Guide d'installation

Novell®
Identity Manager

4.0.1

15 avril 2011

www.novell.com

Mentions légales

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

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

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

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).

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).

Éléments tiers

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

Table des matières

À propos de ce guide 7

Partie I Planification 9

1 Mise en place d'un environnement de développement 11

2 Création d'un plan de projet 13

2.1 Phase de découverte . . . 13
2.1.1 Définition des processus d'entreprise actuels . . . 14
2.1.2 Définition de l'action de la solution Identity Manager sur les processus d'entreprise actuels . . . 15
2.1.3 Identification des principales parties prenantes professionnelles et techniques . . . 16
2.1.4 Interrogation de toutes les parties prenantes . . . 16
2.1.5 Création d'une stratégie de haut niveau et d'un chemin d'exécution conforme . . . 17
2.2 Phase d'analyse des besoins et de la conception . . . 17
2.2.1 Définition des besoins de votre entreprise . . . 18
2.2.2 Analyse de vos processus d'entreprise . . . 20
2.2.3 Conception d'un modèle de données d'entreprise . . . 20
2.3 Démonstration de faisabilité . . . 22
2.4 Validation et préparation des données . . . 22
2.5 Pilote de production . . . 23
2.6 Planification du déploiement vers la production . . . 23
2.7 Déploiement vers la production . . . 23

3 Directives techniques 25

3.1 Instructions pour les outils de gestion . . . 26
3.1.1 Instructions pour Analyzer . . . 27
3.1.2 Instructions pour Designer . . . 27
3.1.3 Instructions pour iManager . . . 27
3.1.4 Instructions pour l'administrateur d'assignation de rôles . . . 27
3.2 Instructions pour le serveur méta-annuaire . . . 28
3.3 Instructions pour eDirectory . . . 29
3.3.1 Objets Identity Manager dans eDirectory . . . 29
3.3.2 Réplication des objets nécessaires à Identity Manager sur le serveur . . . 30
3.3.3 Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents . . . 31
3.4 Application utilisateur . . . 34
3.5 Instructions pour l'audit et la création de rapport . . . 34

Partie II Installation 37

4 Liste de vérification pour un système Identity Manager de base 39

4.1 Conditions préalables . . . 40
4.2 Planification . . . 40
4.3 Installation . . . 40

4.4 Configuration du pilote avec le chargeur distant 41
4.5 Configuration de pilotes sans chargeur distant 41
4.6 Configuration supplémentaire 42

5 Où se procurer Identity Manager 43

6 Configuration système requise 47

6.1 eDirectory et iManager 48
6.2 Serveur méta-annuaire 49
6.2.1 Processeurs pris en charge 50
6.2.2 Systèmes d'exploitation du serveur 50
6.3 Chargeur distant 51
6.4 Application utilisateur 54
6.5 Audit et création de rapports 54
6.6 Postes de travail 55
6.6.1 Plates-formes des postes de travail 56
6.6.2 Navigateurs Web 57
6.7 Ressources requises 57

7 Installation d'Identity Manager 59

7.1 Installation d'Analyzer 59
7.2 Installation de Designer 60
7.3 Installation d'eDirectory 61
7.4 Installation d'iManager 61
7.5 Installation du serveur méta-annuaire 62
7.5.1 Installation non-root du serveur méta-annuaire 63
7.5.2 Installation en mode silencieux du serveur méta-annuaire 65
7.6 Installation du chargeur distant 66
7.6.1 Configuration requise 66
7.6.2 Pilotes pris en charge 66
7.6.3 Procédure d'installation 67
7.6.4 Installation silencieuse du chargeur distant 69
7.6.5 Installation du chargeur distant Java sous UNIX ou Linux 70
7.6.6 Coexistence de chargeurs distants 32 et 64 bits 71
7.7 Installation des fichiers de pilote 71
7.8 Installation du module de provisioning basé sur les rôles 72
7.9 Installation d'un pilote personnalisé 72
7.10 Installation de l'administrateur de l'assignation de rôles 73
7.11 Installation du module Identity Reporting ou de Sentinel 74

8 Activation des produits Novell Identity Manager 75

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

9 Dépannage d'Identity Manager 79

10 Nouveautés 85

10.1 Nouveautés d'Identity Manager 4.0.1 . . . 85
10.1.1 Identity Manager Advanced Edition et Standard Edition . . . 85
10.1.2 Télémétrie . . . 85
10.1.3 Activité de requête de ressource . . . 85
10.1.4 Nouveaux rapports ajoutés au module Identity Reporting . . . 86
10.1.5 Applications ajoutées à la palette de Designer . . . 86
10.2 Nouveautés d'Identity Manager 4.0 . . . 86
10.2.1 Module Identity Reporting . . . 86
10.2.2 Nouveaux pilotes . . . 87
10.2.3 Prise en charge de l'audit XDAS . . . 87
10.2.4 Remplacement des fichiers de configuration de pilote par des paquetages . . . 88
10.2.5 Administrateur d'assignation de rôles . . . 88
10.2.6 Analyzer . . . 88
10.2.7 Programme d'installation intégré . . . 88

Partie III Mise à niveau d'Identity Manager 89

11 Mise à niveau et migration 91

Partie IV Désinstallation d'Identity Manager 93

12 Désinstallation des composants d'Identity Manager 95

12.1 Suppression d'objets dans eDirectory . . . 95
12.2 Désinstallation du serveur méta-annuaire . . . 96
12.2.1 Désinstallation sous Linux/UNIX . . . 96
12.2.2 Désinstallation sous Windows . . . 96
12.2.3 Suppression d'une installation non-root . . . 96
12.3 Désinstallation du chargeur distant . . . 96
12.3.1 Désinstallation sous Linux/UNIX . . . 97
12.3.2 Désinstallation sous Windows . . . 97
12.4 Désinstallation du module de provisioning basé sur les rôles . . . 97
12.4.1 Suppression des pilotes . . . 97
12.4.2 Désinstallation de l'application utilisateur . . . 97
12.4.3 Désinstallation du serveur d'applications et de la base de données . . . 98
12.5 Désinstallation des composants du module Identity Reporting . . . 99
12.5.1 Suppression des pilotes de création de rapports . . . 99
12.5.2 Désinstallation du module Identity Reporting . . . 99
12.5.3 Désinstallation du service d'audit d'événements . . . 99
12.6 Désinstallation d'iManager . . . 100
12.7 Désinstallation d'eDirectory . . . 100
12.8 Désinstallation d'Analyzer . . . 101
12.9 Désinstallation de Designer . . . 101
12.10 Désinstallation de l'administrateur d'assignation de rôles . . . 102

À propos de ce guide

Novell Identity Manager est un service de partage et de synchronisation de données qui permet à des applications, annuaires et bases de données de partager des informations. Il relie des informations dispersées et permet d'établir des stratégies qui régiront les mises à jour automatiques de certains systèmes en cas de changement d'identités. Identity Manager est à la base du provisioning des comptes, de la sécurité, du Single Sign-on, du self-service utilisateur, de l'authentification, des autorisations, des workflows automatisés et des services Web. Il permet d'intégrer, de gérer et de contrôler vos informations d'identité distribuées, de manière à proposer les bonnes ressources aux bonnes personnes.

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

- Partie I, « Planification », page 9
  - Chapitre 1, « Mise en place d'un environnement de développement », page 11
  - Chapitre 2, « Création d'un plan de projet », page 13
  - Chapitre 3, « Directives techniques », page 25
- Partie II, « Installation », page 37
  - Chapitre 4, « Liste de vérification pour un système Identity Manager de base », page 39
  - Chapitre 5, « Où se procurer Identity Manager », page 43
  - Chapitre 6, « Configuration système requise », page 47
  - Chapitre 7, « Installation d'Identity Manager », page 59
  - Chapitre 8, « Activation des produits Novell Identity Manager », page 75
  - Chapitre 9, « Dépannage d'Identity Manager », page 79
  - Chapitre 10, « Nouveautés », page 85
- Partie III, « Mise à niveau d'Identity Manager », page 89
  - Chapitre 11, « Mise à niveau et migration », page 91
- Partie IV, « Désinstallation d'Identity Manager », page 93

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/idm401/index.html).

Documentation complémentaire

Pour obtenir de la documentation supplémentaire sur les pilotes Identity Manager, reportez-vous au site Web de documentation des pilotes Identity Manager (http://www.novell.com/documentation/idm401drivers/index.html).

Pour obtenir la documentation relative à l'application utilisateur, reportez-vous au site Web de documentation du module de provisioning basé sur les rôles Identity Manager (http://www.novell.com/documentation/idmrbpm401/index.html).

Planification

Identity Manager 4.0.1 vous aide à gérer les identités et les ressources de votre entreprise. Il automatise également de nombreux processus d'entreprise qui sont actuellement exécutés manuellement.

Si vous avez des questions concernant les différents composants d'une solution Identity Manager, reportez-vous au guide *Présentation d'Identity Manager 4.0.1*, qui fournit des informations détaillées sur chaque composant.

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

Si vous créez une solution Identity Manager dont tous les composants résident sur le même serveur, reportez-vous au *Guide du programme d'installation intégré d'Identity Manager 4.0.1* pour vous aider à l'installer. Il s'agit d'un programme d'installation simplifié qui vous permet de configurer votre système plus rapidement.

Il est vivement recommandé d'engager un expert Identity Manager pour vous aider dans chaque phase de la mise en œuvre de votre solution. Pour plus d'informations sur les options de partenariat, accédez au site Web Novell Solution Partner (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 11
- Chapitre 2, « Création d'un plan de projet », page 13
- Chapitre 3, « Directives techniques », page 25

Mise en place d'un environnement de développement

1

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

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

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

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

L'outil le plus important à utiliser pour développer votre solution Identity Manager s'intitule Designer. Il permet de recueillir toutes les informations concernant votre environnement, puis de les exploiter pour créer une solution Identity Manager adaptée à vos besoins. Utilisez Designer au cours des différentes phases de la planification, afin de recueillir toutes les informations. Designer simplifie la création d'un plan de projet contenant les informations d'entreprise et les données techniques. Pour en savoir plus sur Designer, reportez-vous au manuel *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

Pour configurer votre environnement de développement, retrouvez les informations dans le Chapitre 4, « Liste de vérification pour un système Identity Manager de base », page 39. Il s'agit d'une liste de vérifications de tous les composants d'Identity Manager. Elle vous permet de vous assurer que vous avez installé et configuré tous les composants d'Identity Manager que vous pouvez utiliser pour développer un plan de projet. Utilisez les informations fournies au Chapitre 3, « Directives techniques », page 25 pour configurer votre environnement de développement et vous documenter sur les aspects techniques à prendre en compte au moment d'installer et de configurer chaque composant d'Identity Manager.

Une fois votre environnement de développement créé, vous pouvez générer le plan de projet afin de mettre en place la solution Identity Manager. Créez le plan du projet à l'aide des informations présentes dans le Chapitre 2, « Création d'un plan de projet », page 13.

Création d'un plan de projet

2

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

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

- Section 2.1, « Phase de découverte », page 13
- Section 2.2, « Phase d'analyse des besoins et de la conception », page 17
- Section 2.3, « Démonstration de faisabilité », page 22
- Section 2.4, « Validation et préparation des données », page 22
- Section 2.5, « Pilote de production », page 23
- Section 2.6, « Planification du déploiement vers la production », page 23
- Section 2.7, « Déploiement vers la production », page 23

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 14
- Section 2.1.2, « Définition de l'action de la solution Identity Manager sur les processus d'entreprise actuels », page 15
- Section 2.1.3, « Identification des principales parties prenantes professionnelles et techniques », page 16

- Section 2.1.4, « Interrogation de toutes les parties prenantes », page 16
- Section 2.1.5, « Création d'une stratégie de haut niveau et d'un chemin d'exécution conforme », page 17

2.1.1 Définition des processus d'entreprise actuels

Identity Manager automatise les processus d'entreprise, afin de gérer aisément les identités de votre environnement. Vous ne pourrez pas concevoir de solution Identity Manager qui automatise ces processus si vous ne connaissez pas les processus d'entreprise actuels. Vous pouvez profiter du mode Architecture de Designer pour recueillir vos processus d'entreprise actuels et les afficher sous forme graphique. Pour plus d'informations, reportez-vous à la section « Architect Mode » (Mode architecte) du manuel *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

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

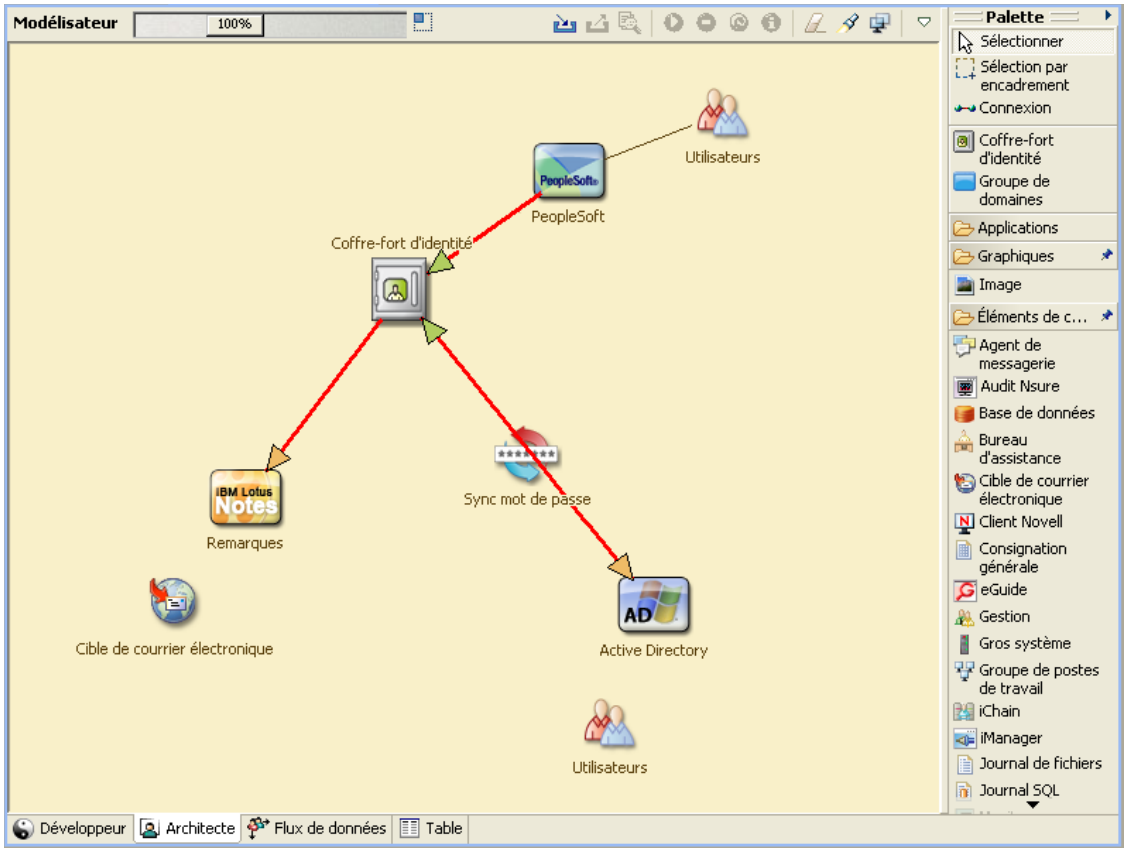
- Lorsqu'un employé est renvoyé, son compte utilisateur dans le système de messagerie est supprimé. Toutefois, dans tous les autres systèmes, il est désactivé et non supprimé.
- Le format d'une adresse de courrier électronique d'un utilisateur.
- Les systèmes ou ressources accessibles aux commerciaux.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

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

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

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

Figure 2-1 *Exemples de processus d'entreprise*



Une fois les processus déterminés, vous devez définir les modalités de mise en œuvre d'Identity Manager. Passez à la Section 2.1.2, « Définition de l'action de la solution Identity Manager sur les processus d'entreprise actuels », page 15.

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

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

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

Créez une liste des processus d'entreprise à automatiser en priorité, puis identifiez les systèmes qui seront affectés par ces changements. Passez ensuite à la Section 2.1.3, « Identification des principales parties prenantes professionnelles et techniques », page 16.

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 connaisssance et la compréhension de tous les aspects professionnels et techniques des processus de l'entreprise. Vous devez identifier les services et les systèmes qui seront touchés par la solution Identity Manager, mais aussi la personne en charge de chacun.

Par exemple, si vous intégrez dans votre solution un système de messagerie électronique, vous devez lister le système de messagerie, son administrateur et ses coordonnées. Vous pouvez ajouter toutes ces informations dans le projet Designer. À chaque icône d'application correspond un espace où il est possible d'enregistrer les informations sur le système et son administrateur. Pour plus d'informations, reportez-vous à la section « Configuring Application Properties » (Configuration des propriétés d'application) du manuel *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

Lorsque vous avez identifié toutes les personnes impliquées dans chaque procédure d'activité, vous pouvez passer à l'étape suivante qui se trouve à la Section 2.1.4, « Interrogation de toutes les parties prenantes », page 16.

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 17.

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

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

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

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

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

Une fois la phase de découverte terminée, passez à la Section 2.2, « Phase d'analyse des besoins et de la conception », page 17.

2.2 Phase d'analyse des besoins et de la conception

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

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

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

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

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

Identity Manager intègre un outil qui vous permet de simplifier le processus d'analyse et de nettoyage de vos données. Pour plus d'informations, reportez-vous au manuel *Analyzer 4.0.1 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 1.2 pour Identity Manager).

Reprenez les informations du Chapitre 3, « Directives techniques », page 25 pour prendre la bonne décision en ce qui concerne votre environnement.

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

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

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

- « Définition des besoins de votre entreprise » page 18
- « Analyse de vos processus d'entreprise » page 20
- « Conception d'un modèle de données d'entreprise » page 20

2.2.1 Définition des besoins de votre entreprise

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

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

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

- Assigner des flux de données entre les applications. Designer vous permet d'afficher ces informations. Pour plus d'informations, reportez-vous à la section « Managing the Flow of Data » (Gestion du flux de données) du manuel *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).
- Identifier les données dont le format doit être modifié (p. ex. remplacement de 25/02/2007 par 25 février 2007), puis utiliser Analyzer pour effectuer les modifications. Pour plus d'informations, reportez-vous au manuel *Analyzer 4.0.1 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 1.2 pour Identity Manager).
- Décrire les dépendances qui existent entre les données.

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

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

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

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

  Vous devez décrire la configuration requise pour la mise en oeuvre d'une phase donnée du déploiement. Cela comprend l'accès aux systèmes connectés qui doivent interagir avec Identity Manager.
- Identifier les sources de données expertes.

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

  Par exemple, l'administrateur de comptes peut vouloir la propriété sur l'octroi des droits d'accès à des fichiers et des répertoires spécifiques pour un employé. Pour cela, vous pouvez mettre en 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, « Analyse de vos processus d'entreprise », page 20.

2.2.2 Analyse de vos processus d'entreprise

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

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

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

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

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

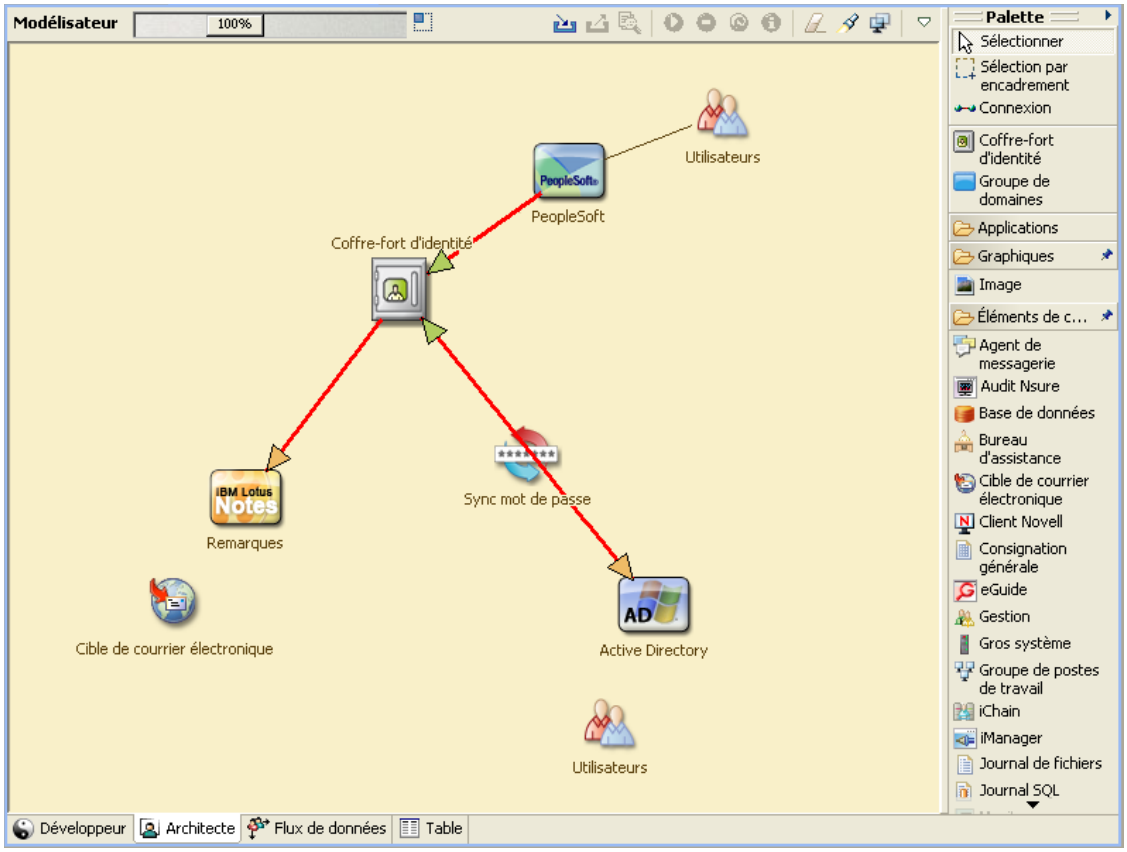
Après avoir rassemblé toutes ces informations, vous pouvez concevoir un modèle de données d'entreprise adapté à votre environnement. Passez à la Section 2.2.3, « Conception d'un modèle de données d'entreprise », page 20 pour démarrer la conception.

2.2.3 Conception d'un modèle de données d'entreprise

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

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

Figure 2-2 *Flux de données dans Designer*



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

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

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

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

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

L'objectif de ce travail est de comprendre chaque système d'annuaire, la manière dont les annuaires sont liés et de connaître les objets et les attributs à synchroniser dans ces systèmes. Une fois la conception achevée, vous pouvez créer une preuve de concept. Passez à la Section 2.3, « Démonstration de faisabilité », page 22.

2.3 Démonstration de faisabilité

Créez et testez votre démonstration de faisabilité en utilisant un exemple de mise en œuvre dans un environnement de laboratoire, afin de refléter le flux de données et la stratégie métier de votre entreprise. La mise en œuvre s'appuie sur le modèle de données développé au cours des phases de conception et d'analyse des besoins, et constitue l'étape finale avant l'introduction du pilote de production. Exécutez les tests dans l'environnement de laboratoire que vous avez créé comme indiqué au Chapitre 1, « Mise en place d'un environnement de développement », page 11.

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

Le Chapitre 3, « Directives techniques », page 25 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 22 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.

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

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

Une fois les données préparées, passez à la Section 2.5, « Pilote de production », page 23.

2.5 Pilote de production

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

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

La solution pilote propose une preuve de conception et une validation en direct pour le modèle de données et les résultats souhaités de la procédure. Une fois que le pilote est terminé, passez à la Section 2.6, « Planification du déploiement vers la production », page 23.

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 23.

2.7 Déploiement vers la production

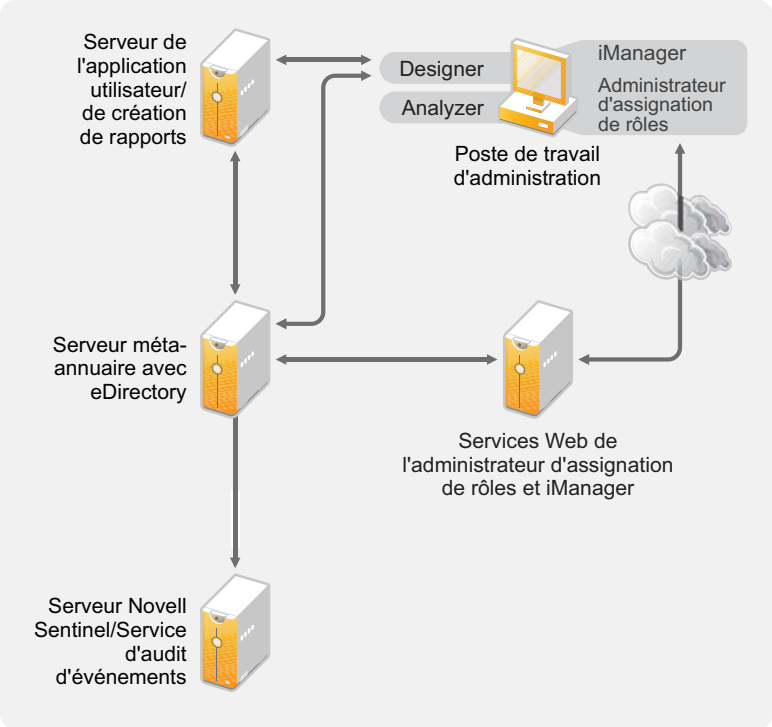
La phase de déploiement en production consiste à mettre à exécution l'ensemble des plans, de manière à créer la solution Identity Manager dans l'environnement réel. Utilisez le plan de déploiement en production pour mettre en place les différents éléments de la solution Identity Manager. En fonction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

Directives techniques

3

Les informations collectées dans Designer permettent de prendre des décisions d'ordre technique, telles que la définition de l'emplacement d'installation et des options de configuration de chaque composant d'Identity Manager. Pour obtenir une présentation de chaque composant, reportez-vous au guide *Présentation d'Identity Manager 4.0.1*. La Figure 3-1 représente une configuration possible d'une solution Identity Manager.

Figure 3-1 *Composants Identity Manager*



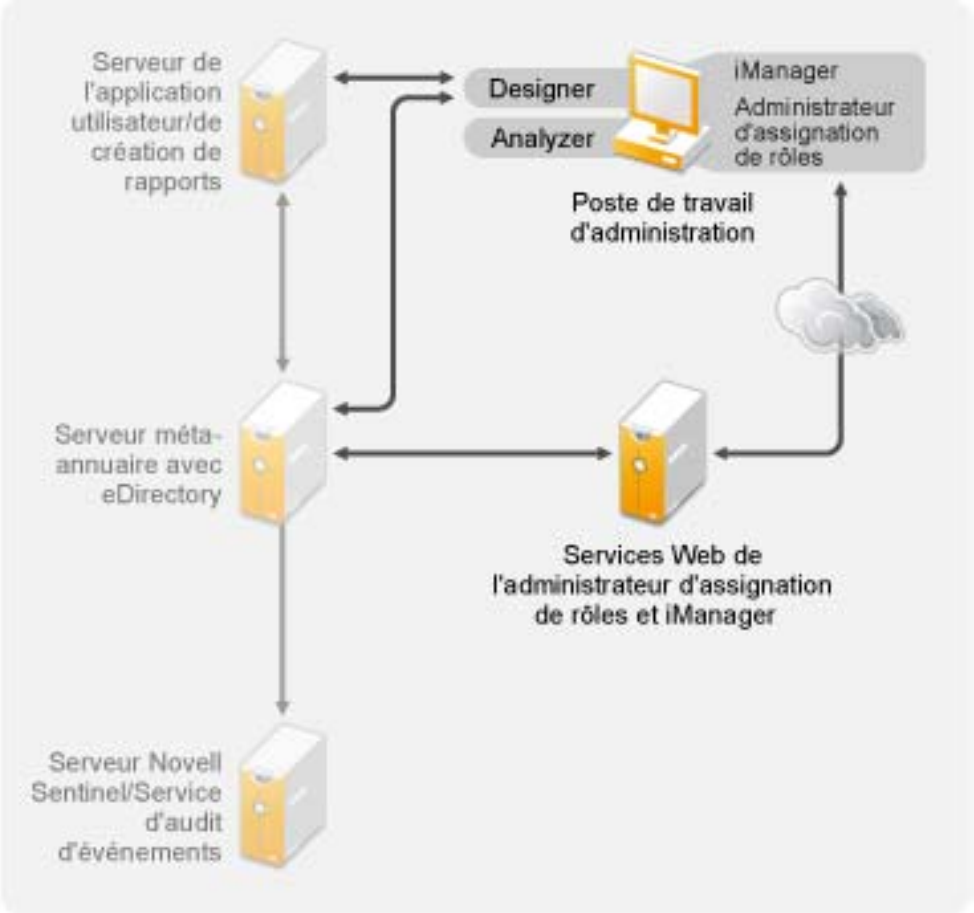
Identity Manager est hautement personnalisable. Les sections suivantes contiennent les bonnes pratiques techniques qui vous aideront à paramétrer et configurer la solution Identity Manager qui conviendra le mieux à votre environnement. L'application de ces instructions à votre environnement est fonction 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 26
- Section 3.2, « Instructions pour le serveur méta-annuaire », page 28
- Section 3.3, « Instructions pour eDirectory », page 29
- Section 3.4, « Application utilisateur », page 34
- Section 3.5, « Instructions pour l'audit et la création de rapport », page 34

3.1 Instructions pour les outils de gestion

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

Figure 3-2 *Outils de gestion Identity Manager*



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

- Section 3.1.1, « Instructions pour Analyzer », page 27
- Section 3.1.2, « Instructions pour Designer », page 27
- Section 3.1.3, « Instructions pour iManager », page 27
- Section 3.1.4, « Instructions pour l'administrateur d'assignation de rôles », page 27

3.1.1 Instructions pour Analyzer

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

Il n'existe pas de considérations particulières concernant l'utilisation d'Analyzer. Pour plus d'informations, reportez-vous au manuel *Analyzer 4.0.1 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 1.2 pour Identity Manager).

3.1.2 Instructions pour Designer

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

Il n'existe pas de considérations particulières concernant l'utilisation de Designer, sauf si plusieurs personnes travaillent sur un même projet. Designer permet le contrôle des versions du projet. Pour plus d'informations, reportez-vous à la section « Version Control » (Contrôle des versions) du manuel *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

3.1.3 Instructions pour iManager

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

Si plus de 10 administrateurs travaillent en continu et simultanément sur iManager, vous devez disposer d'un serveur n'hébergeant que iManager. La Figure 3-2 page 26 montre cette configuration de votre solution Identity Manager. Si vous ne disposez que d'un administrateur, vous pouvez exécuter facilement iManager sur votre serveur méta-annuaire.

3.1.4 Instructions pour l'administrateur d'assignation de rôles

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

Il n'existe pas de considérations particulières concernant l'utilisation de l'administrateur d'assignation de rôles. Vous pouvez l'exécuter sur un serveur distinct, comme le montre la Figure 3-2 page 26, ou sur le serveur méta-annuaire. Pour plus d'informations, reportez-vous au manuel *Identity Manager Role Mapping Administrator 4.0.1 Installation and Configuration Guide* (Guide d'installation et de configuration de la version 4.0.1 de l'administrateur de l'assignation de rôles d'Identity Manager).

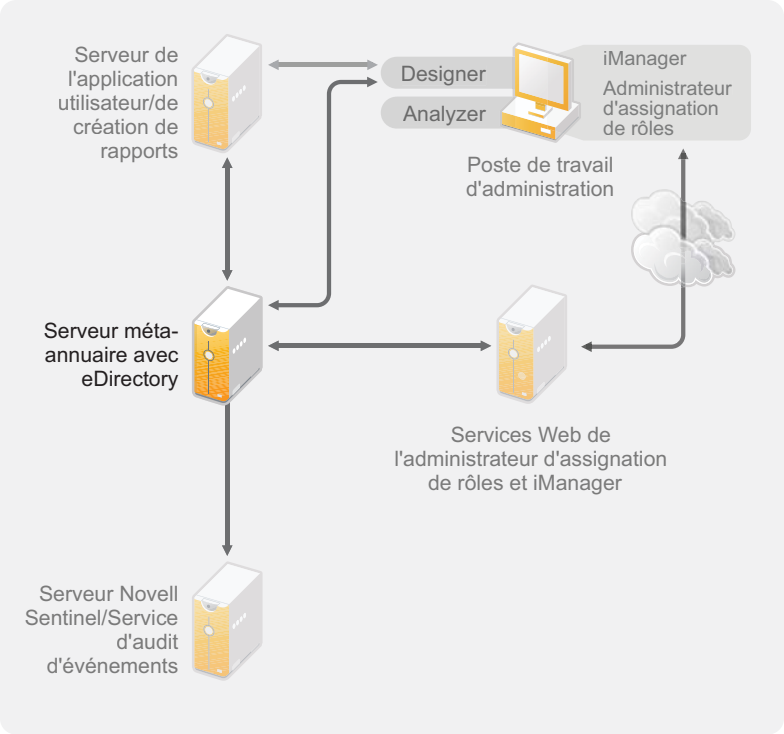
3.2 Instructions pour le serveur méta-annuaire

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

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

Il améliore la flexibilité de votre solution Identity Manager. Pour plus d'informations, reportez-vous au manuel *Identity Manager 4.0.1 Remote Loader Guide* (Guide du chargeur distant d'Identity Manager 4.0).

Figure 3-3 *Serveur méta-annuaire*



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

La configuration de la solution Identity Manager dans un environnement de laboratoire vous permet de tester les futures performances des serveurs. Vous pouvez utiliser les outils de contrôle de l'état de santé dans iManager pour obtenir une ligne de base, puis prendre les meilleures décisions pour votre environnement. Pour plus d'informations sur les outils de contrôle de l'état de santé, reportez-vous à la section « Monitoring Driver Health » (Contrôle de l'état de santé des pilotes) du manuel *Identity Manager 4.0.1 Common Driver Administration Guide* (Guide d'administration des pilotes communs d'Identity Manager 4.0).

Pour des informations sur chaque pilote, reportez-vous au site Web de la documentation des pilotes d'Identity Manager (http://www.novell.com/documentation/idm36drivers/index.html). 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 29
- Section 3.3.2, « Réplication des objets nécessaires à Identity Manager sur le serveur », page 30
- Section 3.3.3, « Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents », page 31

3.3.1 Objets Identity Manager dans eDirectory

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

- **Ensemble de pilotes :** un ensemble de pilotes est un conteneur pour les pilotes Identity Manager et les objets de bibliothèque. Vous ne pouvez activer qu'un seul ensemble de pilotes à la fois sur un serveur. Cependant, plusieurs serveurs peuvent être associés à un même ensemble de pilotes. De plus, un pilote peut être associé à plus d'un serveur à la fois. Toutefois, le pilote ne doit être exécuté que sur un serveur à la fois. Il doit être à l'état désactivé sur les autres serveurs. Le serveur méta-annuaire doit être installé sur tous les serveurs associés à un ensemble de pilotes.
- **Bibliothèque :** l'objet de bibliothèque est un espace de stockage des stratégies souvent utilisées et pouvant être référencées depuis plusieurs sites. La bibliothèque est stockée dans l'ensemble de pilotes. Vous pouvez placer une stratégie dans la bibliothèque, de façon à ce qu'elle puisse être référencée par chaque pilote de l'ensemble.
- **Pilote :** un pilote assure la connexion entre une application et le coffre-fort d'identité. Il permet également de synchroniser et de partager des données entre différents systèmes. Le pilote est conservé dans l'ensemble de pilotes.
- **Travail :** un travail permet d'automatiser une tâche récurrente. Par exemple, un travail peut configurer un système afin qu'il désactive un compte un jour donné ou qu'il initie un workflow pour demander l'extension de l'accès d'une personne à une ressource de l'entreprise. Le travail est stocké dans l'ensemble de pilotes.

3.3.2 Réplication des objets nécessaires à Identity Manager sur le serveur

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

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

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

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

- L'objet Ensemble des pilotes de ce serveur.

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

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

- L'objet Serveur de ce serveur.

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

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

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

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

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

  - **Regrouper les utilisateurs sur un seul serveur :** Pour créer un seul serveur avec tous les utilisateurs, ajoutez des répliques sur un serveur existant. Les répliques filtrées peuvent être utilisées pour réduire la taille de la base de données eDirectory si nécessaire, à condition que les objets et attributs utilisateur nécessaires fassent partie de la réplique filtrée.

- **Utilisez plusieurs instances du pilote sur plusieurs serveurs, avec un filtrage des étendues :** Si vous ne voulez pas regrouper les utilisateurs sur un seul serveur, vous devez déterminer l'ensemble de serveurs qui contiendra tous les utilisateurs et configurer une instance du pilote Identity Manager sur chacun de ces serveurs.

  Pour éviter que les instances séparées d'un pilote tentent de synchroniser les mêmes utilisateurs, vous devez utiliser le filtrage des étendues pour définir les utilisateurs que chaque instance du pilote doit synchroniser. Le filtrage des étendues signifie que vous ajoutez des règles à chaque pilote pour limiter l'étendue de la gestion du pilote à des conteneurs spécifiques. Reportez-vous à la section « Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents » page 31.

- **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.

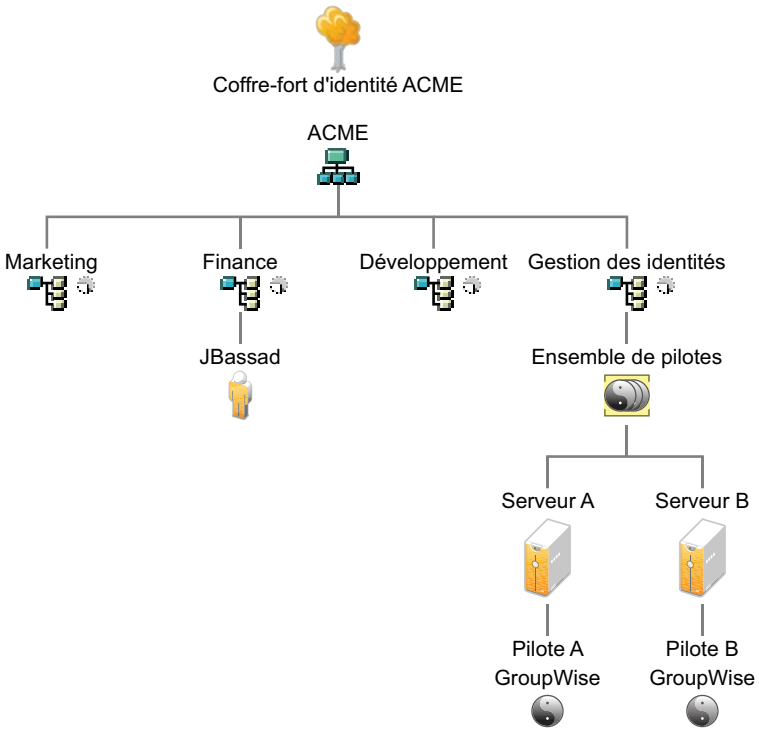
Pour synchroniser tous les utilisateurs sans les répliquer sur un seul serveur, vous devez déterminer l'ensemble de serveurs qui contient tous les utilisateurs, puis créer une instance du pilote Identity Manager sur chacun de ces serveurs. Pour éviter que deux instances du pilote tentent de synchroniser 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 33. Aucun des serveurs ne contient une copie de tous les utilisateurs. Chaque serveur contient deux des trois partitions, l'étendue de ce que les serveurs peuvent contenir est donc en chevauchement.

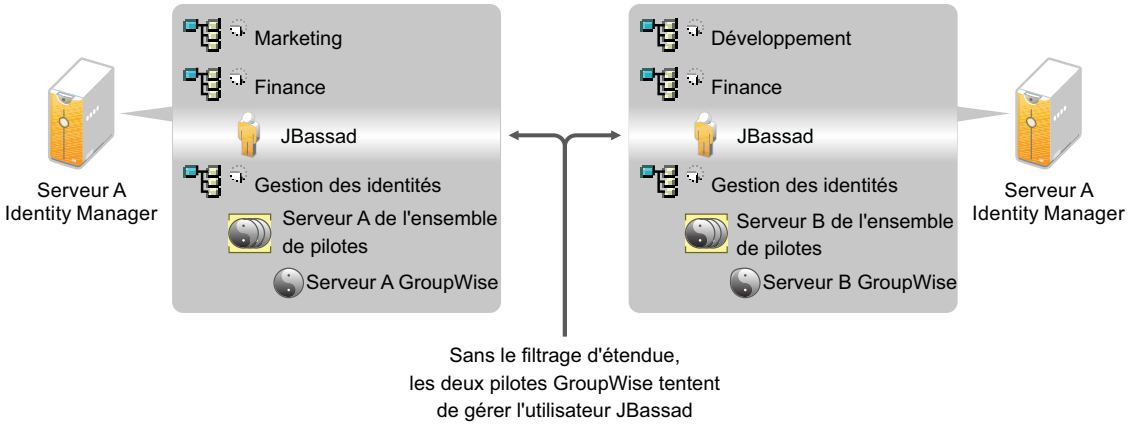
L'administrateur souhaite que tous les utilisateurs de l'arborescence soient synchronisés par le pilote GroupWise, mais ne veut pas regrouper les répliques des utilisateurs sur un seul serveur. Il choisit plutôt d'utiliser deux instances du pilote GroupWise, une sur chaque serveur. Il installe Identity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

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

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

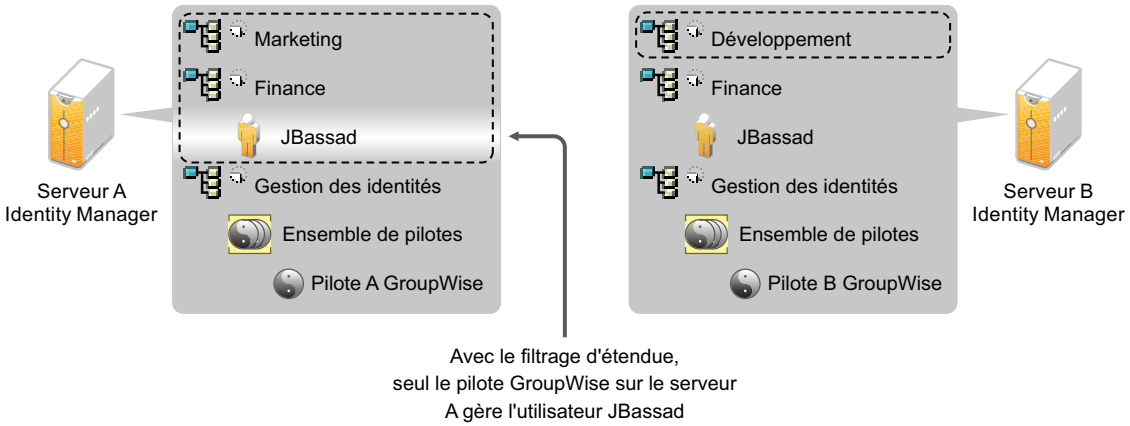
Comme le serveur A et le serveur B contiennent une réplique du conteneur Finance, ils contiennent tous deux l'utilisateur JBassad, qui est dans le conteneur Finance. Sans filtrage des étendues, le pilote GroupWise A et le pilote GroupWise B synchroniseraient JBassad.

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



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

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



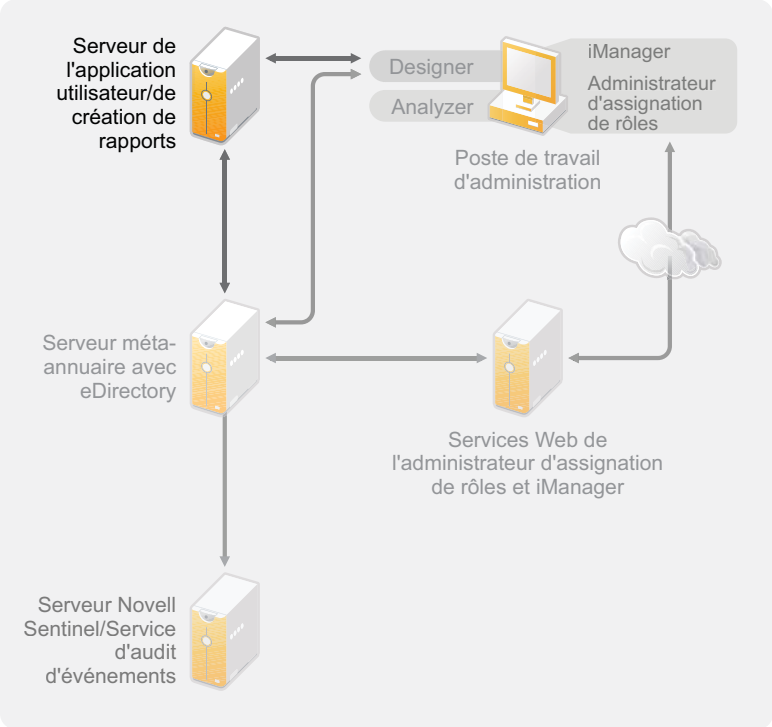
Identity Manager comporte des règles prédéfinies. Deux règles permettent de filtrer les étendues. Les stratégies « Transformation de l'événement - Filtrage de l'étendue - Inclure les sous-arborescences » et « Transformation de l'événement - Filtrage de l'étendue - Exclure les sous-arborescences » sont documentées dans la section *Understanding Policies for Identity Manager 4.0.1* (Présentation des stratégies d'Identity Manager 4.0).

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

3.4 Application utilisateur

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

Figure 3-7 *Application utilisateur*

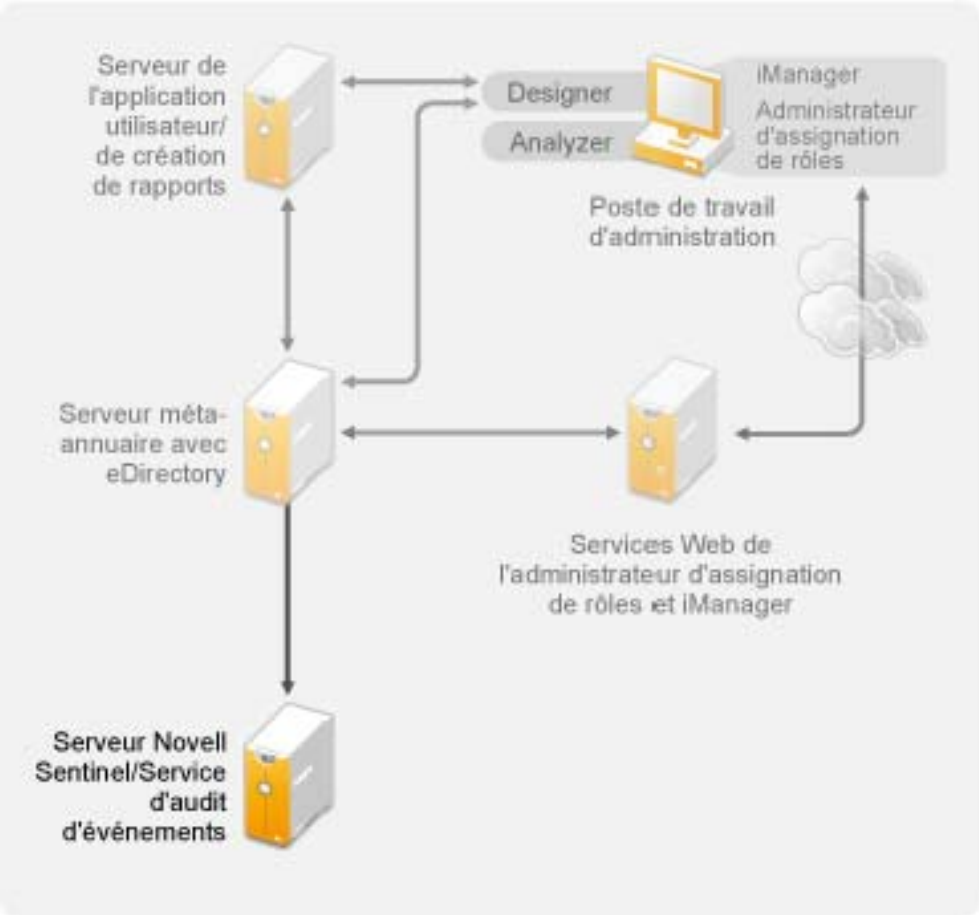


Utilisez les informations de la section Affinage des performances (http://www.novell.com/documentation/idmrbpm40/agpro/data/b2gx735.html) du *Guide d'administration de l'application utilisateur* pour déterminer la meilleure manière de configurer le serveur de l'application utilisateur.

3.5 Instructions pour l'audit et la création de rapport

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

Figure 3-8 *Sentinel*



Installation

Les sections suivantes contiennent les informations nécessaires pour installer un système Identity Manager sans utiliser le programme d'installation intégré. Pour une installation et une configuration simples, utilisez le nouveau programme d'installation intégré au lieu d'installer les composants séparément. Pour plus d'informations sur le programme d'installation intégré, reportez-vous au *Guide du programme d'installation intégré d'Identity Manager 4.0.1*.

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

- Chapitre 4, « Liste de vérification pour un système Identity Manager de base », page 39
- Chapitre 5, « Où se procurer Identity Manager », page 43
- Chapitre 6, « Configuration système requise », page 47
- Chapitre 7, « Installation d'Identity Manager », page 59
- Chapitre 8, « Activation des produits Novell Identity Manager », page 75
- Chapitre 9, « Dépannage d'Identity Manager », page 79
- Chapitre 10, « Nouveautés », page 85

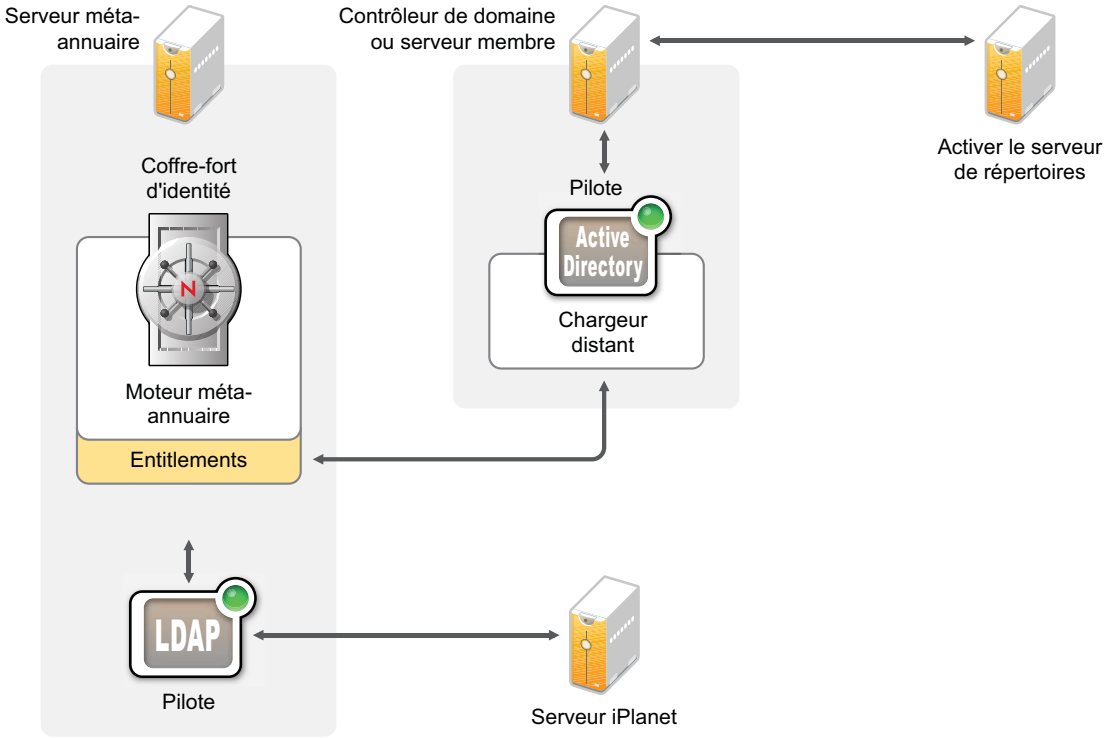
Liste de vérification pour un système Identity Manager de base

4

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

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

Figure 4-1 *Système Identity Manager de base*



- Section 4.1, « Conditions préalables », page 40
- Section 4.2, « Planification », page 40
- Section 4.3, « Installation », page 40
- Section 4.4, « Configuration du pilote avec le chargeur distant », page 41
- Section 4.5, « Configuration de pilotes sans chargeur distant », page 41
- Section 4.6, « Configuration supplémentaire », page 42

4.1 Conditions préalables

- ❑ Vérifiez que votre système répond à la configuration système requise définie au Chapitre 6, « Configuration système requise », page 47.

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 11.
- ❑ Créez un plan de projet pour déployer Identity Manager. Le plan de projet passe par la définition de vos principaux processus d'entreprise, la création d'une solution Identity Manager qui automatise ces processus et l'établissement d'un plan de mise en œuvre technique. Pour réussir le déploiement d'Identity Manager, vous devez appliquer un plan de projet. Pour plus d'informations, reportez-vous au Chapitre 2, « Création d'un plan de projet », page 13.
- ❑ Une fois le plan de projet créé, utilisez Analyzer pour nettoyer et préparer vos données en vue de leur synchronisation. Pour plus d'informations, reportez-vous au manuel *Analyzer 4.0.1 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 1.2 pour Identity Manager).

4.3 Installation

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

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

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

Les droits sont mis en place grâce à trois agents :

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

Pour plus d'informations sur les droits, reportez-vous au manuel *Identity Manager 4.0.1 Entitlements Guide* (Guide des droits d'Identity Manager 4.0).

4.4 Configuration du pilote avec le chargeur distant

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

- ❑ Installez le chargeur distant sur une machine qui communique avec le système connecté. Le chargeur distant assure la communication entre le système connecté et le serveur méta-annuaire, et permet à Identity Manager de communiquer avec une machine sur laquelle eDirectory n'est pas installé. Pour plus d'informations, reportez-vous à la section « Installing the Remote Loader » (Installation du chargeur distant) du manuel *Identity Manager 4.0.1 Remote Loader Guide* (Guide du chargeur distant d'Identity Manager 4.0).
- ❑ Configurez le chargeur distant pour un pilote. Vous définissez une instance spécifique du chargeur distant pour communiquer avec un pilote spécifique. Pour plus d'informations, reportez-vous à la section « Configuring the Remote Loader » (Configuration du chargeur distant) du manuel *Identity Manager 4.0.1 Remote Loader Guide* (Guide du chargeur distant d'Identity Manager 4.0).
- ❑ Configurez le pilote pour qu'il communique avec le chargeur distant. Il existe un guide pour chaque pilote. Pour obtenir des informations spécifiques sur votre pilote, reportez-vous au site Web de documentation des pilotes Identity Manager 4.0.1 (http://www.novell.com/documentation/idm401drivers/).
- ❑ (Facultatif) Activez les droits sur le pilote. Vérifiez que vous disposez des bonnes stratégies pour exécuter le droit. Pour plus d'informations, reportez-vous au manuel *Identity Manager 4.0.1 Entitlements Guide* (Guide des droits d'Identity Manager 4.0).
- ❑ Répétez ces étapes pour chaque pilote de votre environnement.

4.5 Configuration de pilotes sans chargeur distant

- ❑ Créez et configurez votre pilote. Il existe un guide pour chaque pilote. Pour obtenir des informations spécifiques sur votre pilote, reportez-vous au site Web de documentation des pilotes Identity Manager 4.0.1 (http://www.novell.com/documentation/idm401drivers/).
- ❑ (Facultatif) Activez les droits sur le pilote. Vérifiez que vous disposez des bonnes stratégies pour exécuter le droit. Pour plus d'informations, reportez-vous au manuel *Identity Manager 4.0.1 Entitlements Guide* (Guide des droits d'Identity Manager 4.0).
- ❑ Répétez ces étapes pour chaque pilote de votre environnement.

4.6 Configuration supplémentaire

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

- **Gestion des mots de passe :** si vous souhaitez gérer des mots de passe avec Identity Manager, la procédure de configuration est un peu plus longue. Utilisez la « Password Management Checklist » (Liste de vérification de gestion des mots de passe) du manuel *Identity Manager 4.0.1 Password Management Guide* (Guide de gestion des mots de passe d'Identity Manager 4.0) pour vérifier que toutes les étapes de configuration sont réalisées.
- **Gestion des rôles :** si vous souhaitez gérer des rôles dans différents systèmes depuis un seul et même emplacement, utilisez l'administrateur d'assignation de rôles, un outil intégré à Identity Manager. Ce dernier permet d'assigner des rôles métier d'un système à un autre, sans devoir comprendre l'infrastructure informatique. Pour plus d'informations, reportez-vous au manuel *Identity Manager Role Mapping Administrator 4.0.1 Installation and Configuration Guide* (Guide d'installation et de configuration de la version 4.0.1 de l'administrateur de l'assignation de rôles d'Identity Manager).
- **Provisioning basé sur les rôles :** pour ajouter la fonction de provisioning basé sur les rôles à votre solution Identity Manager, utilisez la « Liste de contrôle de l'installation » du *Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0.1* afin de vérifier que toutes les étapes de configuration sont réalisées.
- **Audit et création de rapports :** l'ajout de la fonction d'audit et de création de rapports à votre solution Identity Manager vous permet de vérifier que vos stratégies métier sont conformes aux stratégies de l'entreprise. Vous pouvez ajouter le module Identity Reporting ou Novell Sentinel à votre solution Identity Manager pour l'audit et la création de rapports. Pour plus d'informations sur le module Identity Reporting, reportez-vous au manuel *Identity Reporting Module Guide* (Guide du module Identity Reporting). Pour plus d'informations sur Novell Sentinel, reportez-vous au manuel *Identity Manager 4.0.1 Reporting Guide for Novell Sentinel* (Guide de création de rapports Identity Manager 4.0 pour Novell Sentinel).

Où se procurer Identity Manager

5

Identity Manager 4.0.1 est disponible en deux versions : Advanced Edition et Standard Edition. Il existe des fichiers ISO distincts pour chaque version. Identity Manager 4.0.1 Advanced Edition comporte un éventail complet de fonctions pour le provisioning des utilisateurs en entreprise. Afin de répondre aux besoins divers des clients, Identity Manager Standard Edition propose un sous-ensemble des fonctions disponibles dans la version Advanced Edition. Identity Manager Standard Edition continue toutefois d'offrir toutes les fonctions qui étaient déjà présentes dans les versions précédentes d'Identity Manager. Pour plus d'informations sur le contenu des versions Advanced Edition et Standard Edition d'Identity Manager 4.0.1, reportez-vous à la section « Fonctionnalités d'Identity Manager 4.0.1 » du *Guide de présentation d'Identity Manager 4.0.1*.

Vous pouvez télécharger une copie d'évaluation d'Identity Manager et l'utiliser gratuitement durant 90 jours. Les composants Identity Manager doivent être activés dans les 90 jours à compter de l'installation, faute de quoi ils ne fonctionneront plus. À tout moment, durant ces 90 jours ou ultérieurement, vous pouvez choisir d'acheter une licence de produit et d'activer Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 8, « Activation des produits Novell Identity Manager », page 75.

Pour télécharger Identity Manager et ses services :

1. Allez sur le site Web de téléchargements Novell (http://download.novell.com).
2. Dans le menu *Produit ou technologie*, sélectionnez *Novell Identity Manager*, puis cliquez sur *Recherche*.
3. Sur la page des téléchargements Novell Identity Manager, cliquez sur le bouton *Télécharger* à côté du fichier souhaité. Le Tableau 5-1 contient une description de chaque fichier.

   Sélectionnez l'image ISO correspondant à vos besoins. Chaque image ISO contient les versions 32 et 64 bits du produit.

   Important : pour passer de la version Advanced Edition d'Identity Manager à la version Standard Edition, désinstallez la version Advanced Edition avant d'installer l'image ISO Standard Edition à partir du support d'Identity Manager. Pour effectuer la mise à niveau de la version Standard Edition vers la version Advanced Edition, utilisez l'image ISO Identity Manager Advanced Edition. Cette opération nécessite toutefois l'application de l'activation adéquate. Pour plus d'informations sur la mise à niveau de la version Standard Edition vers la version Advanced Edition, reportez-vous au manuel *Identity Manager 4.0.1 Upgrade and Migration Guide* (Guide de mise à niveau et de migration d'Identity Manager 4.0.1).

   ---

4. Suivez les instructions à l'écran pour télécharger le fichier vers un répertoire de votre ordinateur.
5. Répétez l'Étape 3 jusqu'à ce que vous ayez téléchargé tous les fichiers dont vous avez besoin.
6. Montez ensuite le fichier `.iso` téléchargé en tant que volume ou utilisez le fichier `.iso` pour créer un DVD du logiciel. Si vous n'avez pas encore vérifié la validité du support que vous avez gravé, vous pouvez le faire à l'aide de l'option *Vérification du support*.

   Remarque : en raison de leur taille importante, les fichiers ISO Linux doivent être copiés sur un DVD double couche.

Tableau 5-1 *Images ISO d'Identity Manager*

ISO	Plate-forme	Description
`Identity_Manager_4.0.1_Windows_Advanced.iso`	Windows	Contient l'image DVD pour le serveur méta-annuaire, Designer, iManager, l'administrateur d'assignation de rôles, d'Analyzer, du module Novell Identity Reporting et du module de provisioning basé sur les rôles.
`Identity_Manager_4.0.1_Windows_Standard.iso`	Windows	Contient l'image DVD pour le serveur méta-annuaire, Designer, iManager, Analyzer, le module Novell Identity Reporting et le module de provisioning basé sur les rôles.
`Identity_Manager_4.0.1_Linux_Advanced.iso`	Linux	Contient l'image DVD pour le serveur méta-annuaire, Designer, iManager, l'administrateur de l'assignation de rôles, Analyzer, le module Novell Identity Reporting et le module de provisioning basé sur les rôles.
`Identity_Manager_4.0.1_Linux_Standard.iso`	Linux	Contient l'image DVD pour le serveur méta-annuaire, Designer, iManager, Analyzer, le module Novell Identity Reporting et le module de provisioning basé sur les rôles.
`Identity_Manager_4.0.1_Solaris_Advanced.iso`	Solaris	Contient l'image DVD pour le serveur méta-annuaire. Les autres composants ne sont pas pris en charge sur la plate-forme Solaris.
`Identity_Manager_4.0.1_Solaris_Standard.iso`	Solaris	Contient l'image DVD pour le serveur méta-annuaire. Les autres composants ne sont pas pris en charge sur les plates-formes Solaris.

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

- **Pilotes de service :** la liste suivante répertorie les pilotes de service qui sont activés en même temps que le serveur méta-annuaire :
  - Service de collecte de données
  - Services de droits
  - Fournisseur d'ID
  - Service de boucle
  - Passerelle système gérée
  - Service de tâche manuelle
  - Service nul
  - Service de rôles et de ressources
  - Application utilisateur
  - Ordre de travail
- **Pilotes communs :** la liste suivante répertorie les pilotes communs qui sont activés en même temps que le serveur méta-annuaire :
  - Active Directory

- ADAM
- eDirectory
- GroupWise
- LDAP
- Lotus Notes

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

Il s'agit d'activations distinctes pour Identity Manager Advanced Edition et Standard Edition. Pour plus d'informations, reportez-vous à la section « Activation des produits Novell Identity Manager » page 75. Le passage de la version Advanced Edition vers la version Standard Edition n'est pas pris en charge. Pour utiliser Identity Manager Standard Edition, vous devez l'installer à partir du support d'Identity Manager.

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

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

- Analyzer
- Designer
- iManager
- Administrateur de l'assignation de rôles

Remarque : l'administrateur de l'assignation de rôles n'est pas disponible avec Identity Manager 4.0.1 Standard Edition.

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

Pour plus d'informations sur les composants d'Identity Manager, reportez-vous au guide *Présentation d'Identity Manager 4.0.1*.

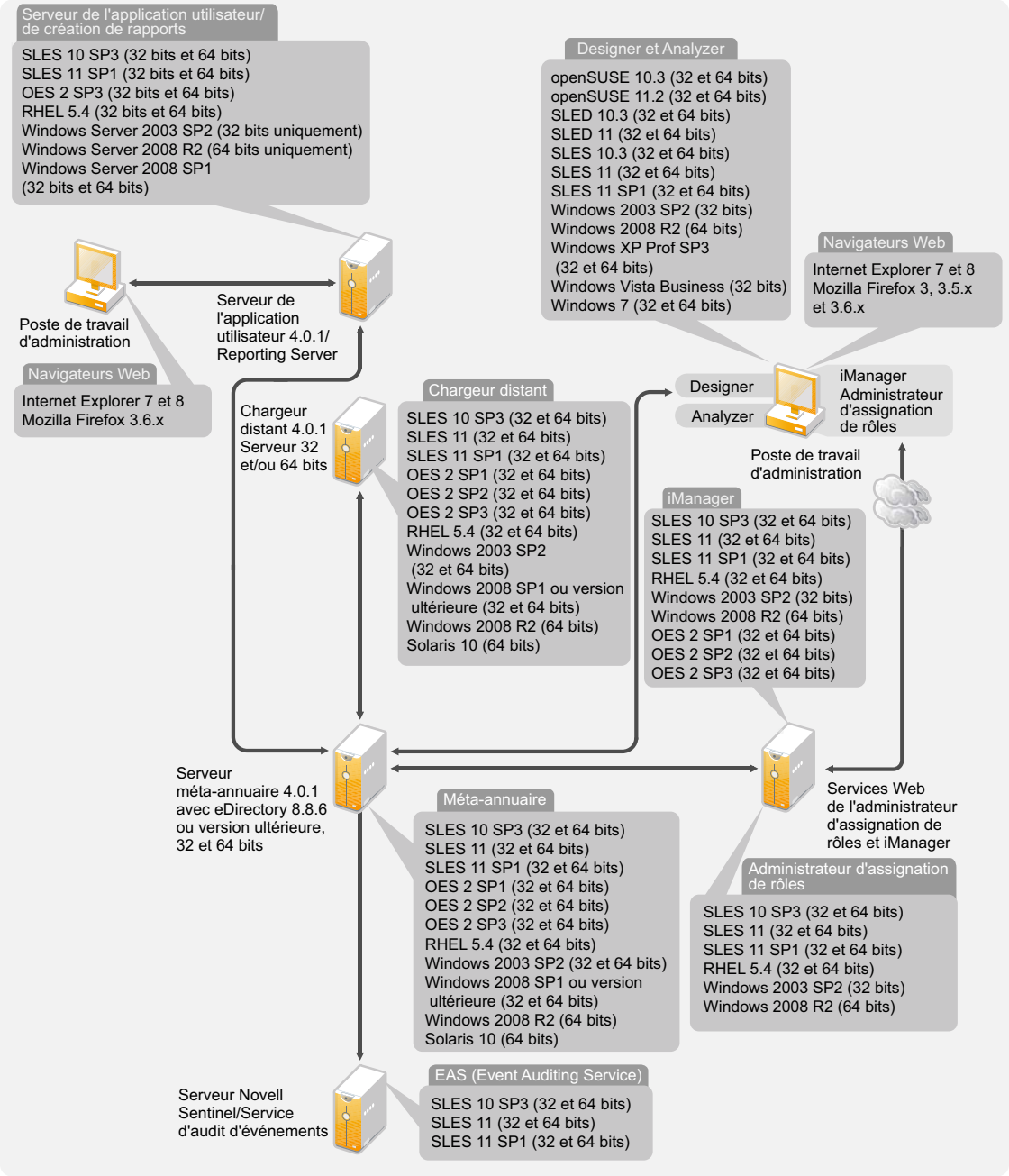
Configuration système requise

6

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

La Figure 6-1 montre les plates-formes et les systèmes pris en charge.

Figure 6-1 *Configuration système pour les composants Identity Manager*



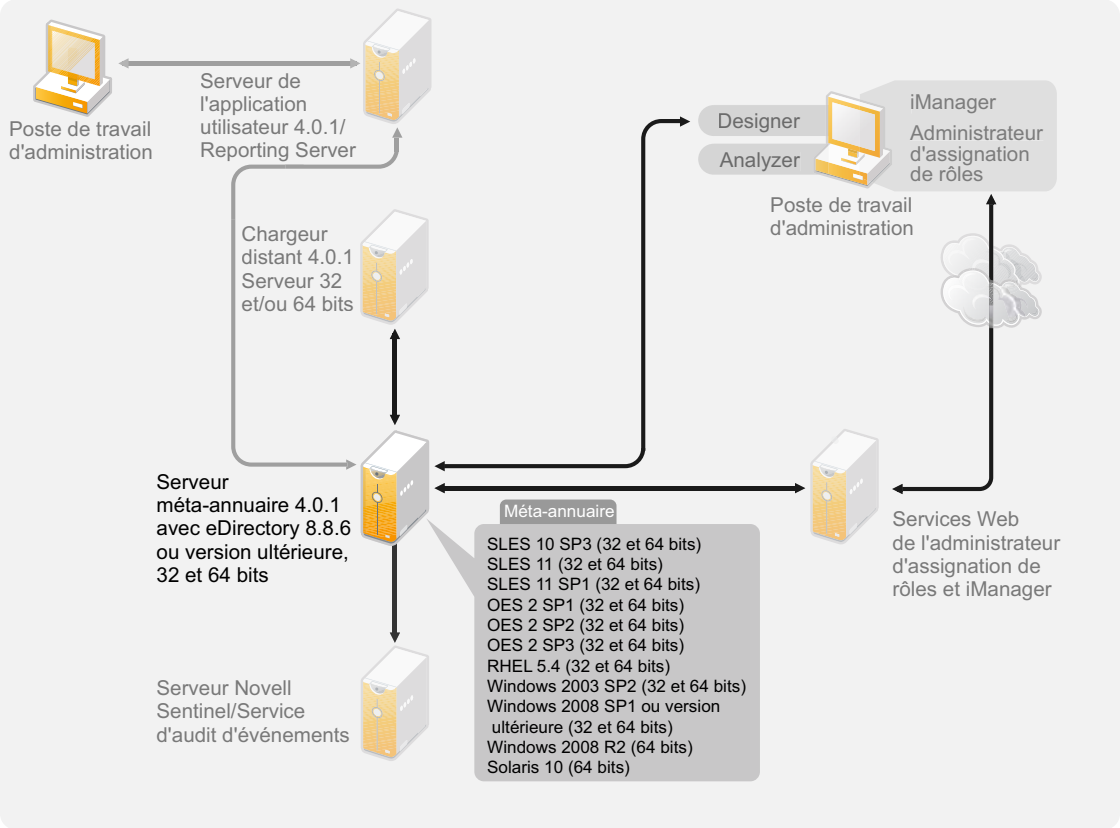
Selon la configuration de votre système, vous devrez peut-être exécuter le programme d'installation Identity Manager plusieurs fois pour installer les composants d'Identity Manager sur les systèmes adéquats.

- Section 6.1, « eDirectory et iManager », page 48
- Section 6.2, « Serveur méta-annuaire », page 49
- Section 6.3, « Chargeur distant », page 51
- Section 6.4, « Application utilisateur », page 54
- Section 6.5, « Audit et création de rapports », page 54
- Section 6.6, « Postes de travail », page 55
- Section 6.7, « Ressources requises », page 57

6.1 eDirectory et iManager

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

Figure 6-2 *Produits de base pour Identity Manager*



Vous devez disposer des versions suivantes de ces produits :

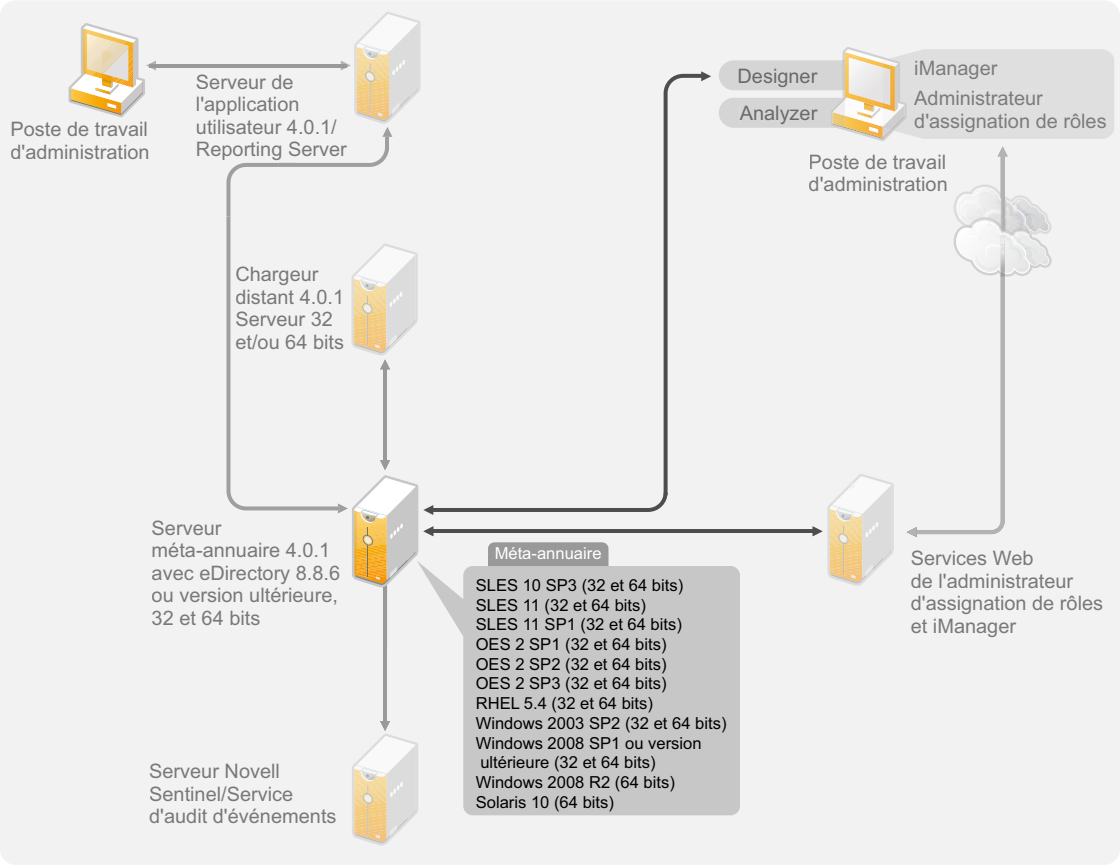
- eDirectory 8.8.6 ou version ultérieure (32 ou 64 bits)
- iManager 2.7.4

Pour plus d'informations sur la configuration système requise pour eDirectory, reportez-vous au *Guide d'installation de Novell eDirectory 8.8* (http://www.novell.com/documentation/edir88/index.html). Pour connaître la configuration système requise pour iManager, reportez-vous à la section Installation d'iManager (http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html) du *Guide d'installation d'iManager 2.7* (http://www.novell.com/documentation/imanager27/index.html).

6.2 Serveur méta-annuaire

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

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



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

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

- Section 6.2.1, « Processeurs pris en charge », page 50
- 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 est utilisé pour les tests de Solaris.

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

- Intel x86-32
- AMD x86-32

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

- Intel EM64T
- AMD Athlon64
- AMD Opteron

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

6.2.2 Systèmes d'exploitation du serveur

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

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

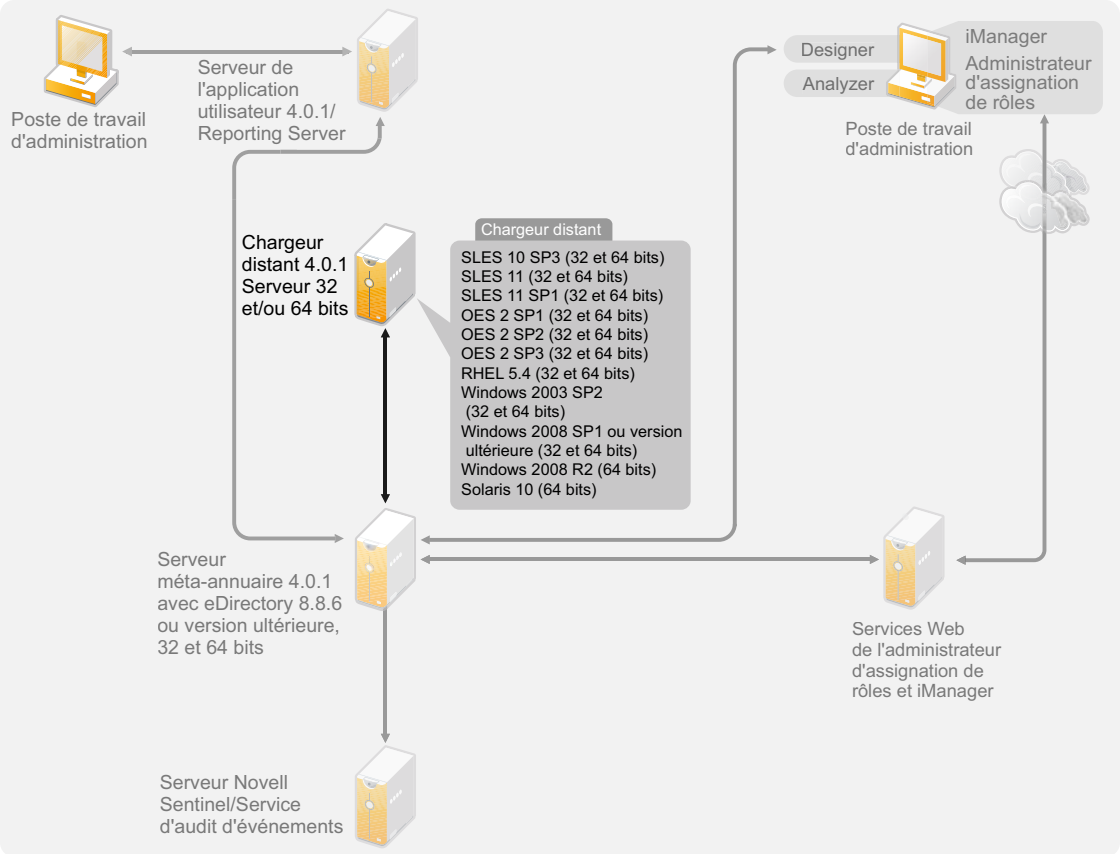
Version du système d'exploitation du serveur	Notes
Windows Server 2003 SP2 ou version ultérieure (32 bits)	Le serveur méta-annuaire s'exécute uniquement en mode 32 bits.
Windows 2008 ou Support Packs ultérieurs (32 et 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.
Windows Server 2008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

Version du système d'exploitation du serveur	Notes
SUSE Linux Enterprise Server 11 (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 SP1 (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.
OES 2 SP1 (32 et 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 et 64 bits.
OES 2 SP2 (32 et 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 et 64 bits.
OES 2 SP3 (32 et 64 bits)	Le serveur méta-annuaire s'exécute en mode 32 et 64 bits.
Solaris 10 (64 bits)	Le serveur méta-annuaire s'exécute uniquement en mode 64 bits.
Xen	Xen est pris en charge lorsque la machine virtuelle Xen exécute SLES 10/SLES 11 en tant que système d'exploitation invité en mode paravirtualisé.
VMware ESX	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.
Virtualisation de Red Hat Enterprise Linux 5	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.
Virtualisation avec Hyper-V de Windows Server 2008 R2	Le serveur méta-annuaire s'exécute en mode 32 ou 64 bits.

6.3 Chargeur distant

Le chargeur distant vous offre une souplesse de configuration pour votre solution Identity Manager. Il offre une prise en charge 32 et 64 bits. Par défaut, le programme d'installation détecte la version du système d'exploitation, puis installe la version correspondante du chargeur distant.

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



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

Le Tableau 6-2 liste les systèmes d'exploitation pris en charge pour le chargeur distant.

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

Version du système d'exploitation du serveur	Notes
Windows Server* 2003 SP2 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
Windows Server 2008 ou Support Packs ultérieurs (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
Windows Server 2008 R2 (64 bits)	Le chargeur distant s'exécute uniquement en mode 64 bits.
Red Hat 5.4 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits. Avant d'installer Identity Manager, Novell recommande d'appliquer les derniers correctifs de système d'exploitation à l'aide du service de mise à jour automatique du fabricant.

Version du système d'exploitation du serveur	Notes
SUSE Linux Enterprise Server 10 SP3 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits. Avant d'installer Identity Manager, Novell recommande d'appliquer les derniers correctifs de système d'exploitation à l'aide du service de mise à jour automatique du fabricant.
SUSE Linux Enterprise Server 11 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits. Avant d'installer Identity Manager, Novell recommande d'appliquer les derniers correctifs de système d'exploitation à l'aide du service de mise à jour automatique du fabricant.
SUSE Linux Enterprise Server 11 SP1 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits. Avant d'installer Identity Manager, Novell recommande d'appliquer les derniers correctifs de système d'exploitation à l'aide du service de mise à jour automatique du fabricant.
OES 2 SP1 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
OES 2 SP2 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
OES 2 SP3 (32 et 64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
Solaris 10 (64 bits)	Le chargeur distant s'exécute uniquement en mode 64 bits.
Xen	Xen est pris en charge lorsque la machine virtuelle Xen exécute SLES 10/SLES 11 en tant que système d'exploitation invité en mode paravirtualisé.
VMware ESX (64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
Virtualisation de Red Hat Enterprise Linux 5 (64 bits)	Le chargeur distant s'exécute en mode 32 et 64 bits.
Virtualisation avec Hyper-V de Windows Server 2008 R2	Le chargeur distant s'exécute en mode 32 et 64 bits.

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

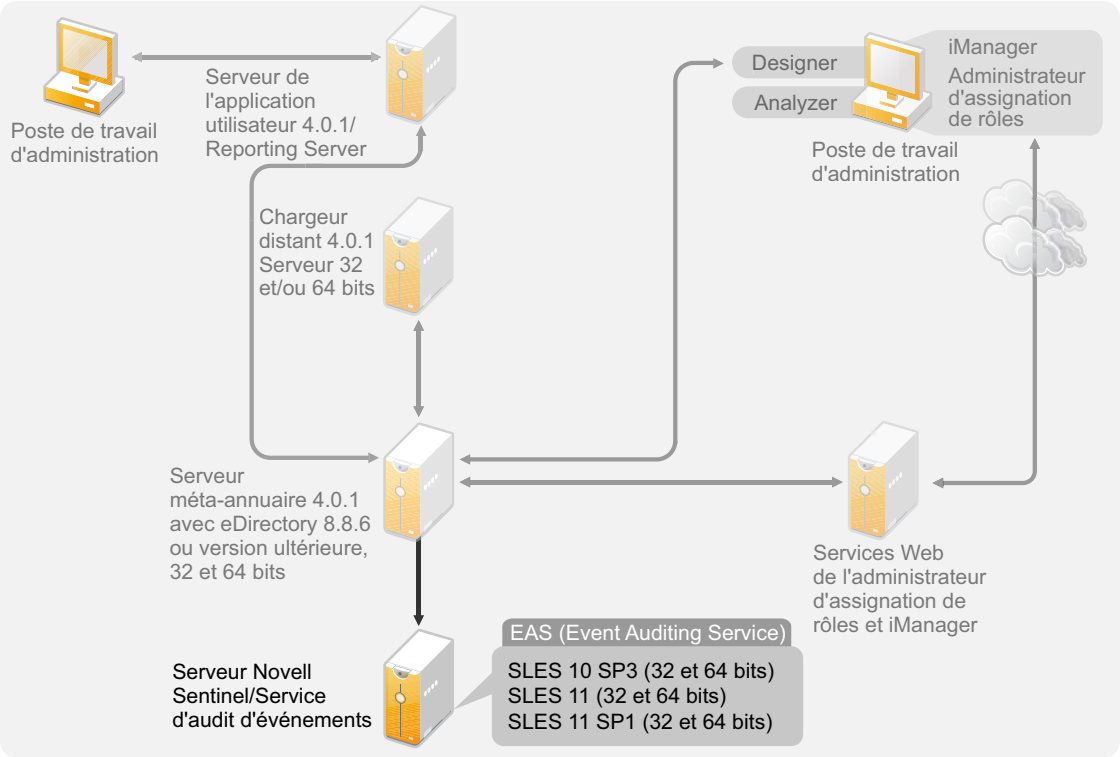
6.4 Application utilisateur

Pour connaître la configuration système requise pour l'application utilisateur, reportez-vous à la section « Configuration système requise » du manuel *Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0.1*. Le module de provisioning basé sur les rôles version 4.0.1 utilise JBoss 5.1 comme serveur d'applications et PostgreSQL 8.4.3 comme base de données.

6.5 Audit et création de rapports

Le module Identity Reporting et Novell Sentinel sont deux outils qui permettent de rassembler des informations d'audit et de création de rapports sur Identity Manager. La Figure 6-5 montre la version de Sentinel prise en charge avec Identity Manager 4.0.1.

Figure 6-5 *Sentinel*



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

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

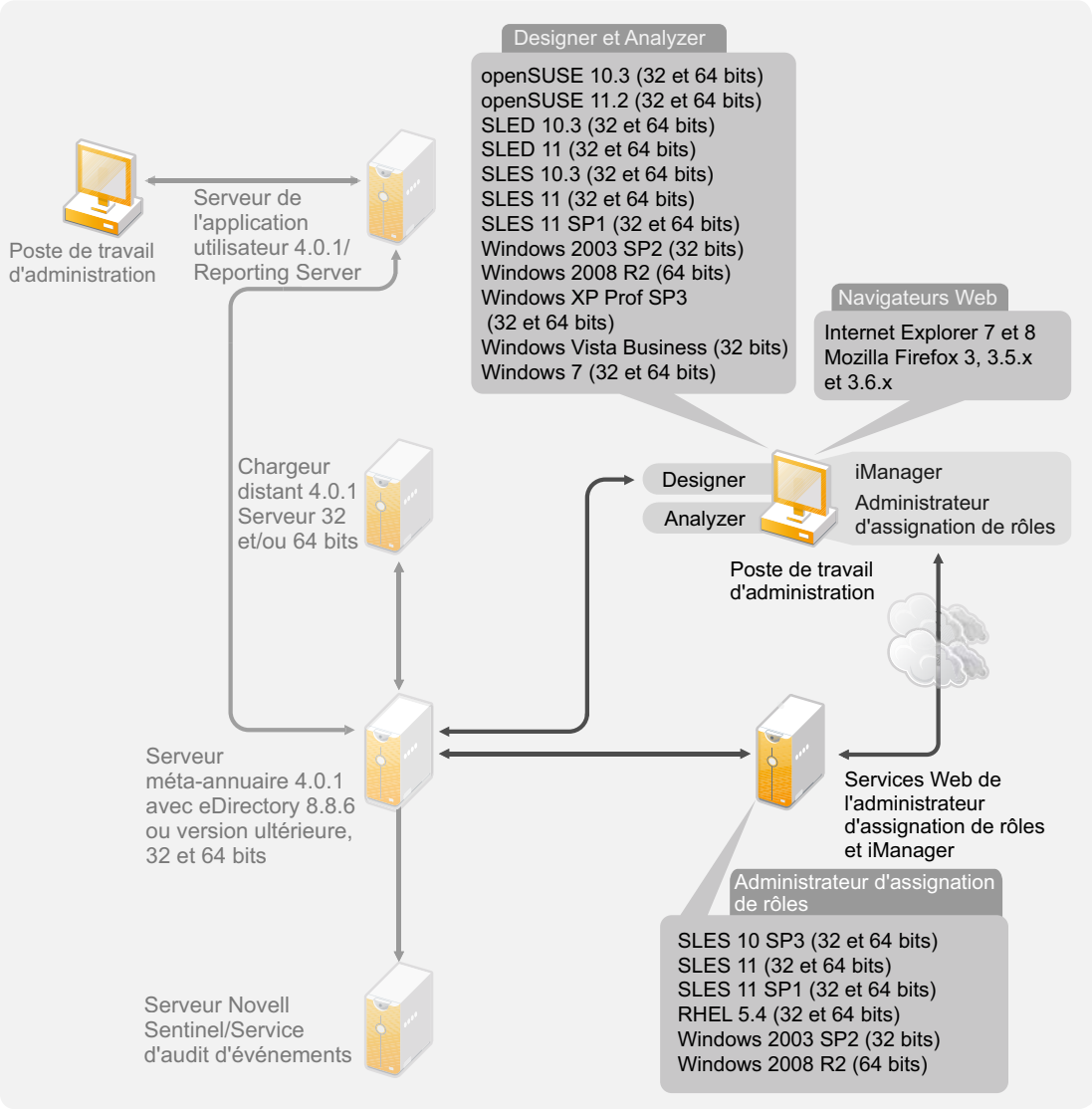
Pour plus d'informations sur la configuration système requise et la configuration du module Identity Reporting, reportez-vous à la section « System Requirements » (Configuration système requise) du manuel *Identity Reporting Module Guide* (Guide du module Identity Reporting). Pour obtenir des

informations de configuration concernant Sentinel avec Identity Manager, reportez-vous au manuel *Identity Manager 4.0.1 Reporting Guide for Novell Sentinel* (Guide de création de rapports d'Identity Manager 4.0 pour Novell Sentinel). Pour connaître la configuration système requise pour Novell Sentinel, reportez-vous au chapitre « Supported Platforms and Best Practices » (Plates-formes prises en charge et meilleures pratiques) du manuel *Novell Sentinel Installation Guide* (http://www.novell.com/documentation/sentinel6/index.html) (Guide d'installation de Novell Sentinel).

6.6 Postes de travail

Les postes de travail permettent d'accéder à Designer, à iManager, à l'administrateur d'assignation de rôles ou à la page Web d'administration de l'application utilisateur. La Figure 6-6 montre les différents composants des postes de travail qui sont pris en charge avec Identity Manager 4.0.1.

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 56
- Section 6.6.2, « Navigateurs Web », page 57

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.

Pour connaître la configuration système requise, reportez-vous à la documentation spécifique du composant.

- iManager : reportez-vous à la section Installation d'iManager (http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html) du *Guide d'installation de Novell iManager 2.7*.
- Designer : reportez-vous à la section « System Requirements » (Configuration système requise) du manuel *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Guide d'administration de Designer 4.0.1 pour Identity Manager 4.0.1).

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

Plates-formes	Détails
Windows 7 (32 et 64 bits)	Les versions 32 et 64 bits sont toutes les deux prises en charge.
Windows Vista (32 bits)	Seule la version 32 bits est prise en charge.
Windows XP Professionnel SP3 (32 et 64 bits)	Les versions 32 et 64 bits sont toutes les deux prises en charge.
Windows 2003 SP2 (32 bits)	Seule la version 32 bits est prise en charge.
Windows 2008 R2 (64 bits)	Seule l'Édition Professionnelle 64 bits est prise en charge.
openSUSE 10.3 (32 et 64 bits)	Appliquez les derniers correctifs à l'aide du système de mise à jour automatique.
openSUSE 11.2 (32 et 64 bits)	Appliquez les derniers correctifs à l'aide du système de mise à jour automatique.
SUSE Linux Enterprise Desktop 10 SP3 (32 et 64 bits)	Appliquez les derniers correctifs à l'aide du système de mise à jour automatique.
SUSE Linux Enterprise Desktop 11 (32 et 64 bits)	Appliquez les derniers correctifs à l'aide du système de mise à jour automatique.
SUSE Linux Enterprise Server 10 SP3 (32 et 64 bits)	Appliquez les derniers correctifs à l'aide du système de mise à jour automatique.
SUSE Linux Enterprise Server 11 (32 et 64 bits)	Appliquez les derniers correctifs à l'aide du système de mise à jour automatique.
SUSE Linux Enterprise Server 11 SP1 (32 et 64 bits)	Appliquez les derniers correctifs à l'aide du système de mise à jour automatique.

6.6.2 Navigateurs Web

iManager exécute tous les plug-ins nécessaires à l'administration d'Identity Manager. L'administrateur d'assignation de rôles permet d'assigner des rôles métier dans différents systèmes, sans devoir comprendre l'infrastructure informatique. Vous pouvez accéder à ces deux applications via un navigateur Web.

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

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

Pour obtenir une liste de la configuration système requise pour l'administrateur de l'assignation de rôles, reportez-vous à la section « System Requirements » (Configuration système requise) du manuel *Identity Manager Role Mapping Administrator 4.0.1 Installation and Configuration Guide* (Guide d'installation et de configuration de la version 4.0.1 de l'administrateur de l'assignation de rôles d'Identity Manager).

6.7 Ressources requises

Tableau 6-4 *Ressources requises pour Identity Manager*

Composant Identity Manager	Configuration minimale
Serveur méta-annuaire	2048 Mo
Chargeur distant	256 Mo
Pilotes	200 Mo
Plug-ins iManager	80 Mo

Installation d'Identity Manager 7

Identity Manager inclut un programme d'installation intégré qui simplifie le processus d'installation en installant et configurant tous les composants en même temps. Si c'est la première fois que vous installez un système Identity Manager, utilisez le programme d'installation intégré. Pour plus d'informations, reportez-vous au *Guide du programme d'installation intégré d'Identity Manager 4.0.1*.

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

Il importe d'installer et d'utiliser Analyzer et Designer pendant la phase de planification de la mise en œuvre d'Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 2, « Création d'un plan de projet », page 13.

Installez les composants dans l'ordre indiqué ci-après. Pour obtenir des explications sur les différents composants, reportez-vous au manuel *Présentation d'Identity Manager 4.0.1*.

- Section 7.1, « Installation d'Analyzer », page 59
- Section 7.2, « Installation de Designer », page 60
- Section 7.3, « Installation d'eDirectory », page 61
- Section 7.4, « Installation d'iManager », page 61
- Section 7.5, « Installation du serveur méta-annuaire », page 62
- Section 7.6, « Installation du chargeur distant », page 66
- Section 7.7, « Installation des fichiers de pilote », page 71
- Section 7.8, « Installation du module de provisioning basé sur les rôles », page 72
- Section 7.9, « Installation d'un pilote personnalisé », page 72
- Section 7.10, « Installation de l'administrateur de l'assignation de rôles », page 73
- Section 7.11, « Installation du module Identity Reporting ou de Sentinel », page 74

7.1 Installation d'Analyzer

Outil basé sur le poste de travail, Analyzer vous permet d'analyser, de nettoyer et de préparer vos données en vue de leur synchronisation avec Identity Manager. Installez Analyzer et utilisez-le durant toute la phase de planification de la mise en œuvre de votre solution Identity Manager. Pour plus d'informations sur la planification, reportez-vous à la Partie I, « Planification », page 9.

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 55.

2. Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au Chapitre 5, « Où se procurer Identity Manager », page 43.

3. Lancez l'installation en exécutant le programme adapté à la plate-forme de votre poste de travail.

   Linux : `IDM4.0.1_Lin/products/Analyzer/install`

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

Windows : `IDM4.0.1_Win:/products/Analyzer/install.exe`

4 Complétez les informations suivantes pour terminer l'installation :

Emplacement d'installation : indiquez l'emplacement d'installation d'Analyzer sur le poste de travail.

Créer des raccourcis et sélectionner une langue : indiquez si vous souhaitez créer des raccourcis pour Analyzer sur le bureau et sélectionnez la langue d'installation d'Analyzer.

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

7.2 Installation de Designer

Outil basé sur le poste de travail, Designer vous permet de concevoir votre solution Identity Manager. Installez Designer et utilisez-le durant toute la phase de planification de la mise en œuvre de votre solution Identity Manager. Pour plus d'informations sur la planification, reportez-vous à la Partie I, « Planification », page 9.

1 Vérifiez que le système d'exploitation de votre poste de travail est bien pris en charge. Pour garantir le bon fonctionnement de Designer, installez le paquetage NICI 32 bits. Si vous installez Designer sur un système 64 bits, assurez-vous que la bibliothèque compat `libgthread-2_0-0-32bit-2.17.2+2.17.3+20080708+r7171-3.1.x86_64.rpm` est installée avant Designer. Pour plus d'informations, reportez-vous à la Section 6.6, « Postes de travail », page 55 et au manuel *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Guide d'administration de Designer 4.0.1 pour Identity Manager 4.0.1).

2 Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au Chapitre 5, « Où se procurer Identity Manager », page 43.

3 Lancez l'installation en exécutant le programme adapté à la plate-forme de votre poste de travail.

Linux : `IDM4.0.1_Lin/products/Designer/install`

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

Windows : `IDM4.0.1_Win:\products\Designer\install.exe`

4 Les informations suivantes permettent de terminer l'installation :

Dossier d'installation : indiquez l'emplacement d'installation de Designer sur le poste de travail.

Créez les raccourcis : choisissez les raccourcis placés sur votre bureau et dans le menu du bureau.

Avant d'installer Designer, assurez-vous que ce paquetage est bien installé. YaST vous permet de vérifier les éventuelles dépendances et les paquetages installés. Pour en savoir plus, reportez-vous au manuel *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

7.3 Installation d'eDirectory

Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au Chapitre 5, « Où se procurer Identity Manager », page 43.

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

- **Linux 32 bits :** `IDM4.0.1_Lin/products/eDirectory/x86/setup/nds-install`
- **Linux 64 bits :** `IDM4.0.1_Lin/products/eDirectory/x64/setup/nds-install`
- **Solaris 32 bits :** `IDM4.0.1_Solaris/products/eDirectory/x86/setup/nds-install`
- **Solaris 64 bits :** `IDM4.0.1_Solaris/products/eDirectory/x64/setup/nds-install`

  Pour exécuter le fichier binaire, saisissez `./nds-install`.
- **Windows 32 bits :** `IDM4.0.1_Win:\products\eDirectory\x86\nt\Setup.exe`
- **Windows 64 bits :** `IDM4.0.1_Win:\products\eDirectory\x64\windows\Setup.exe`

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

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

7.4 Installation d'iManager

Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au Chapitre 5, « Où se procurer Identity Manager », page 43.

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

- **Linux :** `IDM4.0.1_Lin/products/iManager/installs/linux/iManagerInstallLinux.bin`

  Pour exécuter le fichier binaire, saisissez `./iManagerInstallLinux.bin`.
- **Windows :** `IDM4.0.1_Win:\products\iManager\installs\win\iManagerInstall.exe`

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

7.5 Installation du serveur méta-annuaire

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

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

1. Vérifiez que vous disposez de la configuration système requise indiquée au Chapitre 6, « Configuration système requise », page 47.
2. Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au Chapitre 5, « Où se procurer Identity Manager », page 43.
3. (Linux/UNIX uniquement) Pour vérifier que les variables d'environnement pour eDirectory sont exportées avant le début de l'installation sur Linux/UNIX, accédez à une invite de commande et saisissez :

   ```
   set | grep PATH
   ```

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

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

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

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

   Linux - installation à partir de l'interface graphique : `IDM4.0.1_Lin/products/IDM/install.bin [-i gui]`

   Linux - installation à partir de la ligne de commande : `IDM4.0.1.1_Lin/products/IDM/install.bin -i console`

   Solaris - installation à partir de l'interface graphique : `IDM4.0.1_Solaris/products/IDM/install.bin [-i gui]`

   Solaris - installation à partir de la ligne de commande : `IDM4.0.1_Solaris/products/IDM/install.bin -i console`

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

   Windows : `IDM4.0.1_Win:\products\IDM\windows\setup\idm_install.exe`
5. Les informations suivantes permettent de terminer l'installation :

Sélectionner les composants : sélectionnez le serveur méta-annuaire, les plug-ins iManager et les utilitaires pour installer le serveur méta-annuaire.

- **Serveur méta-annuaire de Novell Identity Manager :** cette option nécessite l'installation du coffre-fort d'identité sur ce serveur et installe la version 64 bits d'Identity Manager. Elle étend le schéma d'Identity Manager et installe le serveur méta-annuaire, les pilotes Identity Manager ainsi que Novell Audit Agent.
- **Serveur méta-annuaire de Novell Identity Manager (32 bits) :** cette option nécessite l'installation du coffre-fort d'identité sur ce serveur et installe la version 32 bits d'Identity Manager. Elle étend le schéma d'Identity Manager et installe le serveur méta-annuaire, les pilotes Identity Manager ainsi que Novell Audit Agent.
- **Serveur de système connecté Novell Identity Manager (64 bits) :** cette option ne nécessite pas l'installation du coffre-fort d'identité sur ce serveur. Ne choisissez cette option que si vous installez le chargeur distant 64 bits. Pour plus d'informations, reportez-vous à la Section 7.6, « Installation du chargeur distant », page 66.
- **Serveur de système connecté Novell Identity Manager (.NET) :** cette option (Windows uniquement) installe le service de chargeur distant .NET et le pilote SharePoint sur ce serveur.
- **Plug-ins Novell Identity Manager pour Identity Manager :** sélectionnez cette option si vous avez installé iManager sur ce serveur. Elle installe les plug-ins iManager pour Identity Manager.
- **Utilitaires :** cette option installe les utilitaires servant à configurer les pilotes pour les systèmes connectés. Tous les pilotes n'ont pas d'utilitaires. Si vous n'êtes pas certain d'en avoir besoin, sélectionnez-les tout de même. Ils n'occupent pas beaucoup d'espace disque.
- **Personnaliser les composants sélectionnés :** cette option permet de personnaliser les composants que vous avez choisi d'installer. Avant de la sélectionner, vous devez choisir les composants à installer.

Authentification : spécifiez un utilisateur et un mot de passe disposant de droits suffisants dans eDirectory pour prolonger le schéma. Indiquez le nom d'utilisateur au format LDAP. Par exemple, `cn=idmadmin,o=company`

6. Activez Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 8, « Activation des produits Novell Identity Manager », page 75.
7. Créez et configurez vos objets de pilotes. Ces informations figurent dans le guide de chaque pilote. Pour plus d'informations, reportez-vous à la documentation des pilotes Identity Manager (http://www.novell.com/documentation/idm40drivers/).

7.5.1 Installation non-root du serveur méta-annuaire

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

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

- **Chargeur distant :** utilisez le chargeur distant Java si vous devez installer le chargeur distant en tant qu'utilisateur non-`root`. Pour plus d'informations, reportez-vous à la Section 7.6.5, « Installation du chargeur distant Java sous UNIX ou Linux », page 70.
- **Pilote du compte UNIX/Linux :** nécessite des privilèges `root` pour fonctionner.

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

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

1. Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au Chapitre 5, « Où se procurer Identity Manager », page 43.
2. Installez eDirectory 8.8.6 ou version ultérieure en tant qu'utilisateur non-`root`. Pour plus d'informations, reportez-vous à la section « Installation d'eDirectory 8.8.6 par un utilisateur non-root » (http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs).
3. Loguez-vous sous l'identité de l'utilisateur non-`root` employé pour installer eDirectory.

   Vous devez installer Identity Manager avec la même identité que celle employée pour installer la version non-`root` d'eDirectory. L'utilisateur qui installe Identity Manager doit disposer d'un accès en écriture aux répertoires et aux fichiers de l'installation non-`root` d'eDirectory.
4. Exécutez le programme d'installation pour votre plate-forme.

   Linux : `IDM4.0.1_Lin/products/IDM/linux/setup/idm-nonroot-install`

   Solaris : `IDM4.0.1_Solaris/products/IDM/solaris/setup/idm-nonroot-install`
5. Les informations suivantes permettent de terminer l'installation :

   Répertoire de base de l'installation non-root d'eDirectory : indiquez le répertoire dans lequel se trouve l'installation non-`root` d'eDirectory. Par exemple, `/home/user/install/eDirectory`.

   Étendre le schéma eDirectory : s'il s'agit du premier serveur Identity Manager installé dans cette instance d'eDirectory, entrez `Y` pour étendre le schéma. Si le schéma ne peut pas être étendu, Identity Manager ne fonctionnera pas.

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

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

   Exécutez le programme `/opt/novell/eDirectory/bin/idm-install-schema` pour étendre le schéma sur d'autres instances d'eDirectory une fois l'installation terminée.

   Utilitaires : (facultatif) si vous avez besoin d'un utilitaire de pilote Identity Manager, vous devez copier les utilitaires du support d'installation d'Identity Manager sur le serveur Identity Manager. Tous les utilitaires se trouvent dans le répertoire `IDM4.0.1_`*`platform`*`/product/IDM/`*`platform`*`/setup/utilities`.
6. Activez Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 8, « Activation des produits Novell Identity Manager », page 75.
7. Créez et configurez les objets de pilote. Ces informations figurent dans le guide de chaque pilote. Pour plus d'informations, reportez-vous à la documentation des pilotes Identity Manager (http://www.novell.com/documentation/idm40drivers/).

7.5.2 Installation en mode silencieux du serveur méta-annuaire

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

- **Linux :** `IDM4.0.1_Lin/products/IDM/linux/setup/silent.properties`
- **Solaris :** `IDM4.0.1_Solaris/products/IDM/solaris/setup/silent.properties`
- **Windows :** `IDM4.0.1_Win:\products\IDM\windows\setup\silent.properties`

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

- **Linux :** `IDM4.0.1_Lin/products/IDM/install.bin -i silent -f <nom_fichier>.properties`
- **Solaris :** `IDM4.0.1_Solaris/products/IDM/install.bin -i silent -f <nom_fichier>.properties`
- **Windows :** `IDM4.0.1_Win:\products\IDM\windows\setup\idm_install.exe -i silent -f <nom_fichier>.properties`

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

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

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

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

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

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

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

7.6 Installation du chargeur distant

Le chargeur distant élargit les possibilités d'Identity Manager en permettant au pilote d'accéder au système connecté sans que le coffre-fort d'identité et le serveur méta-annuaire soient installés sur le même serveur que le système connecté. Dans le cadre de la planification, vous devez décider si vous voulez ou non utiliser le chargeur distant. Pour plus d'informations sur la procédure de planification, reportez-vous au Chapitre 3, « Directives techniques », page 25.

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

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

7.6.1 Configuration requise

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

7.6.2 Pilotes pris en charge

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

- Active Directory
- Avaya PBX
- Services de collecte de données
- Texte délimité
- GroupWise (disponible uniquement pour le chargeur distant 32 bits)
- JDBC
- JMS
- LDAP
- Pilote pour Linux et UNIX
- Lotus Notes
- Passerelle système gérée
- Services de tâches manuelles
- PeopleSoft 5.2

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

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

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

7.6.3 Procédure d'installation

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

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

Pour installer le chargeur distant :

1. Vérifiez que vous respectez la configuration système listée dans le Chapitre 6, « Configuration système requise », page 47.
2. Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au Chapitre 5, « Où se procurer Identity Manager », page 43.
3. Lancez l'installation à l'aide du programme adapté à votre plate-forme.

   Linux - installation à partir de l'interface graphique : `IDM4.0.1_Lin/products/IDM/install.bin [-i gui]`

   Linux - installation à partir de la ligne de commande : `IDM4.0.1_Lin/products/IDM/install.bin -i console`

   Solaris - installation à partir de l'interface graphique : `IDM4.0.1_Solaris/products/IDM/install.bin [-i gui]`

Solaris - installation à partir de la ligne de commande : `IDM4.0.1_Solaris/products/IDM/install.bin -i console`

Windows : `IDM4.0.1_Win:\products\IDM\windows\setup\idm_install.exe`

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

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

Sélectionner les composants : choisissez le serveur et les utilitaires du système connecté pour installer le chargeur distant.

- **Serveur méta-annuaire de Novell Identity Manager :** ne choisissez cette option que si vous installez le serveur méta-annuaire. cette option nécessite que le coffre-fort d'identité soit installé sur ce serveur. Pour plus d'informations, reportez-vous à la Section 7.5, « Installation du serveur méta-annuaire », page 62.
- **Serveur de système connecté Novell Identity Manager 32 bits :** cette option ne nécessite pas l'installation du coffre-fort d'identité sur ce serveur. Elle installe la version 32 bits du service de chargeur distant sur votre serveur d'applications.
- **Serveur de système connecté Novell Identity Manager 64 bits :** cette option ne nécessite pas l'installation du coffre-fort d'identité sur ce serveur. Elle installe la version 64 bits du service de chargeur distant sur votre serveur d'applications.
- **Serveur de système connecté Novell Identity Manager (.NET) :** cette option (Windows uniquement) installe le service de chargeur distant .NET et le pilote SharePoint sur ce serveur.
- **Plug-ins Novell Identity Manager pour Identity Manager :** sélectionnez cette option si vous avez installé iManager sur ce serveur. Elle installe les plug-ins iManager pour Identity Manager.
- **Utilitaires :** cette option installe les utilitaires servant à configurer les pilotes pour les systèmes connectés. Tous les pilotes n'ont pas d'utilitaires. Si vous n'êtes pas certain d'en avoir besoin, sélectionnez-les tout de même. Ils n'occupent pas beaucoup d'espace disque.
- **Personnalisé :** sélectionnez cette option pour personnaliser les fonctions installées. Vous pouvez alors sélectionner les options listées ci-dessous. Avant de sélectionner cette option, vous devez choisir les composants à installer.
  - **Service de chargeur distant 32 bits :** service qui communique avec le serveur méta-annuaire.
  - **Service de chargeur distant 64 bits :** service qui communique avec le serveur méta-annuaire.
  - **Pilotes :** sélectionnez les fichiers de pilotes à installer. Il est recommandé d'installer tous les fichiers de pilote. Vous n'avez pas besoin d'exécuter à nouveau l'installation pour ajouter une autre instance du chargeur distant.
  - **Serveur de système connecté Novell Identity Manager (.NET) :** (Windows uniquement) installe le service de chargeur distant .NET et le pilote SharePoint.

  Les autres options doivent être sélectionnées lorsque vous sélectionnez la personnalisation pour que l'installation se poursuive.

(Windows uniquement) Emplacement d'installation pour le serveur du système connecté : indiquez le répertoire dans lequel est installé le serveur du système connecté.

(Windows uniquement) Emplacement d'installation du chargeur distant .NET : indiquez le répertoire dans lequel est installé le chargeur distant .NET.

(Windows seulement) Emplacement d'installation pour les utilitaires : indiquez le répertoire dans lequel sont installés les utilitaires.

5. Créez et configurez vos objets de pilote pour utiliser le chargeur distant. Ces informations figurent dans le guide de chaque pilote. Pour plus d'informations, reportez-vous à la documentation des pilotes Identity Manager (http://www.novell.com/documentation/idm40drivers/).
6. Créez un fichier de configuration de chargeur distant pour travailler avec votre système connecté. Pour plus d'informations, reportez-vous à la section « Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File » (Configuration du chargeur distant pour Linux/UNIX en créant un fichier de configuration) du manuel *Identity Manager 4.0.1 Remote Loader Guide* (Guide du chargeur distant d'Identity Manager 4.0).

7.6.4 Installation silencieuse du chargeur distant

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

- **Linux :** `IDM4.0.1_Lin/products/IDM/linux/setup/silent.properties`
- **Solaris :** `IDM4.0.1_Solaris/products/IDM/solaris/setup/silent.properties`
- **Windows :** `IDM4.0.1_Win:\products\IDM\windows\setup\silent.properties`

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

- **Linux :** `IDM4.0.1_Lin/products/IDM/install.bin -i silent -f <nom_fichier>.properties`
- **Solaris :** `IDM4.0.1_Solaris/products/IDM/install.bin -i silent -f <nom_fichier>.properties`
- **Windows :** `IDM4.0.1_Win:\products\IDM\windows\setup\idm_install.exe -i silent -f <nom_fichier>.properties`

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

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

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

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

7.6.5 Installation du chargeur distant Java sous UNIX ou Linux

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

1. Vérifiez que le JDK/JRE 1.5.x de Java est disponible sur le système hôte.
2. Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au Chapitre 5, « Où se procurer Identity Manager », page 43.
3. Recherchez les fichiers d'installation du chargeur distant Java sur le support d'Identity Manager :

   Linux : `IDM4.0.1_Lin/products/IDM/java_remoteloader`

   Solaris : `IDM4.0.1_Solaris/products/IDM/java_remoteloader`
4. Copiez le fichier `dirxml_jremote_dev.tar.gz` à l'emplacement souhaité sur le serveur distant.
5. Copiez le fichier `dirxml_jremote.tar.gz` ou `dirxml_jremote_mvs.tar` à l'emplacement souhaité sur le serveur distant.

   Par exemple : `/usr/idm`

   Pour plus d'informations sur mvs, décompressez le fichier `dirxml_jremote_mvs.tar`, puis reportez-vous au document `usage.html`.
6. Décompressez et extrayez les fichiers `dirxml_jremote.tar.gz` et `dirxml_jremote_dev.tar.gz`.

   Par exemple : `gunzip dirxml_jremote.tar.gz` ou `tar -xvf dirxml_jremote_dev.tar`
7. Copiez les fichiers `.jar` du module d'interface d'application dans le sous-répertoire `lib` créé lors de l'extraction du fichier `dirxml_jremote.tar`.

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

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

8 Personnalisez le script `dirxml_jremote` en effectuant l'une des opérations suivantes :

- Vérifiez que l'exécutable Java peut être atteint via la variable d'environnement PATH en définissant la variable d'environnement RDXML_PATH. Saisissez les commandes suivantes pour définir la variable d'environnement :
  1. `set RDXML_PATH=path`
  2. `export RDXML_PATH`
- Modifiez le script `dirxml_jremote` et préfixez la ligne de script exécutant Java avec le chemin vers l'exécutable Java.

9 Configurez le fichier d'exemple `config8000.txt` à utiliser avec votre module d'interface d'application. Pour plus d'informations, reportez-vous à la section « Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File » (Configuration du chargeur distant pour Linux/UNIX en créant un fichier de configuration) du manuel *Identity Manager 4.0.1 Remote Loader Guide* (Guide du chargeur distant d'Identity Manager 4.0).

7.6.6 Coexistence de chargeurs distants 32 et 64 bits

Identity Manager 4.0.1 permet à des chargeurs distants 32 et 64 bits de coexister sur un système d'exploitation 64 bits. Si vous mettez à niveau un chargeur distant 32 bits installé sur un système d'exploitation 64 bits, il est mis à niveau et un chargeur distant 64 bits est également installé. Vous pouvez avoir un chargeur distant 32 bits et un chargeur distant 64 bits sur la même machine.

Si vous choisissez d'héberger les chargeurs distants 32 et 64 bits sur la même machine, les événements d'audit sont uniquement générés avec le chargeur distant 64 bits. Si un chargeur distant 64 bits est installé avant un chargeur distant 32 bits, les événements sont consignés dans le fichier lcache 32 bits.

7.7 Installation des fichiers de pilote

Vous pouvez installer les fichiers de pilote sans le serveur méta-annuaire ou le chargeur distant. Ces fichiers contiennent des modules d'interface pilote et les utilitaires de pilote.

Pour installer les fichiers de pilote :

1 Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au Chapitre 5, « Où se procurer Identity Manager », page 43.

2 Lancez l'installation à l'aide du programme adapté à votre plate-forme.

Linux - installation à partir de l'interface graphique : `IDM4.0.1_Lin/products/IDM/install.bin [-i gui]`

Linux - installation à partir de la ligne de commande : `IDM4.0.1_Lin/products/IDM/install.bin -i console`

Solaris - installation à partir de l'interface graphique : `IDM4.0.1_Solaris/products/IDM/install.bin [-i gui]`

Solaris - installation à partir de la ligne de commande : `IDM4.0.1_Solaris/products/IDM/install.bin -i console`

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

Windows : `IDM4.0.1_Win:\products\IDM\windows\setup\idm_install.exe`

3. Lisez et acceptez l'accord de licence, puis cliquez sur *Suivant*.
4. Dans la page Sélectionner les composants, spécifiez les options suivantes :

   Serveur méta-annuaire de Novell Identity Manager : vous pouvez sélectionner cette option ou celle nommée *Serveur de système connecté*. Il n'est pas nécessaire de sélectionner les deux.

   Les fichiers de pilote sont inclus avec cette option.

   Serveur système Novell Identity Manager connecté : vous pouvez sélectionner cette option ou celle nommée *Serveur méta-annuaire*. Il n'est pas nécessaire de sélectionner les deux.

   Les fichiers de pilote sont inclus avec cette option.

   Utilitaires Novell : sélectionnez cette option pour installer des utilitaires qui aident à configurer certains pilotes.

   Personnaliser les composants sélectionnés : cette option vous permet d'installer les fichiers de pilote sans le serveur méta-annuaire ou le chargeur distant.
5. Cliquez sur *Suivant*.
6. Désélectionnez les options *Moteur méta-annuaire* et *Service du chargeur distant*.
7. Vérifiez que l'option *Pilotes* est sélectionnée sous *Serveur méta-annuaire* ou *Serveur de système connecté*.

   Vous pouvez développer l'option *Pilotes* et sélectionner uniquement les pilotes que vous souhaitez installer. Par défaut, tous les pilotes sont sélectionnés.
8. Cliquez sur *Suivant*.
9. Dans la page *Authentification*, spécifiez le nom et le mot de passe d'un utilisateur disposant de droits suffisants dans eDirectory pour étendre le schéma. Indiquez le nom d'utilisateur au format LDAP. Par exemple, `cn=idmadmin,o=company`
10. Cliquez sur *Suivant*.
11. Vérifiez le résumé de l'installation, puis cliquez sur *Suivant*.
12. Lisez le message de fin d'installation, puis cliquez sur *Terminé*.

Les fichiers des pilotes sont à présent installés avec le chargeur distant ou le serveur méta-annuaire.

7.8 Installation du module de provisioning basé sur les rôles

Pour installer le module de provisioning basé sur les rôles, reportez-vous au *Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0.1*.

7.9 Installation d'un pilote personnalisé

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

7.10 Installation de l'administrateur de l'assignation de rôles

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

Remarque : l'administrateur de l'assignation de rôles n'est pas disponible avec la version Standard Edition.

Pour installer l'administrateur d'assignation de rôles :

1. Assurez-vous que vous avez téléchargé tous les fichiers Identity Manager nécessaires depuis le site Web de téléchargement Novell. Pour plus d'informations, reportez-vous au Chapitre 5, « Où se procurer Identity Manager », page 43.
2. Recherchez le fichier d'installation de l'administrateur d'assignation de rôles sur le support d'Identity Manager situé ici :

   Linux : `IDM4.0.1_Lin/products/RMA/IDMRMAP.jar`

   Windows : `IDM4.0.1_Win:\products\RMA\IDMRMAP.jar`
3. Accédez au répertoire d'installation de l'administrateur d'assignation de rôles à partir d'une ligne de commande, puis saisissez `java -jar IDMRMAP.jar`.

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

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

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

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

Une fois l'administrateur d'assignation de rôles installé et démarré, vous devez le configurer. Pour plus d'informations sur la configuration, reportez-vous à la section « Configuring the Application » (Configuration de l'application) du manuel *Identity Manager Role Mapping Administrator 4.0.1 Installation and Configuration Guide* (Guide d'installation et de configuration de la version 4.0.1 de l'administrateur d'assignation de rôles).

7.11 Installation du module Identity Reporting ou de Sentinel

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

Pour plus d'informations sur l'installation et la configuration du module Identity Reporting, reportez-vous au manuel *Identity Reporting Module Guide* (Guide du module Identity Reporting). Pour obtenir des informations de configuration concernant Sentinel avec Identity Manager, reportez-vous au manuel *Identity Manager 4.0.1 Reporting Guide for Novell Sentinel* (Guide de création de rapports d'Identity Manager 4.0 pour Novell Sentinel). Pour plus d'informations sur la configuration système requise pour Sentinel, reportez-vous au *Guide d'installation de Novell Sentinel* (http://www.novell.com/documentation/sentinel6/index.html).

Activation des produits Novell Identity Manager

8

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

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

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

8.1 Achat d'une licence de produit Identity Manager

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

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

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 accéder à ce site.
2. Cliquez sur le lien de téléchargement de licence et effectuez l'une des opérations suivantes :
   - Enregistrez le fichier de référence d'activation 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-----).

  Avertissement : si l'activation Standard Edition est appliquée à un système Advanced Edition non activé existant, elle arrête les pilotes et le serveur méta-annuaire Identity Manager.

  ---

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 à utiliser. Vous pouvez activer n'importe quelle arborescence avec la référence.

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

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

1. Ouvrez iManager.
2. Cliquez sur *Identity Manager > Présentation d'Identity Manager.*
3. Cliquez sur pour rechercher et sélectionner un ensemble de pilotes dans l'arborescence, puis sur pour exécuter la recherche.
4. Sur la page Présentation d'Identity Manager, cliquez sur l'ensemble de pilotes pour lequel afficher les informations d'activation.

5 Sur la page Présentation de l'ensemble des pilotes, cliquez sur *Activation* > *Information*.

Vous pouvez afficher le texte de la référence d'activation ou, si une erreur est signalée, vous pouvez supprimer une référence d'activation.

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

8.4 Activation des pilotes Identity Manager

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

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

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

Vous devez effectuer les étapes décrites à la Section 8.2, « Installation d'une référence d'activation de produit », page 75 pour chaque module afin d'activer les pilotes.

8.5 Activation d'Analyzer

Lors du premier démarrage d'Analyzer, vous êtes invité à l'activer. Si vous ne l'activez pas, vous ne pouvez pas utiliser Analyzer. Pour plus d'informations, reportez-vous à la section « Activating Analyzer » (Activation d'Analyzer) dans le manuel *Analyzer 4.0.1 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 1.2 pour Identity Manager).

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

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

Dépannage d'Identity Manager

9

Les informations suivantes sont utiles lorsque vous installez Identity Manager :

- « Problème lié au pilote Lotus Notes lors de l'installation d'Identity Manager » page 79
- « L'installation d'Identity Manager peut parfois échouer sur la plate-forme Windows 2008 SP2 32 bits » page 79
- « Lorsque deux événements interviennent au niveau de l'attribut stream de syntaxe, la première modification de l'attribut est perdue » page 83
- « Problème de processus lcache lors de la mise à niveau d'Identity Manager » page 83
- « La mise à niveau d'Identity Manager nécessite l'utilisation du compte Administrateur adéquat pour éviter la perte des réponses de vérification d'identité » page 83

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

Source : Sous Solaris 10, le message d'erreur de pilote Lotus Notes suivant peut s'afficher lors de l'installation d'Identity Manager 4.0.1 en tant qu'utilisateur non-`root` :

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

Action : Créez manuellement les liens symboliques. Pour plus d'informations sur la vérification et la recréation des liens symboliques, reportez-vous à la section « Troubleshooting Installation Problems » (Dépannage des problèmes d'installation) du manuel *Identity Manager 4.0.1 Driver for Lotus Notes Implementation Guide* (Guide de mise en oeuvre du pilote Identity Manager 4.0 pour Lotus Notes).

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

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

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

Action : Pour contourner ce problème :

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

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

2 Étendez le schéma Identity Manager à l'aide d'iManager en utilisant l'*assistant Importation/Conversion/Exportation* sous *Maintenance d'eDirectory*.

3 Créez les objets par défaut à l'aide du fichier LDIF.

- Fichier LDIF de stratégie de mot de passe par défaut

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

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

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

- Fichier LDIF de stratégie de collection de notification par défaut

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

dn: cn=Password Expiration Notification,cn=Default
Notification Collection,cn=Security
notfMergeTemplateSubject: Password Expiration
Notification
notfMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbGwuY29tL
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4gDQo8Zm9ybTp0b2tlbi1kZX
NjcmlwdGlvbnM+IA0KPGZvcm06dG9rZW4tZGVzY3JpcHRpb24gZGV
zY3JpcHRpb249IkZ1bGwgbmFtZSBieSB3aGljaCB0byBhZGRyZXNz
IHVzZXIiIGl0ZW0tbmFtZT0iVXNlckZ1bGxOYW1lIi8+IA0KPGZvc
m06dG9rZW4tZGVzY3JpcHRpb24gZGVzY3JpcHRpb249Ik51bWJlci
BvZiBkYXlzIHVudGlsIHBhc3N3b3JkIGV4cGlyZXMiIGl0ZW0tbmF
tZT0iRXhwRGF5cyIvPiANCjwvZm9ybTp0b2tlbi1kZXNjcmlwdGlv
bnM+IA0KPGhlYWQ+IA0KPHRpdGxlPlBhc3N3b3JkIEV4cGlyYXRpb
24gTm90aWZpY2F0aW9uPC90aXRsZT4gDQo8c3R5bGU+IA0KPCEtLS
Bib2R5IHsgZm9udC1mYW1pbHk6IFRyZWJ1Y2hldCBNUyB9IC0tPiA
NCjwvc3R5bGU+IA0KPC9oZWFkPiANCjxib2R5IEJHQ09MT1I9IiNG
RkZGRkYiPiANCjxwPkRlYXIgJFVzZXJGdWxsTmFtZSQsPC9wPiANC
jxwPlRoaXMgbWVzc2FnZSBpcyB0byBpbmZvcm0geW91IHRoYXQgeW
91ciBwYXNzd29yZCB3aWxsIGV4cGlyZSBpbjwvcD4gDQo8YnIvPiA
NCiAgJEV4cERheXMkIGRheXM8YnIvPiANCjxici8+IA0KPHA+UGxl
YXNlIHBsYW4gdG8gY2hhbmdlIHlvdXIgcGFzc3dvcmQgYmVmb3JlI
Gl0IGV4cGlyZXMuPC9wPiANCjxwPiAtIEF1dG9tYXRlZCBTZWN1cm
l0eSAtIDwvcD4gDQo8cD4gPC9wPiANCjwvYm9keT4gDQo8L2h0bWw
iIFNSQz0iY2lkOnBvd2VyZWRfYnlfbm92ZWxsLmdpZiIg
```

```
aGVpZ2h0PSIyOSIgd2lkdGg9IjgwIi8+IA0KPC9wPiANCjwvYm9ke
T4gDQo8L2h0bWw+IA0K
objectClass: notfMergeTemplate
objectClass: Top
cn: Password Expiration Notification

dn: cn=Password Reset Fail,cn=Default Notification
Collection,cn=Security
notfMergeTemplateSubject: Notice of Password Reset
Failure
notfMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbGwuY29tL
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvcm06dG9rZW4tZG
VzY3JpcHRpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9
uIGl0ZW0tbmFtZT0iVXNlckZ1bGxOYW1lIiBkZXNjcmlwdGlvbj0i
VGhlIHVzZXIncyBmdWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2tlb
i1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVzZXJHaXZlbk5hbWUiIG
Rlc2NyaXB0aW9uPSJUaGUgdXNlcidzIGdpdmVuIG5hbWdDT0xPUj0
iI0ZGRkZGRiI+DQogIDxwPkRlYXIgJFVzZXJGdWxsTmFtZSQsPC9w
Pg0KICA8cD5UaGlzIGlzIGEgbm90aWNlIHRoYXQgeW91ciBwYXNzd
29yZCBjb3VsZCBub3QgYmUgcmVzZXQgaW4gdGhlICRDb25uZWN0ZW
RTeXN0ZW1OYW1lJCBzeXN0ZW0uLiAgVGhlIHJlYXNvbiBmb3IgZmF
pbHVyZSBpcyBpbmRpY2F0ZWQgYmVsb3c6PC9wPg0KICA8cD5SZWFz
b246ICRGYWlsdXJlUmVhc29uJDwvcD4NCiAgPHA+SWYgeW91IGhhd
mUgYW55IGZ1cnRoZXIgcXVlc3Rpb25zLA0KICBwbGVhc2UgY2
udGFjdCB0aGUgaGVscCBkZXNrIGF0ICgwMTIpIDM0NS02Nzg5IG9
yIGVtYWlsDQogICAgIGF0IDxhIGhyZWY9Im1haWx0bzpoZWxwLmRl
c2tAbXljb21wYW55LmNvbSI+DQogICAgIGhlbHAuZGVza0BteWNvb
XBhbnkuY29tIDwvYT48L3A+DQogIDxwPiAtIEF1dG9tYXRlZCBTZW
N1cml0eTwvcD4NCiAgPHA+PGltZyBTUkM9ImNpZDpwb3dlcmVkX2J
5X25vdmVsbC5naWYiIEFMVD0iUG93ZXJlZCBieSBOb3ZlbGwiIHdp
ZHRoPSI4MCIgaGVpZ2h0PSIyOSIvPjwvcD4NCjwvYm9keT4NCjwva
HRtbD4NCg==
objectClass: notfMergeTemplate
objectClass: Top
cn: Password Reset Fail

dn: cn=Password Set Fail,cn=Default Notification
Collection,cn=Security
notfMergeTemplateSubject: Notice of Password Set
Failure
notfMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbGwuY29tL
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvcm06dG9rZW4tZG
VzY3JpcHRpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9
uIGl0ZW0tbmFtZT0iVXNlckZ1bGxOYW1lIiBkZXNjcmlwdGlvbj0i
VGhlIHVzZXIncyBmdWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2tlb
i1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVzZXJHaXZlbk5hbWUiIG
Rlc2NyaXB0aW9uPSJUaGUgdXNlcidzIGdpdmVuIG5hbWUiLz4NCiA
gICA8Zm9ybTp0b2tlbi1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVz
ZXJMYXN0TmFtZSIgZGVzY3JpcHRpb249IlRoZSB1c2VyJ3MgbGFzd
CBuYW1lIi8+DQogICAgPGZvcm06dG9rZW4tZGVzY3JpcHRpb24gaX
RlbS1uYW1lPSJDb25uZWN0ZWRTeXN0ZW1OYW1lIiBkZXNjcmlwdGl
vbj0iVGhlIGV4dGVybmFsIGFwcGxpY2F0b24gbmFtZSIvPg0KICAg
IDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmFtZT0iRmFpb
HVyZVJlYXNvbiIgZGVzY3JpcHRpb249IlRoZSBmYWlsdXJlIHJlYX
NvbiIvPg0KICA8L2Zvcm06dG9rZW4tZGVzY3JpcHRpb25zPg0KPGh
lYWQ+DQogIDx0aXRsZT5Ob3RpY2Ugb2YgUGFzc3dvcmQgU2V0IEZh
aWx1cmU8L3RpdGxlPg0KICA8c3R5bGU+IDwhLS0gYm9keSB7IGZvb
```

```
nQtZmFtaWx5OiBUcmVidWNoZXQgTVMgfSAtLT4gPC9zdHlsZT4NCj
wvaGVhZD4NCjxib2R5IEJHQ09MT1I9IiNGRkZGRkYiPg0KPHA+RGV
hciAkVXNlckZ1bGxOYW1lJCw8L3A+DQogIDxwPlRoaXMgaXMgYSBu
b3RpY2UgdGhhdCB5b3VyIHBhc3N3b3JkIGNvdWxkIG5vdCBiZSBzZ
XQgaW4gdGhlICRDb25uZWN0ZWRTeXN0ZW1OYW1lJCBzeXN0ZW0uLi
AgVGhlIHJlYXNvbiBmb3IgZmFpbHVyZSBpcyBpbmRpY2F0ZWQgYmV
sb3c6PC9wPg0KICA8cD5SZWFzb246ICRGYWlsdXJlUmVhc29uJDwv
cD4NCiAgPHA+W91IGhhdmUgYW55IGZ1cnRoZXIgcXVlc3Rpb
25zLA0KICAgICBwbGVhc2UgY29udGFjdCB0aGUgaGVscCBkZXNrIG
F0ICgwMTIpIDM0NS02Nzg5IG9yIGVtYWlsDQogICAgIGF0IDxhIGh
yZWY9Im1haWx0bzpoZWxwLmRlc2tAbXljb21wYW55LmNvbSI+DQog
ICAgIGhlbHAuZGVza0BteWNvbXBhbnkuY29tIDwvYT48L3A+DQogI
DxwPiAtIEF1dG9tYXRlZCBTZWN1cml0eTwvcD4NCiAgPHA+PGltZy
BTUkM9ImNpZDpwb3dlcmVkX2J5X25vdmVsbC5naWYiIEFMVD0iUG9
3ZXJlZCBieSBOb3ZlbGwiIHdpZHRoPSI4MCIgaGVpZ2h0PSIyOSIv
PjwvcD4NCjwvYm9keT4NCjwvaHRtbD4NCg==
objectClass: notfMergeTemplate
objectClass: Top
cn: Password Set Fail

dn: cn=Password Sync Fail,cn=Default Notification
Collection,cn=Security
notfMergeTemplateSubject: Notice of Password
Synchronization Failure
notfMergeTemplateData::
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbGwuY29tL
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvcm06dG9rZW4tZG
VzY3JpcHRpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9
uIGl0ZW0tbmFtZT0iVXNlckZ1bGxOYW1lIiBkZXNjcmlwdGlvbj0i
VGhlIHVzZXIncyBmdWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2tlb
i1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVzZXJHaXZlbk5hbWUiIG
Rlc2NyaXB0aW9uPSJUaGUgdXNlcidzIGdpdmVuIG5hbWUiLz4NCiA
gICA8Zm9ybTp0b2tlbi1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVz
ZXJMYXN0TmFtZSIgZGVzY3JpcHRpb249IlRoZSB1c2VyJ3MgbGFzd
CBuYW1lIi8+DQogICAgPGZvcm06dG9rZW4tZGVzY3JpcHRpb24gaX
RlbS1uYW1lPSJDb25uZWN0ZWRTeXN0ZW1OYW1lIiBkZXNjcmlwdGl
vbj0iVGhlIGV4dGVybmFsIGFwcGxpY2F0b24gbmFtZSIvPg0KICAg
IDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmFtZT0iRmFpb
HVyZVJlYXNvbiIgZGVzY3JpcHRpb249IlRoZSBmYWlsdXJlIHJlYX
NvbiIvPg0KICA8L2Zvcm06dG9rZW4tZGVzY3JpcHRpb25zPg0KPGh
lYWQ+DQogIDx0aXRsZT5Ob3RpY2UgdGhhdCB5b3VyIHBhc3N3b3Jk
IGNvdWxkIG5vdCBiZSBzZXQgYWN0aXZlIGRpcmVjdG9yeSBiZWNhd
XNlIGEgcGFzc3dvcmQgZG9lc24ndCBtZWV0IHRoZSBjdXJyZW50IG
RpcmVjdG9yeSBwYXNzd29yZCBwb2xpY3kgcmVxdWlyZW1lbnRzLiA
gUGxlYXNlIGNvbm5lY3RlZFN5c3RlbU5hbWUkIHdhcyB1bmFibG
UgdG8gc3luY2hyb25pemUgdG8gb3RoZXIgY29ubmVjdGVkIHN5c3R
lbXMuICBUaGUgcmVhc29uIGZvciBmYWlsdXJlIGlzIGluZGljYXRl
ZCBiZWxvdzo8L3A+DQogIDxwPlJlYXNvbjogJEZhaWx1cmVSZWFzb
24kPC9wPg0KICA8cD5JZiB5b3UgaGF2ZSBhbnkgZnVydGhlciBxdW
VzdGlvbnMsIHBsZWFzZSBjb250YWN0IHRoZSBoZWxwIGRlc2sgYXQ
gKDAxMikNCiAgICAgMzQ1LTY3ODkgb3IgZW1haWwgYXQgPGEgaHJl
Zj0ibWFpbHRvOmhlbHAuZGVza0BteWNvbXBhbnkuY29tIj4NCiAgI
CAgaGVscC5kZXNrQG15Y29tcGFueS5jb20gPC9hPjwvcD4NCiAgPH
```

```
A+IC0gQXV0b21hdGVkIFNlY3VyaXR5PC9wPg0KICA8cD48aW1nIFN
SQz0iY2lkOnBvd2VyZWRfYnlfbm92ZWxsLmdpZiIgQUxUPSJQb3dl
cmVkIGJ5IE5vdmVsbCIgd2lkdGg9IjgwIiBoZWlnaHQ9IjI5Ii8+P
C9wPg0KPC9ib2R5Pg0KPC9odG1sPg0K
objectClass: notfMergeTemplate
objectClass: Top
cn: Password Sync Fail
```

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

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

Lorsque deux événements interviennent au niveau de l'attribut stream de syntaxe, la première modification de l'attribut est perdue

Source : Le moteur Identity Manager 4.0.1 ne conserve pas les attributs STREAM et OCTET_STRING dans le cache. Lorsqu'un événement est synchronisé avec le système connecté, le moteur lit ces attributs à partir du coffre-fort d'identité et met à jour le système connecté. Si ces attributs sont modifiés avant que le moteur les lise à partir du coffre-fort d'identité, la valeur changée est mise à jour au niveau du système connecté et la modification intermédiaire risque d'être perdue.

Action : Si l'attribut change régulièrement, utilisez une syntaxe appropriée autre que SYN_STREAM.

Par exemple, si un objet XML est stocké dans l'attribut STREAM, utilisez la syntaxe XMLData au lieu de SYN_STREAM.

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

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

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

La mise à niveau d'Identity Manager nécessite l'utilisation du compte Administrateur adéquat pour éviter la perte des réponses de vérification d'identité

Source : Lors de la mise à niveau depuis une version antérieure d'Identity Manager sur une plate-forme Windows, utilisez le même compte Administrateur que lors de l'installation d'eDirectory.

Explication : Par exemple, si un compte Administrateur de domaine a été utilisé pour installer eDirectory, employez ce même compte pour l'installation d'Identity Manager, et pas un compte Administrateur local.

Action : Si vous n'utilisez pas le même compte Administrateur, les réponses de vérification d'identité des utilisateurs ne seront plus accessibles. En effet, en raison de l'utilisation d'un autre compte Administrateur, la clé de l'arborescence est recréée lors de l'installation et cette nouvelle clé ne permet pas d'accéder aux réponses stockées. Les utilisateurs sont alors invités à fournir de nouvelles réponses lorsqu'ils se loguent.

Nouveautés

10

Identity Manager 4.0.1 comporte plusieurs améliorations et nouvelles fonctions :

- Section 10.1, « Nouveautés d'Identity Manager 4.0.1 », page 85
- Section 10.2, « Nouveautés d'Identity Manager 4.0 », page 86

10.1 Nouveautés d'Identity Manager 4.0.1

- Section 10.1.1, « Identity Manager Advanced Edition et Standard Edition », page 85
- Section 10.1.2, « Télémétrie », page 85
- Section 10.1.3, « Activité de requête de ressource », page 85
- Section 10.1.4, « Nouveaux rapports ajoutés au module Identity Reporting », page 86
- Section 10.1.5, « Applications ajoutées à la palette de Designer », page 86

10.1.1 Identity Manager Advanced Edition et Standard Edition

Afin de répondre aux différents besoins des clients, Identity Manager 4.0.1 est proposé en deux versions, à savoir Advanced Edition et Standard Edition. La version Advanced Edition comporte un éventail complet de fonctions pour le provisioning des utilisateurs en entreprise. La version Standard Edition intègre une partie des fonctions disponibles dans Identity Manager Advanced Edition, en plus de toutes les fonctions qui étaient déjà présentes dans les versions précédentes d'Identity Manager. Pour une comparaison des fonctions proposées par les versions Standard et Advanced Edition d'Identity Manager, reportez-vous à la comparaison des versions d'Identity Manager (http://www.novell.com/products/identitymanager/features/identitymanager-version-comparison.html).

10.1.2 Télémétrie

La télémétrie Identity Manager est une nouvelle tâche introduite dans Identity Manager 4.0.1. Elle fonctionne comme un compteur d'utilisation ou un outil de contrôle des licences qui facilite le travail des clients Identity Manager en leur permettant d'ajouter des licences nécessaires ou d'en supprimer des superflues. Les clients peuvent également bénéficier d'avantages tels que le tarif pour les comptes utilisateur inactifs.

10.1.3 Activité de requête de ressource

L'activité de requête de ressource vous permet d'automatiser l'octroi ou la révocation de ressources pour les utilisateurs. Par exemple, vous pouvez créer une définition de requête de provisioning qui provisionne toutes les ressources dont un nouvel employé a besoin le jour de son arrivée. L'activité de requête de ressource peut aussi être utilisée afin d'automatiser l'approbation de cet employé pour des ressources déterminées. Pour plus d'informations sur l'activité de requête de ressource, reportez-vous à la section « *Resource Request Activity* » (Activité de requête de ressource) du manuel *User Application: Design Guide* (Guide de conception de l'application utilisateur).

10.1.4 Nouveaux rapports ajoutés au module Identity Reporting

Les rapports suivants ont été ajoutés :

- **Modification de l'état de l'utilisateur dans le coffre-fort d'identité :** affiche les événements importants pour les utilisateurs du coffre-fort d'identité.
- **Modifications de mot de passe utilisateur dans le coffre-fort d'identité :** affiche toutes les modifications de mot de passe utilisateur dans le coffre-fort d'identité.
- **Demandes d'accès par destinataire :** affiche les processus de workflow d'assignation de ressource organisés par destinataire.
- **Demandes d'accès par demandeur :** affiche les processus de workflow d'assignation de ressource organisés par demandeur.
- **Demandes d'accès par ressource :** affiche les processus de workflow d'assignation de ressource organisés par ressources.

Pour plus d'informations sur les nouveaux rapports, reportez-vous au manuel *Identity Reporting Module Guide* (Guide du module Identity Reporting).

10.1.5 Applications ajoutées à la palette de Designer

Les applications suivantes ont été ajoutées à la palette de Designer :

- Blackboard
- Google Apps
- RSA

10.2 Nouveautés d'Identity Manager 4.0

- Section 10.2.1, « Module Identity Reporting », page 86
- Section 10.2.2, « Nouveaux pilotes », page 87
- Section 10.2.3, « Prise en charge de l'audit XDAS », page 87
- Section 10.2.4, « Remplacement des fichiers de configuration de pilote par des paquetages », page 88
- Section 10.2.5, « Administrateur d'assignation de rôles », page 88
- Section 10.2.6, « Analyzer », page 88
- Section 10.2.7, « Programme d'installation intégré », page 88

10.2.1 Module Identity Reporting

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

Le module Identity Reporting nécessite deux nouveaux pilotes de service :

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

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

10.2.2 Nouveaux pilotes

Les nouveaux pilotes suivants sont fournis avec Identity Manager 4.0.1 :

- « Pilote SharePoint (chargeur distant .NET) » page 87
- « Pilote Salesforce.com » page 87

Pilote SharePoint (chargeur distant .NET)

Le pilote SharePoint pour Novell Identity Manager permet de synchroniser les événements d'adhésion utilisateur et à un groupe entre le coffre-fort d'identité et un ensemble de sites SharePoint 2007 ou 2010. Un seul pilote peut traiter ces événements pour un seul ensemble de sites, qui gère les informations d'adhésion utilisateur et à un groupe d'un ou plusieurs sites SharePoint. Pour plus d'informations, reportez-vous au manuel *Identity Manager Driver for Lotus Notes Implementation Guide* (Guide de mise en oeuvre du pilote Identity Manager 4.0.1 pour SharePoint).

Pilote Salesforce.com

Identity Manager 4.0.1 permet de provisionner et de synchroniser automatiquement des utilisateurs avec des applications nuage. Le nouveau pilote Salesforce.com pour Novell Identity Manager permet de provisionner et de déprovisionner, de façon transparente, des utilisateurs avec une application nuage Salesforce.com, ce qui garantit la cohérence des informations d'identité utilisateur entre le coffre-fort d'identité et l'application nuage. Il prend également en charge la synchronisation sécurisée des mots de passe entre le coffre-fort d'identité et le nuage Salesforce.com, de même qu'un serveur proxy authentifié et un profil utilisateur configurable pour le provisioning automatique des utilisateurs. Pour plus d'informations, reportez-vous au manuel *Identity Manager 4.0.1 Driver for Salesforce.com Implementation Guide* (Guide de mise en oeuvre du pilote Identity Manager 4.0 pour Salesforce.com).

10.2.3 Prise en charge de l'audit XDAS

Identity Manager 4.0.1 prend en charge l'audit XDAS, ce qui permet d'accroître les capacités d'audit de l'agent de la plate-forme d'audit Novell. Il utilise le schéma XDAS commun pour Identity Manager, NMAS, eDirectory et l'administrateur d'assignation de rôles. Le nouveau service d'audit prend également en charge les appenders Syslog et fichier. Pour plus d'informations, reportez-vous aux manuels *Identity Reporting Module Guide* (Guide du module Identity Reporting) et *Identity Manager 4.0.1 Reporting Guide for Novell Sentinel* (Guide de création de rapports Identity Manager 4.0 pour Novell Sentinel).

10.2.4 Remplacement des fichiers de configuration de pilote par des paquetages

Identity Manager 4.0.1 introduit des paquetages qui contiennent des blocs de construction de qualité supérieure du contenu de stratégie d'Identity Manager. Désormais, les pilotes ne sont plus créés à l'aide de fichiers de configuration de pilote, mais au moyen de paquetages. Pour plus d'informations, reportez-vous à la section « Managing the Identity Manager Content » (Gestion du contenu d'Identity Manager) du manuel *Designer 4.0.1 for Identity Manager 4.0.1 Administration Guide* (Guide d'administration de Designer 4.0 pour Identity Manager 4.0).

10.2.5 Administrateur d'assignation de rôles

L'administrateur d'assignation de rôles est un nouvel outil qui vous permet d'analyser les autorisations pouvant être octroyées au sein de vos systèmes informatiques et de les accorder. Les autorisations peuvent être octroyées non seulement par des consultants ou le personnel informatique, mais également par un analyste d'entreprise. Pour plus d'informations, reportez-vous au manuel *Novell Identity Manager Role Mapping Administrator 4.0.1 User Guide* (Guide de l'utilisateur de la version 2.0 de l'administrateur d'assignation de rôles de Novell Identity Manager).

10.2.6 Analyzer

Analyzer vous permet de diagnostiquer, de nettoyer et de préparer des données d'identité en vue de les gérer avec Identity Manager. Pour plus d'informations, reportez-vous au manuel *Analyzer 4.0.1 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 1.2 pour Identity Manager).

10.2.7 Programme d'installation intégré

Identity Manager 4.0.1 est fourni avec un programme d'installation intégré qui installe et configure tous les composants Identity Manager en une seule fois. Le programme d'installation est utilisé pour les nouvelles installations dans des environnements de taille petite à moyenne. Pour plus d'informations, reportez-vous au *Guide du programme d'installation intégré d'Identity Manager 4.0.1*.

Mise à niveau d'Identity Manager

Pour effectuer la mise à niveau des composants Identity Manager vers la version 4.0.1, utilisez les programmes d'installation spécifiques des produits. La mise à niveau de la version Standard Edition d'Identity Manager 4.0.1 vers la version Advanced Edition s'opère toutefois selon une procédure différente qui implique uniquement des changements de configuration. Dans ce cas, il n'est pas nécessaire d'exécuter le programme d'installation d'Identity Manager. Pour plus d'informations sur la mise à niveau d'Identity Manager, reportez-vous à la section « Mise à niveau » du *Guide de mise à niveau et de migration d'Identity Manager 4.0.1*.

Mise à niveau et migration

11

Avant de commencer, assurez-vous d'avoir examiné les différences entre une mise à niveau et une migration. Reportez-vous à la section « Upgrading or Migrating » (Mise à niveau ou migration) du manuel *Identity Manager 4.0.1 Upgrade and Migration Guide* (Guide de mise à niveau et de migration d'Identity Manager 4.0.1).

Désinstallation d'Identity Manager

IV

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

- Chapitre 12, « Désinstallation des composants d'Identity Manager », page 95

Désinstallation des composants d'Identity Manager

12

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

- Section 12.1, « Suppression d'objets dans eDirectory », page 95
- Section 12.2, « Désinstallation du serveur méta-annuaire », page 96
- Section 12.3, « Désinstallation du chargeur distant », page 96
- Section 12.4, « Désinstallation du module de provisioning basé sur les rôles », page 97
- Section 12.5, « Désinstallation des composants du module Identity Reporting », page 99
- Section 12.6, « Désinstallation d'iManager », page 100
- Section 12.7, « Désinstallation d'eDirectory », page 100
- Section 12.8, « Désinstallation d'Analyzer », page 101
- Section 12.9, « Désinstallation de Designer », page 101
- Section 12.10, « Désinstallation de l'administrateur d'assignation de rôles », page 102

12.1 Suppression d'objets dans eDirectory

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

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

   Pour plus d'informations, reportez-vous à la section Keeping eDirectory Healthy (Conserver la bonne santé d'eDirectory) (http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html) du *Guide d'administration de Novell eDirectory 8.8*.
2. Connectez-vous à iManager en tant qu'administrateur avec tous les droits dans l'arborescence eDirectory.
3. Sélectionnez *Partitions et répliques* > *Fusionner la partition*.
4. Naviguez jusqu'à l'objet Ensemble des pilotes qui soit l'objet racine de partition et sélectionnez-le, puis cliquez sur *OK*.
5. Attendez que la procédure de fusion soit terminée, puis cliquez sur *OK*.
6. Effacez l'objet Ensemble des pilotes.

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

7 Répétez la procédure de l'Étape 3 jusquà 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.

12.2 Désinstallation du serveur méta-annuaire

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

- Section 12.2.1, « Désinstallation sous Linux/UNIX », page 96
- Section 12.2.2, « Désinstallation sous Windows », page 96
- Section 12.2.3, « Suppression d'une installation non-root », page 96

12.2.1 Désinstallation sous Linux/UNIX

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

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

12.2.2 Désinstallation sous Windows

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

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

12.2.3 Suppression d'une installation non-root

Pour supprimer une installation non-root d'Identity Manager, vous devez exécuter le script de désinstallation sous l'identité de l'utilisateur qui l'a installé. Ce script se trouve à l'emplacement `/`*`eDirectory_Base_Directory`*`/opt/novell/eDirectory/bin/idm-uninstall`.

Le script nettoie la base de données RPM utilisateur créée lors de l'installation d'Identity Manager.

12.3 Désinstallation du chargeur distant

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

- Section 12.3.1, « Désinstallation sous Linux/UNIX », page 97
- Section 12.3.2, « Désinstallation sous Windows », page 97

12.3.1 Désinstallation sous Linux/UNIX

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

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

12.3.2 Désinstallation sous Windows

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

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

12.4 Désinstallation du module de provisioning basé sur les rôles

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

- Section 12.4.1, « Suppression des pilotes », page 97
- Section 12.4.2, « Désinstallation de l'application utilisateur », page 97
- Section 12.4.3, « Désinstallation du serveur d'applications et de la base de données », page 98

12.4.1 Suppression des pilotes

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

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

12.4.2 Désinstallation de l'application utilisateur

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

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

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

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

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

Tableau 12-1 *Serveurs d'applications et bases de données pris en charge*

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

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

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

  Pour exécuter le script, saisissez `./Uninstall_JBossPostgreSQL`.
- **Windows :** la procédure de désinstallation de JBoss et PostgreSQL est différente pour chacune des plates-formes Windows prises en charge.
  - **Windows 2003 SP2 (32 et 64 bits) :** dans le Panneau de configuration, sélectionnez *Ajouter ou supprimer des programmes* > *JBossPostgreSQL*, puis cliquez sur *Modifier/Supprimer*.

- **Windows 2008 SP1 (32 et 64 bits) :** cliquez sur *Programmes et fonctionnalités* > *JBossPostgreSQL*, puis cliquez avec le bouton droit et sélectionnez *Désinstaller*.

12.5 Désinstallation des composants du module Identity Reporting

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

- Section 12.5.1, « Suppression des pilotes de création de rapports », page 99
- Section 12.5.2, « Désinstallation du module Identity Reporting », page 99
- Section 12.5.3, « Désinstallation du service d'audit d'événements », page 99

12.5.1 Suppression des pilotes de création de rapports

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

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

12.5.2 Désinstallation du module Identity Reporting

- **Linux :** exécutez le script de désinstallation situé à l'emplacement `/opt/novell/IdentityReporting/Uninstall_Identity Reporting`.

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

12.5.3 Désinstallation du service d'audit d'événements

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

12.6 Désinstallation d'iManager

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

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

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

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

12.7 Désinstallation d'eDirectory

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

Avant de désinstaller eDirectory, répondez aux questions suivantes :

- ❑ Votre arborescence comporte-t-elle plusieurs serveurs ?

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

- ❑ Ce serveur contient-il des répliques maîtresses ?

  Si la réponse est oui, vous devez promouvoir un autre serveur de l'anneau de répliques en tant que maître avant de supprimer eDirectory. Pour plus d'informations, reportez-vous à la section « Gestion des partitions et des répliques » (http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiik.html) du *Guide d'administration d'eDirectory 8.8*.

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

  Si la réponse est oui, vous devez fusionner cette partition avec la partition parente ou ajouter une réplique de cette partition à un autre serveur et faire de ce dernier le détenteur de la réplique maîtresse. Pour plus d'informations, reportez-vous à la section « Gestion des partitions et des répliques » (http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiik.html) du *Guide d'administration d'eDirectory 8.8*.

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

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

2 Désinstallez eDirectory.

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

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

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

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

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

12.8 Désinstallation d'Analyzer

1 Assurez-vous qu'Analyzer est fermé.

2 Désinstallez Analyzer :

- **Linux :** exécutez le script de désinstallation situé à l'emplacement `<répertoire_installation>/analyzer/UninstallAnalyzer/Uninstall Analyzer for Identity Manager`.

  Pour exécuter le script, saisissez `./Uninstall\ Analyzer\ for\ Identity\ Manager`.

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

12.9 Désinstallation de Designer

1 Assurez-vous que Designer est fermé.

2 Désinstallez Designer.:

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

  Pour exécuter le script, saisissez `./Uninstall\ Designer\ for\ Identity\ Manager`.

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

12.10 Désinstallation de l'administrateur d'assignation de rôles

1. Accédez au répertoire d'installation de l'administrateur d'assignation de rôles.

   Étant donné que ce répertoire est défini lors de l'installation, il peut être différent pour chaque installation.
2. Arrêtez l'administrateur d'assignation de rôles à partir de la ligne de commande en exécutant le script `stop`
   - **Linux :** `stop.sh`

     Pour exécuter le script, saisissez `./stop.sh`
   - **Windows :** `stop.bat`
3. Exécutez le script de désinstallation à partir de la ligne de commande.
   - **Linux :** `rma-uninstall.sh [-h] [-s]`
     - `[-h]` : correspond à l'aide.
     - `[-s]` : correspond au mode silencieux.

     Pour exécuter le script, saisissez `./rma-uninstall.sh`.
   - **Windows :** `rma-uninstall.bat [-h] [-s]`
4. Supprimez le répertoire d'installation.