur », page 99](#). 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 Naviguez jusqu'au nouveau serveur Identity Manager 3.6.1 et sélectionnez-le, puis cliquez sur *OK*.

14.2 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

Cela peut être fait dans Designer ou dans iManager. Si vous utilisez Designer, le processus est automatisé. Si vous utilisez iManager, le processus est manuel.

- ♦ [Section 14.2.1, « Modification des informations spécifiques du serveur dans Designer. », page 99](#)
- ♦ [Section 14.2.2, « Modification des informations spécifiques du serveur dans iManager », page 100](#)

14.2.1 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 informations sont écrites dans deux files d'attente, ce qui peut provoquer des altérations.
- 6 Cliquez sur *Migrer*.

Après la migration des informations spécifiques du serveur, vous devez déployer les pilotes modifiés vers le coffre-fort d'identité. Pour plus d'informations, reportez-vous à « [Déploiement d'un pilote vers un coffre-fort d'identité](#) » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.

La dernière étape consiste à démarrer les pilotes. Pour plus d'informations, reportez-vous à la [Section 13.10, « Lancement des pilotes », page 94](#).

14.2.2 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 Vous devez modifier chaque paramètre de pilote, valeur de configuration globale, valeur de contrôle de moteur, mot de passe nommé, information d'authentification de pilote et options de démarrage de pilote qui contiennent les informations de l'ancien serveur en fonction de celles du nouveau 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.

14.3 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 14.3.1, « Utilisation de Designer pour retirer l'ancien serveur de l'ensemble de pilotes », page 100](#)
- ♦ [Section 14.3.2, « Utilisation d'iManager pour retirer l'ancien serveur de l'ensemble de pilotes », page 101](#)
- ♦ [Section 14.3.3, « Déclassement de l'ancien serveur », page 101](#)


14.3.1 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.

Cette modification doit être déployée vers le coffre-fort d'identité. Pour plus d'informations, reportez-vous à « **Déploiement d'un pilote vers un coffre-fort d'identité** » dans le *Guide d'administration de Designer 3.0.1 pour Identity Manager 3.6*.

14.3.2 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*.

14.3.3 Déclassement de l'ancien serveur

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

- 1 Supprimez les répliques d'eDirectory de ce serveur. Pour plus d'informations, reportez-vous à [Suppression de répliques \(http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html\)](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)*.
- 2 Supprimez eDirectory de ce serveur. Pour plus d'informations, reportez-vous à [TID 10056593, Removing a Server From an NDS Tree Permanently \(Suppression définitive d'un serveur dans une arborescence NDS\) \(http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=10056593&sliceId=&docTypeID=DT_TID_1_1&dialogID=35218849&stateId=0%20%2035214815\)](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

Si vous devez désinstaller Identity Manager, procédez dans l'ordre, tel qu'indiqué dans les sections suivantes.

- ♦ [Chapitre 15, « Suppression d'objets dans eDirectory », page 105](#)
- ♦ [Chapitre 16, « Désinstallation du serveur et des pilotes méta-annuaire », page 107](#)
- ♦ [Chapitre 17, « Désinstallation de Designer », page 109](#)

Suppression d'objets dans eDirectory

15

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 des pilotes sont des objets racine de partition dans eDirectory™, la partition doit être fusionnée à la partition parent avant que l'objet Ensemble des pilotes ne puisse être supprimé. Lorsque l'ensemble des pilotes est créé, l'assistant vous invite à faire une partition de l'ensemble des pilotes.

Effacez les objets Identity Manager :

- 1** Contrôlez l'état de santé sur la base de données eDirectory. En cas d'erreurs, résolvez-les avant de continuer. Pour plus d'informations, reportez-vous à [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>) dans le *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.

Passez au [Chapitre 16, « Désinstallation du serveur et des pilotes méta-annuaire », page 107](#).

Désinstallation du serveur et des pilotes méta-annuaire

16

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 16.1, « Désinstallation sous Windows », page 107](#)
- ♦ [Section 16.2, « Désinstallation sous Linux/UNIX », page 107](#)

16.1 Désinstallation sous Windows

Pour désinstaller Identity Manager sous Windows :

- ♦ Pour Windows 32 bits, procédez de l'une des manières suivantes :
 - ♦ Accédez au Panneau de configuration sur le serveur Windows. Sous Windows Server 2003, cliquez sur *Ajouter ou supprimer des programmes*. Sous Windows Server 2008, cliquez sur *Programmes et fonctions*.

Remarque : cette méthode ne concerne pas Windows Server 2008 Server Core.

- ♦ Exécutez le script de désinstallation (`Uninstall Identity Manager.exe`) situé dans `C:\Program Files\Novell\Identity Manager\Uninstall_Identity_Manager`.
- ♦ Pour Windows 64 bits, procédez de l'une des manières suivantes :
 - ♦ Accédez au Panneau de configuration sur le serveur Windows. Sous Windows Server 2003, cliquez sur *Ajouter ou supprimer des programmes*. Sous Windows Server 2008, cliquez sur *Programmes et fonctions*.

Remarque : cette méthode ne concerne pas Windows Server 2008 Server Core.

- ♦ Exécutez le script de désinstallation (`Uninstall Identity Manager.exe`) situé dans `C:\Program Files (x86)\Novell\Identity Manager\Uninstall_Identity_Manager`.

16.2 Désinstallation sous Linux/UNIX

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

Désinstallation de Designer

17

La désinstallation de Designer est très semblable à celle du serveur et du pilote méta-annuaire.

- ♦ Sous Windows, sélectionnez *Ajout/Suppression de programmes* dans le Panneau de configuration.
- ♦ Pour Linux/UNIX, exécutez le script de désinstallation situé à `~/designer/UninstallDesigner/Uninstall_Designer_for_Identity_Manager`.

