Guide du programme d'installation intégré

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

Novell Identity Manager 4.0.1 est un service de partage et de synchronisation de données qui permet à des applications, annuaires et bases de données de partager des informations. Il relie des informations dispersées et permet d'établir des stratégies qui régissent les mises à jour automatiques de certains systèmes en cas de changement d'identités.

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

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

Public

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

Commentaires

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

Mises à jour de la documentation

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

Documentation complémentaire

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

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

Présentation du programme d'installation intégré

1

Identity Manager 4.0.1 assure la mise en conformité efficace, ainsi qu'une réduction des coûts pour la gestion des identités et du provisioning depuis l'environnement du centre de données vers le cloud. Le programme d'installation intégré facilite le déploiement d'Identity Manager 4.0.1 pour les administrateurs et les consultants. Il s'agit d'un programme d'installation simplifié pour vous aider à configurer un système, car il ne nécessite pas d'installation individuelle de chaque composant.

1.1 Programmes d'installation intégré et autonome

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

Fonctions	Intégré	Autonome
Structure de l'arborescence	La structure de l'arborescence est prédéfinie pour correspondre à la plupart des déploiements d'Identity Manager. Pour plus d'informations sur la structure de l'arborescence, reportez-vous à la Section 2.9, « Structure du coffre-fort d'identité », page 16.	La structure de l'arborescence est personnalisable.
Installation personnalisée de pilotes	Par défaut, tous les pilotes sont installés.	L'installation personnalisée des pilotes est prise en charge.
Ensemble de pilotes	Créé en tant que partition distincte lors de la configuration du serveur méta-annuaire.	Non créé. Peut être créé manuellement à l'aide d'iManager.
Installation non-root	Non prise en charge.	L'installation non-root de certains composants est prise en charge.
Installation du plug-in iManager	Installé automatiquement.	Installé manuellement.
Dépendances	Gère automatiquement les dépendances.	Les dépendances sont gérées manuellement.
Durée de l'installation	Automatise plusieurs étapes manuelles pour configurer rapidement le système.	Nécessite généralement plus de temps.

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

Si vous créez une solution Identity Manager où vous devez installer un ou plusieurs composants Identity Manager séparément ou qui nécessite de nombreuses options personnalisées, reportez-vous au *Guide d'installation de la structure d'Identity Manager 4.0.1* pour obtenir de l'aide. Pour des instructions concernant l'installation, reportez-vous à la section « Installation » du manuel *Guide d'installation de la structure d'Identity Manager 4.0.1*.

Le programme d'installation intégré sert principalement aux nouvelles installations d'Identity Manager 4.0.1. Pour plus d'informations sur la mise à niveau d'une installation existante, reportez-vous au Chapitre 6, « Mise à niveau d'Identity Manager », page 41.

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

1.2 Configuration des pilotes

Les composants suivants d'Identity Manager 4.0.1 peuvent être installés et configurés à l'aide du programme d'installation intégré.

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

Le programme d'installation intégré configure les pilotes requis pour le module de provisioning basé sur les rôles et le module Identity Reporting. Pour configurer des périphériques supplémentaires, reportez-vous au site Web de documentation sur les pilotes Identity Manager 4.0.1 (http://www.novell.com/documentation/idm401drivers/).

1.3 Différences d'installation entre les versions Standard Edition et Advanced Edition d'Identity Manager 4.0.1

Identity Manager 4.0.1 est disponible en deux versions : Advanced Edition et Standard Edition. Il existe des fichiers ISO distincts pour chaque version. Les programmes d'installation de ces deux versions présentent quelques différences :

L'administrateur de l'assignation de rôles n'est pas fourni avec la version Standard Edition :

l'administrateur de l'assignation de rôles ne figure pas dans la liste des composants Identity Manager de la page Sélectionner les composants du programme d'installation intégré.

La configuration du pilote de passerelle de messagerie n'est pas prise en charge : vous ne pouvez pas configurer le pilote de passerelle de messagerie via le programme d'installation de la version Standard Edition.

Deux rôles supplémentaires d'administrateur de l'application utilisateur ont été ajoutés :

outre le rôle d'administrateur de l'application utilisateur, la version Standard Edition comporte les rôles d'administrateur de rapports et d'administrateur de la sécurité. Vous devez spécifier les références pour ces deux administrateurs lors de la configuration de l'application utilisateur via le programme d'installation intégré.

De nouveaux rapports ont été ajoutés au module Identity Reporting : trois nouveaux rapports ont été ajoutés au module Identity Reporting. Certains rapports relatifs à des données telles que les rôles, les ressources et les processus de workflow, ne sont pas disponibles dans la version Standard Edition. Pour plus d'informations sur les nouveaux rapports, reportez-vous à la section « Nouvelles fonctionnalités d'Identity Manager 4.0.1 » du *Guide de présentation d'Identity Manager 4.0.1*.

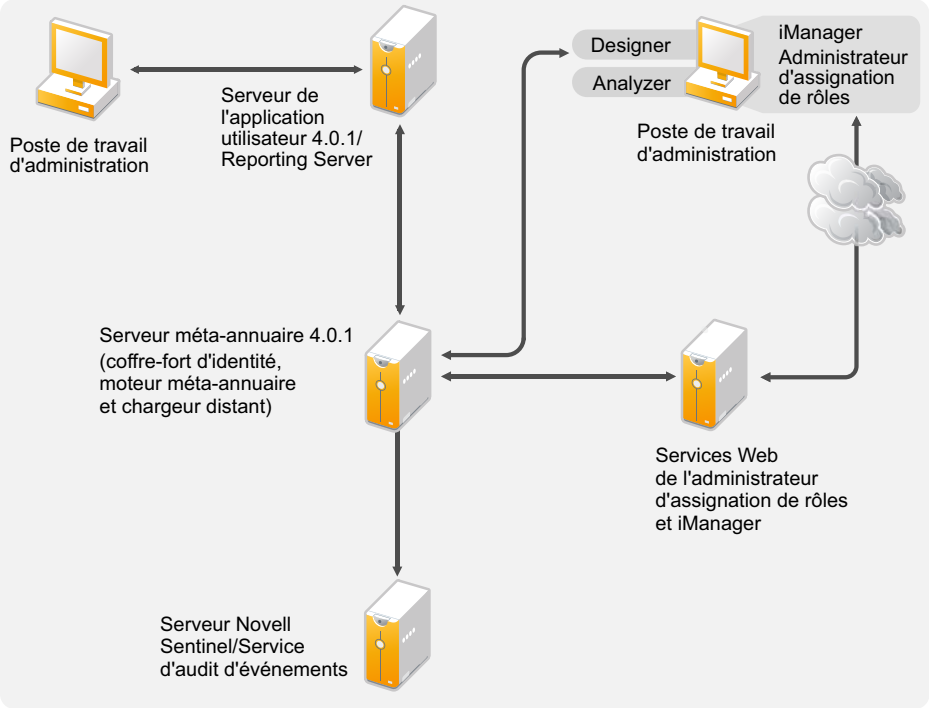
Pour plus d'informations sur l'installation d'Identity Manager, reportez-vous au Chapitre 4, « Installation d'Identity Manager », page 21.

Composants Identity Manager

2

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

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



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

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

Au cours de l'installation d'Identity Manager, le coffre-fort d'identité est automatiquement installé.

2.2 Processeurs pris en charge

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

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

- Intel x86-32
- AMD x86-32

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

- Intel EM64T
- AMD Athlon64
- AMD Opteron

Le processeur SPARC est utilisé pour le test de Solaris.

2.3 Systèmes d'exploitation du serveur

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

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

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

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. Avant d'installer Identity Manager, Novell recommande d'appliquer les derniers correctifs de système d'exploitation à l'aide du service de mise à jour automatique du fabricant.
Solaris 10 (64 bits)	Le serveur méta-annuaire s'exécute uniquement en mode 64 bits.

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

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

Remarque : Open Enterprise Server 2 n'est pas pris en charge par le programme d'installation intégré d'Identity Manager.

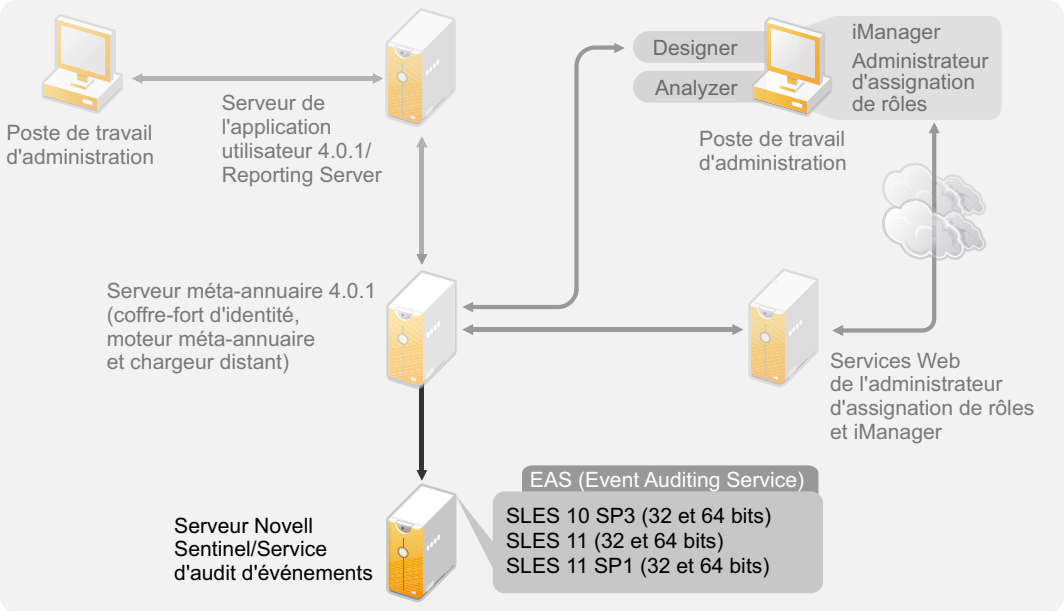
2.4 Audit et création de rapports

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

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

Le module Identity Reporting est un composant d'Identity Manager 4.0.1. Novell Sentinel n'est pas fourni avec Identity Manager, mais constitue un composant facultatif que vous pouvez ajouter à votre système Identity Manager.

Figure 2-2 *Audit et création de rapports*



Pour plus d'informations sur la configuration système requise pour le 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 plus d'informations sur la configuration système requise pour Novell Sentinel, reportez-vous au *Guide d'installation de Novell Sentinel* (http://www.novell.com/documentation/sentinel6/index.html).

2.5 Application utilisateur

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

Le module de provisioning basé sur les rôles version 4.0.1 utilise JBoss 5.1 comme serveur d'applications et PostgreSQL 8.4.3 comme base de données.

Pour connaître la configuration système requise pour l'application utilisateur, reportez-vous à la section « Configuration système requise » du *Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0.1*.

2.6 Administrateur d'assignation de rôles

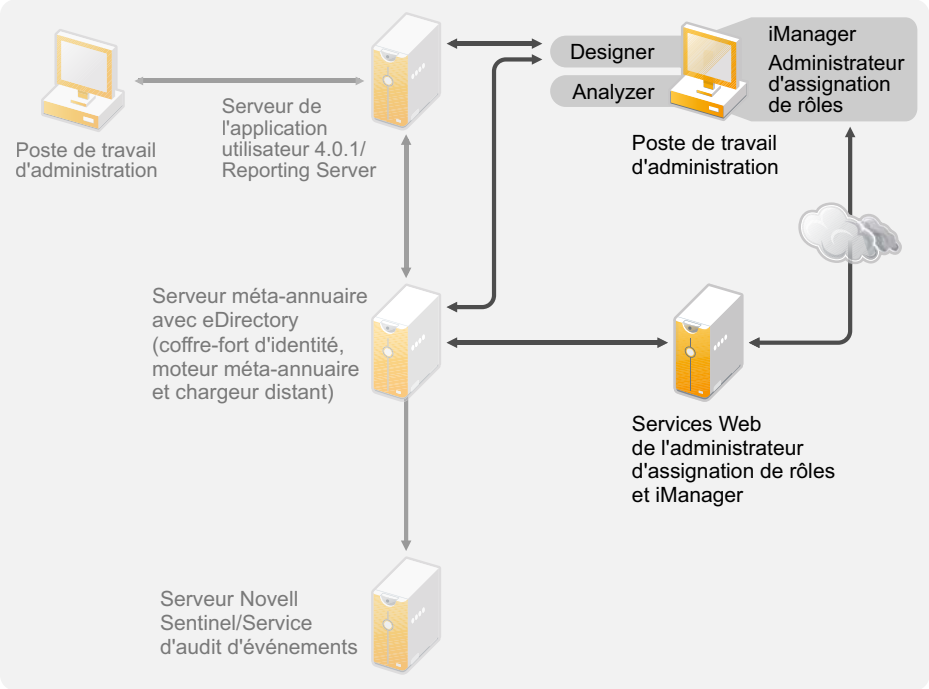
L'administrateur d'assignation de rôles vous permet d'assigner des rôles système gérés, des rôles composites ainsi que des profils (appelés collectivement autorisations) à des rôles Identity Manager. Lorsqu'un utilisateur est assigné à un rôle via le module de provisioning basé sur les rôles Identity Manager, il reçoit toutes les autorisations assignées à ce rôle. Pour connaître la configuration système requise pour l'administrateur de l'assignation de rôles, reportez-vous à la section « System

Requirements » (Configuration système requise) du manuel *Novell Identity Manager Role Mapping Administrator 4.0.1 User Guide* (Guide de l'utilisateur de la version 4.0.1 de l'administrateur de l'assignation de rôles de Novell Identity Manager).

2.7 iManager, Designer et Analyzer

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

Figure 2-3 *Outils pour Identity Manager*



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).
- Analyzer : reportez-vous à la section « Installing Analyzer » (Installation d'Analyzer) du manuel *Analyzer 4.0.1 for Identity Manager Administration Guide* (Guide d'administration d'Analyzer 4.0.1 pour Identity Manager).
- 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).

2.8 Navigateurs Web

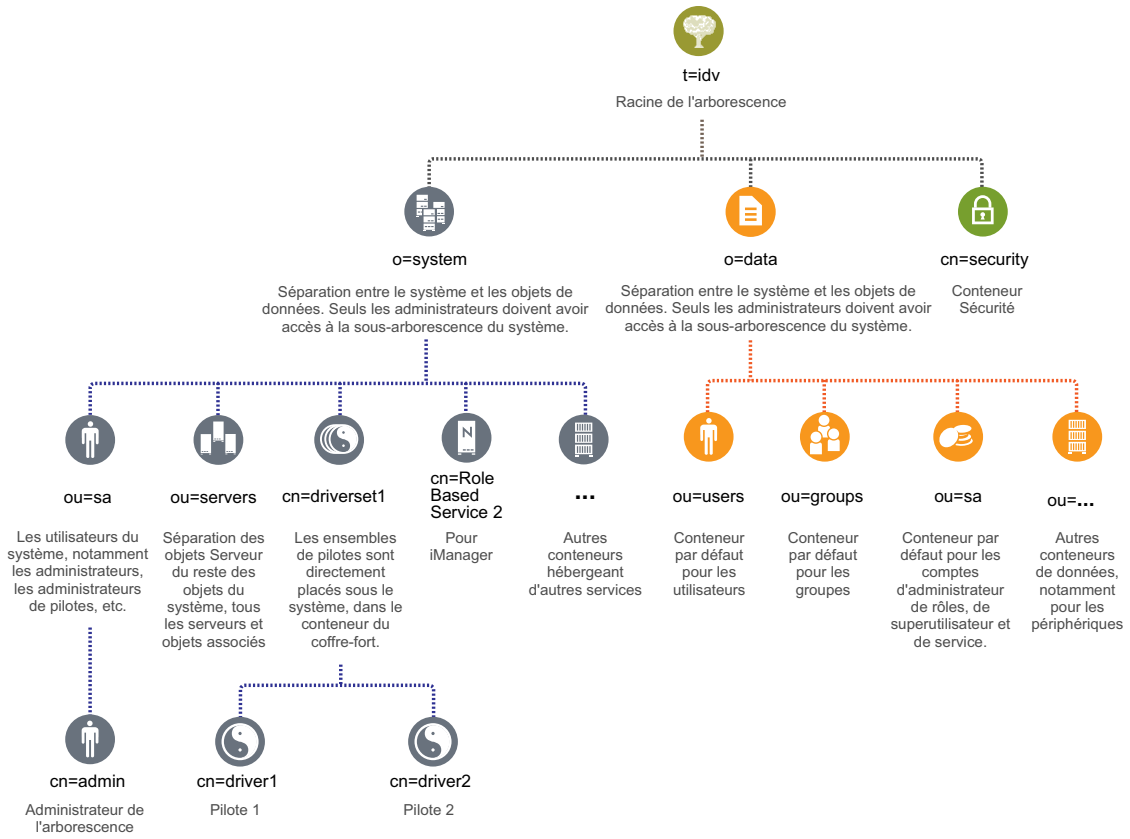
Les navigateurs Web pris en charge pour gérer Identity Manager sont les suivants :

- Internet Explorer 6 SP2
- Internet Explorer 7 et 8
- Firefox 3, 3.5.*x* et 3.6.*x*

2.9 Structure du coffre-fort d'identité

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

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



La Figure 2-4 montre la structure du coffre-fort d'identité pour Identity Manager. Cette structure est surtout utile pour une installation dans un seul environnement. Il s'agit de la structure par défaut des petits et moyens déploiements d'Identity Manager. Les environnements multi-tenants peuvent présenter une structure légèrement différente. En outre, les arborescences vastes et distribuées ne peuvent pas être structurées de cette façon. Le type de structure d'arborescence est créé lorsque vous créez une nouvelle arborescence via le programme d'installation intégré.

Identity Manager 4.0.1 utilise la plupart du temps des conteneurs Organisation, de sorte que les utilisateurs, les groupes et les administrateurs de services sont placés dans le même conteneur. Utilisez les organisations autant que possible et réservez les unités organisationnelles aux situations où elles sont vraiment pertinentes. La structure d'Identity Manager 4.0.1 est conçue pour garantir l'évolutivité grâce à trois composants principaux :

- Section 2.9.1, « Sécurité », page 17
- Section 2.9.2, « Données », page 17
- Section 2.9.3, « Système », page 17

2.9.1 Sécurité

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

2.9.2 Données

Le conteneur de données contient les groupes, les utilisateurs, les administrateurs de rôles, les périphériques, etc. Il s'agit des données qui constituent votre système. Les groupes, utilisateurs et conteneurs d'administrateurs de services sont des unités organisationnelles. Vous pouvez avoir des unités organisationnelles supplémentaires pour structurer vos données selon vos pratiques organisationnelles.

ou=sa

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

2.9.3 Système

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

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

ou=sa

Le conteneur d'administrateurs de services contient des objets administratifs pour le coffre-fort d'identité et les pilotes. Seuls les administrateurs peuvent accéder à la sous-arborescence du système. L'administrateur du coffre-fort d'identité par défaut est admin.sa.system.

Serveurs

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

Tous les objets Serveur doivent se trouver sous le conteneur servers.system. Toutefois, un administrateur peut créer des conteneurs de serveurs individuels pour chaque serveur déployé dans l'environnement. Le nom du conteneur est celui de l'objet Serveur. Tous les objets associés au serveur (volumes, licences, certificats) sont en place et il est plus facile de retrouver ceux dont vous avez besoin.

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

Ensembles de pilotes

Les ensembles de pilotes sont créés en tant que partition distincte au cours de la configuration du serveur méta-annuaire. Tous les objets Ensemble de pilotes sont stockés dans le conteneur système. Votre système Identity Manager 4.0.1 peut compter plusieurs ensembles de pilotes. Cette structure vous permet d'évoluer en ajoutant des ensembles de pilotes au conteneur système. Les services basés sur les rôles pour iManager sont également stockés dans le conteneur système.

Configuration système requise

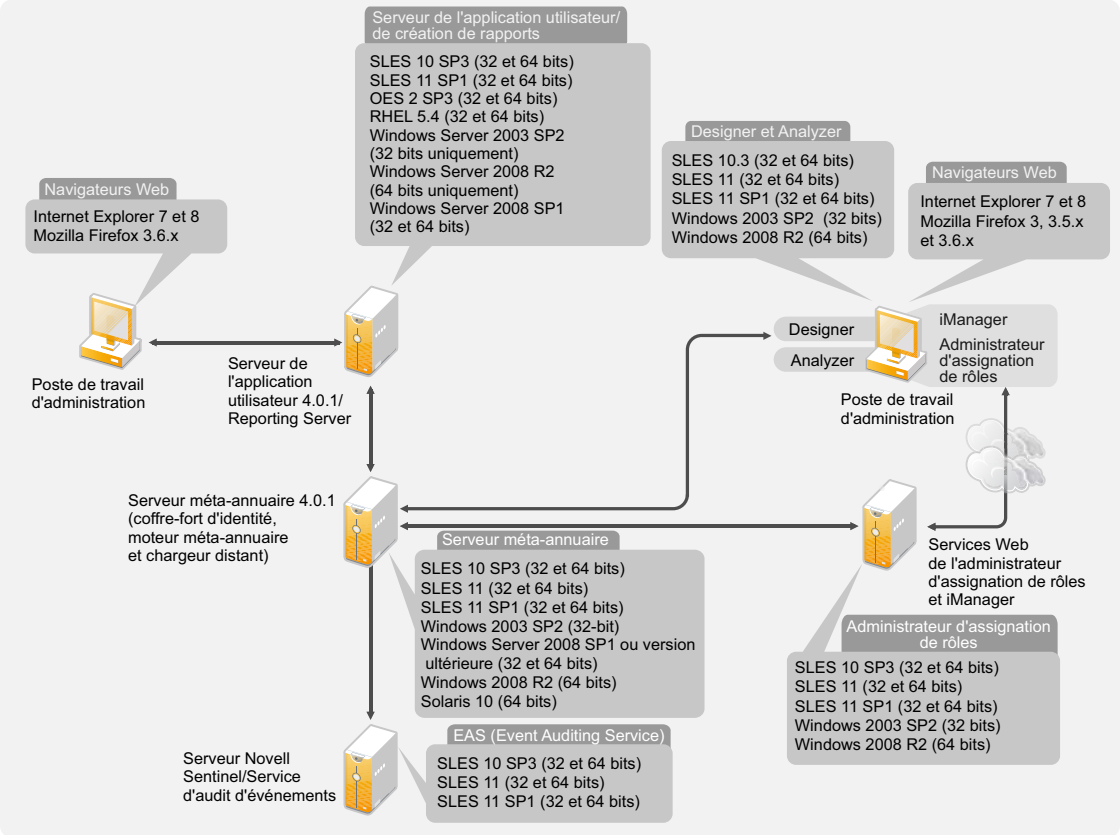
3

Le programme d'installation intégré permet d'installer les composants de Novell Identity Manager sur plusieurs systèmes et plates-formes.

3.1 Plates-formes prises en charge

La Figure 3-1 montre les plates-formes prises en charge par le programme d'installation intégré de Novell Identity Manager 4.0.1.

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



- Avec Identity Manager 4.0.1, le service d'audit d'événements n'est pris en charge que sur les plates-formes SLES. Il ne l'est pas sous Windows ni sous RHEL. Le serveur du service d'audit d'événements est installé sur une machine distante. Le programme d'installation affiche un champ supplémentaire pour la configuration du module Identity Reporting. Vous pouvez ainsi spécifier le mot de passe système du service d'audit d'événements pour le serveur. Copiez le mot de passe système depuis le fichier `/etc/opt/novell/sentinel_eas/config/activemqusers.properties` situé sur la machine hébergeant le service d'audit d'événements, puis collez-le dans le champ du mot de passe système de ce service.

- Avec Identity Manager 4.0.1, seul le serveur méta-annuaire est pris en charge sous Solaris.
- Tous les composants Identity Manager ne peuvent pas être installés sur toutes les plates-formes. Par exemple, le serveur méta-annuaire est pris en charge uniquement sous Solaris ou le service d'audit d'événements, uniquement sur les plates-formes SLES.

3.2 Ressources requises

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

- 3072 Mo de RAM au minimum.
- 10 Go d'espace disque disponible pour installer tous les composants.
- Espace disque supplémentaire pour configurer et charger les données. Celui-ci dépend des systèmes connectés et du nombre d'objets contenus dans le coffre-fort d'identité.
- Un serveur multiprocesseur avec processeur de 2 GHz est préférable.

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

Installation d'Identity Manager

4

Vous pouvez installer et configurer tous les composants simultanément ou en plusieurs fois à l'aide du programme d'installation intégré. Si vous souhaitez installer chaque composant séparément, utilisez le programme d'installation de la structure d'Identity Manager qui dispose de programmes d'installation différents pour chaque composant et installez les composants dans l'ordre stipulé à la section « Installation d'Identity Manager » du *Guide d'installation de la structure d'Identity Manager 4.0.1*. Pour obtenir une explication des différents composants, reportez-vous au guide *Présentation d'Identity Manager 4.0.1*.

Pour obtenir une liste des différents composants installés par le programme d'installation intégré d'Identity Manager, reportez-vous au Chapitre 1, « Présentation du programme d'installation intégré », page 7. Pour des informations détaillées sur chaque composant, reportez-vous au guide *Présentation d'Identity Manager 4.0.1*.

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

Pour plus d'informations sur la mise à niveau d'une installation existante d'Identity Manager, reportez-vous au Chapitre 6, « Mise à niveau d'Identity Manager », page 41.

4.1 Téléchargement du fichier ISO

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 les versions Standard Edition et Advanced 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 acheter la version qui répond le mieux à vos besoins. Vous pouvez également télécharger une version d'évaluation d'Identity Manager et l'utiliser gratuitement pendant 90 jours. Les composants Identity Manager doivent être activés dans les 90 jours à compter de l'installation, faute de quoi ils ne fonctionneront plus. À tout moment, durant ces 90 jours ou ultérieurement, vous pouvez choisir d'acheter une licence de produit et d'activer Identity Manager. Pour plus d'informations, reportez-vous au Chapitre 5, « Activation des produits Novell Identity Manager », page 37.

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 4-1 contient une description de chaque fichier.
4. Sélectionnez l'image ISO correspondant à vos besoins. Chaque image ISO contient les versions 32 et 64 bits du produit.
5. Suivez les invites à l'écran pour télécharger le fichier vers un répertoire de votre ordinateur.
6. Recommencez à partir de l'Étape 3 jusqu'à ce que vous ayez téléchargé tous les fichiers dont vous avez besoin.
7. Montez le fichier `.iso` téléchargé en tant que volume ou utilisez ce fichier `.iso` pour créer un DVD du logiciel. Si vous n'avez pas encore vérifié la validité du support que vous avez gravé, vous pouvez le faire à l'aide de l'option *Vérification du support*.

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

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

ISO	Plate-forme	Description
`Identity_Manager_4.0.1_Linux_Advanced.iso`	Linux	Contient l'image DVD pour le serveur méta-annuaire, le service d'audit d'événements, Designer, iManager, l'administrateur d'assignation de rôles, Analyzer, le module Identity Reporting et le module de provisioning basé sur les rôles.
`Identity_Manager_4.0.1_Linux_Standard.iso`	Linux	Contient l'image DVD pour le serveur méta-annuaire, le service d'audit d'événements, Designer, iManager, Analyzer, le module Identity Reporting et le module de provisioning basé sur les rôles.
`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_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 la plate-forme Solaris.

Important : pour passer de la version Advanced Edition d'Identity Manager à la version Standard Edition, désinstallez la première puis installez la seconde. 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).

4.2 Nouvelle installation à partir d'un média physique ou d'une image ISO

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

- Section 4.2.1, « Installation », page 23
- Section 4.2.2, « Configuration », page 24

Important : si vous installez Identity Manager à l'aide du programme d'installation intégré 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 préalablement installée.

4.2.1 Installation

1. Accédez aux fichiers d'installation d'Identity Manager 4.0.1, soit en montant le fichier `.iso`, soit en utilisant le DVD que vous avez créé à partir de ce fichier `.iso`.

   Pour plus d'informations, reportez-vous à la Section 4.1, « Téléchargement du fichier ISO », page 21.

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

   Linux/Solaris : `./install.bin`

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

   Windows : `install.exe`

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

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

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

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

   - Serveur méta-annuaire
   - Module de provisioning basé sur les rôles
   - Module Novell Identity Reporting
   - Service d'audit d'événements
   - Administrateur d'assignation de rôles
   - iManager

- Designer
- Analyzer

Remarque : les modules RBPM et Identity Reporting peuvent être installés sur un système dépourvu du coffre-fort d'identité. Vous devez toujours installer ces deux modules sur la même machine. Le module de provisioning basé sur les rôles utilise JBoss et PostgreSQL comme serveur d'applications et base de données.

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

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

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

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

Résumé de l'installation terminée : lisez le résumé post-installation pour vérifier l'état d'installation des composants sélectionnés et l'emplacement du fichier journal pour chacun d'eux. Reportez-vous au Tableau 4-2 page 35 pour plus d'informations sur l'emplacement des fichiers journaux.

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

4.2.2 Configuration

Vous pouvez configurer les composants Identity Manager que vous avez déjà installés à l'aide du programme d'installation intégré. Vérifiez que vous avez terminé la Section 4.2.1, « Installation », page 23 avant de poursuivre la configuration.

Important : lorsque vous créez une nouvelle arborescence ou ajoutez un élément à une arborescence existante, si le fichier `/etc/hosts` contient l'entrée 127.0.0.2, la configuration échoue car le certificat IP par défaut est créé pour l'adresse de bouclage 127.0.0.2. Pour éviter ce problème, mettez en commentaire l'adresse de bouclage 127.0.0.2 et assurez-vous que l'adresse de bouclage 127.0.0.1 et l'adresse IP réelle figurent dans le fichier.

Pour configurer les composants Identity Manager :

1. Si vous venez de l'Étape 3 page 23 de la procédure d'installation, passez à l'Étape 2. Si ce n'est pas le cas, démarrez la configuration avec le programme adapté à votre plate-forme :

   Linux : `./configure.bin`

   Solaris : `./configure.bin`

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

Windows : `configure.exe`

2 Sélectionnez les composants que vous souhaitez configurer et cliquez sur *Suivant*.

3 Sélectionnez l'une des options suivantes pour effectuer la configuration des composants Identity Manager :

- « Création d'une nouvelle arborescence » page 25
- « Ajout à une arborescence existante » page 30

Remarque : ◆si vous ajoutez un élément à une arborescence existante alors que le serveur primaire héberge Identity Manager 3.6 ou version supérieure, exécutez l'utilitaire NrfCaseUpdate sur ce serveur afin de prendre en charge les recherches en casse mixte pour les rôles et les ressources.

Sans l'exécution de cet utilitaire, la configuration du serveur méta-annuaire échoue. Pour plus d'informations sur l'exécution de l'utilitaire NrfCaseUpdate, reportez-vous à la section « Exécution de l'utilitaire NrfCaseUpdate » du *Guide d'installation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 4.0.1*.

◆Le programme d'installation intégré n'effectue aucune vérification de l'état de santé avant l'ajout d'un serveur secondaire Vous devez exécuter ndscheck avant d'ajouter un serveur secondaire via le programme d'installation intégré. Sous Windows, exécutez ndscheck à partir de l'emplacement `<emplacement_installation>\NDS`. Sous Linux/Solaris, exécutez-le à partir du répertoire `/opt/novell/eDirectory/bin/ndscheck`. Spécifiez les paramètres obligatoires et exécutez la commande comme suit :

```
ndscheck [-h <nom_hôte_port]>] [-a <FDN_admin>] [[-w <mot_de_passe>]
```

◆Le fichier `logevent.cfg` est modifié pour prendre en compte les détails du serveur de consignation sur les plates-formes Windows et Linux lorsque le module RBPM ou Identity Reporting est configuré par le biais du programme d'installation intégré. Si vous configurez uniquement le serveur méta-annuaire, ajoutez manuellement ces détails au fichier `logevent.cfg`.

Création d'une nouvelle arborescence

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

1 Utilisez les informations suivantes pour configurer vos composants Identity Manager si vous avez choisi de créer une nouvelle arborescence.

- « Coffre-fort d'identité » page 26
- « Coffre-fort d'identité > Avancé » page 26
- « Module de provisioning basé sur les rôles (RBPM) » page 27
- « Module de provisioning basé sur les rôles (RBPM) > Avancé » page 27
- « Module Novell Identity Reporting » page 28
- « Module Identity Reporting > Avancé » page 28
- « Service d'audit d'événements » page 29
- « Service d'audit d'événements > Avancé » page 30
- « iManager > Avancé » page 30

2 Examinez le résumé avant configuration, puis cliquez sur *Configurer*.

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

Si des problèmes se sont produits lors de la configuration, parcourez les journaux de configuration. Pour plus d'informations, reportez-vous à la section « Emplacement des fichiers journaux et de propriétés » page 35.

Coffre-fort d'identité

Remplissez les champs suivants pour créer une nouvelle arborescence :

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

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

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

Coffre-fort d'identité > Avancé

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

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

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

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

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

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

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

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

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

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

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

Exiger TLS pour les liaisons simples avec un mot de passe : sélectionnez cette option pour que toutes les connexions LDAP se fassent sur le port sécurisé (636 par défaut). Si vous désélectionnez cette option, les utilisateurs qui s'authentifient auprès du serveur LDAP sur le port en texte clair (389

par défaut) transmettent leur mot de passe en texte clair. Pour plus d'informations, reportez-vous à la section « Communicating with eDirectory through LDAP » (http://www.novell.com/documentation/edir88/edirin88/data/a7f08yl.html) (Communication avec eDirectory via LDAP) du manuel *Novell eDirectory 8.8 Installation Guide* (http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html) (Guide d'installation de Novell eDirectory 8.8).

Module de provisioning basé sur les rôles (RBPM)

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

Adresse du serveur EAS : spécifiez le nom DNS ou l'adresse IP du serveur qui héberge le service EAS. Vous pouvez utiliser ce serveur ou en ajouter un autre. Le module Identity Reporting ne peut être configuré que sur un seul serveur EAS.

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

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

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

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

(Facultatif) Mot de passe de l'administrateur de la sécurité : spécifiez le mot de passe de l'administrateur de la sécurité.

Ce champ est uniquement requis pour Identity Manager SE.

(Facultatif) Confirmer le mot de passe de l'administrateur de la sécurité : spécifiez à nouveau le mot de passe de l'administrateur de la sécurité.

Ce champ est uniquement requis pour Identity Manager SE.

(Facultatif) Mot de passe de l'administrateur de rapports : spécifiez le mot de passe de l'administrateur du module Identity Reporting.

Ce champ est uniquement requis pour Identity Manager SE.

(Facultatif) Confirmer le mot de passe de l'administrateur de rapports : spécifiez à nouveau le mot de passe de l'administrateur du module Identity Reporting.

Ce champ est uniquement requis pour Identity Manager SE.

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

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

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

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

Nom de l'administrateur de l'application utilisateur : spécifiez le nom de l'administrateur de l'application utilisateur. Un administrateur de l'application utilisateur est autorisé à exécuter toutes les fonctions de gestion de l'application utilisateur Identity Manager, y compris accéder à l'onglet Administration de l'interface utilisateur Identity Manager pour réaliser toute opération d'administration prise en charge.

(Facultatif) Nom de l'administrateur de la sécurité : spécifiez le nom de l'administrateur de la sécurité pour l'application utilisateur. Ce rôle permet aux membres d'accéder à toutes les fonctionnalités du domaine Sécurité. L'administrateur de la sécurité peut effectuer toutes les opérations possibles sur tous les objets au sein du domaine Sécurité.

Ce champ est uniquement requis pour Identity Manager Standard Edition.

(Facultatif) Nom de l'administrateur de la création de rapports : spécifiez le nom de l'administrateur de la création de rapports. Cet utilisateur peut accéder à toutes les fonctionnalités du domaine Création de rapports. L'administrateur de la création de rapports peut effectuer toutes les opérations possibles sur tous les objets au sein du domaine Création de rapports.

Ce champ est uniquement requis pour Identity Manager Standard Edition.

Module Novell Identity Reporting

Renseignez les champs suivants pour configurer le module Identity Reporting :

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

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

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

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

Ce champ est uniquement requis pour Identity Manager AE.

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

Module Identity Reporting > Avancé

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

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

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

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

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

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

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

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

Port LDAP : si vous avez sélectionné une connexion LDAP sécurisée pour la communication, spécifiez le port LDAP sécurisé. Dans le cas contraire, indiquez le port en texte en clair.

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

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

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

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

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

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

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

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

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

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

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

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

Service d'audit d'événements

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

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

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

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

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

Service d'audit d'événements > Avancé

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

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

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

iManager > Avancé

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

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

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

Ajout à une arborescence existante

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

1. Utilisez les informations suivantes pour configurer les composants Identity Manager si vous avez choisi d'ajouter ce serveur à une arborescence existante.
   - « Coffre-fort d'identité » page 31
   - « Coffre-fort d'identité > Avancé » page 31
   - « Serveur méta-annuaire » page 32
   - « Module de provisioning basé sur les rôles (RBPM) » page 32
   - « Module de provisioning basé sur les rôles (RBPM) > Avancé » page 33
   - « Module Novell Identity Reporting » page 33
   - « Service d'audit d'événements » page 33
   - « iManager > Avancé » page 34
2. Examinez la page de résumé de configuration, puis cliquez sur *Terminé*.

   Si des problèmes se sont produits lors de la configuration, parcourez les journaux de configuration. Pour plus d'informations, reportez-vous à la section « Emplacement des fichiers journaux et de propriétés » page 35.

Coffre-fort d'identité

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

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

Numéro de port du serveur existant : spécifiez le port NCP du serveur spécifié ci-dessus. Le port par défaut pour NCP est 524.

DN du contexte du serveur existant : indiquez le DN du conteneur si vous souhaitez que ce serveur soit placé dans votre arborescence existante. Par exemple, ou=server,o=system.

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

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

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

Coffre-fort d'identité > Avancé

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

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

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

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

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

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

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

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

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

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

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

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

Serveur méta-annuaire

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

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

Module de provisioning basé sur les rôles (RBPM)

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

Adresse du serveur EAS : spécifiez le nom DNS ou l'adresse IP du serveur qui héberge le service EAS. Vous pouvez utiliser ce serveur ou en ajouter un autre. Le module Identity Reporting ne peut être configuré que sur un seul serveur EAS.

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

DN de l'administrateur de l'application utilisateur : spécifiez le DN pour l'administrateur de l'application utilisateur au format LDAP. L'administrateur de l'application utilisateur est autorisé à exécuter toutes les fonctions de gestion de l'application utilisateur Identity Manager, y compris accéder à l'onglet Administration de l'interface utilisateur Identity Manager pour réaliser toute opération d'administration prise en charge.

Important : veillez à spécifier des DN différents pour les champs *DN d'administrateur de l'application utilisateur, DN de l'administrateur de la sécurité et DN de l'administrateur de rapports*. Si ces DN existent déjà sur le serveur primaire, la configuration de l'application utilisateur échoue.

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

DN du conteneur de pilote de l'application utilisateur : spécifiez le DN du conteneur racine de l'administrateur de l'application utilisateur au format LDAP.

(Conditionnel) DN de l'administrateur de la sécurité : spécifiez le DN de l'administrateur de la sécurité au format LDAP. Ce rôle permet aux membres d'accéder à toutes les fonctionnalités du domaine Sécurité. L'administrateur de la sécurité peut effectuer toutes les opérations possibles sur tous les objets au sein du domaine Sécurité.

Ce champ est uniquement requis pour Identity Manager Standard Edition.

(Conditionnel) Mot de passe de l'administrateur de la sécurité : spécifiez le mot de passe de l'administrateur de la sécurité.

Ce champ est uniquement requis pour Identity Manager Standard Edition.

(Conditionnel) DN de l'administrateur de rapports : spécifiez le DN de l'administrateur de la création de rapports au format LDAP. Cet utilisateur peut accéder à toutes les fonctionnalités du domaine Création de rapports. L'administrateur de la création de rapports peut effectuer toutes les opérations possibles sur tous les objets au sein du domaine Création de rapports.

Ce champ est uniquement requis pour Identity Manager Standard Edition.

(Conditionnel) Mot de passe de l'administrateur de rapports : spécifiez le mot de passe de l'administrateur de création de rapports.

Ce champ est uniquement requis pour Identity Manager Standard Edition.

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

Les options de configuration avancées du module RBPM sont identiques pour les configurations de nouvelle arborescence et d'arborescence existante. Reportez-vous à la section « Module de provisioning basé sur les rôles (RBPM) > Avancé » page 27.

Pour l'installation du serveur secondaire après la configuration du module RBPM, vous devez changer l'*ID d'authentification* du pilote d'application utilisateur :

1. Loguez-vous à l'arborescence existante via iManager.
2. Accédez à *Administration Identity Manager* > *Présentation d'Identity Manager* et sélectionnez l'ensemble de pilotes.
3. Cliquez sur l'option *Modifier les propriétés* du pilote d'application utilisateur, remplacez la valeur de l'option *ID d'authentification* par l'ID de l'administrateur de l'application utilisateur au format LDAP.

Module Novell Identity Reporting

Les options de configuration du module Identity Reporting sont identiques pour les configurations de nouvelle arborescence et d'arborescence existante. Reportez-vous aux sections « Module Novell Identity Reporting » page 28 et « Module Identity Reporting > Avancé » page 28.

Service d'audit d'événements

Les options de configuration du service d'audit d'événements sont identiques pour les configurations de nouvelle arborescence et d'arborescence existante. Reportez-vous aux sections « Service d'audit d'événements » page 29 et « Service d'audit d'événements > Avancé » page 30.

iManager > Avancé

Les options de configuration d'iManager sont identiques pour les configurations de nouvelle arborescence et d'arborescence existante. Reportez-vous à la section « iManager > Avancé » page 30.

4.3 Procédure post-installation

Le programme d'installation intégré ne crée pas l'objet DirMXL-PasswordPolicy dans le coffre-fort d'identité. Cette stratégie est assignée à chaque ensemble de pilotes Identity Manager d'une arborescence. Une fois Identity Manager installé, procédez comme suit afin de créer l'objet DirXML-PasswordPolicy :

1. Créez un fichier LDIF avec les attributs suivants :

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

dn: cn=driverset1,o=system #(driver-set dn, which the policy is assigned
to)
changetype: modify
add: objectclass
objectclass: nsimPasswordPolicyAux

dn: cn=driverset1,o=system #(driver-set dn, which the policy is assigned
to)
changetype: modify
add: nspmPasswordPolicyDN
nspmPasswordPolicyDN: cn=DirXML-PasswordPolicy,cn=Password
Policies,cn=Security

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: cn=driverset1,o=system #(driver-set dn, which the policy
is assigned to)
```

2. Utilisez ldapmodify pour importer des attributs depuis le fichier LDIF.

```
ldapmodify -x -ZZ -c -h <hostname> -p 389 -D "cn=admin,ou=sa,o=system" -w
<password> -f <ldif_file_name>
```

Remarque : sous Windows, utilisez le fichier `ldapmodify.exe`de l'image ISO du programme d'installation intégré (p. ex. <Chemin_ISO_II>/install/utilities)

Emplacement des fichiers journaux et de propriétés

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

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

Plate-forme	Fichiers journaux	Installation des fichiers de propriétés
Windows	`<emplacement_installation>\install\logs`	`<emplacement_installation>\install\propfiles`
	L'emplacement par défaut est `C:\Novell\IdentityManager\install\logs`	L'emplacement par défaut est `C:\Novell\IdentityManager\install\logs\propfiles\`
Linux/ Solaris	`/var/opt/novell/idm/install/logs`	`/var/opt/novell/idm/install/logs/propfiles/`

4.4 Installation et configuration en mode silencieux

4.4.1 Installation en mode silencieux

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

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

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

- **Linux :** `./install.bin -i silent -f <nom_fichier>.properties`
- **Solaris :** `./install.bin -i silent -f <nom_fichier>.properties`

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

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

Serveur méta-annuaire : IA_IDVAULT_ADMIN_PASSWORD.

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

Module Novell Identity Reporting : IA_REPORTING_NOVL_DB_USER_PASSWORD, IA_REPORTING_IDM_USER_PASSWORD et IA_REPORTING_IDM_SERVER_PASSWORD.

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

4.4.2 Configuration en mode silencieux

Vous pouvez également exécuter une configuration en mode silencieux des composants Identity Manager en créant un fichier de propriétés reprenant les paramètres nécessaires à l'exécution de la configuration. Deux exemples de fichiers sont disponibles sur le support d'Identity Manager. L'un sert à créer une nouvelle arborescence, l'autre à ajouter le serveur à une arborescence existante.

- **Linux :** reportez-vous à l'emplacement suivant :
  - `./install/propfiles/configure_new_tree.properties`
  - `./install/propfiles/configure_existing_tree.properties`
- **Solaris :** reportez-vous à l'emplacement suivant :
  - `./install/propfiles/configure_new_tree.properties`
  - `./install/propfiles/configure_existing_tree.properties`
- **Windows :** reportez-vous à l'emplacement suivant :
  - `\install\propfiles\configure_new_tree.properties`
  - `IDM4.0.1_Win:\install\propfiles\configure_existing_tree.properties`

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

- **Linux :** `./configure.bin -i silent -f <nom_fichier>.properties`
- **Solaris :** `./configure.bin -i silent -f <nom_fichier>.properties`

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

Les exemples de fichiers de propriétés disponibles à l'emplacement `install\propfiles` ne peuvent être utilisés que lorsque tous les composants sont configurés simultanément.

Pour connaître les paramètres obligatoires, exécutez la commande suivante :

```
./install/bin -i silent -DSELECTED_PRODUCTS=<composants à configurer>
```

La description des ID des composants Identity Manager est disponible dans le fichier de propriétés.

Créez un fichier de propriétés avec le résultat de la commande susmentionnée, ajoutez `SELECTED_PRODUCTS` aux composants à configurer, puis réexécutez la commande d'installation en mode silencieux pour que les composants sélectionnés soient configurés en mode silencieux.

Activation des produits Novell Identity Manager

5

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

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

5.1 Achat d'une licence de produit Identity Manager

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

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

5.2 Installation d'une référence d'activation de produit

Installez la référence d'activation de produit via iManager.

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

     ou

- Ouvrez le fichier de référence d'activation du produit, puis copiez son contenu dans le Presse-papiers.

  Copiez attentivement le contenu et veillez à n'inclure aucune ligne ni aucun espace supplémentaire. Vous devez commencer la copie à partir du premier tiret (-) de la référence (----DÉBUT DE LA RÉFÉRENCE D'ACTIVATION DU PRODUIT) jusqu'au dernier tiret (-) de la référence (FIN DE LA RÉFÉRENCE D'ACTIVATION DU PRODUIT-----).

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

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

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

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

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

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

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

5.4 Activation des pilotes Identity Manager

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

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

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

Vous devez effectuer les étapes décrites à la Section 5.2, « Installation d'une référence d'activation de produit », page 37 pour chaque module afin d'activer les pilotes.

5.5 Activation d'Analyzer

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

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

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

Mise à niveau d'Identity Manager

6

Les composants Identity Manager ne peuvent pas être mis à niveau via le programme d'installation intégré. Pour effectuer la mise à niveau vers la version 4.0.1, utilisez les programmes d'installation spécifiques des produits. Notez toutefois que la mise à niveau de la version Standard Edition d'Identity Manager 4.0.1 vers la version Advanced Edition s'opère 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 les mises 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*.

Dépannage d'Identity Manager 7

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

Problèmes d'installation

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

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

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

Par exemple,

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

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

Transmission de paramètres obligatoires lors de la configuration

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

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

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

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

Action : Procédez comme suit :

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

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

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

Action : Deux solutions sont possibles :

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

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

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

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

Action : Créez le répertoire `tmp` du système.

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

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

Installation du serveur secondaire

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

Les services ne fonctionnent pas

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

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

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

Détection de l'état actuel du système

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

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

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

Sous Windows, le programme d'installation intégré risque de se bloquer lors de la désinstallation d'Identity Manager

Cause possible : Le programme d'installation tente d'arrêter tous les services dépendants avant de désinstaller Identity Manager. Néanmoins, parfois, il ne parvient pas à arrêter le service DHost car d'autres services en dépendent.

Action : Déterminez si le programme d'installation s'est bloqué lors de la désinstallation du coffre-fort d'identité en procédant comme suit :

1. Allez dans le *Panneau de configuration*, ouvrez les *Services Novell eDirectory*, puis cliquez sur le bouton *Démarrage*. Si le programme d'installation se bloque, le message suivant s'affiche :

```
Novell eDirectory Service is in a NT service Stop Pending
State.
```

2. Pour poursuivre la désinstallation, arrêtez manuellement le service DHost à partir du Gestionnaire des tâches.

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

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

```
:\Users\Administrator\IDM4\products\eDirectory\x64\windows\x6
4\redist_pkg\vcredist_x86.exe" /q:a /c:"msiexec /i
vcredist.msi /qn /l
C:\Users\ADMINI~1\AppData\Local\Temp\vcredist32_Windows_x64_I
nstall.log"
execute command exitValue = 3010
```

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

Configuration de l'image ISO extraite via des outils d'extraction ISO tiers sous UNIX

Explication : La configuration du programme d'installation intégré d'Identity Manager 4.0.1 échoue si l'image est extraite par des outils d'extraction ISO tiers sur UNIX.

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

L'activation de XDAS diminue les performances

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

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

Problèmes de désinstallation de composant Identity Manager

Source : Lors de la désinstallation, si l'opération échoue pour un ou plusieurs composants, l'option *Désinstaller* est désactivée si vous retentez de les désinstaller. L'une des raisons possibles de cet échec sous Windows peut être que les variables JAVA_HOME et PATH ne sont pas définies.

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

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

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

désinstallez le coffre-fort d'identité :

```
/opt/novell/eDirectory/sbin/nds-uninstall
```

- **JBoss :** exécutez la commande suivante :

  ```
  $IA_RBPM_POSTGRESQL_INSTALL_PATH$/
  JBossPostgreSQL_Uninstaller/Uninstall_JBossPostgreSQL
  ```

- **Module de provisioning basé sur les rôles :** exécutez la commande suivante :

  ```
  java -jar /opt/novell/idm/rbpm/RemoveUserApp/
  uninstaller.jar
  ```

- **Module Novell Identity Reporting :** exécutez la commande suivante :

  ```
  /opt/novell/idm/rbpm/Uninstall_Identity Reporting/
  Uninstall Identity Reporting
  ```

- **Service d'audit d'événements :** exécutez la commande suivante :

  ```
  /opt/novell/sentinel_eas/Uninstall_Event Auditing
  Service/Uninstall Event Auditing Service
  ```

- **Administrateur d'assignation de rôles :** exécutez la commande suivante :

  ```
  /opt/novell/idm/rma/rma-uninstall.sh -s
  ```

- **Designer :** exécutez la commande suivante :

  ```
  /opt/novell/idm/Designer/UninstallDesigner/Uninstall
  Designer for Identity Manager
  ```

- **Analyzer :** exécutez la commande suivante :

  ```
  /opt/novell/idm/Analyzer/UninstallAnalyzer/Uninstall
  Analyzer for Identity Manager
  ```

- **iManager :** exécutez la commande suivante :

  ```
  /var/opt/novell/tomcat5/webapps/nps/UninstallerData/
  UninstalliManager
  ```

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

Désinstallation d'Identity Manager

8

Le script de désinstallation désinstalle tous les composants Identity Manager installés à l'aide du programme d'installation intégré. Si vous souhaitez désinstaller un seul composant, reportez-vous à la section « Désinstallation d'Identity Manager » du *Guide d'installation de la structure d'Identity Manager 4.0.1*.

8.1 Désinstallation de l'interface graphique

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

Pour désinstaller les composants Identity Manager :

1. Exécutez la désinstallation à l'aide du programme adéquat pour votre plate-forme :
   - **Linux/Solaris :** `./Uninstall_Identity Manager Components.bin`

     Le fichier binaire se situe à l'emplacement `/opt/novell/idm/Uninstall_Identity Manager Components/Uninstall Identity Manager Components.bin`.
   - **Windows :** `Uninstall_Identity Manager Components.exe`

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

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

     ---
2. Cochez la case pour chaque composant à désinstaller, puis cliquez sur *Suivant*.
3. Spécifiez les références pour chacun de ces composants au format LDAP, puis cliquez sur *Suivant*.

   Le programme de désinstallation a besoin des références pour déconfigurer les composants avant désinstallation.
4. Lisez le résumé concernant la désinstallation des composants, puis cliquez sur *Désinstaller*.

   Si vous devez modifier la liste des composants sélectionnés, cliquez sur *Précédent* et apportez vos modifications.
5. Parcourez la page Résumé de désinstallation terminée qui affiche la liste des composants qui ont été désinstallés, puis cliquez sur *Terminé* pour terminer le processus de désinstallation.

8.2 Désinstallation silencieuse

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

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

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

- **Linux :** `/opt/novell/idm/Uninstall_Identity Manager Components/Uninstall Identity Manager Components.bin -i silent -f <nom_fichier>.properties`
- **Solaris :** `/opt/novell/idm/Uninstall_Identity Manager Components/Uninstall Identity Manager Components.bin -i silent -f <nom_fichier>.properties`
- **Windows :** `<emplacement_installation>\Uninstall_Identity Manager Components/Uninstall Identity Manager Components.exe -i silent -f <nom_fichier>.properties`