Novell Identity Manager

3.5.1

www.novell.com

GUIDE D'INSTALLATION

28 septembre 2007

Novell®

Mentions légales

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

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

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

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

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
États-Unis
www.novell.com

Documentation en ligne : pour accéder à la documentation en ligne la plus récente concernant ce produit Novell et d'autres, reportez-vous au site Web de documentation Novell (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.

Tables des matières

À propos de ce guide

Novell® Identity Manager, anciennement DirXML®, est un service de partage des données et de synchronisation 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 libre-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 présente les technologies Identity Manager et décrit les fonctions d'installation, d'administration et de configuration d'Identity Manager.

Public

Ce guide est destiné aux administrateurs, consultants et ingénieurs réseau qui planifieront et mettront en oeuvre Identity Manager dans un environnement 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/idm35/index.html).

Documentation complémentaire

Pour savoir comment utiliser les pilotes Identity Manager, reportez-vous au site Web des pilotes Identity Manager (http://www.novell.com/documentation/idm35drivers/index.html).

Conventions relatives à la documentation

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

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

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

Présentation

1

1.1 Introduction à Identity Manager

Novell® Identity Manager est une solution primée par l'industrie de partage de données et de synchronisation qui révolutionne la gestion des données. Ce service alimente une banque de données centrale—votre coffre-fort d'identité—pour synchroniser, transformer et distribuer des informations dans des applications, des bases de données et des annuaires.

Mais Identity Manager est bien plus que cela. Voici quelques exemples de fonctions d'Identity Manager :

- Synchronisation des mots de passe
- Mot de passe en libre service
- Services de consignation et d'audit
- Gestion des utilisateurs grâce à l'application utilisateur
- Provisioning du workflow
- Notification par messagerie
- Conception de pilotes et de stratégies grâce à Designer (également appelé le concepteur)

Pour connaître les nouveautés sur ces composants dans la version d'Identity Manager, reportez-vous à Section 1.3, « Nouveautés d'Identity Manager 3.5.1 », page 14. Pour avoir une meilleure vision des différents composants et services que comprend Identity Manager, reportez-vous à Section 1.4, « Programmes d'installation et services Identity Manager », page 19.

Identity Manager permet à un système connecté (comme SAP*, PeopleSoft*, Lotus* Notes*, Microsoft* Exchange, Active Directory* et autres) d'effectuer ce qui suit :

- Partager des données avec le coffre-fort d'identité.
- Synchroniser et transformer des données partagées avec le coffre-fort d'identité lorsque celui-ci est modifié dans des systèmes connectés.
- Synchroniser et transformer des données partagées avec des systèmes connectés lorsque les données sont modifiées dans le coffre-fort d'identité.

Identity Manager effectue cela en offrant un cadre bidirectionnel qui permet aux administrateurs d'indiquer les données qui passent du coffre-fort d'identité à l'application et de l'application au coffre-fort d'identité. Ce cadre utilise XML pour offrir des fonctions qui permettent la conversion

des données et événements du coffre-fort d'identité au format d'application spécifié. Il convertit également des formats d'application à un format compréhensible par le coffre-fort d'identité. Toutes les interactions avec l'application se produisent via l'API native de l'application.

Identity Manager permet de ne sélectionner que les attributs et les classes correspondant aux champs et aux enregistrements du système connecté concerné. Par exemple, une banque de données d'annuaire peut choisir de partager des Objets de type utilisateur avec une banque de données des Ressources Humaines, mais pas des objets de type ressource réseau tels que les serveurs, les imprimantes et les volumes. La banque de données des Ressources Humaines peut à son tour partager des prénoms, noms, initiales, numéros de téléphone et lieux de travail d'utilisateurs avec d'autres membres du personnel sans partager les informations plus personnelles des utilisateurs (comme des informations sur la famille et les emplois précédents).

Si le coffre-fort d'identité n'a pas de classe ni d'attribut pour les données que vous voulez partager avec d'autres applications, vous pouvez étendre le schéma eDirectory afin de les inclure. Dans ce cas, votre coffre-fort d'identité devient un référentiel d'informations dont il n'a pas besoin, mais que d'autres applications peuvent utiliser. La banque de données de l'application assure la gestion de ce référentiel pour les informations nécessaires uniquement à l'application.

Identity Manager accomplit les tâches suivantes :

- Utilise des événements pour capturer les changements dans le coffre-fort d'identité.
- Centralise ou distribue la gestion des données en servant de hub pour rassembler toutes les données.
- Expose des données de l'annuaire au format XML, ce qui permet leur utilisation et leur partage par les applications XML ou les applications intégrées via Identity Manager.
- Gestion précise des associations entre objets du coffre-fort d'identité et objets de tous les autres systèmes intégrés, afin de garantir que les modifications de données sont reflétées de façon appropriée dans tous les systèmes connectés.

Les stratégies sont la clé de la synchronisation des données. Une stratégie :

- Contrôle du flux de données à l'aide de filtres spécifiques qui régissent les éléments de données définis dans le système.
- Met en oeuvre des sources de données expertes via l'utilisation d'autorisations et de filtres.
- Applique des règles aux données des banques de données au format XML. Ces règles gouvernent l'interprétation et la transformation des données au fur à et mesure que les modifications passent par Identity Manager.
- Transforme les données de XML dans pratiquement n'importe quel format de données. Cela permet à Identity Manager de partager des données avec n'importe quelle application.

Avec Identity Manager, votre entreprise peut simplifier les procédures de gestion des ressources humaines, réduire les coûts de gestion des données, établir des relations client via un service personnalisé performant et supprimer les barrières d'interfonctionnement qui entravent le succès. Voici ci-dessous plusieurs exemples d'activités permises par Identity Manager :

Tableau 1-1 *Ce que Identity Manager peut faire pour vous*

Activité	Solution Identity Manager
Gestion des comptes utilisateur	En une seule opération : Identity Manager accorde ou retire immédiatement à un employé les droits d'accès à des ressources. Identity Manager contient une fonction provisioning d'employé automatique qui permet à un nouvel employé d'accéder au réseau, à la messagerie électronique, aux applications, etc. Grâce au provisioning de workflow, ce processus peut être paramétré de façon à lancer un processus d'approbation. Identity Manager peut également limiter ou désactiver l'accès lorsqu'un employé quitte l'entreprise.
Suivi et intégration des biens	Identity Manager peut ajouter des profils pour tous les éléments du stock des biens (ordinateurs, écrans, téléphones, ressources de bibliothèque, chaises, bureaux, etc.) au coffre-fort d'identité et les intégrer aux profils utilisateur tels que des individus, des services ou des organisations.
Automatisation des annuaires pages blanches/pages jaunes	Identity Manager peut créer des annuaires unifiés comportant différents niveaux d'informations à usage interne et externe. Les annuaires externes peuvent ne contenir que des adresses électroniques ; les annuaires internes peuvent inclure notamment le lieu de travail, le numéro de téléphone, le numéro de télécopie, le numéro de téléphone portable, l'adresse du domicile.
Optimisation des profils utilisateur	Identity Manager permet d'optimiser les profils utilisateur grâce à l'ajout ou à la synchronisation d'informations telles que l'adresse électronique, le numéro de téléphone, l'adresse personnelle, les préférences, les rapports hiérarchiques, les biens matériels, les téléphones, les clés, les articles de stock, entre autres.
Unification de l'accès aux communications	Identity Manager simplifie l'accès au réseau, au téléphone, à l'alphapage, à Internet, aux équipements sans fil, tant pour les personnes que pour les groupes, grâce à la synchronisation des différents annuaires avec une interface commune de gestion.
Renforcement des relations avec les partenaires	Identity Manager renforce les partenariats en créant des profils (employé, client, etc.) dans les systèmes partenaires en dehors du pare-feu pour permettre aux partenaires de fournir un service immédiat si nécessaire.
Amélioration de la chaîne d'approvisionnement	Identity Manager permet d'améliorer les services client en reconnaissant et en consolidant des instances de comptes client multiples.
Fidélisation des clients	Identity Manager offre de nouveaux services en reconnaissant les besoins des clients de visualiser les données au même endroit au lieu qu'elles soient isolées dans des applications ou des zones séparées.

Activité	Solution Identity Manager
Personnalisation des services	Identity Manager offre aux utilisateurs (employé, clients, partenaires, etc.) des profils complets avec des informations synchronisées, y compris les relations, le statut et les notes de service. Ces profils peuvent être utilisés pour fournir différents niveaux d'accès aux services et aux informations et pour offrir des services en temps réel, personnalisés en fonction des clients.
Gestion des mots de passe	Par l'intermédiaire de l'application utilisateur, les administrateurs peuvent définir des questions de vérification d'identité et permettre aux utilisateurs de définir leurs propres mots de passe. L'utilitaire d'extension du login du client (Client Login Extension) pour Novell Identity Manager 3.5.1 facilite le libre-service des mots de passe en ajoutant un lien vers les clients de login Novell et Microsoft GINA. Les clients autorisent l'accès à la fonction de libre-service des mots de passe de l'application utilisateur Identity Manager. Si le pilote Identity Manager prend en charge la synchronisation des mots de passe, ces derniers peuvent être synchronisés sur les systèmes connectés.

1.2 Modifications de terminologie

Les termes suivants ont changé par rapport aux versions précédentes :

Tableau 1-2 *Modifications de terminologie*

Termes précédents	Nouveaux termes
DirXML®	Identity Manager
Serveur DirXML	Serveur méta-annuaire
Moteur DirXML	Moteur méta-annuaire
eDirectory™	Coffre-fort d'identité (sauf lorsque les attributs ou classes eDirectory sont concernés)

1.3 Nouveautés d'Identity Manager 3.5.1

1.3.1 Identity Manager

Prise en charge d'Open Enterprise Server 2

Open Enterprise Server 2 contient un grand nombre de composants logiciels prérequis, notamment SUSE® Linux Enterprise Server 10 Support Pack 1, NetWare® 6.5 Support Pack 7, eDirectory 8.8 Support Pack 2, iManager 2.7 et Security Services 2.0.5. Identity Manager est pris en charge sur les plates-formes Linux et NetWare Open Enterprise Server 2.

Plug-ins iManager

Les plug-ins iManager dans cette version d'Identity Manager sont également compatibles avec Identity Manager 3.0. Outre la compatibilité avec les versions précédentes, Identity Manager 3.5.1 intègre des plug-ins capables de fournir des informations exploitables dans des rapports à partir du fichier de cache des pilotes.

Prise en charge renforcée des plates-formes de systèmes d'exploitation

Identity Manager prend en charge l'ensemble des plates-formes de systèmes d'exploitation prises en charge par la version précédente d'Identity Manager. En outre, certains composants d'Identity Manager fonctionneront avec Microsoft Windows Vista*, AIX* 5.3, Red Hat* 5 AS/ES 64 bits et Open Enterprise Server 2, qui inclut SUSE Linux Enterprise Server 10 SP1 et NetWare 6.5 SP7.

Prise en charge renforcée d'applications

Identity Manager prend en charge l'ensemble des applications prises en charge par la version précédente d'Identity Manager. En outre, Identity Manager prend également en charge eDirectory 8.8 SP2 et iManager 2.7 avec les plates-formes sur lesquelles ces applications sont exécutées.

Installation non-root

Identity Manager 3.5.1 comporte des informations et des scripts pour installer le moteur méta-annuaire d'Identity Manager dans une installation non-root d'eDirectory. Pour connaître les étapes d'une installation non-root d'Identity Manager, reportez-vous à Section 4.9, « Installation non-root d'Identity Manager », page 94.

Composants intégrés

Identity Manager comprend l'utilitaire Client Login Extension pour Novell Identity Manager 3.5.1 et Designer 2.1.

Nouveau composant d'Identity Manager, Client Login Extension pour Novell Identity Manager 3.5.1 facilite le libre-service des mots de passe en ajoutant un lien vers les clients de login·Novell et Microsoft GINA. Lorsque les utilisateurs cliquent sur le lien *Mot de passe oublié* dans leur client de login, Client Login Extension lance un navigateur restreint pour accéder à la fonction de libre-service des mots de passe de l'application utilisateur Identity Manager. Cette fonction favorise la réduction des appels au service d'assistance des utilisateurs ayant oublié leur mot de passe.

Pour plus d'informations sur Client Login Extension pour Novell Identity Manager 3.5.1, reportez-vous à « Client Login Extension pour Novell Identity Manager 3.5.1 » dans le *Guide d'administration de Novell Identity Manager 3.5.1*. Pour plus d'informations sur Designer 2.1, reportez-vous à Section 1.3.2, « Concepteur pour Identity Manager », page 16.

1.3.2 Concepteur pour Identity Manager

Cette section décrit les améliorations de Designer pour Identity Manager. Pour obtenir la liste plus détaillée des améliorations et des changements instroduits dans Designer 2.1, reportez-vous à Nouveautés (http://www.novell.com/documentation/designer21/index.html).

Prise en charge des préférences locales

La vue de provisioning de Designer pour Identity Manager permet désormais de définir :

- Les préférences locales par défaut de l'application utilisateur. (Il s'agit des préférences locales utilisées pour afficher le contenu lorsque aucune correspondance n'a été trouvée pour l'utilisateur.)
- Les préférences locales prises en charge par le pilote de l'application utilisateur.

De surcroît, Designer peut désormais importer et exporter des données de localisation pour les modèles de message électronique.

Éditeur d'équipe de provisioning

Designer pour Identity Manager inclut désormais un plug-in d'éditeur d'équipe de provisioning. Ce nouvel éditeur permet de définir un ensemble d'utilisateurs pouvant agir comme équipe pour l'onglet *Requêtes et approbations* de l'application utilisateur. La définition d'une équipe détermine qui peut gérer les requêtes de provisioning et les tâches d'approbation qui lui sont associées.

L'éditeur d'équipe de provisioning offre une alternative au plug-in iManager de gestion d'équipe.

Amélioration de l'utilisation de la vue de provisioning

La vue de provisioning a été améliorée pour permettre de :

- Organiser les définitions de requête de provisioning dans des catégories. Vous pouvez utiliser l'éditeur de la couche d'abstraction de l'annuaire·pour définir les catégories.
- Assignez plusieurs propriétés (comme l'assignation des ayants droit) pour plusieurs définitions de requête de provisioning simultanément.

Activité de messagerie électronique

L'activité de messagerie électronique offre un moyen d'envoyer un courrier électronique aux parties intéressées en dehors d'une activité d'approbation.

Activité d'approbation

L'activité d'approbation offre désormais un moyen de créer un nouveau formulaire à partir de la page des propriétés de l'activité d'approbation.

L'activité d'approbation offre également la possibilité de définir dans les notifications par messagerie un champ d'adresse Répondre à différent du champ d'adresse De.

Activité de consignation

L'activité de consignation permet désormais l'ajout de messages personnalisés à l'historique des commentaires d'un workflow.

Amélioration des formulaires

Les formulaires prennent désormais en charge l'événement onload.

Améliorations ECMA

Les méthodes de champ suivants sont désormais prises en charge :

- getName()
- validate()
- hide()
- show()
- focus()
- select()
- activate()
- setRequired()

Amélioration des noms d'affichage de la définition de requête de provisioning

Le nom d'affichage de la définition de requête de provisioning peut maintenant être défini comme une chaîne statique ou une expression ECMA localisable. En définissant une expression, vous pouvez personnaliser le nom d'affichage de la tâche d'approbation. Cela·permet à différentes instances du même workflow d'afficher des entrées uniques de la liste des tâches dans l'application utilisateur.

1.3.3 Application utilisateur

- « Améliorations de l'interface utilisateur » page 18
- « Modifications liées à la prise en charge multi plate-forme » page 18
- « Changements relatifs à l'interopérabilité » page 18
- « Amélioration des points d'extrémité SOAP » page 19

- « Amélioration des autres fonctions » page 19

Améliorations de l'interface utilisateur

L'affichage des tâches de l'équipe a été amélioré pour offrir davantage de souplesse dans l'interface et optimiser l'expérience de l'utilisateur. La page Tâches de l'équipe affiche le contenu dynamique dans deux nouvelles vues de présentation, la vue Modèle et la vue Exposer. Les deux formats utilisent un tableau pour présenter les données à l'utilisateur. Dans ces deux formats, l'utilisateur peut choisir les colonnes à afficher, spécifier l'ordre dans lequel apparaissent les colonnes et trier les tâches sur les valeurs d'une colonne.

Le choix du format d'affichage est contrôlé par l'administrateur. Les administrateurs peuvent choisir une vue par rapport à l'autre du fait des préférences de présentation ou pour bénéficier des fonctions de différenciation suivantes :

- La vue Modèle (par défaut) offre la prise en charge de l'accessibilité des utilisateurs malvoyants. De plus, elle comporte une fonction de pagination personnalisable.
- La vue Exposer prend en charge le filtrage et offre une fonction d'exportation de données.

Modifications liées à la prise en charge multi plate-forme

Cette version ajoute la prise en charge d'exécution pour les plates-formes de serveur d'applications suivantes :

- JBoss* 4.2.0 sur SUSE Linux Enterprise Server 10.1, SUSE Linux Enterprise Server 9 SP2 et Windows 2003 Server SP1
- WebSphere* 6.1 sur Solaris* 10 et Windows 2003 SP1

  Le programme d'installation de l'application utilisateur installe automatiquement le fichier WAR. En revanche, vous devez déployer le fichier WAR dans WebSphere manuellement.

  La prise en charge des bases de données pour WebSphere inclut Oracle* 10g, MS SQL* 2005 SP1 et DB2.

  Pour obtenir la liste complète des plates-formes prises en charge, reportez-vous à « Configuration système requise pour Identity Manager » page 28.

Cette version ajoute également la prise en charge des environnements de navigateur suivants :

- Internet Explorer 7 sur Windows 2000 Professional SP4, Windows XP SP2 et Windows Vista Enterprise Version 6
- Firefox* 2 sur Red Hat Enterprise Linux WS 4.0, Novell Linux Desktop 9, SUSE Linux 10.1 et SUSE Linux Enterprise Desktop 10

Changements relatifs à l'interopérabilité

Les changements suivants relatifs à l'interopérabilité ont été apportés à cette version :

- L'administrateur peut désormais utiliser un paramètre de configuration pour spécifier si l'application utilisateur doit afficher l'indice dans l'écran Mot de passe oublié.
- L'administrateur peut désormais utiliser un paramètre de configuration pour activer ou désactiver la fonction de saisie automatique du mot de passe dans la boîte de dialogue Login. Cela permet de contrôler l'autorisation d'enregistrement des références de l'utilisateur accordée par le navigateur.

- Le processus de login prend désormais en charge l'authentification de proxy par carte à puce par l'intermédiaire d'Access Manager. Pour rendre cela possible, l'application utilisateur accepte les assertions SAML injectées dans l'en-tête HTTP et les utilise pour réaliser un login SASL à l'annuaire.

Amélioration des points d'extrémité SOAP

Les changements suivants ont été apportés aux points d'extrémité SOAP dans cette version :

- Un nouveau service VDX a été ajouté pour fournir un point d'extrémité SOAP pour effectuer des requêtes par rapport à la couche d'abstraction de l'annuaire.
- Un nouveau service de notification a été ajouté pour fournir un point d'extrémité SOAP pour envoyer des notifications par courrier électronique.
- Une nouvelle méthode appelée getProcessesArray() a été ajoutée au service de provisioning qui inclut un argument pour permettre de limiter le nombre de processus renvoyés.
- Une nouvelle méthode appelée startWithCorrelationId() a également été ajoutée au service de provisioning pour permettre de démarrer un ensemble de workflows associés et les suivre en utilisant un ID de corrélation.

Les points d'extrémité SOAP offrent aux développeurs un moyen pour créer leurs propres applications. Ils ne sont pas exposés dans l'interface utilisateur prête à l'emploi de l'application utilisateur.

Amélioration des autres fonctions

L'application utilisateur permet maintenant de spécifier les paramètres d'URL pour accéder directement à un formulaire de requête de provisioning.

1.4 Programmes d'installation et services Identity Manager

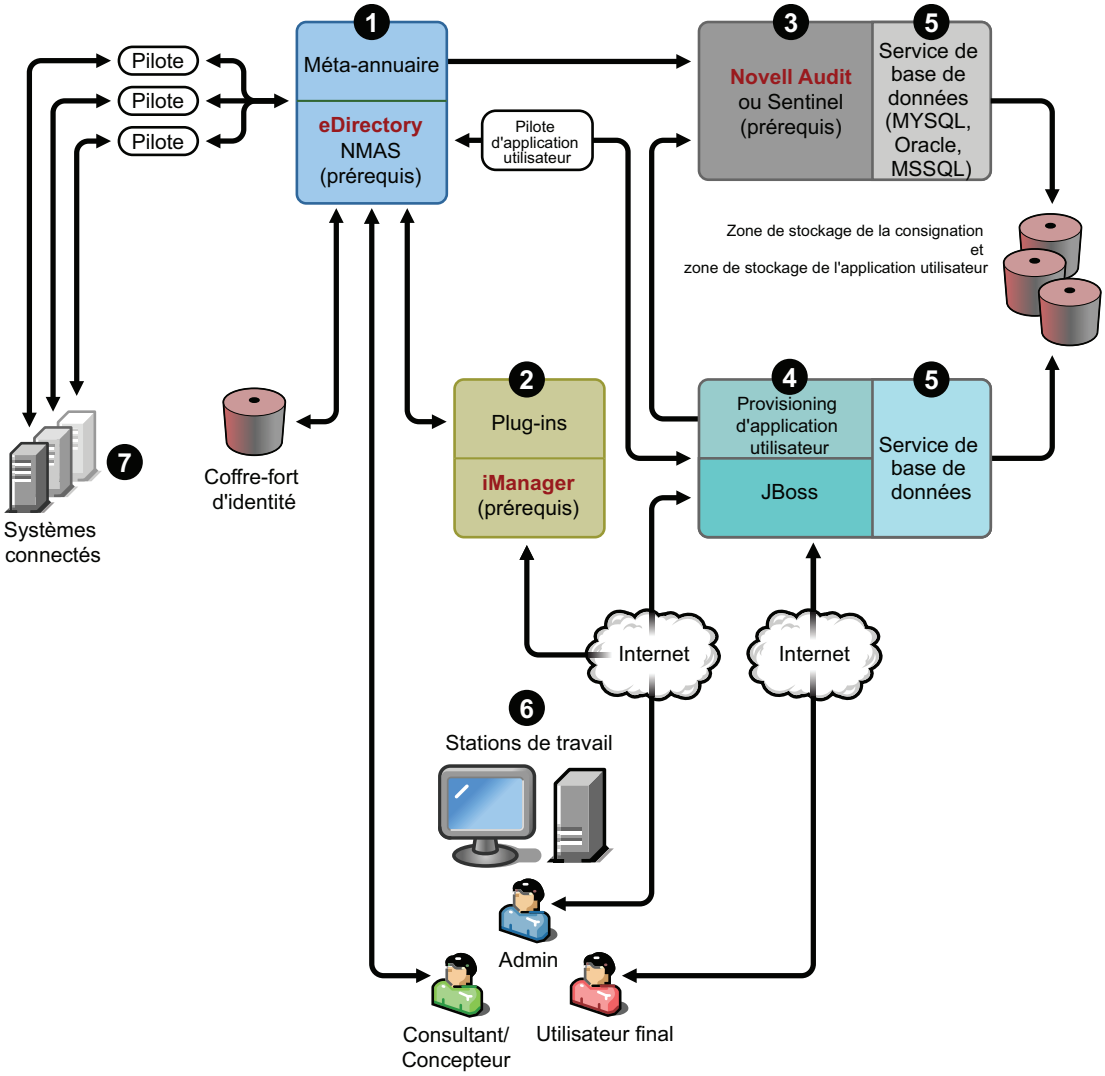
Les sections suivantes expliquent Programmes d'installation et Services d'Identity Manager. Cette section souligne les différents services qui confèrent à Identity Manager une efficacité opérationnelle optimale.

- Section 1.4.1, « Programmes d'installation », page 19
- Section 1.4.2, « Services », page 21

1.4.1 Programmes d'installation

Identity Manager compte trois programmes d'installation distincts avec sept services à installer et à configurer. Le schéma ci-dessous présente tous les services nécessaires pour rendre Identity Manager totalement fonctionnel.

Figure 1-1 *Présentation graphique des sept services Identity Manager*



Voici une liste des programmes d'installation et des opérations réalisées par chaque installation :

- « Installation du système méta-annuaire Identity Manager » page 21
- « Installation de l'application utilisateur et du module de provisioning » page 21
- « Installation du concepteur » page 21

Remarque : avant d'installer les composants Identity Manager, vous devez d'abord installer les logiciels prérequis dont eDirectory 8.7.3.6 ou une version supérieure (pour les services indiqués aux numéros 1 et 3 du graphique ci-dessus), Security Services 2.0.4 avec NMAS 3.1.3 (pour les numéros 1 et 3), iManager 2.6 ou une version supérieure (pour le numéro 2) et Novell Audit 2.0.2 Starter Pack ou Sentinel 5.1.3 (pour le numéro 3). Vous pouvez obtenir les logiciels prérequis depuis le site Web de téléchargement Novell (http://download.novell.com). Pour obtenir une liste détaillée des prérequis et exigences, reportez-vous à Section 1.5, « Configuration système requise pour Identity Manager », page 28.

Installation du système méta-annuaire Identity Manager

Le processus d'installation effectue les fonctions suivantes :

- Il étend le schéma eDirectory pour le produit Identity Manager dans son ensemble.
- Il installe le moteur méta-annuaire et le service du système.
- Il installe les plug-ins Identity Manager pour iManager.
- Il installe le chargeur distant du système méta-annuaire (s'il est sélectionné).
- Il installe les pilotes des systèmes connectés. (Les pilotes sont installés, mais en consultation jusqu'à ce que leur utilisation soit lancée).
- Il installe les rapports Identity Manager et les utilitaires et outils système du méta-annuaire.

Installation de l'application utilisateur et du module de provisioning

Les services suivants sont installés sous Linux* et Windows :

- JBoss et MySQL* (s'ils sont sélectionnés).
- Le fichier WAR requis pour exécuter l'application utilisateur.

Installation du concepteur

Il existe un programme d'installation pour Linux et un autre pour Windows. Ils effectuent les tâches suivantes :

- Installation de l'infrastructure Eclipse*.
- Installation des plug-ins de base.
- Installation des plug-ins du méta-annuaire.
- Installation des plug-ins de la couche d'abstraction de l'annuaire.
- Installation du plug-in de l'éditeur de workflow.

1.4.2 Services

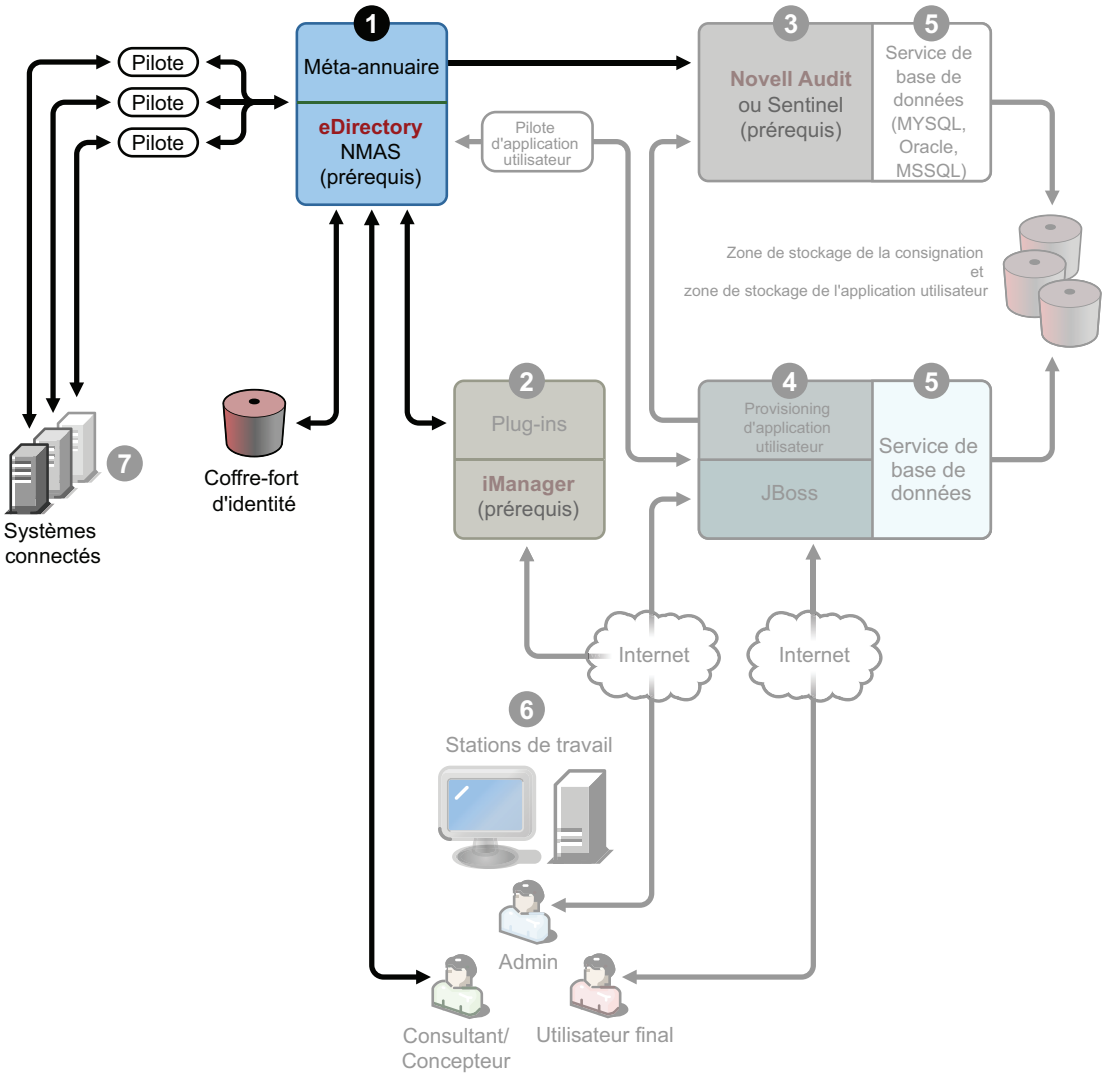
Identité gestionnaire services installation Bien que cela ne soit pas recommandé pour un environnement de production, vous pouvez installer et configurer les sept services sur un seul ordinateur. Vous pouvez également déployer un service par ordinateur, ou n'importe quelle configuration entre les deux. Les prérequis logiciels et matériels pris en charge pour chaque service sont indiqués dans Section 1.5, « Configuration système requise pour Identity Manager », page 28.

- « Service du système méta-annuaire » page 22
- « Service d'administration basé sur le Web » page 23
- « Services de consignation sécurisée » page 24
- « Application utilisateur et module de provisioning » page 25
- « Service de base de données » page 25
- « Postes de travail » page 27
- « Systèmes connectés » page 27

Service du système méta-annuaire

Ce système est utilisé comme coffre-fort d'identité et vous n'avez besoin que d'une instance du moteur méta-annuaire dans un environnement de production.

Figure 1-2 *Service du système méta-annuaire*

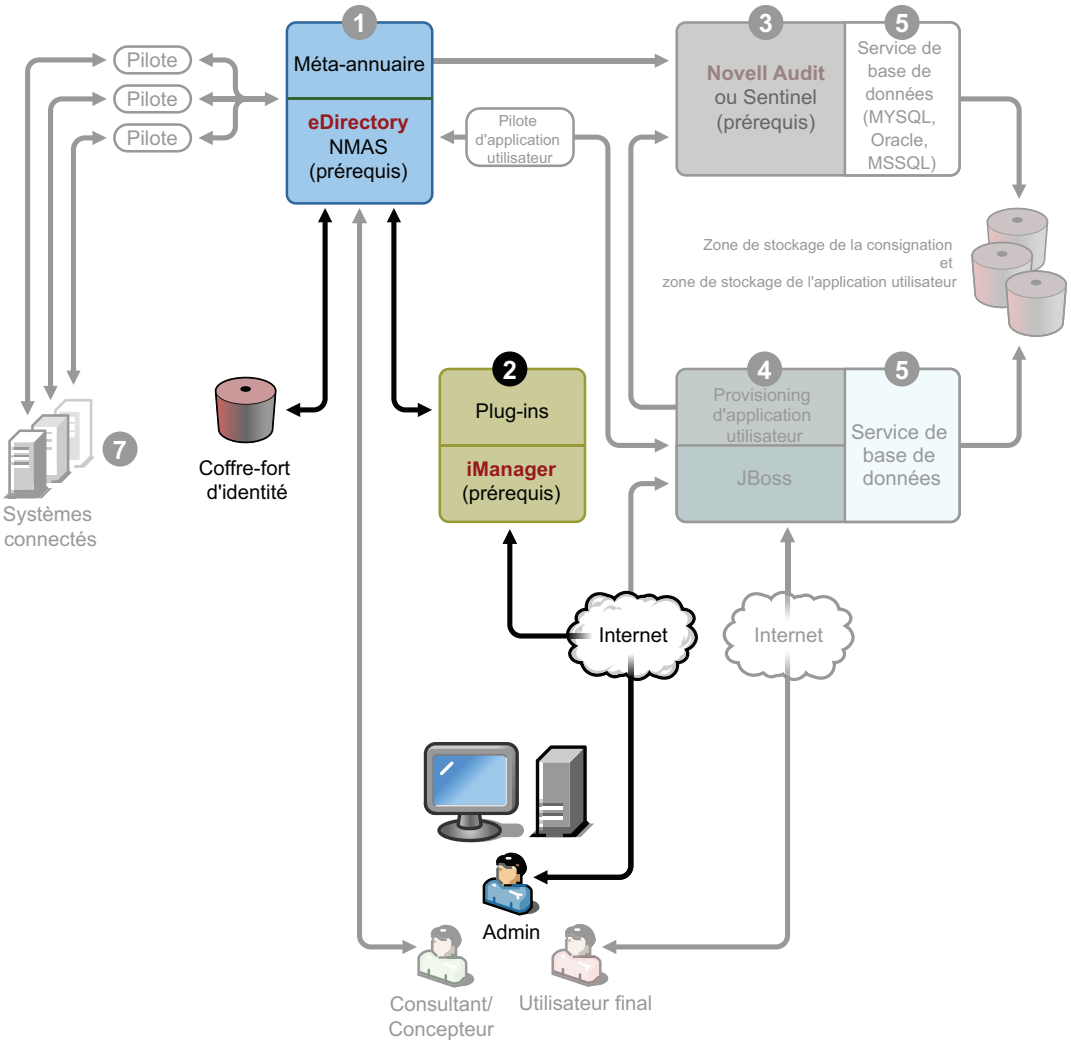


Lorsque les données d'un système changent, le moteur méta-annuaire inclus dans Identity Manager détecte et propage ces changements vers d'autres systèmes connectés selon les règles que vous définissez. Cette solution permet d'extraire des éléments de données spécifiques de sources de données expertes (par exemple, une application RH peut gérer l'ID d'un utilisateur alors qu'un système de messagerie peut contenir des informations sur le compte de messagerie d'un utilisateur).

Pour installer Identity Manager et ce service, reportez-vous à Chapitre 4, « Installation d'Identity Manager », page 67. Pour consulter les prérequis avant d'installer Identity Manager, reportez-vous aux exigences système pour « Système méta-annuaire » page 29.

Service d'administration basé sur le Web

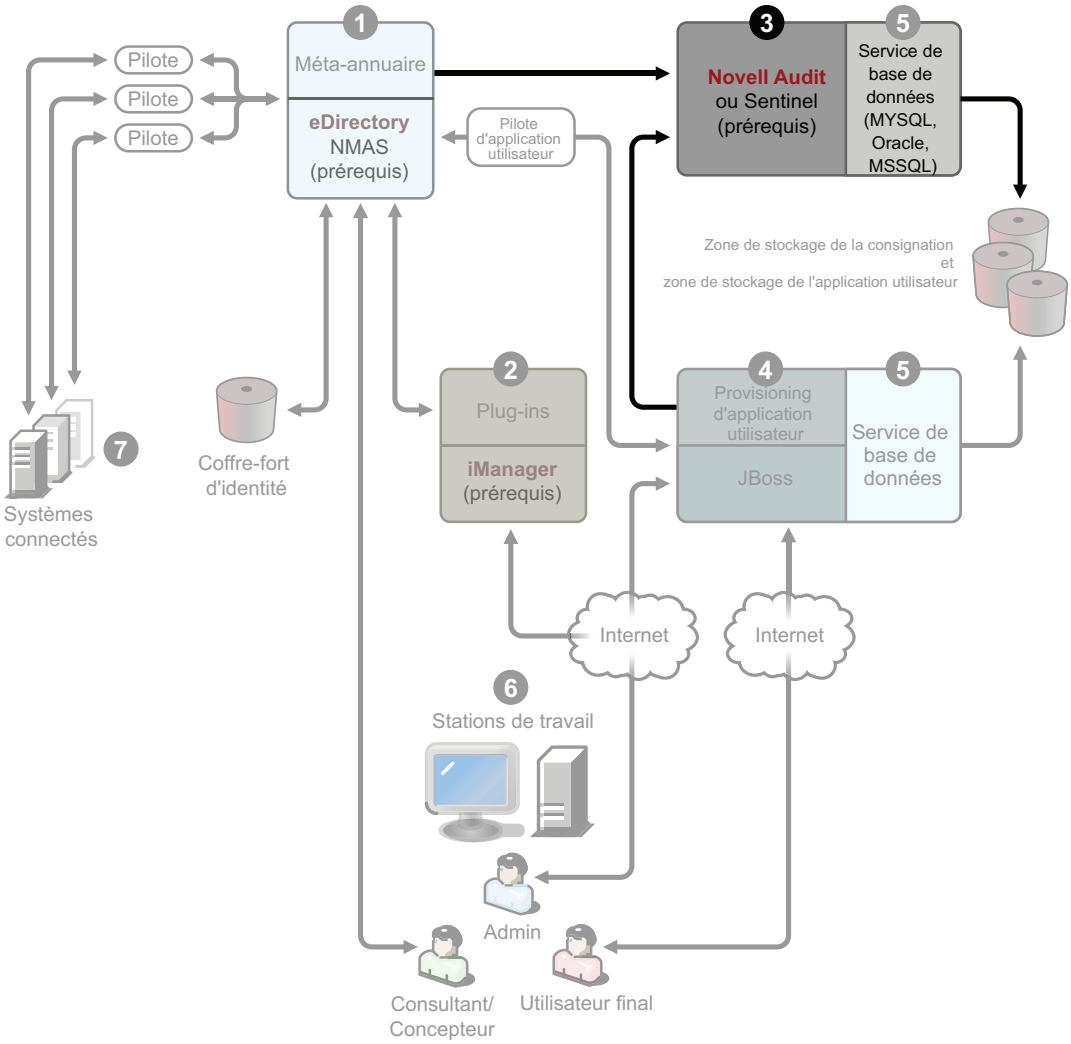
Figure 1-3 *Service d'administration basé sur le Web*



Utilisez ce service pour l'administration d'eDirectory et du système méta-annuaire à l'aide d'iManager 2.5 et des versions supérieures en ayant installé Identity Manager et les plug-ins de l'application utilisateur. Vous installez les plug-ins Identity Manager dans iManager sur le serveur sur lequel vous installez Identity Manager. Pour installer les plug-ins Identity Manager et ce service, reportez-vous à Chapitre 4, « Installation d'Identity Manager », page 67.

Services de consignation sécurisée

Figure 1-4 *Service de consignation sécurisée*

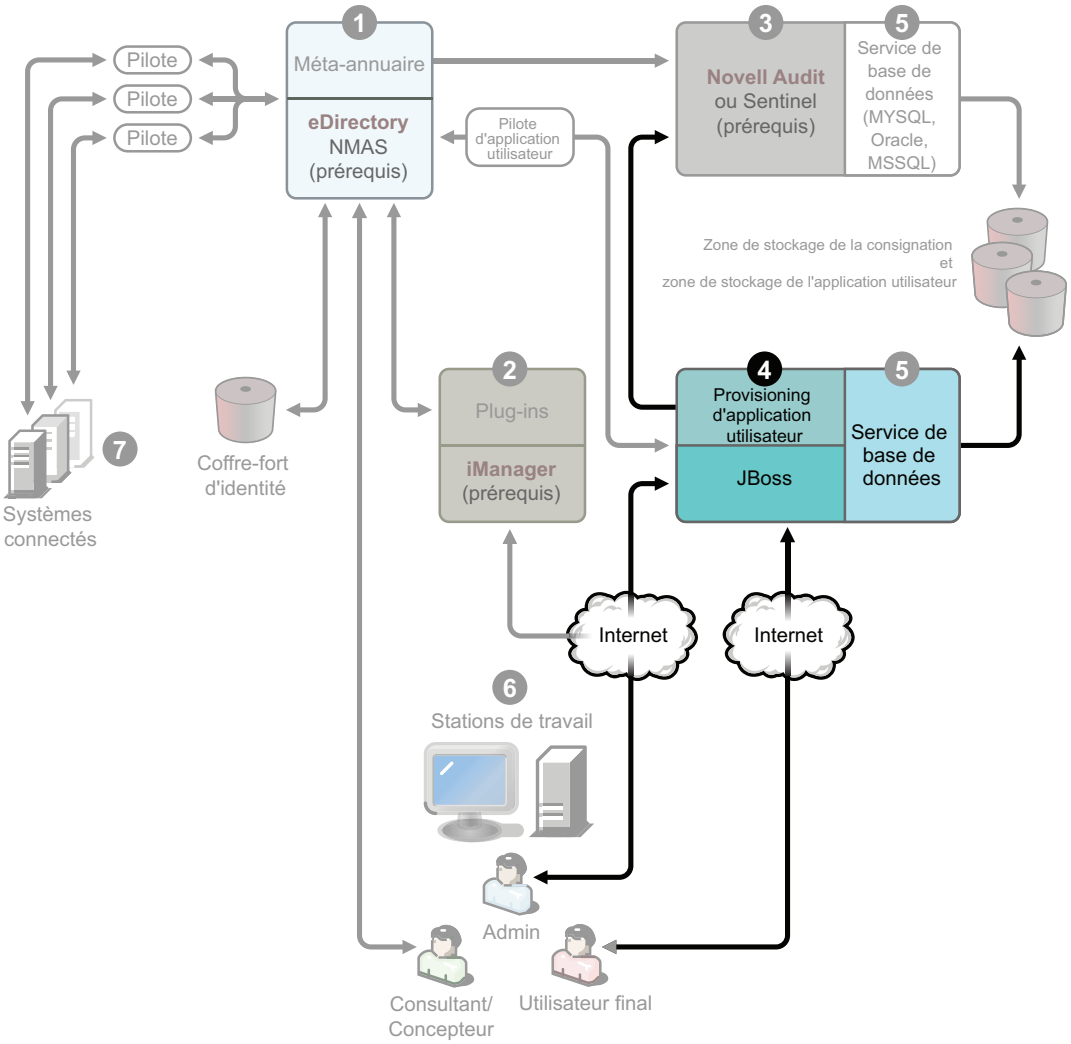


Référentiel de consignation des événements (le logiciel Identity Manager n'est pas installé sur ce serveur, mais un service de consignation sécurisée est obligatoire). Il s'agit d'un service central utilisé par Identity Manager, l'application utilisateur et les services système du workflow. Il est téléchargé séparément depuis le site Web de téléchargement Novell (http://download.novell.com).

Dans le menu déroulant *Product or Technology (Produit ou Technologie)* sur le site Web de téléchargement, sélectionnez *Audit*, puis cliquez sur *Search (Rechercher)*. Cliquez sur *Audit 2.0.2 Starter Pack*. Suivez les instructions d'installation fournies avec le Starter Pack.

Application utilisateur et module de provisioning

Figure 1-5 *Application utilisateur et module de provisioning*

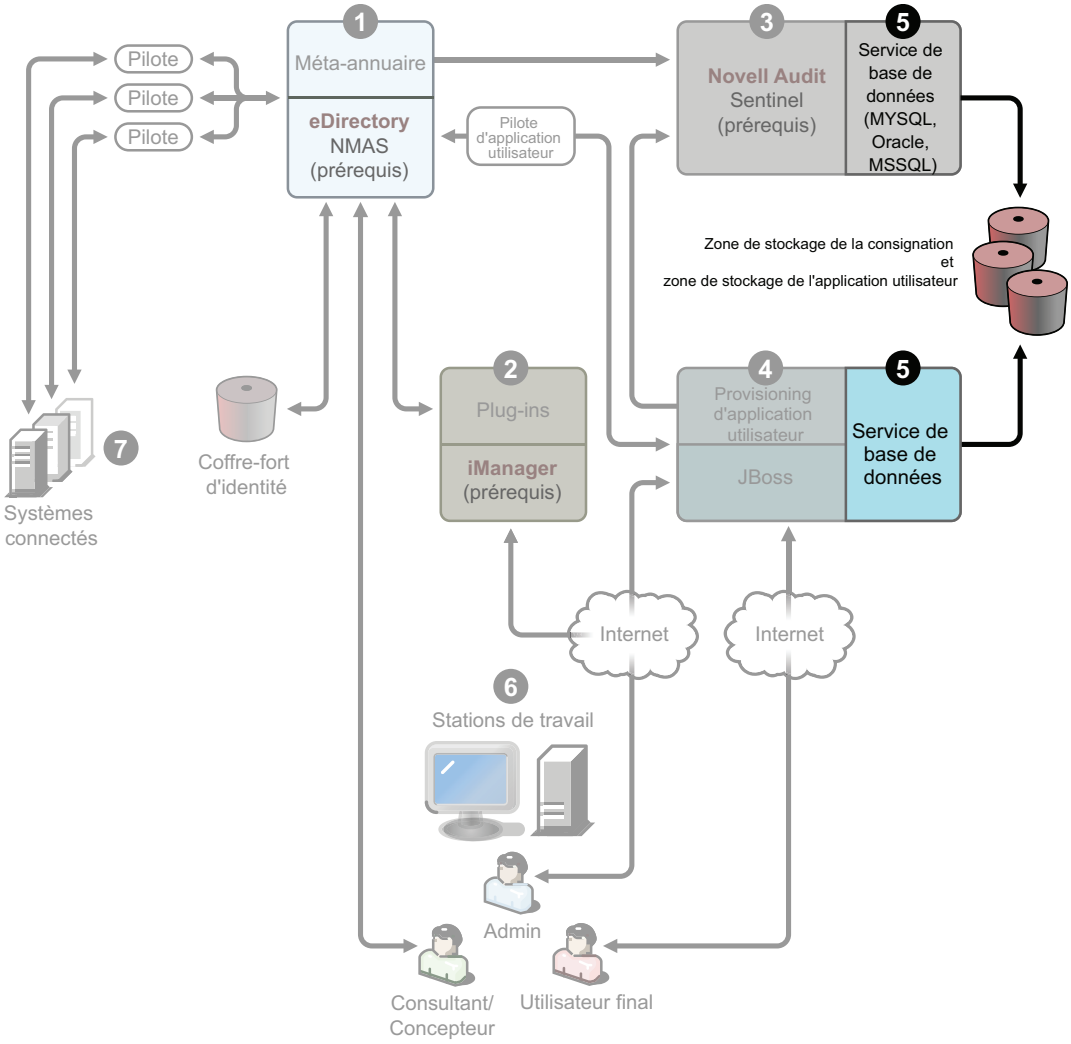


Pour installer ce service, reportez-vous à Chapitre 5, « Installation de l'application utilisateur », page 99. Les prérequis logiciels et matériels pris en charge pour chaque service sont indiqués dans Section 5.1, « Conditions préalables à l'installation », page 99.

Service de base de données

Le service de consignation sécurisée ainsi que le système de workflow/application utilisateur final nécessitent une base de données. Vous pouvez configurer une base de données pour servir les deux applications, ou vous pouvez configurer des bases de données indépendantes pour chacune.

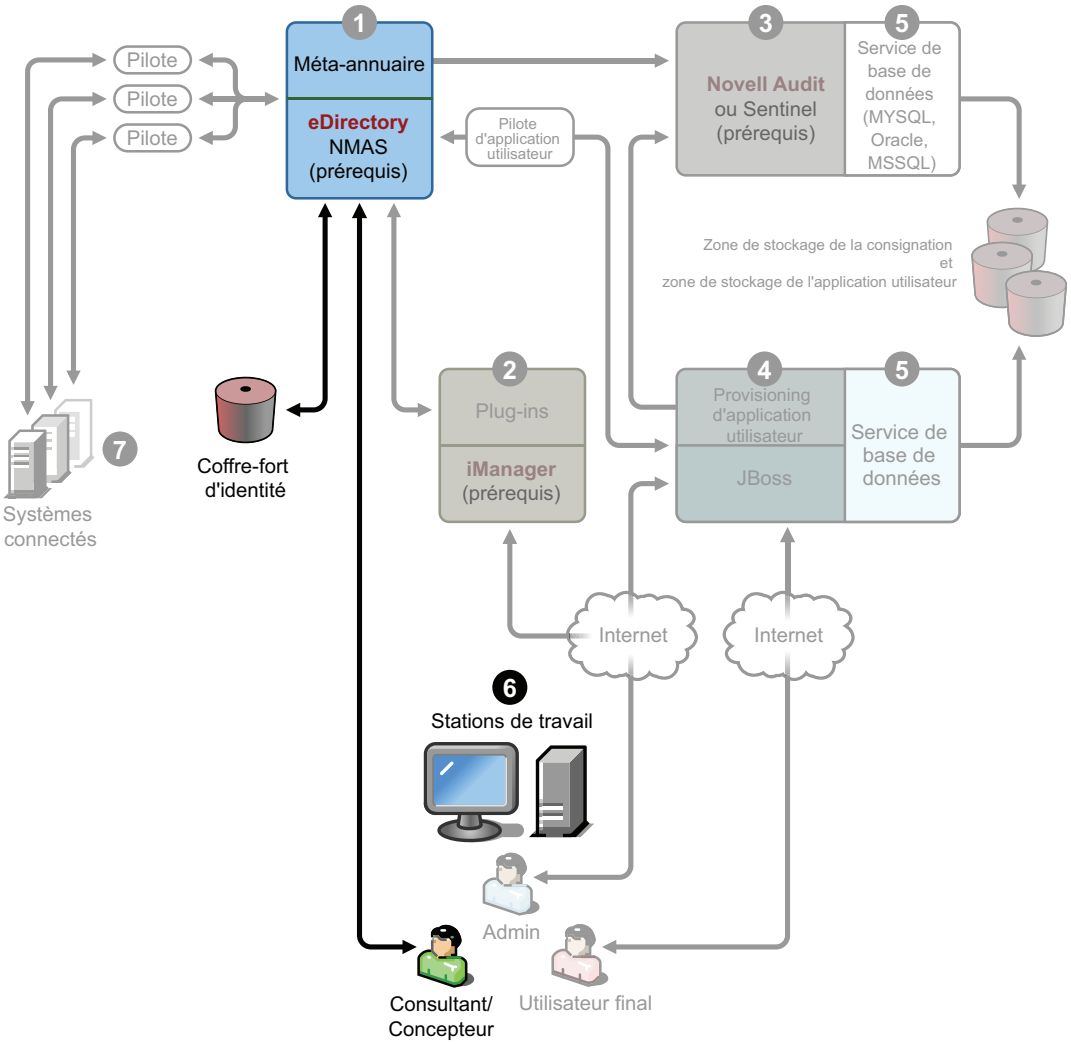
Figure 1-6 *Service de base de données*



Le service de consignation sécurisée ne comprend pas de base de données spécifique. Cependant, vous pouvez utiliser la base de données MySQL qui est fournie avec l'application utilisateur et le provisioning. L'application utilisateur est livrée avecJBoss Application Server Version 4.2.0 et nécessite JRE* 1.5.0_10. Pour installer ce service, reportez-vous à Section 5.2, « Installation et configuration », page 107.

Postes de travail

Figure 1-7 *Services de poste de travail pour le concepteur*

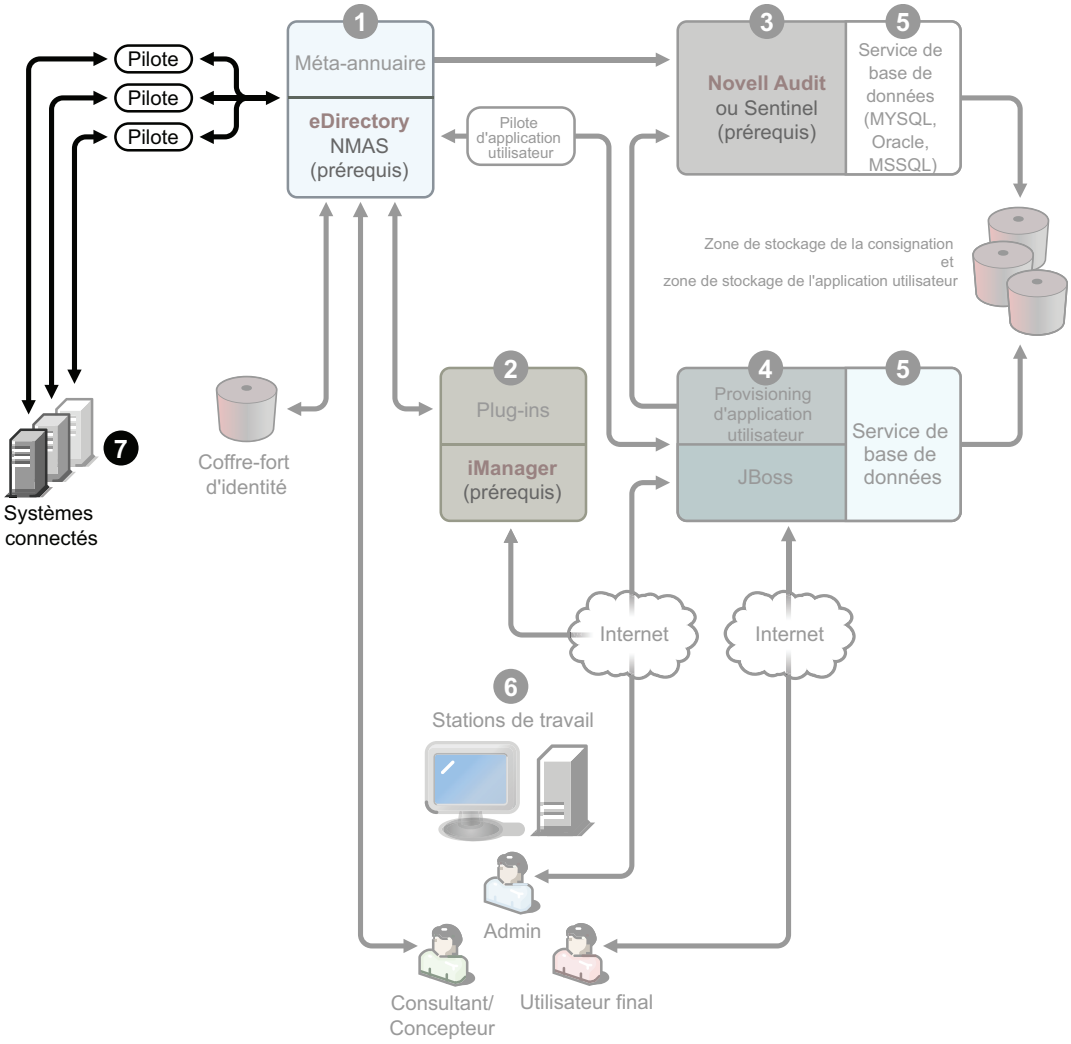


Utilisé pour le concepteur pour concevoir, déployer et documenter le système Identity Manager et pour les utilitaires, rapports et outils inclus dans le produit. Pour installer le concepteur sur un poste de travail, reportez-vous à « Installation » dans le *Manuel de la version 2.1 du concepteur pour Identity Manager 3.5.1*.

Systèmes connectés

Il s'agit de l'endroit où les pilotes sont hébergés ; ces systèmes connectés peuvent être des applications, bases de données, serveurs et autres services. Chaque application connectée exige des connaissances spécifiques à l'application et une responsabilité des individus. Chaque pilote exige que le système connecté soit disponible et les API pertinentes fournies.

Figure 1-8 *Systèmes connectés*



Vous installez les pilotes dans le cadre du processus d'installation d'Identity Manager. Pour installer Identity Manager et ce service, reportez-vous à Chapitre 4, « Installation d'Identity Manager », page 67. Pour en savoir plus sur les pilotes de configuration, lisez la documentation spécifique aux pilotes sur le site Web de la documentation sur les pilotes Identity Manager (http://www.novell.com/documentation/idmdrivers).

1.5 Configuration système requise pour Identity Manager

Novell Identity Manager contient des composants que vous pouvez installer sur plusieurs systèmes et plates-formes de votre environnement. 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.

Le tableau suivant répertorie les composants d'installation d'Identity Manager ainsi que leurs exigences.

Tableau 1-3 *Configuration requise et composants du système Identity Manager*

Composant système	Configuration système requise	Remarques
Système méta-annuaire ◆ Moteur méta-annuaire ◆ L'agent Novell Audit ◆ Pilotes de service ◆ Identity Manager Drivers (Pilotes d'Identity Manager) ◆ Utilitaires (dont les outils d'application et l'outil de configuration Novell Audit)	L'un des systèmes d'exploitation suivants : ◆ NetWare 6.5 avec le dernier Support Pack ◆ Novell Open Enterprise Server (OES) 1.0 avec le dernier Support Pack ◆ Novell Open Enterprise Server (OES) 2.0 ◆ Windows 2000 Server avec le dernier Service Pack (32 bits) ◆ Windows Server 2003 avec le dernier Service Pack (32 bits) ◆ Linux Red Hat 3.0, 4.0 et 5.0 ES et AS (les versions 32 bits et 64 bits sont prises en charge) ◆ SUSE Linux Enterprise Server 9 et 10 avec le dernier Support Pack (prise en charge 32 bits et 64 bits) ◆ Solaris 9 ou 10 ◆ AIX 5.2L, versions 5.2 et 5.3 Une des versions suivantes d'eDirectory : ◆ eDirectory 8.7.3.6 avec le dernier Support Pack ◆ eDirectory 8.8 avec le dernier Support Pack Security Services 2.0.5 (NMAS 3.1.3)	L'utilisation de VMWare* dans votre mise en oeuvre est prise en charge si vous utilisez une plate-forme de système méta-annuaire. Tous les composants logiciels d'Identity Manager de cette version sont 32 bits, même s'ils sont exécutés sur un processeur 64 bits ou avec un système d'exploitation 64 bits. À moins d'indication contraire, les plate-formes OES, NetWare, Windows et Linux (Red Hat et SUSE) prennent en charge tous les processeurs au mode 32 bits : ◆ Intel* x86-32 ◆ AMD x86-32 ◆ Intel EM64T ◆ AMD Athlon64* et Opteron* Identity Manager prend en charge ces fonctions d'eDirectory 8.8 : ◆ Instances multiples d'eDirectory sur le même serveur ◆ Attributs codés eDirectory 8.8 prend en charge Red Hat Linux 4.0 64 bits. Une version 64 bits de la synchronisation des mots de passe sur Windows Server 2003 est disponible. Veillez à sauvegarder toute la base de données eDirectory avant d'installer eDirectory 8.8. eDirectory 8.8 met à niveau des sections de la structure de la base de données et ne lui permettra pas de revenir à l'état initial après le processus de mise à niveau. La virtualisation Xen est désormais prise en charge sur le serveur SUSE Linux Enterprise Server 10 lorsque la machine virtuel (VM) Xen exécute SLES 10 comme système d'exploitation invité au mode paravirtualisé. Un correctif Xen pour SLES 10 est nécessaire (reportez-vous au TID n° 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=20406933&stateId=0%200%200414606)).

Composant système	Configuration système requise	Remarques
Serveur d'administration basé sur le Web ◆ Synchronisation des mots de passe ◆ iManager 2.6 et les plug-ins ◆ iManager 2.7 et les plug-ins ◆ Les configurations des pilotes	L'un des systèmes d'exploitation suivants : ◆ Novell Open Enterprise Server (OES) 1.0 sur NetWare avec le dernier Support Pack ◆ Novell Open Enterprise Server (OES) 2.0 ◆ NetWare 6.5 avec le dernier Support Pack ◆ Windows 2000 Server avec le dernier Service Pack (32 bits) ◆ Windows Server 2003 avec le dernier Service Pack (32 bits) ◆ Microsoft Windows Vista ◆ Linux Red Hat 3.0, 4.0 et 5.0 ES et AS (les versions 32 bits et 64 bits sont prises en charge) ◆ Solaris 9 ou 10 avec le dernier Support Pack ◆ SUSE Linux Enterprise Server 9 et 10 avec le dernier Support Pack (prise en charge 32 bits et 64 bits) Systèmes d'exploitation pris en charge via le poste de travail iManager : ◆ Windows 2000 Professional avec le dernier Service Pack ◆ Windows XP avec SP2 ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 Le logiciel suivant. ◆ Novell iManager 2.6 et 2.7 avec le support pack et les plug-ins les plus récents	Tous les composants logiciels d'Identity Manager de cette version sont 32 bits, même s'ils sont exécutés sur un processeur 64 bits ou avec un système d'exploitation 64 bits. À moins d'indication contraire, les plates-formes OES, NetWare, Windows et Linux (Red Hat et SUSE) prennent en charge tous les processeurs suivants au mode 32 bits : ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 et Opteron ◆ La prise en charge du navigateur est déterminée par iManager 2.6. Cette liste comprend actuellement : ◆ Internet Explorer 6, SP1 et versions supérieures ◆ Internet Explorer 7 ◆ Firefox* 2.0 et versions supérieures ◆ Vous devez passer par l'assistant de configuration iManager ou le concepteur pour installer ou déployer le contenu du portail dans eDirectory. ◆ (Windows) Le logiciel Novell Client™ 4.9 est disponible sur le site de téléchargement de logiciels Novell (http://download.novell.com/index.jsp). ◆ Lors de la consignation dans d'autres arborescences avec iManager pour gérer les serveurs distants Identity Manager, vous rencontrerez peut-être des erreurs si vous utilisez le nom du serveur au lieu de l'adresse IP du serveur distant. ◆ Seul l'agent de synchronisation des mots de passe est pris en charge sous Windows 2003 64 bits.

Composant système	Configuration système requise	Remarques
Service de consignation sécurisée ◆ Le serveur de consignation sécurisée ◆ L'agent de plate-forme (composant client) ◆ Novell Audit 2.0.2 ou Sentinel 5.1.3	Pour le serveur de consignation sécurisée, un des systèmes d'exploitation suivants : ◆ Novell Open Enterprise Server (OES) 1.0 et 2.0 le support pack le plus récent ◆ NetWare 6.5 avec le dernier Support Pack ◆ Windows 2000 Server avec le dernier Service Pack (32 bits) ◆ Windows 2003 Server avec le dernier Service Pack (32 bits) ◆ Red Hat Linux 3.0, 4.0 ou 5.0 AS et ES (32 bits et 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits) ◆ Solaris 9 ou 10 avec le dernier Support Pack ◆ SUSE Linux Enterprise Server 9 ou 10 (32 bits et 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits) ◆ Novell eDirectory 8.7.3.6 ou 8.8 avec le support pack le plus récent (doit être installé sur le serveur de consignation sécurisée) Pour l'agent de plate-forme, un des systèmes d'exploitation suivants : ◆ Novell Open Enterprise Server (OES) 1.0 SP1 ou le dernier Support Pack ◆ NetWare 6.5 avec le dernier Support Pack ◆ Serveur Windows 2000 ou 2000, XP ou Windows Server 2003 avec le dernier Service Pack (32 bits) ◆ Red Hat Linux 3 ou 4 AS et ES (32 bits et 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits) ◆ Solaris 8, 9 ou 10 ◆ SUSE Linux Enterprise Server 9 ou 10 (32 bits et 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits) iManager 2.6 et 2.7 avec le support pack et les plug-ins les plus récents	Les plates-formes OES, NetWare, Windows et Linux (Red Hat et SUSE) prennent en charge tous les processeurs suivants au mode 32 bits : ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 et Opteron La configuration minimum requise pour le serveur sécurisé comprend : ◆ Un seul processeur, PC de classe serveur avec Pentium* II 400 MHz ◆ Un minimum de 40 Mo d'espace disque ◆ 512 Mo de RAM L'instrumentation eDirectory, qui permet la consignation d'événements eDirectory, prend en charge les versions suivantes d'eDirectory : ◆ eDirectory 8.7.3 (NetWare, Windows, Linux et Solaris) ◆ eDirectory 8.8 avec le support pack le plus récent L'instrumentation NetWare, qui permet la consignation d'événements NetWare, prend en charge les versions suivantes de NetWare : ◆ NetWare 5.1 avec le dernier Support Pack ◆ NetWare 6.0 avec le dernier Support Pack ◆ NetWare 6.5 ou NetWare 6.5 avec le dernier Support Pack ◆ Novell Open Enterprise Server (OES) avec le dernier Support Pack

Composant système	Configuration système requise	Remarques
Application utilisateur	**Serveur d'applications** L'application utilisateur s'exécute sur JBoss et WebSphere, comme indiqué ci-dessous. JBoss 4.2.0 est pris en charge sur : ◆ Novell Open Enterprise Server (OES) 1.0 SP2 ou le support pack le plus récent -- Linux seulement ◆ Novell Open Enterprise Server (OES) 2--SLES 10 SP1 et NetWare 6.5 SP7 ◆ SUSE Linux Enterprise Server 9 SP2 (inclus dans OES 1.0 SP2) et 10.1.x (JVM 64 bits*) ◆ Windows 2000 Server avec SP4 (32 bits) ◆ Windows 2003 Server avec SP1 (32 bits) ◆ Solaris 10 support pack daté du 6/06 WebSphere 6.1 est pris en charge sur : ◆ Solaris 10 (64 bits) ◆ Windows 2003 SP1 WebLogic 10 est pris en charge sur : ◆ Solaris 10 (64 bits) ◆ Windows Server 2003 SP1 L'application utilisateur requiert JRE* 1.5.0_10 (reportez-vous à Section 5.1, « Conditions préalables à l'installation », page 99) **Navigateur** L'application utilisateur prend en charge Firefox et Internet Explorer, comme indiqué ci-dessous. Firefox 2 est pris en charge sur : ◆ Windows 2000 Professionnel avec SP4 ◆ Windows XP avec SP2 ◆ Red Hat Enterprise Linux WS 4.0 ◆ Novell Linux Desktop 9 ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 Internet Explorer 7 est pris en charge sur : ◆ Windows 2000 Professionnel avec SP4 ◆ Windows XP avec SP2 ◆ Windows Vista Enterprise version 6 Internet Explorer 6 est pris en charge sur : ◆ Windows 2000 Professionnel avec SP4 ◆ Windows XP avec SP2	SUSE Linux Enterprise Server prend en charge les processeurs suivants au mode 32 bits : ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 et Opteron SUSE Linux Enterprise Server fonctionnera au mode 64 bits sur les processeurs suivants : ◆ Intel EM64T ◆ AMD Athlon64 ◆ AMD Opteron ◆ Sun* SPARC* La virtualisation Xen* est désormais prise en charge sur le serveur SUSE Linux Enterprise Server 10 lorsque la machine virtuel (VM) Xen exécute SLES 10 comme système d'exploitation invité au mode paravirtualisé. Un correctif Xen pour SLES 10 est nécessaire (reportez-vous au TID n° 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=20406933&stateId=0%200%200414606)).

Composant système	Configuration système requise	Remarques
Serveur de base de données pour l'application utilisateur ◆ MySQL ◆ Oracle ◆ MS SQL ◆ DB2	Les bases de données suivantes sont prises en charge avec JBoss : ◆ MySQL version 5.0.27 ◆ Oracle 9i (9.2.0.1.0 et 9.2.0.5.0) ◆ Oracle 10g version·2 (10.2.0.) ◆ MS SQL 2005 avec SP1 Les bases de données suivantes sont prises en charge avec WebSphere : ◆ Oracle 10g version·2 (10.2.0.) ◆ MS SQL 2005 avec SP1 ◆ DB2 DV2 v9.1.0.0	L'application utilisateur utilise une base de données pour diverses tâches, telles que le stockage des données de configuration et le stockage de données pour toute activité de workflow en cours. Le service de consignation sécurisée ainsi que l'application utilisateur et le provisioning de workflow nécessitent une base de données. Vous pouvez configurer une base de données pour servir les deux applications, ou vous pouvez configurer des bases de données indépendantes pour chacune. Le service de consignation sécurisée ne comprend pas de base de données spécifique. Oracle est pris en charge avec le pilote du client léger et le pilote du client OCI.
Postes de travail ◆ Concepteur ◆ Accès en ligne à iManager	Le concepteur a été testé sur les plates-formes suivantes : Windows : ◆ Windows 2000 Professional avec le dernier Service Pack ◆ Windows XP SP2 ◆ Windows Server 2003 avec le dernier Service Pack (32 bits) ◆ Microsoft Windows Vista Linux : ◆ SUSE Linux Enterprise Server 10 (concepteur uniquement) ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ Red Hat Linux 4.0 (concepteur uniquement) ◆ Red Hat Fedora* Core 5 (Designer uniquement) ◆ Novell Linux Desktop 9 ◆ GNOME*, KDE, Red Hat Fedora	Le concepteur utilise Eclipse comme plate-forme de développement. Reportez-vous au site Web d'Eclipse (http://www.eclipse.org/) pour obtenir des informations spécifiques à la plate-forme. Configuration matérielle minimum et recommandée pour le concepteur : ◆ 1 GHz minimum ; 2 GHz ou plus recommandés. ◆ 512 Mo de RAM minimum ; 1 Go de RAM ou plus recommandé. ◆ Résolution minimum 1024 x 768 ; 1280 x 1024 recommandé. Logiciels prérequis : ◆ Microsoft Internet Explorer 6.0 avec SP1 ◆ Microsoft Internet Explorer 7 ◆ ou Mozilla* Firefox 2.0

Composant système	Configuration système requise	Remarques
Serveur de système connecté (hôte sur un serveur séparé exécutant le chargeur distant) ◆ Chargeur distant ◆ Outil de configuration du chargeur distant (Windows uniquement) ◆ L'agent Novell Audit ◆ Agent de synchronisation des mots de passe ◆ Un module d'interface pilote pour le système connecté ◆ Outils pour le système connecté	Chaque pilote exige que le système connecté soit disponible et les API pertinentes fournies. Reportez-vous à la documentation sur les pilotes Identity Manager (http://www.novell.com/documentation/idmdrivers) pour connaître les exigences de système d'exploitation et de système connecté spécifiques à chaque système.	Chaque application connectée exige des connaissances spécifiques à l'application et une responsabilité des individus. Système de chargeur distant : ◆ Windows NT* 4.0, serveur Windows 2000 ou Windows Server 2003 avec les derniers Support Packs ◆ Windows Server 2003 (64 bits) avec le service pack le plus récent ◆ L'agent de synchronisation des mots de passe est pris en charge sous Windows Server 2003 (64 bits). ◆ Red Hat Linux 3.0, 4.0, et 5.0 ES et AS ◆ SUSE® Linux Enterprise Server 9 ou 10 ◆ Solaris 9 ou 10 ◆ AIX 5.2L, versions 5.2 et 5.3 Système de chargeur distant Java : ◆ HP-UX* 11i ◆ OS/400 ◆ zOS* ◆ L'utilisation doit être possible sur tout système équipé de JVM 1.4.2 ou une version supérieure

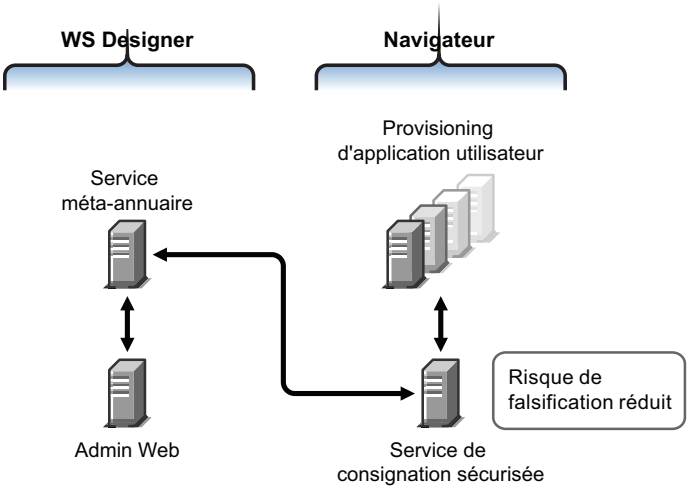
1.6 Stratégies de déploiement recommandées

Comme indiqué précédemment, Identity Manager est fourni avec un certain nombre de services que vous devez installer et configurer. Bien que cela ne soit pas recommandé pour un environnement de production, vous pouvez installer et configurer tous les services nécessaires sur un seul ordinateur. Vous pouvez également déployer un service par serveur, ou n'importe quelle configuration entre les deux.

La charge de travail est le principal facteur de conception des déploiements d'Identity Manager. Plus vous pouvez disperser le trafic, meilleur sera le débit potentiel de vos applications.

La figure 1-3 illustre une stratégie de déploiement possible, avec un serveur pour le service de méta-annuaire, un serveur pour le service d'administration basé sur le Web, un serveur pour le service de consignation sécurisée et un serveur pour l'application utilisateur et le service de provisioning.

Figure 1-9 *Stratégies de déploiement d'Identity Manager*



Service de méta-annuaire

La façon dont vous déployez les services Identity Manager dépend de la charge du service. Par exemple, vous pouvez installer le service de méta-annuaire d'Identity Manager sur un serveur qui communique avec les systèmes connectés. Il suffit d'installer le moteur méta-annuaire sur un serveur exécutant eDirectory.

Étant donné le fort débit potentiel avec iManager, vous devrez peut-être ne pas installer le service d'administration basé sur le Web avec le service méta-annuaire. Si vous installez iManager sur le même serveur que Identity Manager, installez d'abord iManager, puis Identity Manager et ses plug-ins.

Service d'administration basé sur le Web

Si vous avez déjà installé iManager 2.6 sur un serveur, il suffit d'exécuter l'installation d'Identity Manager et d'installer les plug-ins Identity Manager pour iManager. Si vous installez l'application utilisateur et les services de provisioning, vous devez également installer l'application utilisateur et uniquement les plug-ins de l'application utilisateur pour iManager. Vous devrez le faire pour l'application utilisateur ou l'application utilisateur avec le module de provisioning (il s'agit de deux produits distincts).

Application utilisateur et services de consignation sécurisée

Si le volume de vos activités de provisioning est important, nous recommandons que l'application utilisateur soit installée sur son propre serveur. Vous pouvez également configurer la mise en grappe si nécessaire. MySQL 5.0.27-max est inclus avec l'application utilisateur. S'il est déployé dans le cadre du programme d'installation de l'application utilisateur ou du programme d'installation de l'application utilisateur avec le module de provisioning, vous n'avez pas besoin de configurer un autre service de base de données.

Cependant, le service de consignation sécurisée ne comprend pas de base de données spécifique ; le service de consignation sécurisée et le service de provisioning/application utilisateur nécessitent tous deux une base de données. Vous pouvez configurer une base de données pour servir les deux applications ou des bases de données indépendantes pour chacune. Cela dépend de la quantité de provisioning effectué et de la charge du service de consignation.

Remarque : si vous voulez configurer Oracle 9i ou 10g sur un serveur (distant) distinct, vous devez installer Oracle et configurer le serveur d'applications afin qu'il offre un login à distance à la base de données.

Utilisation de la configuration du chargeur distant

Vous pouvez utiliser l'option *Système connecté* lors de l'installation d'Identity Manager si vous ne voulez pas installer de services eDirectory et le moteur méta-annuaire sur un serveur de système connecté. Le chargeur distant offre également un chemin de communication sécurisé entre le moteur méta-annuaire et le pilote via la technologie SSL. N'oubliez pas cela lors du login·de systèmes à Identity Manager.

Pour plus d'informations sur la planification de votre système Identity Manager, reportez-vous à Chapitre 2, « Planification », page 39.

1.7 Où obtenir Identity Manager et ses services

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

Les composants Identity Manager suivants sont téléchargeables.

Tableau 1-4 *Fonctionnement des images ISO*

Composants Identity Manager	Plates-formes	ISO
DVD Identity Manager Les composants Identity Manager suivants sont disponibles sur une image ISO pour graver un DVD. Ces composants sont également téléchargeables individuellement. ◆ Identity Manager et pilotes ◆ Concepteur pour Identity Manager	Identity Manager : Linux, NetWare, Windows et UNIX* Concepteur : Linux et Windows	Identity_Manager_3_5_1_DVD.iso

Composants Identity Manager	Plates-formes	ISO
Identity Manager et pilotes	NetWare et Windows	Identity_Manager_3_5_1_NW_Win.iso
Identity Manager et pilotes	Linux	Identity_Manager_3_5_1_Linux.iso
Identity Manager et pilotes	UNIX	Identity_Manager_3_5_1_Unix.iso
Application utilisateur Il s'agit de la version standard de l'application utilisateur incluse avec votre acquisition d'Identity Manager 3.	Linux et Windows	Identity_Manager_3_5_1_User_Application.iso
Application utilisateur avec le module de provisioning pour Identity Manager Il s'agit de la version de provisioning de l'application utilisateur, qui est un ajout à Identity Manager et requiert un achat séparé.	Linux et Windows	Identity_Manager_3_5_1_User_Application_Provisioning.iso
Concepteur pour Identity Manager	Windows	Identity_Manager_3_5_1_Designer_Win.iso
Concepteur pour Identity Manager	Linux	Identity_Manager_3_5_1_Designer_Linux.iso

Le produit Identity Manager que vous avez acheté comprend les modules d'intégration pour plusieurs systèmes utilisateur courants pour lesquels vous disposez peut-être déjà de licences : Novell eDirectory, Microsoft Active Directory, Microsoft Windows NT, LDAP v3 Directories, Novell GroupWise®, Microsoft Exchange et Lotus Notes. Tous les autres modules d'intégration d'Identity Manager doivent être achetés séparément.

Le composant de l'application utilisateur est fourni sur deux images ISO : l'image ISO de l'application utilisateur est une version standard et qu'elle est incluse dans votre achat d'Identity Manager 3. L'application utilisateur avec le module de provisioning pour Identity Manager est un produit ajouté qui intègre un workflow d'approbation puissant. Ce module de provisioning est fourni sur une image ISO séparée ; il est acheté séparément.

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

1.7.1 Installation d'Identity Manager 3.5.1

- Pour installer Identity Manager 3.5.1 sous Windows, NetWare, UNIX et Linux, reportez-vous à Chapitre 4, « Installation d'Identity Manager », page 67
- Pour installer l'application utilisateur ou l'application utilisateur avec le module de provisioning, reportez-vous à Chapitre 5, « Installation de l'application utilisateur », page 99
- Pour installer Designer, reportez-vous à « Installation de Designer » dans le *Manuel de la version 2.1 de Designer pour Identity Manager 3.5.1*.

Remarque : les programmes d'installation des pilotes de Linux et UNIX (anciennement NIS), Mainframe et Midrange se trouvent dans le répertoire `/platform/setup` . Vous devez exécuter ces installations séparément des programmes d'installation d'Identity Manager et de l'application utilisateur.

Pour répertorier les problèmes connus, reportez-vous au fichier `Lisez-moi` qui est fourni avec Identity Manager.

1.7.2 Activation des produits Identity Manager 3.5.1

Les produits Identity Manager requièrent une activation (sauf le concepteur.) Les produits suivants peuvent être utilisés pendant une période d'évaluation de 90 jours avant de devoir interrompre leur utilisation ou acheter une activation.

- Identity Manager 3.5.1
- Application utilisateur avec le module de provisioning pour Identity Manager
- Modules d'intégration

Important : afin que l'application utilisateur s'active correctement, vous devez télécharger la bonne image ISO. Par exemple, si vous achetez Identity Manager, mais si ensuite vous téléchargez le module de provisioning de l'application utilisateur sans acheter séparément le module de provisioning, la mise en oeuvre de votre application utilisateur arrête de fonctionner au bout de 90 jours.

Pour plus d'informations sur l'activation, reportez-vous à Chapitre 6, « Activation des produits Novell Identity Manager », page 189.

Planification

2

2.1 Planification des aspects de gestion de projets de la mise en oeuvre d'Identity Manager

Cette section définit les aspects politiques de haut niveau et de gestion de projets de la mise en oeuvre d'Identity Manager. (Pour les aspects techniques, reportez-vous à Section 2.3, « Planification des aspects techniques de la mise en oeuvre d'Identity Manager », page 55.)

Ce document de planification fournit une présentation du type d'activités qui sont normalement prises depuis le début d'un projet Identity Manager jusqu'au déploiement complet en production. La mise en oeuvre d'une stratégie de gestion de l'identité demande de découvrir les besoins et les intervenants dans votre environnement, de concevoir une solution, d'obtenir le ralliement des intervenants et de tester et produire la solution. Cette section vise à vous donner les informations nécessaires concernant le processus afin que vous puissiez optimiser les performances d'Identity Manager.

Il est vivement conseillé de faire appel à un expert Identity Manager pour vous assister dans chacune des phases du déploiement de la 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.

Il est vivement conseillé de configurer un environnement de test/développement dans lequel vous pouvez tester, analyser et développer vos solutions. Dès que tout fonctionne comme vous le souhaitez, déployez le produit final dans votre environnement de production.

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.

2.1.1 Déploiement de Novell Identity Manager

Plusieurs activités sont conseillées dans le cadre d'un déploiement optimal d'Identity Manager :

- « Déploiement vers la production » page 45

Découverte

Vous pouvez commencer votre mise en oeuvre d'Identity Manager par un processus de découverte qui permettra effectuer les opérations suivantes :

- Identifier les objectifs principaux de la gestion des informations d'identité
- Définir ou clarifier les objectifs d'entreprise analysés
- Déterminer les initiatives nécessaires pour résoudre les problèmes restants
- Déterminer les ressources nécessaires pour mener une ou plusieurs de ces initiatives
- Développer une stratégie globale ou un « plan de mise en oeuvre de la solution » ainsi qu'une ligne directive approuvée pour son exécution

La procédure de découverte offre à tous les participants une vue claire des problèmes et solutions. Elle fournit une excellente base pour la phase d'analyse qui exige que les participants disposent de connaissances de base concernant les annuaires, Novell Identity Manager et l'intégration XML en général.

- Elle apporte des connaissances de base à tous les participants.
- Elle permet de regrouper les informations clés concernant l'entreprise et les systèmes que chaque participant fournit.
- Elle permet de développer un plan de mise en oeuvre de la solution.

La procédure de découverte identifie également les étapes à effectuer sans plus attendre. Ces étapes peuvent être les suivantes :

- Identification des activités de planification en préparation d'une phase d'évaluation des besoins et de conception
- Définition d'une formation complémentaire destinée aux participants

Principaux livrables

- Entrevues structurées avec tous les participants au projet, c'est-à-dire les professionnels intervenant dans les processus clés de l'entreprise et les techniciens
- Résumé détaillé des problèmes et techniques et d'entreprise
- Recommandations pour les étapes suivantes
- Présentation complète soulignant les résultats de la découverte

Analyse des besoins et de la conception

Cette phase d'analyse capture à la fois tous les aspects techniques et commerciaux du projet et crée un modèle de données ainsi qu'une conception détaillée de l'architecture Identity Manager. Cette activité constitue une étape essentielle et sert de base à la mise en oeuvre de 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. Voici un exemple des éléments que vous pouvez évaluer :

- Quelles sont les versions de logiciels utilisées ?

- La structure de l'annuaire est-elle adaptée ?
- Le répertoire est-il utilisé pour héberger le coffre-fort d'identité et Identity Manager ou pour étendre d'autres services ?
- La qualité des données dans tous les systèmes est-elle suffisante ? (Si la qualité des données est insuffisante, la stratégie commerciale risque de ne pas être mise en oeuvre comme souhaité.)
- La manipulation des données est-elle requise pour votre environnement ?

Après l'analyse des besoins, vous pouvez définir l'étendue et le plan du projet pour la mise en oeuvre et déterminer si des activités préalables doivent être effectuées. Pour éviter des erreurs coûteuses, soyez aussi méticuleux que possible lors de la collecte des informations et de la description des besoins.

Vous pouvez effectuer les tâches suivantes lors de l'évaluation des besoins :

- « Définir les procédures d'entreprise » page 41
- « Analyser vos processus d'entreprise » page 42
- « Conception d'un modèle de données d'entreprise » page 43

Définir les procédures d'entreprise

Collectez les informations relatives aux processus d'entreprise de votre organisation et aux procédures qui définissent ces processus.

Par exemple, une procédure d'entreprise 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.

Les tâches suivantes peuvent vous aider à définir les procédures d'entreprise :

- Établir les flux de processus, les déclencheurs de processus et les relations d'assignation de données.

  Par exemple, si un événement va survenir dans un processus donné, quelles seront les conséquences de ce processus ? Quels sont les autres processus déclenchés ?
- Assigner des flux de données entre les applications.
- Identifier les transformations de données devant être effectuées d'un format à un autre (par exemple de 2/25/2007 à 25 Fév 2007).
- Décrire les dépendances qui existent entre les données.

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

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

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

  Il peut s'avérer nécessaire de diviser le déploiement en phases qui permettront de mettre en oeuvre une première partie de la solution, puis les autres parties ultérieurement. Vous pouvez

également adopter une approche de déploiement par phases. Celle-ci doit être basée sur des groupes de personnes de votre organisation.

- Définir la configuration requise.

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

- Identifier les sources de données expertes.

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

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

Analyser vos processus d'entreprise

L'analyse des processus d'entreprise commence souvent par l'interrogation des personnes clés telles que des directeurs, des administrateurs et des employés qui utilisent effectivement 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 ?

Par exemple, les questions ci-après peuvent être posées à l'administrateur d'un système PeopleSoft de gestion 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 sur le système de provisioning (telles qu'ajouts, modifications ou suppressions) ?
- Lesquelles sont obligatoires ? Lesquelles sont facultatives ?
- Quelles opérations doivent être déclenchées en fonction d'opérations effectuées dans PeopleSoft ?
- Quels événements, opérations et actions doivent être ignorés ?
- Comment les données doivent-elles être transformées et assignées à Identity Manager ?

Les 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.

Conception d'un modèle de données d'entreprise

Une fois vos processus d'entreprise définis, vous pouvez commencer la conception d'un modèle de données qui reflète votre processus d'entreprise actuel.

Le modèle doit indiquer la provenance des données, leur destination ainsi que les déplacements impossibles. Il doit également rendre compte de la manière dont les événements critiques affectent le flux de données.

Vous pouvez également développer un diagramme qui reflète le processus d'entreprise proposé et l'avantage de mettre en oeuvre une solution de provisioning automatisée 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.

Principaux livrables

- Modèle de données affichant tous les systèmes, sources de données expertes, événements, flux d'informations et normes de format de données, et relations d'assignation entre systèmes connectés et attributs au sein d'Identity Manager
- Architecture Identity Manager appropriée pour la solution
- Conditions détaillées pour le login à des systèmes supplémentaires
- Stratégies de validation des données et de concordance des enregistrements
- Conception de l'annuaire pour la prise en charge de l'infrastructure Identity Manager

Dépendances

- Le personnel familier avec tous les systèmes externes (tels que l'administrateur de la base de données HR et l'administrateur en charge du réseau et du système de messagerie)
- Disponibilité des schémas système et de l'exemple de données
- Modèle de données issu de la phase d'analyse et de conception

- Disponibilité des informations de base telles que l'organigramme de l'organisation, l'infrastructure WAN et de serveur

Preuve de conception

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

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

Principaux livrables

- Preuve de la conception d'une solution Identity Manager fonctionnant avec tous les logins système opérationnels

Dépendances

- Plate-forme et équipement matériels
- Logiciels requis
- Phase d'analyse et de conception qui identifie les logins·requis
- Disponibilité et accès aux autres systèmes à des fins de test
- Modèle de données issu de la phase d'analyse et de conception

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.

Principaux livrables

- Ensembles de données de production adaptés au chargement dans le coffre-fort d'identité (tels qu'identifiés dans les activités d'analyse et de conception). Cela comprend la méthode de chargement (chargement en bloc ou via des connecteurs). Les conditions requises pour les données validées ou formatées sont également identifiées.
- Les facteurs de performance sont également identifiés et validés par rapport à l'équipement utilisé et l'architecture distribuée générale du déploiement d'Identity Manager.

Dépendances

- Le modèle de données issu de la phase d'analyse et de conception (concordance des enregistrements et stratégie de format des données proposées)
- Accès aux ensembles de données de production

Pilote de production

L'objectif de cette activité est de commencer la migration vers l'environnement de production. Pendant cette phase, des opérations de personnalisation supplémentaires peuvent avoir lieu. Dans cette courte introduction, les résultats des activités précédentes peuvent être confirmés et un accord peut être conclu pour le déploiement vers la production.

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

Principaux livrables

- Solution de pilote qui propose une preuve de conception en direct et une validation du modèle de données et des résultats de processus souhaités

Dépendances

- Toutes les activités précédentes (analyse et conception, plate-forme de technologie Identity Manager).

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 l'introduction du coffre-fort d'identité dans une coexistence mixte
- Confirmer les stratégies de partitionnement et de réplication
- Confirmer la mise en oeuvre d'Identity Manager
- Planifier le passage au nouveau processus
- Planifier une stratégie de retour à l'état initial en cas d'incident

Principaux livrables

- Plan de déploiement de production
- Plan de passage au nouveau processus
- Plan de secours de retour à l'état initial en cas d'incident

Dépendances

- Toutes les activités précédentes

Déploiement vers la production

Il s'agit de la phase dans laquelle la solution de pilote est étendue afin de prendre en compte toutes les données actuelles de l'environnement de production. Elle s'appuie généralement sur le fait que le pilote de production répond à tous les critères techniques et d'entreprise.

Principaux livrables

- Solution de production prête pour la transition

Dépendances

- Toutes les activités précédentes

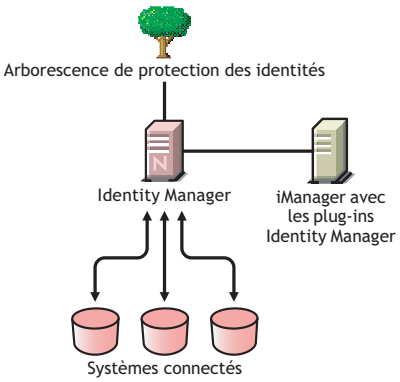
2.2 Planification des scénarios d'installation courants

Les scénarios suivants sont des exemples de l'environnement dans lequel Identity Manager pourrait être utilisé. Pour chaque scénarioso, des directives sont fournies pour vous aider dans votre mise en oeuvre.

- Section 2.2.1, « Nouvelle installation d'Identity Manager », page 46
- Section 2.2.2, « Utilisation d'Identity Manager et de DirXML 1.1a dans le même environnement », page 48
- Section 2.2.3, « Mise à niveau depuis le Starter Pack vers Identity Manager », page 50
- Section 2.2.4, « Mise à niveau depuis la version 1.0 de la synchronisation des mots de passe vers la version Identity Manager », page 52

2.2.1 Nouvelle installation d'Identity Manager

Figure 2-1 *Nouvelle installation*



Identity Manager est une solution de partage des données qui exploite votre coffre-fort d'identité pour synchroniser, transformer et distribuer automatiquement les informations entre les applications, les bases de données et les annuaires.

Votre solution Identity Manager comprend les composants suivants :

- « Coffre-fort d'identité avec Identity Manager » page 47
- « iManager Server avec les plug-ins Identity Manager » page 47
- « Systèmes connectés » page 47
- « Tâches courantes d'Identity Manager » page 47

Coffre-fort d'identité avec Identity Manager

Le coffre-fort d'identité contient les données de l'utilisateur ou de l'objet que vous voulez partager ou synchroniser avec d'autres systèmes connectés. Il est conseillé d'installer Identity Manager dans sa propre instance eDirectory™ et de l'utiliser comme coffre-fort d'identité.

iManager Server avec les plug-ins Identity Manager

Vous utilisez Novell iManager et les plug-ins Identity Manager pour administrer votre solution Identity Manager.

Systèmes connectés

Les systèmes connectés peuvent comprendre d'autres applications, répertoires et bases de données dont vous voulez partager ou synchroniser les données avec le coffre-fort d'identité. Pour établir un login depuis votre coffre-fort d'identité vers le système connecté, installez le pilote approprié à ce système connecté. Reportez-vous aux guides de mise en oeuvre des pilotes (http://www.novell.com/documentation/idm35drivers/index.html) pour obtenir des instructions spécifiques.

Tâches courantes d'Identity Manager

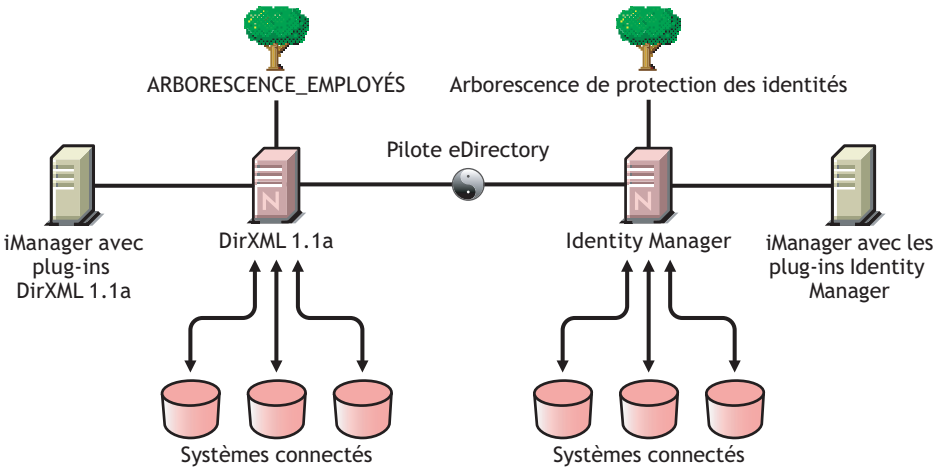
- **Installation de composants système :** comme votre solution Identity Manager peut être distribuée sur plusieurs ordinateurs, serveurs ou plates-formes, vous devez exécuter le programme d'installation et installer les composants appropriés au système. Reportez-vous à Section 1.4, « Programmes d'installation et services Identity Manager », page 19 pour plus d'informations.
- **Configuration de systèmes connectés :** reportez-vous à Section 1.4, « Programmes d'installation et services Identity Manager », page 19 et aux guides de mise en oeuvre des pilotes (http://www.novell.com/documentation/idm35drivers/index.html) pour obtenir des instructions spécifiques.
- **Activation de votre solution :** les produits Identity Manager (professionnels, éditions serveur, modules d'intégration et applications utilisateur) requièrent une activation sous 90 jours suivant l'installation. Reportez-vous à Chapitre 6, « Activation des produits Novell Identity Manager », page 189.
- **Définition de stratégies commerciales :** les stratégies commerciales permettent de personnaliser le flux d'informations entrant et sortant du coffre-fort d'identité pour un environnement particulier. Les stratégies créent aussi de nouveaux objets, mettent à jour des valeurs d'attributs, apportent des transformations aux schémas, définissent des critères de correspondance, gèrent des associations Identity Manager, etc. Un guide détaillé des stratégies est fourni dans *Stratégies d'iManager pour Identity Manager 3.5.1*.
- **Configuration de la gestion des mots de passe :** grâce à des stratégies de mots de passe, vous pouvez configurer des règles de création de mots de passe par les utilisateurs pour augmenter la sécurité. Pour réduire les coûts d'assistance technique, vous pouvez également fournir aux utilisateurs des options de libre service pour les mots de passe oubliés et pour la réinitialisation de mots de passe. Pour obtenir des informations détaillées sur la gestion des mots de passe, reportez-vous à Gestion des mots de passe à l'aide de stratégies de mots de passe (http://www.novell.com/documentation/password_management31/index.html?page=/documentation/password_management31/pwm_administration/data/ampxjj0.html).
- **Configurer les droits :** les définitions des droits permettent d'accorder des droits sur des systèmes connectés à un groupe défini d'utilisateurs dans le coffre-fort d'identité. Les stratégies de droit permettent de rationaliser la gestion des stratégies d'entreprise et de limiter la

configuration des pilotes Identity Manager nécessaires. Pour plus d'informations, reportez-vous à « Création et utilisation de droits » dans le *Guide d'administration Novell Identity Manager 3.5.1*.

- **Consignation d'événements avec Novell Audit :** identity Manager est paramétré pour utiliser Novell Audit à des fins d'audit et de création de rapport. Novell Audit est un recueil de technologies fournissant des capacités de surveillance, de consignation, de création de rapports et de notification. Grâce à l'intégration avec Novell Audit, Identity Manager fournit des informations détaillées sur l'état actuel et passé de l'activité du pilote et du moteur. Ces informations sont fournies par un ensemble de rapports préconfigurés, de services de notification standard et d'une consignation définie par l'utilisateur. Reportez-vous à « Utilisation des journaux d'état » dans *Consignation et rapports dans Identity Manager 3.5.1*.
- **Approbation de workflow et application utilisateur :** l'application utilisateur Novell Identity Manager est une application Web puissante (avec des outils de prise en charge), conçue pour fournir une expérience riche, intuitive, hautement configurable et hautement administrable sur une structure sophistiquée de services d'identité. Utilisée conjointement au module de provisioning pour Identity Manager et à Novell Audit, l'application utilisateur Identity Manager offre une solution complète de provisioning de bout en bout qui est à la fois sécurisée, évolutive et facile à gérer. Reportez-vous à la Documentation sur l'application utilisateur (http://www.novell.com/documentation/idm35).

2.2.2 Utilisation d'Identity Manager et de DirXML 1.1a dans le même environnement

Figure 2-2 *Installation d'Identity Manager dans la même arborescence que DirXML 1.1a*



Si vous exécutez Identity Manager et DirXML® 1.1a dans le même environnement, n'oubliez pas ce qui suit :

- « Création d'un coffre-fort d'identité » page 49
- « Outils de gestion » page 49
- « Compatibilité avec les versions précédentes » page 49
- « Gestion des mots de passe » page 50

Création d'un coffre-fort d'identité

Il est conseillé d'installer Identity Manager dans une instance eDirectory distincte et de l'utiliser comme coffre-fort d'identité.

Outils de gestion

- ConsoleOne® est pris en charge pour DirXML 1.1a, mais pas pour Identity Manager.
- Deux serveurs iManager sont nécessaires, un pour les plug-ins DirXML 1.1a et un pour les plug-ins Identity Manager. Les plug-ins ont été améliorés et Identity Manager utilise le script DirXML.
- Les plug-ins iManager pour DirXML 1.1a ne peuvent pas lire le script DirXML, qui est utilisé dans la configuration du pilote définie pour la plupart des pilotes Identity Manager.
- Le concepteur est un outil qui permet de concevoir, tester, mettre à jour et documenter les pilotes Identity Manager.

Compatibilité avec les versions précédentes

- Vous pouvez exécuter les modules d'interface et les configurations des pilotes DirXML 1.1a sur un serveur Identity Manager et vous pouvez afficher les pilotes dans iManager dans la présentation Identity Manager de l'ensemble des pilotes. Cependant, les plug-ins Identity Manager ne permettent pas d'afficher ni de modifier la configuration des pilotes avant de les avoir convertis au format Identity Manager.

  Dans les plug-ins Identity Manager, si vous cliquez sur un pilote qui est au format 1.1a, vous êtes invité à effectuer la conversion. Il s'agit d'un processus simple effectué avec un assistant et cela ne modifie pas la fonction de la configuration des pilotes. Dans le cadre du processus, une copie de sauvegarde de la version DirXML 1.1a est enregistrée.
- L'activation des pilotes DirXML 1.1a est toujours valide lors de leur exécution avec le moteur Identity Manager. Cependant, si vous mettez à niveau le module d'interface pilote vers une version d'Identity Manager, vous devez obtenir une nouvelle référence d'activation. Reportez-vous à Annexe 6, « Activation des produits Novell Identity Manager », page 189 pour plus d'informations.
- Dans la plupart des cas, un module d'interface pilote Identity Manager peut être exécuté avec une configuration DirXML 1.1a. Reportez-vous aux guides de mise en oeuvre des pilotes (http://www.novell.com/documentation/idm35drivers/index.html) individuels pour obtenir des informations sur la mise à niveau.

  Une exception notable est que la version 1.0 de la synchronisation des mots de passe n'est pas correctement exécutée sous Windows AD et Windows NT après la mise à niveau du module d'interface pilote à moins d'ajouter des stratégies de pilote. Pour obtenir des instructions, reportez-vous aux sections sur la version de la synchronisation des mots de passe dans les guides de mise en oeuvre des pilotes (http://www.novell.com/documentation/idm35drivers/index.html) pour les pilotes Identity Manager pour Active Directory et NT Domain.
- L'exécution des configurations de pilote et des modules d'interface pilote Identity Manager avec le moteur DirXML 1.1a n'est pas prise en charge.
- L'exécution des configurations de pilote Identity Manager avec les modules d'interface pilote DirXML 1.1a n'est pas prise en charge.

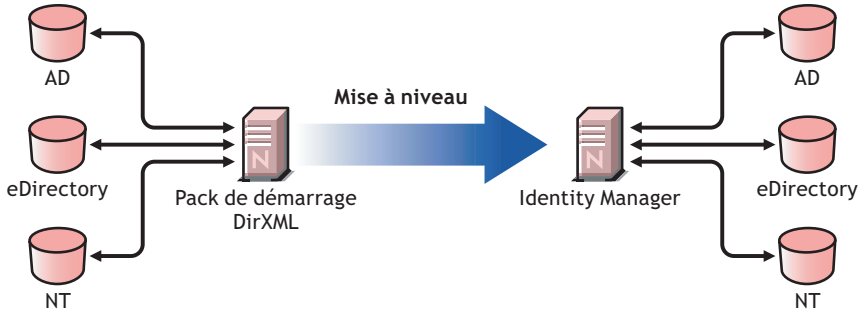
- Si vous exécutez la même configuration pilote Identity Manager sur plusieurs serveurs, veillez à ce que les serveurs exécutent la même version d'Identity Manager, et la même version d'eDirectory.

Gestion des mots de passe

- Vous pouvez créer des stratégies de mot de passe qui présentent des fonctions telles que des règles de mot de passe avancées pour exiger des mots de passe plus forts, ainsi que des mots de passe oubliés en libre service et la réinitialisation de mots de passe en libre service pour les utilisateurs. Reportez-vous à la section Synchronisation de la gestion des mots de passe dans le Guide de la gestion des mots de passe 3.1 (http://www.novell.com/documentation/password_management31/index.html).
- Si vous avez commencé à utiliser un mot de passe universel avec la version initiale de NetWare® 6.5, des étapes de mise à niveau sont nécessaires avant de pouvoir utiliser les nouvelles fonctions de stratégies de mot de passe. Reportez-vous à (NetWare 6.5 uniquement) Déploiement d'un mot de passe universel dans le Guide de gestion des mots de passe 3.1 (http://www.novell.com/documentation/password_management31/index.html). Cette procédure n'est pas nécessaire si vous avez commencé à utiliser le mot de passe universel avec NetWare 6.5 SP2.
- La version de la synchronisation des mots de passe Identity Manager offre une synchronisation des mots de passe bidirectionnelle et prend en charge plus de plates-formes que la version 1.0 de la synchronisation des mots de passe.
- Si vous utilisez la version 1.0 de la synchronisation des mots de passe sous Windows AD ou Windows NT, veillez à relire les instructions de mise à niveau avant d'installer les nouveaux modules d'interface pilote. Reportez-vous à Section 2.2.4, « Mise à niveau depuis la version 1.0 de la synchronisation des mots de passe vers la version Identity Manager », page 52.
- Des « recouvrements » de stratégies de pilote sont fournis pour vous aider à ajouter une fonction bidirectionnelle de synchronisation des mots de passe aux pilotes existants. Reportez-vous à « Mise à niveau des configurations pilote existantes pour prendre en charge la version de la synchronisation des mots de passe » dans le *Guide d'administration Novell Identity Manager 3.5.1*.

2.2.3 Mise à niveau depuis le Starter Pack vers Identity Manager

Figure 2-3 *Mise à niveau depuis le Starter Pack vers Identity Manager*



Les solutions du Starter Pack Identity Manager incluses avec d'autres produits Novell offrent une synchronisation licenciée des informations contenues dans les domaines NT, Active Directory et

eDirectory. De plus, des pilotes d'évaluation pour plusieurs autres systèmes, y compris PeopleSoft, GroupWise® et Lotus Notes, sont fournis pour permettre d'explorer la synchronisation des données de vos autres systèmes.

Cette solution permet également de synchroniser les mots de passe utilisateur. Avec PasswordSync, un utilisateur ne doit se rappeler que d'un mot de passe pour se loguer à n'importe lequel de ces systèmes. Les administrateurs peuvent gérer les mots de passe du système de leur choix. À chaque fois qu'un mot de passe est changé dans l'un de ces environnements, il est mis à jour dans tous les autres.

Les Starter Packs Identity Manager fournis avec NetWare 6.5 et Nterprise™ Linux Services 1.0 étaient basés sur la technologie DirXML 1.1a. Lors de la mise à niveau depuis un Starter Pack vers la dernière version d'Identity Manager, n'oubliez pas ce qui suit :

- « Compatibilité avec les versions précédentes » page 51
- « Gestion des mots de passe » page 52
- « Activation » page 52

Compatibilité avec les versions précédentes

- Vous pouvez exécuter les modules d'interface et les configurations des pilotes DirXML 1.1a sur un serveur Identity Manager et vous pouvez afficher les pilotes dans iManager dans la présentation Identity Manager de l'ensemble des pilotes. Cependant, les plug-ins Identity Manager ne permettent pas d'afficher ni de modifier la configuration des pilotes avant de les avoir convertis au format Identity Manager.

  Dans les plug-ins Identity Manager, si vous cliquez sur un pilote qui est au format 1.1a, vous êtes invité à effectuer la conversion. Il s'agit d'un processus simple effectué avec un assistant et cela ne modifie pas la fonction de la configuration des pilotes. Dans le cadre du processus, une copie de sauvegarde de la version DirXML 1.1a est enregistrée.
- L'activation des pilotes DirXML 1.1a est toujours valide lors de leur exécution avec le moteur Identity Manager. Cependant, si vous mettez à niveau le module d'interface pilote vers une version d'Identity Manager, vous devez obtenir une nouvelle activation.
- Dans la plupart des cas, un module d'interface pilote Identity Manager peut être exécuté avec une configuration DirXML 1.1a. Reportez-vous aux guides de mise en oeuvre des pilotes (http://www.novell.com/documentation/idm35drivers/index.html) individuels pour obtenir des informations sur la mise à niveau.

  Une exception notable est que la version 1.0 de la synchronisation des mots de passe n'est pas correctement exécutée sous Windows AD et Windows NT après la mise à niveau du module d'interface pilote à moins d'ajouter des stratégies de pilote. Pour obtenir des instructions, reportez-vous aux sections sur la version de la synchronisation des mots de passe dans les guides de mise en oeuvre des pilotes (http://www.novell.com/documentation/idm35drivers/index.html) pour les pilotes Identity Manager pour Active Directory et NT Domain.
- L'exécution des configurations de pilote et des modules d'interface pilote Identity Manager avec le moteur DirXML 1.1a n'est pas prise en charge.
- L'exécution des configurations de pilote Identity Manager avec les modules d'interface pilote DirXML 1.1a n'est pas prise en charge.
- Si vous exécutez la même configuration pilote Identity Manager sur plusieurs serveurs, veillez à ce que les serveurs exécutent la même version d'Identity Manager, et la même version d'eDirectory.

Gestion des mots de passe

- La version 1.0 de la synchronisation des mots de passe, fournie avec les Starter Packs (DirXML 1.1a), ne fonctionnera pas correctement pour AD et NT après une mise à niveau du module d'interface pilote à moins d'ajouter certaines stratégies de pilote. Pour obtenir des instructions, reportez-vous aux sections sur la version de la synchronisation des mots de passe dans les guides de mise en oeuvre des pilotes (http://www.novell.com/documentation/idm35drivers/index.html) pour les pilotes Identity Manager pour Active Directory et NT Domain.
- Reportez-vous à Section 2.2.4, « Mise à niveau depuis la version 1.0 de la synchronisation des mots de passe vers la version Identity Manager », page 52 pour des instructions spécifiques sur ce processus de mise à niveau.

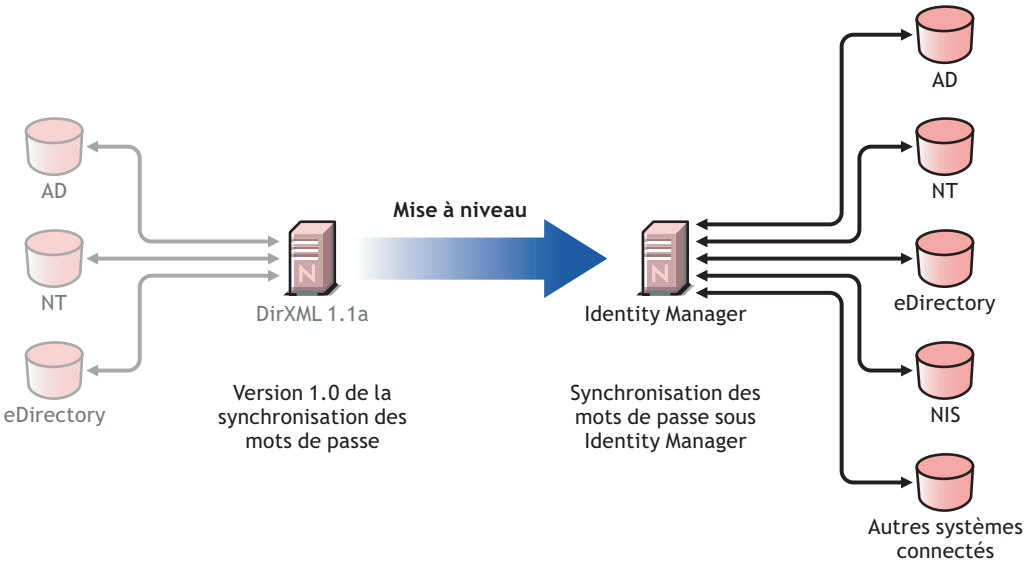
Activation

- Tous les produits Identity Manager doivent être activés dans un délai de 90 jours. Lorsque vous avez acheté d'autres logiciels Novell, le Starter Pack DirXML comportait des activations pour le moteur DirXML 1.1a et les pilotes NT, AD et eDirectory. Lors de la mise à niveau depuis le Starter Pack Identity Manager, vous devrez peut-être appliquer à nouveau vos références d'activation pour ces pilotes.

  Pour plus d'informations sur l'activation, reportez-vous à Annexe 6, « Activation des produits Novell Identity Manager », page 189.

2.2.4 Mise à niveau depuis la version 1.0 de la synchronisation des mots de passe vers la version Identity Manager

Figure 2-4 *Mise à niveau depuis la version 1.0 de la synchronisation des mots de passe vers la version Identity Manager*



La synchronisation des mots de passe Identity Manager offre de nombreuses fonctions, y compris la synchronisation bidirectionnelle des mots de passe, des plates-formes supplémentaires et une notification par courrier électronique lors d'un échec de synchronisation des mots de passe.

Si vous utilisez la version 1.0 de la synchronisation des mots de passe avec Active Directory ou NT Domain, il est très important de relire les instructions de mise à niveau avant d'installer les nouveaux modules d'interface pilote.

Si vous exécutez Identity Manager 2.x avec la version 2.0 de la synchronisation des mots de passe, il n'est pas nécessaire de suivre cette procédure.

Pour obtenir des informations sur la version Identity Manager de la synchronisation des mots de passe en général, reportez-vous à « Synchronisation des mots de passe dans les systèmes connectés » dans le *Guide d'administration Novell Identity Manager 3.5.1*. Cette section contient des informations conceptuelles, y compris une comparaison des fonctions anciennes et nouvelles, des prérequis, une liste des fonctions prises en charge pour chaque système connecté, des instructions sur l'ajout de prise en charge aux pilotes existants et plusieurs scénarios indiquant comment utiliser les nouvelles fonctions.

Dans cette section :

Mise à niveau de la synchronisation des mots de passe pour Active Directory ou Windows NT

La nouvelle fonction de synchronisation des mots de passe est assurée par des stratégies de pilotes et non pas par un agent séparé. Cela signifie que, si vous installez le nouveau module d'interface pilote sans mettre à niveau la configuration du pilote en même temps, la version 1.0 de la synchronisation des mots de passe ne continue de fonctionner que pour les utilisateurs existants. Les utilisateurs nouveaux, déplacés ou renommés ne participent pas à la synchronisation des mots de passe avant la mise à niveau complète de la configuration des pilotes.

Suivez les étapes générales suivantes pour la mise à niveau :

1. Mettez votre environnement à niveau de façon à ce qu'il prenne en charge le mot de passe universel, dont la mise à niveau de Novell Client™ si vous l'utilisez.
2. Installez le module d'interface pilote Identity Manager 3.5.1 pour remplacer le module d'interface pilote DirXML 1.1a pour Active Directory ou Windows NT.
3. Créez immédiatement une compatibilité avec la version 1.0 de la synchronisation des mots de passe, en ajoutant une nouvelle stratégie à la configuration des pilotes.

   Cette étape permet à la version 1.0 de la synchronisation des mots de passe de continuer à fonctionner correctement jusqu'à ce que vous passiez à la version Identity Manager de la synchronisation des mots de passe.
4. Utilisez des stratégies de pilotes pour ajouter la prise en charge de la nouvelle version Identity Manager de la synchronisation des mots de passe.
5. Installez et configurez les nouveaux filtres de la synchronisation des mots de passe.
6. Configurez SSL, si nécessaire.
7. Activez le mot de passe universel via des stratégies de mot de passe, si nécessaire.

8. Configurez le scénarioso de synchronisation des mots de passe Identity Manager que vous souhaitez utiliser.

   Reportez-vous à « Mise en oeuvre de la version de la synchronisation des mots de passe » dans le *Guide d'administration Novell Identity Manager 3.5.1*.

9. Supprimez la version 1.0 de la synchronisation des mots de passe.

Pour obtenir des informations détaillées, reportez-vous aux guides de mise en oeuvre des pilotes (http://www.novell.com/documentation/idm35drivers/index.html) des pilotes Identity Manager pour Active Directory et NT Domain.

Mise à niveau de la version de la synchronisation des mots de passe pour eDirectory

La mise à niveau pour eDirectory est relativement simple. Le module d'interface pilote doit fonctionner avec votre configuration de pilote DirXML 1.1a existante sans changement, en supposant que votre module d'interface pilote et votre configuration disposent des derniers correctifs. Pour obtenir des instructions, reportez-vous à *Pilote Identity Manager 3.5.1 pour eDirectory : guide de mise en oeuvre*.

Mise à niveau d'autres pilotes de systèmes connectés

La version Identity Manager de la synchronisation des mots de passe prend en charge plus de systèmes connectés que la version 1.0.

Pour obtenir une liste des fonctions prises en charge pour d'autres systèmes, reportez-vous à « Prise en charge de système connecté pour la synchronisation des mots de passe » dans le *Guide d'administration Novell Identity Manager 3.5.1*.

Des « recouvrements » de stratégie de pilote sont fournis pour vous aider à ajouter une fonction bidirectionnelle de synchronisation des mots de passe aux pilotes existants pour les systèmes connectés non pris en charge auparavant. Reportez-vous à « Mise à niveau des configurations pilote existantes pour prendre en charge la version de la synchronisation des mots de passe » dans le *Guide d'administration Novell Identity Manager 3.5.1*.

Gestion des donnés sensibles

Le mot de passe universel est protégé par quatre couches de codage dans eDirectory, ce qui le rend très sécurisé dans cet environnement. Si vous choisissez d'utiliser la synchronisation de mots de passe bidirectionnelle, et si vous synchronisez le mot de passe universel avec le mot de passe de distribution, n'oubliez pas que vous extrayez le mot de passe eDirectory et que vous l'envoyez à d'autres systèmes connectés. Vous devez sécuriser le transport du mot de passe, de même que les systèmes connectés vers lesquels il sera synchronisé.

En plus des mots de passe, vous pouvez également utiliser Novell SecretStore® et Novell SecureLogin pour synchroniser des références. Ces logiciels permettent de déployer la question de phrase secrète et la réponse de SecureLogin dans des environnements où le non-rejet est souhaité. Reportez-vous à « Sécurité : meilleures pratiques » dans le *Guide d'administration Novell Identity Manager 3.5.1*.

2.3 Planification des aspects techniques de la mise en oeuvre d'Identity Manager

2.3.1 Utilisation du concepteur

Identity Manager est fourni avec un utilitaire appelé Designer (concepteur). Le concepteur permet de concevoir, tester et documenter les pilotes Identity Manager. Le concepteur permet de visualiser le flux de la synchronisation des mots de passe et des données. Pour plus d'informations, reportez-vous au *Guide d'administration de la version 2.1 du concepteur pour Identity Manager 3.5.1*.

2.3.2 Réplication des objets dont Identity Manager a besoin sur le serveur

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

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

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

Un serveur eDirectory qui exécute un pilote Identity Manager (ou auquel le pilote fait référence, si vous utilisez le chargeur distant) doit contenir une réplique maîtresse ou lisible et inscriptible de ce qui suit :

- L'objet Ensemble des pilotes de ce serveur.

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

  Remarque : lors de la création d'un objet Ensemble des pilotes, le paramètre par défaut est la création d'une partition séparée. Novell 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. Si le serveur comprend une réplique complète de l'emplacement où l'objet Ensemble des pilotes est installé, la partition n'est pas nécessaire.

- 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 des objets dans *tous* les conteneurs répliqués sur le serveur à moins de créer des règles d'indication contraire (règles de filtrage des étendues).

Si vous voulez qu'un pilote synchronise tous les objets utilisateur, par exemple, la manière la plus simple consiste à utiliser une instance du pilote sur un serveur qui contient une réplique maîtresse ou lisible/inscriptible de tous vos utilisateurs.

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

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

  Pour éviter que les instances séparées d'un pilote tentent de synchroniser les mêmes utilisateurs, vous devez utiliser le filtrage des étendues pour définir les utilisateurs que chaque instance du pilote doit synchroniser. Le filtrage des étendues signifie que vous ajoutez des règles à chaque pilote pour limiter l'étendue de la gestion du pilote à des conteneurs spécifiques. Reportez-vous à « Utilisation du filtrage de l'étendue pour gérer les utilisateurs sur des serveurs différents » page 57.
- **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.

2.3.3 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.

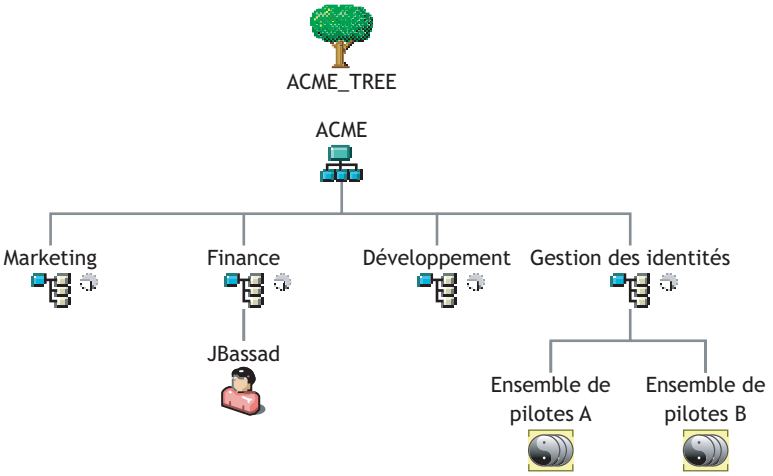
  Pour synchroniser tous les utilisateurs sans les répliquer sur un seul serveur, vous devez déterminer l'ensemble de serveurs qui contient tous les utilisateurs, puis créer une instance du pilote Identity Manager sur chacun de ces serveurs. Pour éviter que deux instances du pilote tentent de synchroniser 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 qui contient les ensembles de pilotes. Chacun de ces conteneurs constitue une partition distincte.

Figure 2-5 *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 Figure 2-6 page 59. 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.

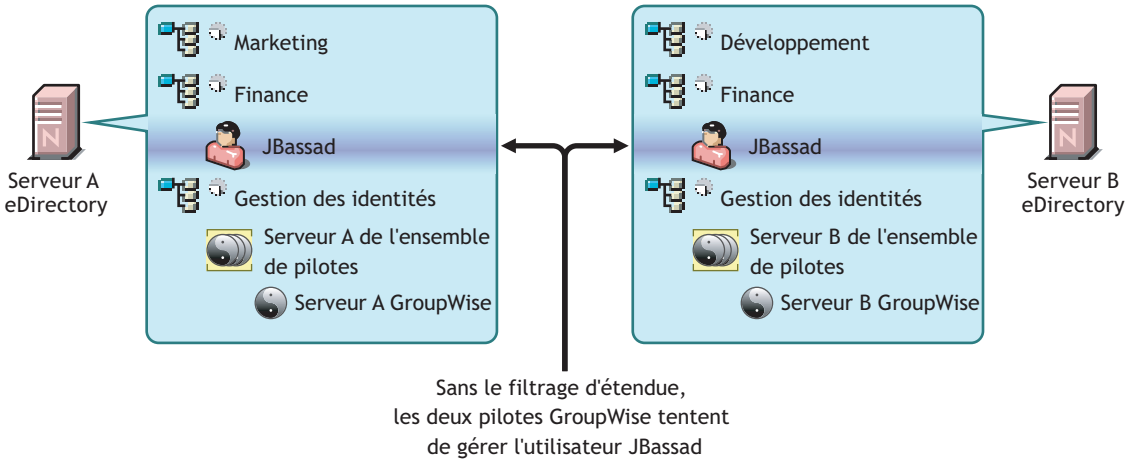
L'administrateur souhaite que tous les utilisateurs de l'arborescence soient synchronisés par le pilote GroupWise®, mais veut éviter d'avoir à regrouper les répliques des utilisateurs sur un seul serveur. Il choisit plutôt d'utiliser deux instances du pilote GroupWise, une sur chaque serveur. Il installe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

Le serveur A contient des répliques des conteneurs Marketing et Finance. Se trouve également sur le serveur une réplique du conteneur Gestion de l'identité, qui contient l'ensemble de pilotes du serveur A et l'objet pilote GroupWise du serveur A.

Le serveur B contient des réplications des conteneurs Développement et Finance, et le conteneur Gestion de l'identité contenant l'ensemble de pilotes du serveur B et l'objet pilote GroupWise du serveur B.

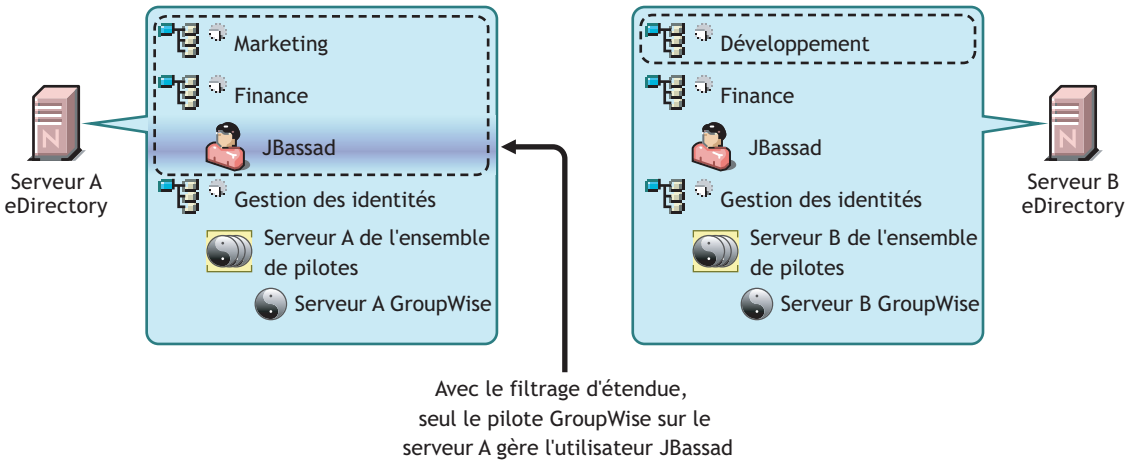
Comme le serveur A et le serveur B contiennent une réplique du conteneur Finance, ils contiennent tous deux l'utilisateur JBassad, qui est dans le conteneur Finance. Sans filtrage des étendues, le pilote GroupWise A et le pilote GroupWise B synchroniseraient JBassad.

Figure 2-6 *Deux serveurs avec des répliques en chevauchement, 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 2-7 *Le filtrage des étendues définit les pilotes qui synchronisent chaque conteneur*



Identity Manager 3.5.1 comporte des règles prédéfinies. Deux règles aident au filtrage des étendues. « Transformation de l'événement - Filtrage des étendues - Inclure des sous-arborescences » et « Transformation de l'événement - Filtrage des étendues - Exclure les sous-arborescences » documentés dans la *Présentation des stratégies d'Identity Manager 3.5.1*.

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.

Mise à niveau

3

Identity Manager comporte différentes parties. Pour mettre Identity Manager à niveau, vous devez vous assurer d'avoir examiné tous les aspects du produit pour réussir la mise à niveau.

Certains scénarios de mise à niveau sont expliqués dans Section 2.2, « Planification des scénarios d'installation courants », page 46.

3.1 Chemins de mise à niveau

Le tableau contient les scénarios de mise à niveau pris en charge pour les différentes versions d'Identity Manager. Chaque scénarioso porte la mention pris en charge ou non pris en charge.

Tableau 3-1 *Scénarios de chemins de mise à niveau*

Version installée	Version en cours	Mise à niveau prise en charge ?
DirXML® 1.1a	Identity Manager 3.5.1	Oui
Identity Manager 2.x	Identity Manager 3.5.1	Oui
Identity Manager 3.0x	Identity Manager 3.5.1	Oui

3.2 Modifications de l'architecture des stratégies

Identity Manager 3.5 et 3.5.1 contiennent une nouvelle architecture des stratégies qui régit la manière dont les pilotes font référence aux stratégies. Alors que l'architecture de pilote 3.5.1 offre des fonctionnalités supplémentaires dans l'environnement Identity Manager 3.5.1, le moteur méta-annuaire 3.0.x ne peut pas exécuter les pilotes 3.5.1.

Cependant, Identity Manager 3.5 et 3.5.1 peuvent exécuter les pilotes 3.0x. Si vous avez des pilotes 3.0.x associés aux moteurs méta-annuaire 3.0.x et 3.5.1, n'effectuez pas la mise à niveau des pilotes 3.0.x. Les pilotes 3.0.x fonctionnent dans un environnement 3.5.1, mais ils ne disposent pas des fonctionnalités supplémentaires que les versions Identity Manager 3.5 et ultérieures prennent en charge. Lorsque des pilotes 3.0.x ne sont associés qu'avec un moteur méta-annuaire 3.5 ou ultérieur, vous devez effectuer la mise à niveau des pilotes 3.0.x vers 3.5.1.

Pour plus d'informations sur l'architecture des stratégies et sur la mise à niveau des pilotes vers 3.5.1, reportez-vous à « Mise à niveau des stratégies d'Identity Manager » dans *Présentation des stratégies d'Identity Manager 3.5.1*.

3.3 Procédure de mise à niveau

Pour assurer une bonne mise à niveau vers Identity Manager 3.5.1, les étapes suivantes doivent être suivies.

3.3.1 Exportation de pilotes

Avant une mise à niveau, l'étape la plus importante consiste à sauvegarder les pilotes actuels ainsi que les informations de configuration associées. Pour sauvegarder les pilotes, vous devez les exporter.

Exportation à partir de ConsoleOne

1. Dans ConsoleOne®, cliquez avec le bouton droit de la souris sur l'objet Ensemble de pilotes, puis sélectionnez *Propriétés* > *DirXML* > *Pilotes*.
2. Sélectionnez le pilote pour lequel vous souhaitez créer un export, puis cliquez sur *Exporter*.
3. Indiquez un nom de fichier. Laissez l'extension par défaut de `.xml`, puis cliquez sur *Enregistrer*.
4. Cliquez sur *Exporter la configuration*.

Dans iManager, vous pouvez exporter un pilote ou la totalité de l'ensemble de pilotes. Si vous exportez l'ensemble de pilotes, un seul fichier de configuration est créé. Si vous exportez chaque pilote, un fichier de configuration est créé pour chaque pilote.

Exportation à partir d'iManager

1. Dans iManager, sélectionnez *Utilitaires DirXML* > *Exporter un pilote*.
2. Recherchez et sélectionnez le pilote ou l'ensemble de pilotes à exporter, puis cliquez sur *Suivant*.
3. Laissez les champs d'invite vierges pour créer une copie exacte du pilote, puis cliquez sur *Suivant*.
4. Si vous sélectionnez l'objet Ensemble de pilotes, une page d'invite s'affiche pour chaque pilote. Laissez les champs vierges pour chaque pilote pour créer une copie exacte.
5. Cliquez sur *Enregistrer sous*.
6. Cliquez sur *Enregistrer* dans la fenêtre Télécharger le fichier.
7. Recherchez et indiquez un emplacement et un nom de fichier pour l'export, puis cliquez sur *Enregistrer*.

Important : le fichier doit avoir une extension `xml` lorsqu'il est enregistré.

Une fois le pilote exporté, testez-le dans un environnement de laboratoire. Importez l'export du pilote et testez le pilote pour vous assurer que tous les paramètres sont corrects et que toutes les fonctions sont présentes.

Exportation depuis le concepteur

1. Depuis le concepteur, cliquez avec le bouton droit de la souris sur l'objet Pilote ou Ensemble de pilotes dans la vue Modeleur, puis cliquez sur *Exporter vers le fichier de configuration*.
2. Dans la fenêtre Exporter la configuration du pilote, recherchez et indiquez un emplacement et un nom de fichier pour l'export, puis cliquez sur *Enregistrer*.

3.3.2 Vérification de la configuration minimale requise

Afin d'effectuer une mise à niveau vers Identity Manager 3.5.1, les serveurs qui exécutent les services Identity Manager doivent satisfaire les exigences minimales. Reportez-vous à Tableau 1-3 page 29 pour obtenir la configuration minimale requise pour chaque plate-forme.

Si les composants de prise de charge doivent être mis à niveau, effectuez les mises à niveau dans l'ordre suivant :

1. Mettez à niveau le système d'exploitation vers une version prise en charge. Par exemple, effectuez une mise à niveau de NetWare® 6.0 vers NetWare 6.5.
2. Mettez eDirectory™ à niveau vers eDirectory 8.7.3.6 avec le dernier Support Pack, ou vers eDirectory 8.8 avec le dernier Support Pack.
3. Vous devez avoir Security Services 2.0.5 avec NMAS™ 3.1.3 pour la prise en charge SSL.
4. Mettez à niveau iManager vers iManager 2.6 ou 2.7 avec le support pack le plus récent (inclut la mise à niveau vers Apache 2.0.52 ou ultérieur et Tomcat 4.1.18 ou ultérieur).
5. Vous devez également avoir installé le Starter Pack Novell® Audit 2.0.2 ou Sentinel™ 5.1.3 sur le réseau.
6. Pour l'application utilisateur et le provisioning d'Identity Manager, reportez-vous à Section 5.1, « Conditions préalables à l'installation », page 99.
7. Mettez Identity Manager à niveau.
8. Activez le moteur méta-annuaire et tout pilote mis à niveau.

3.3.3 Mise à niveau du moteur

Une fois les composants de prise en charge mis à niveau, le moteur DirXML ou Identity Manager est mis à niveau.

1. Assurez-vous d'avoir un export valide des pilotes avant la mise à niveau. Reportez-vous à Section 3.3.1, « Exportation de pilotes », page 62.
2. Arrêtez les pilotes.
   - **2a** Dans iManager, sélectionnez *Identity Manager > Présentation d'Identity Manager*.
   - **2b** Recherchez et sélectionnez l'objet Ensemble de pilotes, puis cliquez sur *Rechercher*.
   - **2c** Cliquez dans l'angle supérieur droit de l'icône du pilote, puis sélectionnez *Arrêter le pilote*.

3 Configurez le démarrage manuel des pilotes.

3a Dans iManager, sélectionnez *Identity Manager* > *Présentation d'Identity Manager*.

3b Recherchez et sélectionnez l'objet Ensemble de pilotes, puis cliquez sur *Rechercher*.

3c Dans l'angle supérieur droit de l'icône du pilote, cliquez sur *Modifier les propriétés*.

3d Sur la page Configuration des pilotes, sous *Options de démarrage*, sélectionnez *Manuel*.

4 Installez Identity Manager 3.5.1.

Les étapes de mise à niveau vers Identity Manager 3.5.1 sont les mêmes que celles de l'installation d'Identity Manager 3.5. Reportez-vous à Chapitre 4, « Installation d'Identity Manager », page 67 pour obtenir des instructions d'installation d'Identity Manager.

Identity Manager 3.5.1 se copie sur des versions précédentes d'Identity Manager, en mettant les binaires à jour. iManager et le concepteur mettent les pilotes à jour vers la nouvelle fonction.

4a Dans iManager, cliquez sur les pilotes pour lancer l'assistant de mise à niveau des pilotes.

Designer lance automatiquement l'assistant de mise à niveau des pilotes dès la détection des anciens pilotes.

5 Définissez les options de démarrage des pilotes.

5a Dans iManager, sélectionnez *Identity Manager* > *Présentation d'Identity Manager*.

5b Recherchez et sélectionnez l'objet Ensemble de pilotes, puis cliquez sur *Rechercher*.

5c Dans l'angle supérieur droit de l'icône du pilote, cliquez sur *Modifier les propriétés*.

5d Sur la page Configuration des pilotes, sous Options de démarrage, sélectionnez *Démarrage automatique* ou sélectionnez votre méthode préférée de démarrage du pilote.

6 Examinez les paramètres et stratégies du pilote pour vous assurer que tout soit défini de la façon désirée.

7 Démarrage du pilote.

7a Dans iManager, sélectionnez *Identity Manager* > *Présentation d'Identity Manager*.

7b Recherchez et sélectionnez l'objet Ensemble de pilotes, puis cliquez sur *Rechercher*.

7c Cliquez dans l'angle supérieur droit de l'icône du pilote, puis sélectionnez *Démarrer le pilote*.

3.3.4 Mise à niveau du chargeur distant

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

1 Créez une sauvegarde des fichiers de configuration du chargeur distant. L'emplacement par défaut des fichiers est :

- Windows `C:\Novell\RemoteLoader\`*`nomchargeurdistant`*`-config.txt`
- Linux : créez votre propre fichier de configuration dans le chemin d'accès de rdxml.

2 Arrêtez le service ou le daemon du chargeur distant.

3 Exécutez les programmes d'installation du chargeur distant.

Cela met à jour les fichiers et les binaires à la version actuelle. Reportez-vous à « Installation des chargeurs distants » dans le *Guide d'administration Novell Identity Manager 3.5.1*.

3.3.5 Mise à niveau dans un environnement UNIX/Linux

La mise à niveau d'Identity Manager 3.0.1 vers Identity Manager 3.5.1 dans un environnement UNIX ou Linux crée deux emplacements de désinstallation et ne supprime pas entièrement les packages. Par exemple, si vous démarrez avec une plate-forme UNIX, telle que SLES 9 et si vous installez Identity Manager 3.0.1, le programme de désinstallation d'Identity Manager se trouve `/root/dirXML`. Saisir `rpm -qa | grep -i dxml` indique quand les packages dxml ont été installés.

Si vous mettez à niveau maintenant ce déploiement vers Identity Manager 3.5.1, un nouvel emplacement de désinstallation est créé dans le répertoire `/root/idm` à cause du changement de dénomination. Saisir `rpm -qa` indique quand les packages mis à jour ont été installés.

Étant donné le changement de répertoire, si l'administrateur désinstalle Identity Manager 3.5.1, le programme de désinstallation ne supprimera pas tous les packages, même s'il indique que tous les éléments ont été supprimés. Pour supprimer le reste des packages, utilisez le programme de désinstallation DirXML.

3.4 Mise à niveau de la version de la synchronisation des mots de passe

Si vous mettez à niveau DirXML 1.1a vers Identity Manager 3.5.1, la synchronisation des mots de passe doit être mise à niveau. Reportez-vous à « Mise à niveau de la version 5.1 de la synchronisation des mots de passe » dans le *Guide d'administration Novell Identity Manager 3.5.1*.

Si vous mettez à niveau depuis Identity Manager 2.x, la version de synchronisation des mots de passe est la même et n'est pas mise à niveau.

3.5 Mise à niveau depuis RNS vers Novell Audit

Bien que le service de création de rapport et de notification RNS soit décrié, le moteur continue à traiter les fonctions RNS si vous utilisez actuellement ce service. Envisagez de passer à Novell Audit, car il étend les fonctionnalités apportées par le service RNS. De plus, ce dernier pourrait ne plus être pris en charge dans les versions futures d'Identity Manager.

Pour plus d'informations, reportez-vous à « Requêtes et rapports » dans *Consignation et rapports dans Identity Manager 3.5.1*.

3.6 Mise à niveau des configurations de pilotes DirXML 1.1a

Lorsque vous mettez à niveau depuis DirXML 1.1a vers Identity Manager 3.5.1, la configuration des pilotes peut être mise à niveau. La mise à niveau des configurations de pilotes comporte deux aspects :

- Conversion des règles DirXML vers les stratégies Identity Manager. Cela s'effectue grâce à un outil de conversion et n'améliore pas la fonction du pilote. Les pilotes hérités s'exécutent sans cette conversion, mais la conversion permet d'afficher la configuration des pilotes existante dans les plug-ins iManager d'Identity Manager.

  Vous devez effectuer des tests complets pour vous assurer que cette étape fonctionne. Il est vivement conseillé de configurer un environnement de test/développement dans lequel vous

pouvez tester, analyser et développer vos solutions. Dès que tout fonctionne comme vous le souhaitez, déployez le produit final dans votre environnement de production.

- Mise à niveau des stratégies de pilotes pour ajouter une nouvelle fonction. Par exemple, Identity Manager utilise désormais un script DirXML pour la fonction qui était dans les feuilles de style. Ce niveau de fonction est mieux géré par un expert Identity Manager.

Reportez-vous à « Mise à niveau de la configuration d'un pilote du format DirXML 5.1a à Identity Manager 1.1.3 » et « Gestion des pilotes DirXML 5.1a dans un environnement Identity Manager » dans le *Guide d'administration Novell Identity Manager 3.5.1*.

Une autre alternative consiste à commencer par les configurations de pilotes Identity Manager, puis à les personnaliser pour faire la même chose que votre configuration de DirXML 1.1a.

3.7 Activation d'Identity Manager

Une fois la mise à niveau terminée, vous avez 90 jours pour activer le moteur méta-annuaire et tous les pilotes que vous avez mis à niveau. Si le moteur et les pilotes ne sont pas activés, leur fonctionnement s'arrêtera au bout de 90 jours. Pour obtenir des instructions sur l'activation d'Identity Manager, reportez-vous àChapitre 6, « Activation des produits Novell Identity Manager », page 189.

Installation d'Identity Manager 4

Cette section contient les exigences et instructions pour l'installation d'Identity Manager et des pilotes Identity Manager.

4.1 Avant l'installation

Avant d'installer Identity Manager, reportez-vous à Chapitre 2, « Planification », page 39.

4.2 Configuration système requise et composants Identity Manager

Novell® Identity Manager contient des composants que vous pouvez installer sur plusieurs systèmes et plates-formes de votre environnement. 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.

Tableau 1-3, « Configuration requise et composants du système Identity Manager », page 29 indique les composants d'installation d'Identity Manager et la configuration requise pour chaque système.

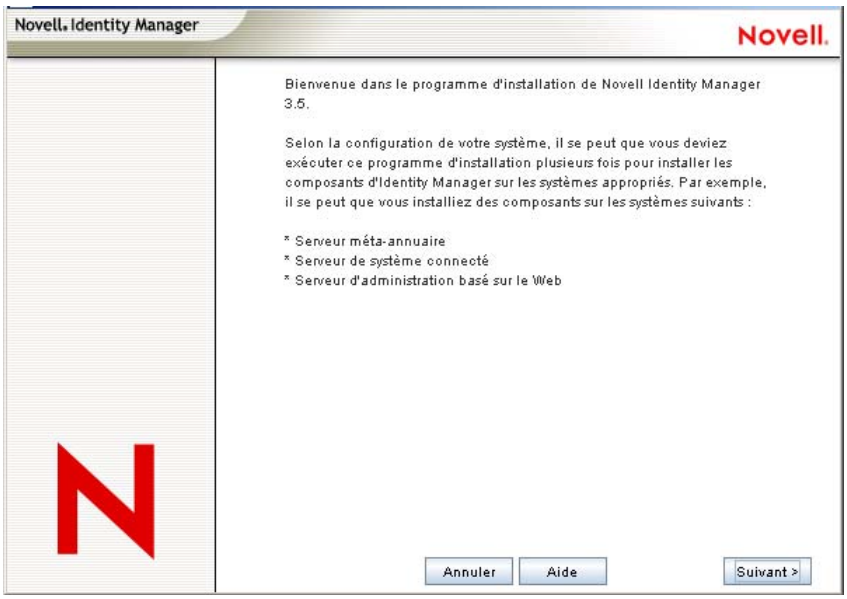
4.3 Installation d'Identity Manager sur NetWare

Cette procédure couvre l'installation du serveur méta-annuaire, des composants Web et des utilitaires pour NetWare®. Avant de commencer, assurez-vous que votre système a la configuration requise indiquée dans Section 4.2, « Configuration système requise et composants Identity Manager », page 67.

1 Téléchargez Identity Manager. Fichier d'image `iso` dont vous avez besoin. Vous pouvez télécharger Identity Manager. Fichiers d'images `iso` du Site de téléchargement Novell (http://download.novell.com).

L'installation NetWare d'Identity Manager se trouve dans `Identity_Manager_3_5_1_NW_Win.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`.

2. Une fois le fichier est extrait et le fichier image placé sur un disque, insérez le disque dans le lecteur CD du serveur et permettez le montage du disque comme volume.
3. Lancez l'interface utilisateur graphique NetWare (saisissez `STARTX` à l'invite de la console du serveur), puis sélectionnez *Novell* > *Installer*.
4. Dans la fenêtre Produits installés, sélectionnez *Ajouter*, puis indiquez le chemin d'accès au fichier Identity Manager `product.ini` dans le répertoire `\NW`. Cliquez sur *OK*, puis à nouveau sur *OK* pour commencer à charger le programme d'installation Identity Manager.
5. Une fois la copie des fichiers terminée, la page Installation de produit Identity Manager apparaît. Cliquez sur *Suivant* pour lancer l'installation.

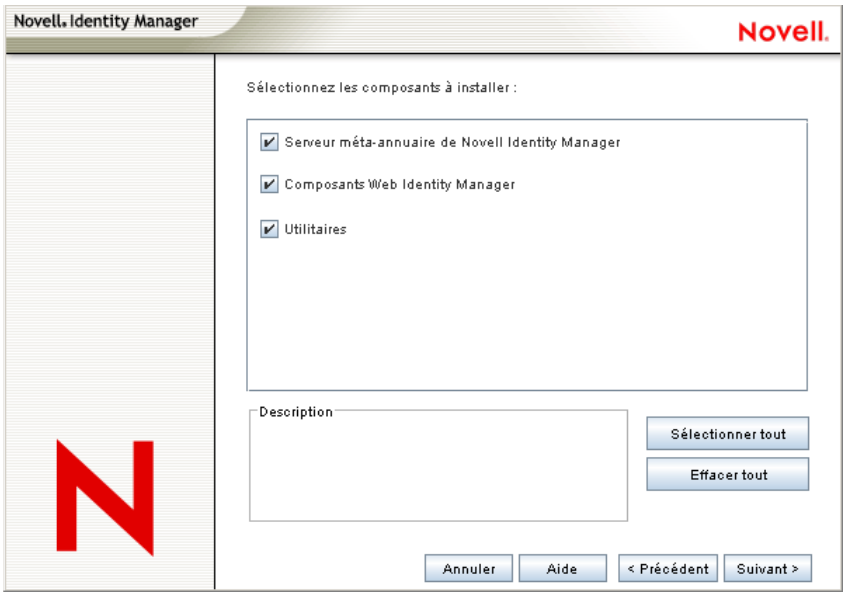


6. Sélectionnez une langue pour afficher l'accord de licence ou utilisez la langue par défaut (anglais).

   Le programme d'installation Identity Manager s'exécute automatiquement dans la langue de la machine sur laquelle vous l'installez. Si le programme d'installation n'a pas été traduit dans la langue que votre machine utilise, il s'exécute par défaut en anglais.
7. Lisez l'accord de licence, puis cliquez sur *J'accepte*.
8. Lisez les pages de présentation qui décrivent les types de systèmes, y compris le serveur méta-annuaire, les composants Web et les utilitaires, puis cliquez sur *Suivant* pour continuer.

   Ces informations sont également abordées dans Tableau 1-3 page 29.

9 Sur la page Installation d'Identity Manager, sélectionnez les composants à installer. Reportez-vous à Tableau 1-3 page 29.



Les options suivantes sont disponibles. Pour la plupart des installations, vous sélectionnez tous les composants.

- **Serveur méta-annuaire :** installe le moteur méta-annuaire et les pilotes de services. Sur la plate-forme NetWare, ceux-ci comprennent les pilotes Identity Manager pour Avaya, Texte délimité, eDirectory™, GroupWise®, JDBC*, JMS*, LDAP, Paramètres Linux/UNIX, RACF*, SOAP, SIF*, Top Secret et Bon de travail. La sélection de cette option étend également le schéma eDirectory.

  Important : Novell eDirectory 8.7.3.6 ou ultérieur et Security Services 2.0.5 (NMAS™ 3.1.3) avec les correctifs actuels doivent être installés avant de pouvoir installer cette option. Installez le composant Serveur méta-annuaire là où vous souhaitez exécuter le moteur méta-annuaire pour Identity Manager. Si vous n'avez pas la bonne version de NMAS, un message d'avertissement s'affiche et vous perdez la fonction d'Identity Manager.

- **Système connecté :** installe le chargeur distant, qui permet d'établir une liaison entre le système connecté et un serveur qui exécute le moteur méta-annuaire.

  Pour l'installation d'Identity Manager sur NetWare, cette option n'est pas disponible et vous ne la voyez pas sur l'écran d'installation.

- **Composants Web Identity Manager :** cette option permet d'installer les plug-ins Identity Manager et les configurations de pilotes.

  Novell iManager doit être installé avant de pouvoir installer cette option.

- **Utilitaires :** installe des scripts supplémentaires pour le pilote JDBC et des utilitaires pour d'autres pilotes. La plupart des pilotes n'ont aucun utilitaire connecté. Les utilitaires de pilotes peuvent comprendre :

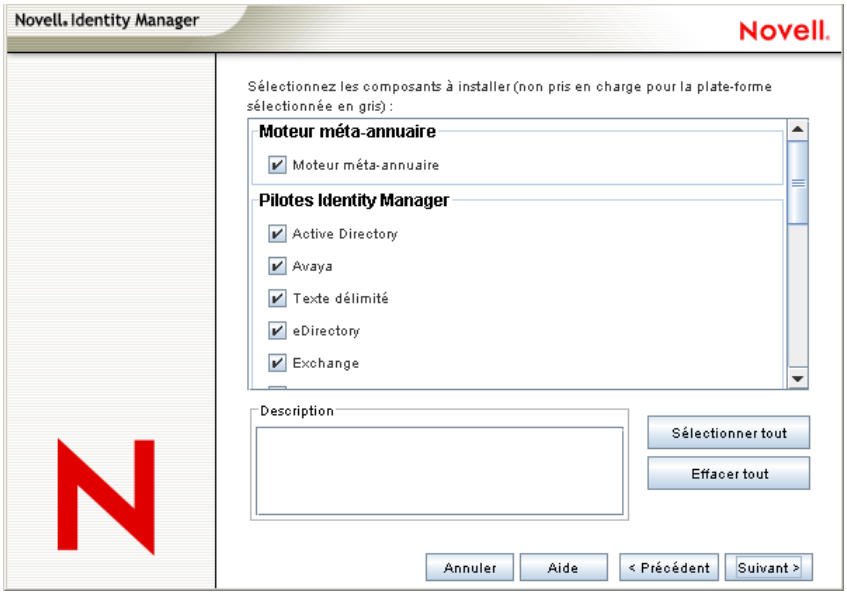
  - Scripts SQL pour le pilote JDBC
  - Composants JMS
  - Composants PeopleSoft

- Outil d'audit de licence
- Outil Active Directory Discovery
- Outil Lotus Notes Discovery
- Utilitaires SAP

Un autre utilitaire permet d'enregistrer les composants système Novell Audit pour Identity Manager (une version eDirectory valide et un serveur de consignation Novell Audit doivent être installés sur l'arborescence avant l'installation de cet utilitaire.)

10 Cliquez sur *Suivant*.

11 Sélectionnez les produits que vous voulez installer, puis cliquez sur *Suivant*.



La page Installation de pilotes sélectionnés du moteur affiche les pilotes que vous pouvez installer sur une plate-forme correspondante. Par exemple, sur un serveur NetWare, vous ne pouvez pas installer le pilote Windows Active Directory.

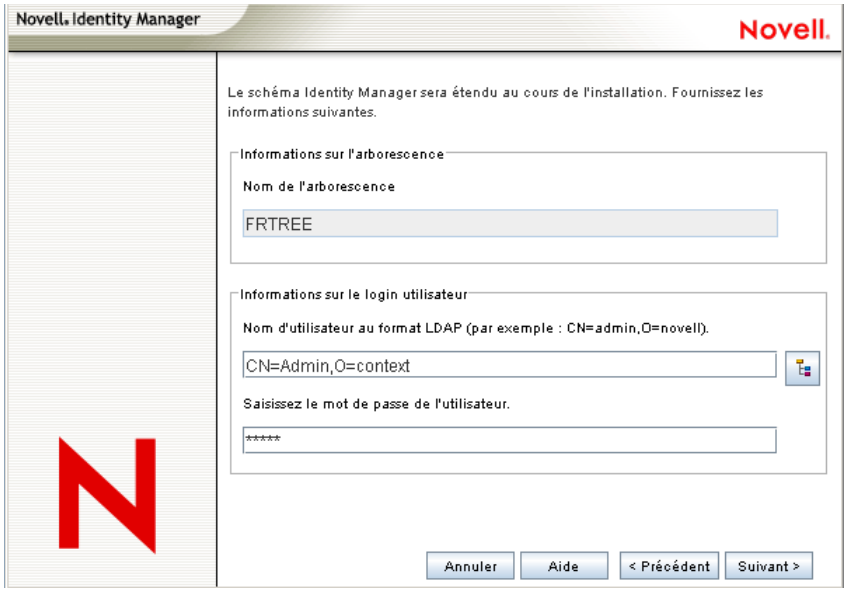
Par défaut, tous les pilotes disponibles pour l'option sont sélectionnés. Nous recommandons l'installation de tous les fichiers de pilotes sélectionnés, ainsi vous n'aurez pas à exécuter le programme d'installation par la suite si vous souhaitez un autre pilote. Les fichiers de pilotes ne sont pas utilisés avant qu'un pilote soit configuré avec iManager ou le concepteur, puis déployé.

Si vous ne voulez pas installer tous les pilotes, vous pouvez cliquer sur *Effacer tout*, puis sélectionner les pilotes dont vous avez besoin, ou cliquer sur les pilotes que vous ne voulez pas installer pour les désélectionner. Si vous avez besoin d'un autre pilote dans l'avenir, vous devez exécuter à nouveau ce programme d'installation pour installer les pilotes que vous n'avez pas sélectionné. Vous pouvez également utiliser le concepteur pour créer, modifier et déployer des fichiers de pilotes.

12 Lorsque vous voyez le message d'information de rappel d'activation du produit, cliquez sur *OK*.

Vous devez activer les pilotes dans un délai de 90 jours à compter de l'installation ; sinon, ils s'arrêteront.

13 Sur la page Extension de schéma, indiquez ce qui suit :



- **Nom d'utilisateur :** indiquez le nom utilisateur (au format LDAP, comme CN=admin,O=novell) d'un utilisateur qui dispose de droits d'étendre le schéma. Sur cette page, sélectionnez un utilisateur qui a suffisamment de droits pour développer le schéma eDirectory (quelqu'un qui dispose des droits de superviseur à la racine de l'arborescence, comme un administrateur).
- **Mot de passe de l'utilisateur :** spécifiez le mot de passe de l'utilisateur.

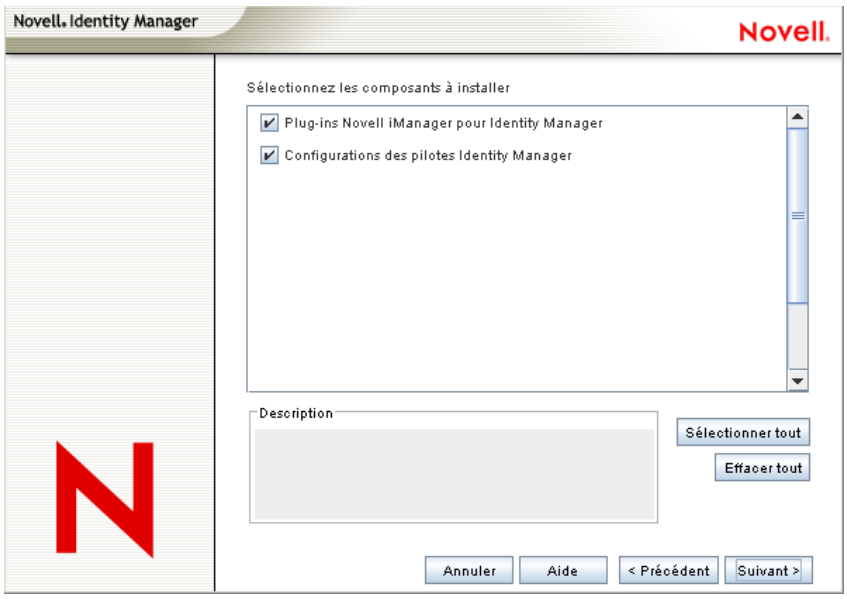
14 Cliquez sur *Suivant*.

Lorsque les informations utilisateur sont validées, vous voyez la première page (sur deux) Composants :

Sur la première page Composants, *Composants système Novell Audit pour Identity Manager* est sélectionné si vous avez installé le système Novell Audit sur le serveur. Sinon, ils ne sont pas sélectionnés. La sélection de *Composants de l'application* installe des composants pour les systèmes d'applications tels que JDBC et PeopleSoft.

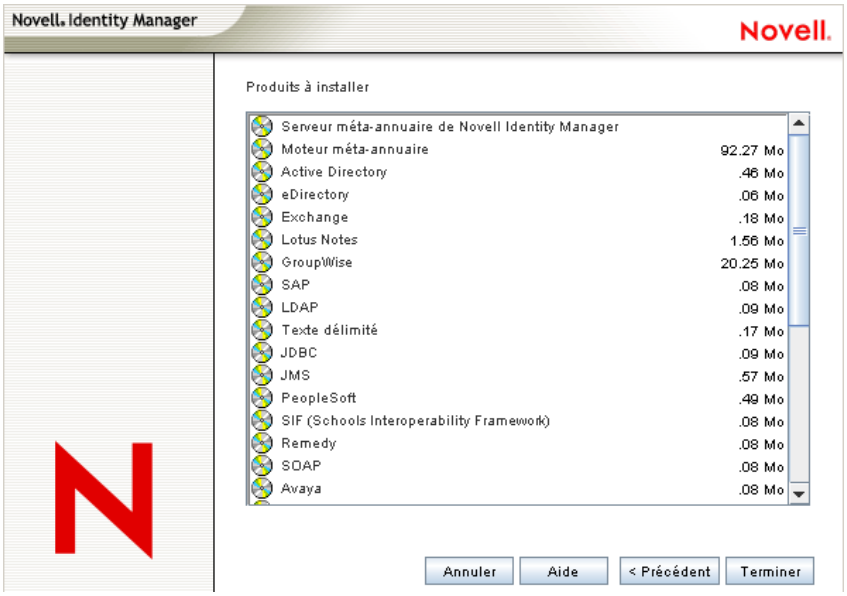
Si le programme d'installation détecte des fichiers de configuration de pilotes existants, il les déplace vers un chemin d'accès de sauvegarde.

15 Cliquez sur *Suivant*.

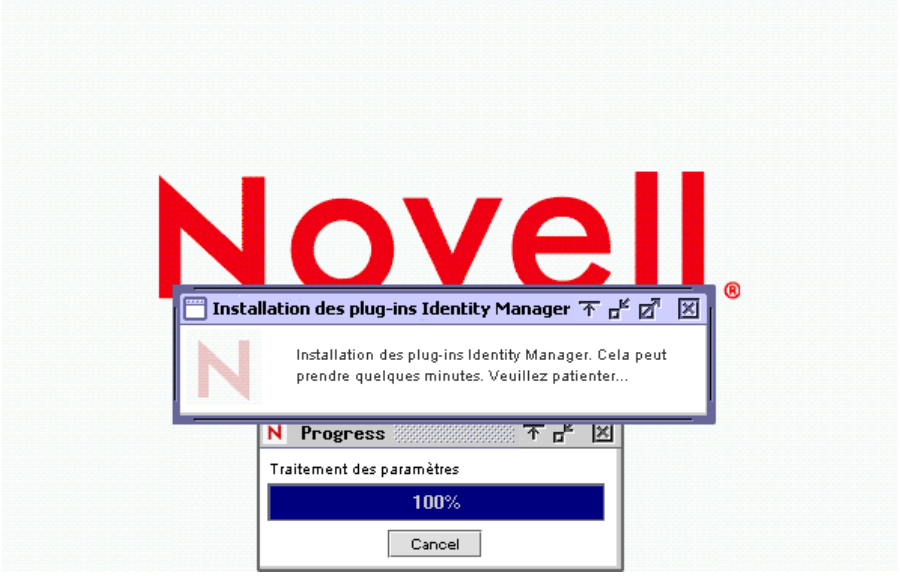


16 La deuxième page Composants permet d'installer les utilitaires. Les utilitaires spécifiques aux plates-formes sont en veilleuse s'ils sont disponibles pour des plates-formes autres que celles sur laquelle vous effectuez l'installation. Sous NetWare, les seules sélections disponibles sont les scripts SQL pour le pilote JDBC et les composants JMS. Sélectionnez les composants dont vous avez besoin et cliquez sur *Suivant*.

17 Lisez et vérifiez vos sélections sur la page Résumé, puis cliquez sur *Terminer*.



Le processus d'installation Novell Identity Manager interrompt l'extension du schéma par eDirectory. Le processus d'installation commence par installer les produits et composants sélectionnés.



18 Une fois l'installation terminée, la boîte de dialogue Installation terminée apparaît, cliquez sur *Fermer*.

19 Afin que iManager reconnaisse les plug-ins que vous avez installés, redémarrez vos services Web maintenant et redémarrez Tomcat.

Si vous avez installé des pilotes Identity Manager, utilisez l'assistant de configuration Identity Manager dans iManager 2.6 ou une version supérieure, ou utilisez le concepteur pour configurer les pilotes.

4.4 Installation d'Identity Manager sous Windows

Cette procédure couvre l'installation du serveur méta-annuaire, des composants Web et des utilitaires sur les plates-formes Windows.

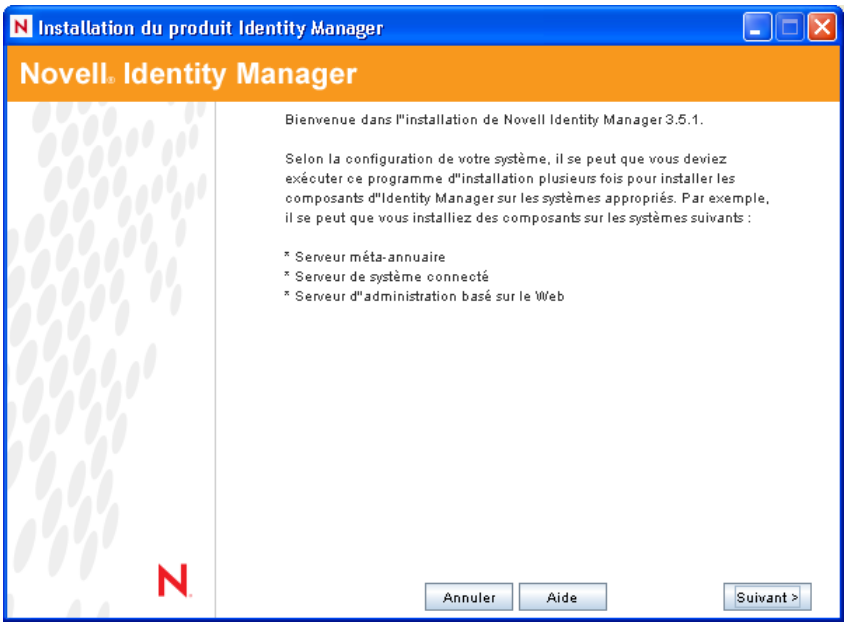
Avant de commencer, assurez-vous que votre système a la configuration requise indiquée dans Tableau 1-3 page 29.

1 Téléchargez Identity Manager. Fichier d'image `iso` dont vous avez besoin. Vous pouvez télécharger Identity Manager. Fichiers d'images `iso` du Site de téléchargement Novell (http://download.novell.com).

L'installation Windows d'Identity Manager se trouve dans `Identity_Manager_3_5_1_NW_Win.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`.

2 Après avoir extrait le fichier, double-cliquez sur le fichier `install.exe` qui se trouve dans le répertoire `\NT`.

Une fois la copie des fichiers terminée, la page Installation de produit Identity Manager apparaît.



3 Cliquez sur *Suivant* pour lancer l'installation.

4 Sélectionnez une langue pour afficher l'accord de licence ou utilisez la langue par défaut (anglais).

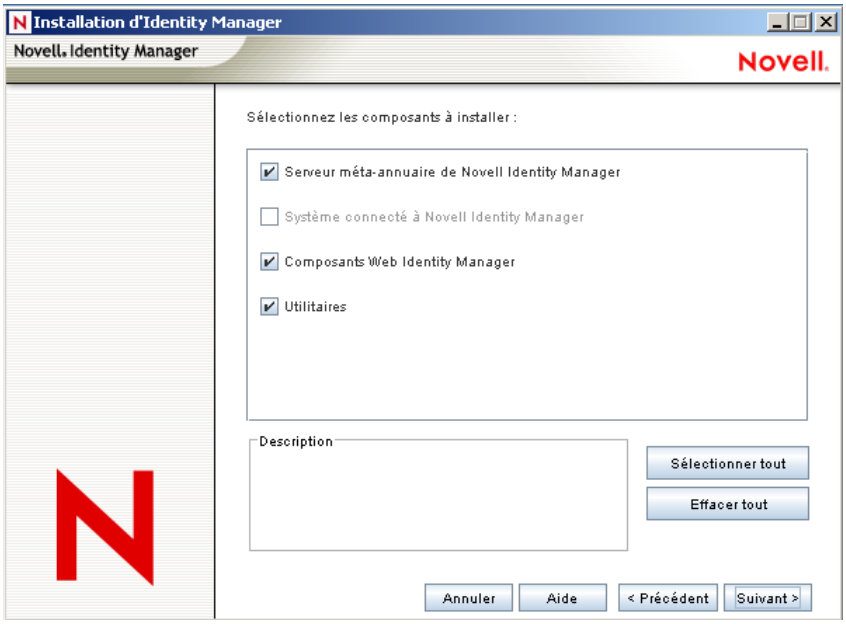
Le programme d'installation Identity Manager s'exécute automatiquement dans la langue de la machine sur laquelle vous l'installez. Si le programme d'installation n'a pas été traduit dans la langue que votre machine utilise, il s'exécute par défaut en anglais.

5 Lisez l'accord de licence, puis cliquez sur *J'accepte*.

6 Lisez les pages de présentation qui décrivent les types de systèmes, y compris le serveur méta-annuaire, les composants Web et les utilitaires, puis cliquez sur *Suivant* pour continuer.

Ces informations sont également abordées dans Tableau 1-3 page 29.

7 Sur la page Installation d'Identity Manager, sélectionnez les composants à installer :



Les options disponibles sont les suivantes :

- **Serveur méta-annuaire :** installe le moteur méta-annuaire et les pilotes de services. La sélection de pilotes Identity Manager comprend Active Directory, Avaya, Texte délimité, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Paramètres Linux/UNIX, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF et Top Secret. La sélection de cette option étend également le schéma eDirectory.

  Important : Novell eDirectory 8.7.3.6 ou 8.8 et Security Services 2.0.5 (NMAS 3.1.3) avec les correctifs actuels doivent être installés avant de pouvoir installer cette option. Installez le composant Serveur méta-annuaire là où vous souhaitez exécuter le moteur méta-annuaire pour Identity Manager. Si vous n'avez pas la bonne version de NMAS, un message d'avertissement s'affiche et vous perdez la fonction d'Identity Manager.

- **Système connecté :** installe le chargeur distant, qui permet d'établir une liaison entre le système connecté et un serveur qui exécute le moteur méta-annuaire. Sous Windows, cette option installe les pilotes suivants : Active Directory, Avaya, Texte délimité, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Paramètres Linux/UNIX, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF et Top Secret.

  Installez le Système connecté pour permettre le login de l'application depuis un serveur d'applications à un serveur basé sur eDirectory qui exécute le moteur méta-annuaire. Cette procédure est expliquée à la section Section 4.5, « Installation de l'option Système connecté sous Windows », page 79.

- **Composants Web :** cette option permet d'installer des configurations de pilotes, des plug-ins iManager et des scripts et utilitaires d'application.

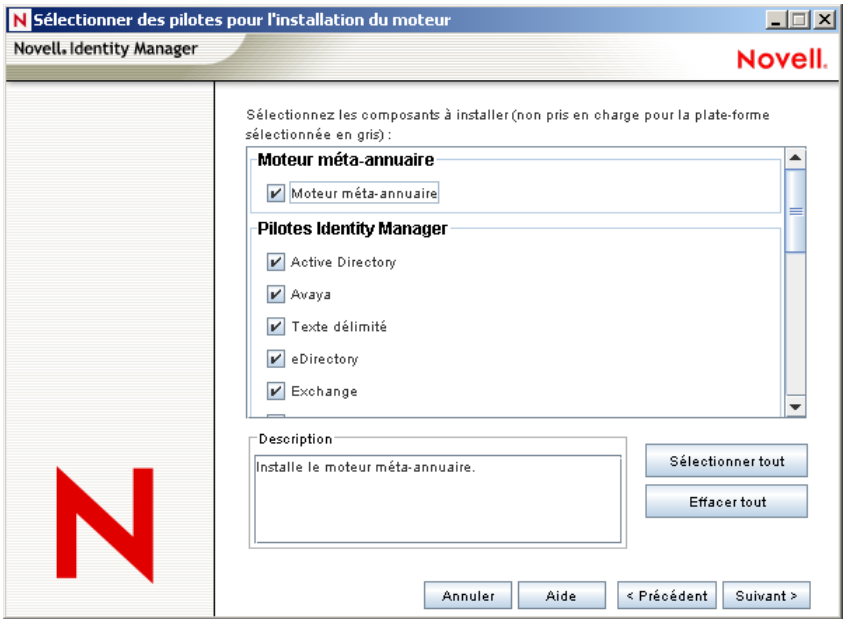
  Novell iManager doit être installé avant de pouvoir installer cette option.

- **Utilitaires :** installe des scripts supplémentaires pour le pilote JDBC et des utilitaires pour d'autres pilotes. La plupart des pilotes n'ont aucun utilitaire connecté. Les utilitaires de pilotes peuvent comprendre :
  - scripts SQL pour le pilote JDBC
  - Composants JMS
  - Composants PeopleSoft
  - Outil d'audit de licence
  - Outil Active Directory Discovery
  - Outil Lotus Notes Discovery
  - Utilitaires SAP
  - Programme d'installation du pilote de script et outil de configuration

  Un autre utilitaire permet d'enregistrer les composants système Novell Audit pour Identity Manager (une version eDirectory valide et un serveur de consignation Novell Audit doivent être installés sur l'arborescence avant l'installation de cet utilitaire.)

8 Cliquez sur *Suivant*.

9 Sélectionnez les produits que vous voulez installer, puis cliquez sur *Suivant*.



La page Installation de pilotes sélectionnés du moteur affiche les pilotes que vous pouvez installer sur une plate-forme correspondante. Par défaut, tous les pilotes disponibles sont sélectionnés.

Nous recommandons l'installation de tous les fichiers de pilotes, ainsi vous n'aurez pas à exécuter le programme d'installation par la suite si vous souhaitez un autre pilote. Les fichiers de pilotes ne sont pas utilisés avant qu'un pilote soit configuré avec iManager ou le concepteur.

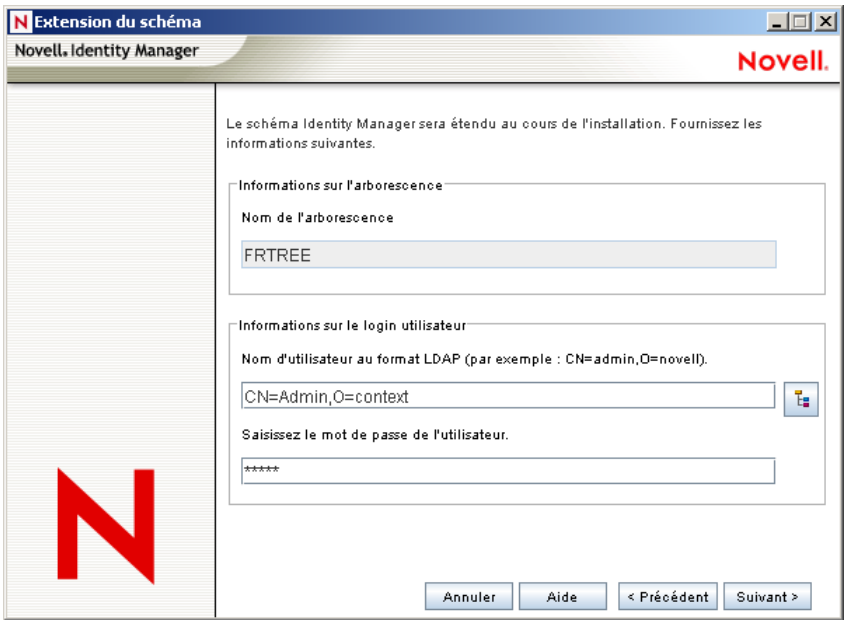
10 Lorsque vous voyez le message d'information de rappel d'activation du produit, cliquez sur *OK*.

Vous devez activer les pilotes dans un délai de 90 jours à compter de l'installation ; sinon, ils s'arrêteront.

11 Lorsque vous voyez le message d'avertissement de mise à niveau de la synchronisation des mots de passe, Cliquez sur *OK*.

Ce message est pour les serveurs Windows qui exécutent la version 1.0 de la synchronisation des mots de passe. Si vous souhaitez une rétro-compatibilité avec la version 1.0, vous devez ajouter des stratégies aux fichiers de configuration des pilotes. Sans stratégie, la version 1.0 de la synchronisation des mots de passe fonctionne pour les comptes existants, mais pas pour des comptes nouveaux ou renommés.

12 Sur la page Extension de schéma, indiquez ce qui suit :



- **Nom d'utilisateur :** indiquez le nom utilisateur (au format LDAP, comme CN=admin,O=novell) d'un utilisateur qui dispose de droits pour étendre le schéma eDirectory (quelqu'un qui a des droits de superviseur à la racine de l'arborescence, comme l'administrateur).
- **Mot de passe de l'utilisateur :** spécifiez le mot de passe de l'utilisateur.

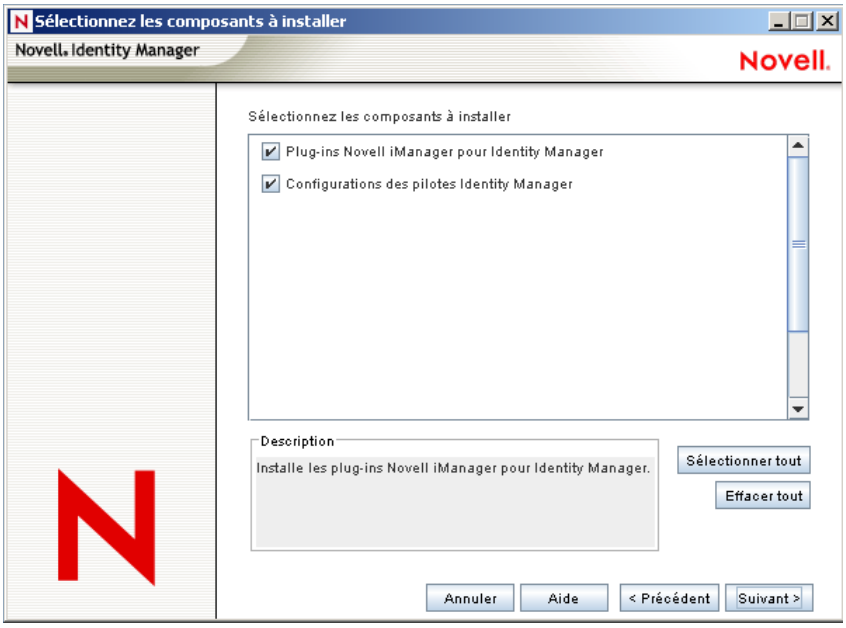
13 Cliquez sur *Suivant*. Lorsque les informations utilisateur sont validées, vous voyez la première des deux pages Composants :

Dans la page Sélectionnez les composants à installer, *Enregistrer les composants du système Novell Audit pour Identity Manager* est sélectionné si vous avez installé une version valide d'eDirectory et du serveur de consignation Novell Audit dans l'arborescence. Sinon, ils ne sont pas sélectionnés. La sélection de *Composants de l'application* installe des composants pour les systèmes d'applications tels que JDBC et PeopleSoft.

Si le programme d'installation détecte des fichiers de configuration de pilotes existants, il les déplace vers un chemin d'accès de sauvegarde.

La sélection de *Client Login Extension pour Novell Identity Manager* copie le programme d'installation de Client Login Extension dans votre système de fichiers. Pour plus d'informations sur Client Login Extension pour Novell Identity Manager, reportez-vous à « Client Login Extension pour Novell Identity Manager 3.5.1 » dans le *Guide d'administration de Novell Identity Manager*.

14 Sélectionnez les composants à installer et cliquez sur *Suivant*.



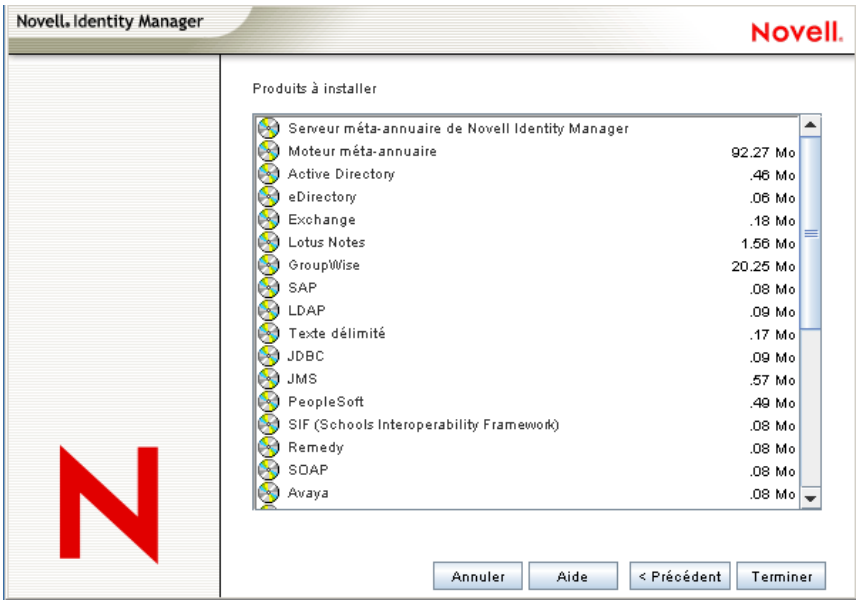
15 Une page supplémentaire s'affiche pour installer les plug-ins Identity Manager pour iManager, via le port SSL 443. Cliquez sur *Suivant*.

16 La deuxième page Composants permet d'installer les utilitaires. L'installation Windows présente une page supplémentaire qui indique le répertoire dans lequel les composants de l'application sont placés. L'emplacement par défaut est `C:\Novell\NDS\DirXMLUtilities`. Cliquez sur *Suivant*.

17 Sur la page Sélectionner les composants à installer, des utilitaires spécifiques aux plates-formes sont en veilleuse s'ils sont disponibles pour des plates-formes autres que celle sur laquelle vous effectuez l'installation. Sous Windows, tous les composants sont disponibles, y compris les scripts SQL pour le pilote JDBC, les composants JMS, les composants PeopleSoft, les outils License Auditing Tool, Active Directory Discovery Tool et Lotus Notes Discovery Tool, les utilitaires SAP, le programme d'installation du pilote de script et l'outil de configuration. Sélectionnez les composants dont vous avez besoin et cliquez sur *Suivant*.

18 Si vous avez choisi de copier le programme d'installation de Client Login Extension pour Novell Identity Manager sur votre système de fichiers, sélectionnez un chemin d'installation ou utilisez le chemin par défaut `C:\Novell\NDS\DirXMLUtilities\cle`. Cliquez sur *Suivant*.

19 Lisez et vérifiez vos sélections sur la page Résumé, puis cliquez sur *Terminer*.



Le processus d'installation Novell Identity Manager interrompt l'extension du schéma par eDirectory. Le processus d'installation commence par installer les produits et composants sélectionnés.

20 Une fois l'installation terminée, la boîte de dialogue Installation terminée apparaît, cliquez sur *Fermer*.

21 Afin que iManager reconnaisse les plug-ins que vous avez installés, redémarrez vos services Web maintenant et redémarrez Tomcat.

Si vous avez installé des pilotes Identity Manager, utilisez l'assistant de configuration Identity Manager dans iManager 2.6 ou une version supérieure, ou utilisez le concepteur pour configurer les pilotes.

4.5 Installation de l'option Système connecté sous Windows

Section 4.4, « Installation d'Identity Manager sous Windows », page 73 a couvert l'installation du serveur méta-annuaire, des composants Web et des utilitaires sous Windows. De plus, les serveurs Windows peuvent également utiliser l'option Système connecté.

Utilisez l'option Système connecté lorsque vous ne souhaitez pas mettre la surcharge des services eDirectory et le moteur méta-annuaire sur un serveur d'applications. Le chargeur distant permet la synchronisation désirée avec Identity Manager sans avoir à charger des applications accessibles ailleurs.

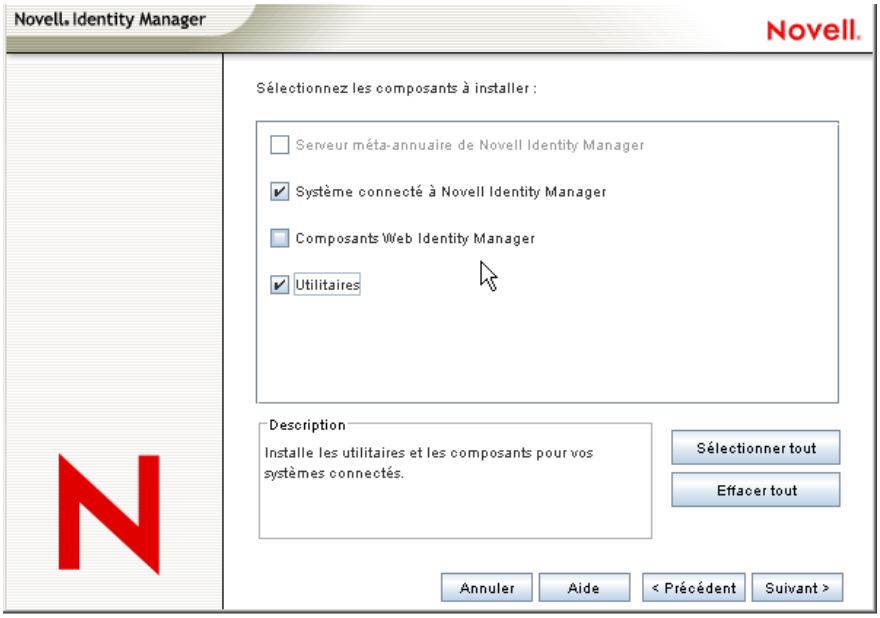
Avant de commencer, assurez-vous que votre système a la configuration requise indiquée dans Tableau 1-3 page 29.

1 Téléchargez Identity Manager. Fichier d'image `iso` dont vous avez besoin. Vous pouvez télécharger Identity Manager. Fichiers d'images `iso` du Site de téléchargement Novell (http://download.novell.com).

L'installation Windows d'Identity Manager se trouve dans `Identity_Manager_3_5_1_NW_Win.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`.

2. Exécutez `install.exe` à partir du répertoire `\NT`.
3. Lisez les informations de l'écran d'accueil, puis cliquez sur *Suivant*.
4. Sélectionnez une langue pour afficher l'accord de licence ou utilisez la langue par défaut (anglais).

   Le programme d'installation Identity Manager s'exécute automatiquement dans la langue de la machine sur laquelle vous l'installez. Si le programme d'installation n'a pas été traduit dans la langue que votre machine utilise, il s'exécute par défaut en anglais.
5. Lisez l'accord de licence, puis cliquez sur *J'accepte*.
6. Lisez les pages de présentation sur les différents systèmes et composants, puis cliquez sur *Suivant* pour commencer l'installation.
7. Pour sélectionner l'option Système connecté, cliquez d'abord sur *Effacer tout*, puis sélectionnez *Système connecté* et *Utilitaires*. Vous devez également sélectionner *Composants Web* si l'utilitaire iManager est installé sur ce serveur et si vous souhaitez ajouter des plug-ins Identity Manager pour Identity Manager et des configurations de pilotes.



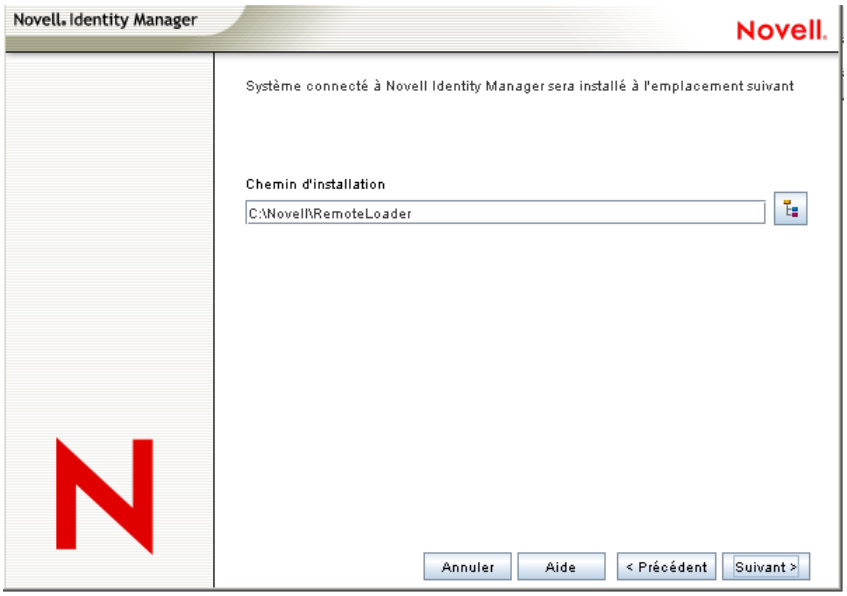
- **Système connecté :** installe le chargeur distant, qui permet d'établir une liaison entre le système connecté et un serveur qui exécute le moteur méta-annuaire. Sous Windows, cette option installe les pilotes suivants : Active Directory, Avaya, Texte délimité, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Paramètres Linux/UNIX, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF et Top Secret.
- **Utilitaires :** installe des scripts supplémentaires pour le pilote JDBC et des utilitaires pour d'autres pilotes. La plupart des pilotes n'ont aucun utilitaire connecté. Les utilitaires de pilotes peuvent comprendre :
  - scripts SQL pour le pilote JDBC
  - Composants JMS

- Composants PeopleSoft
- Outil d'audit de licence
- Outil Active Directory Discovery
- Outil Lotus Notes Discovery
- Utilitaires SAP
- Programme d'installation du pilote de script et outil de configuration

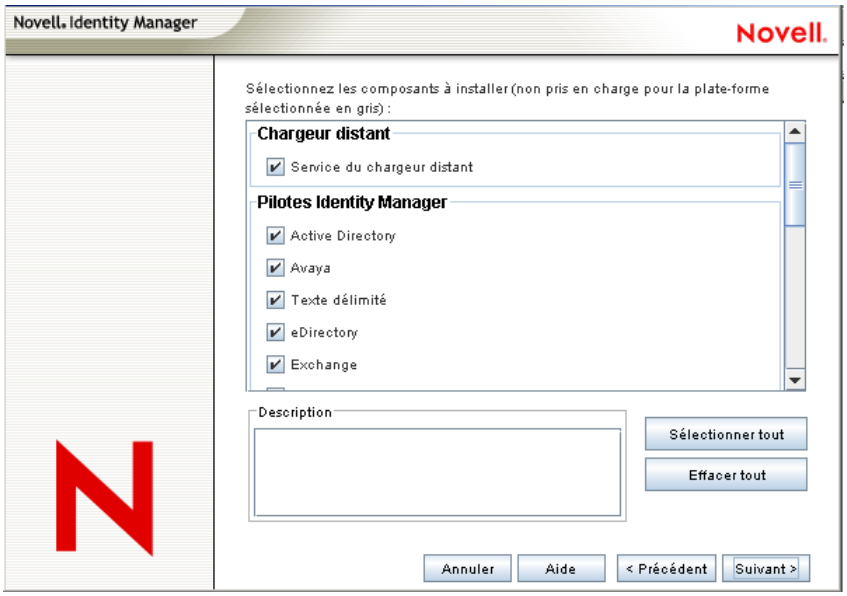
Un autre utilitaire permet d'enregistrer les composants système Novell Audit pour Identity Manager (une version eDirectory valide et un serveur de consignation Novell Audit doivent être installés sur l'arborescence avant l'installation de cet utilitaire.)

8 Cliquez sur *Suivant*.

9 Sur la page Emplacement d'installation, cliquez sur *Suivant* pour accepter le chemin d'accès au répertoire par défaut, qui est `C:\Novell\RemoteLoader`.



10 Sur la page Sélectionner les pilotes de l'installation du chargeur distant, sélectionnez les pilotes Identity Manager que vous souhaitez charger, puis cliquez sur *Suivant*.



La sélection de pilotes comprend Active Directory, Avaya, Texte délimité, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Paramètres Linux/UNIX, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF et Top Secret.

Si vous ne voulez pas installer tous les pilotes, vous pouvez cliquer sur *Effacer tout*, puis sélectionner les pilotes dont vous avez besoin, ou cliquer sur les pilotes que vous ne voulez pas installer pour les désélectionner. Si vous avez besoin d'un autre pilote dans l'avenir, vous devez exécuter à nouveau ce programme d'installation pour installer les pilotes que vous n'avez pas sélectionné. Vous pouvez également utiliser le concepteur pour créer, modifier et déployer des fichiers de pilotes.

11 Lorsque vous voyez le message d'information de rappel d'activation du produit, cliquez sur *OK*.

Vous devez activer les pilotes dans un délai de 90 jours à compter de l'installation ; sinon, ils s'arrêteront.

12 Lorsque vous voyez le message d'avertissement de mise à niveau de la synchronisation des mots de passe, Cliquez sur *OK*.

Ce message est pour les serveurs Windows qui exécutent la version 1.0 de la synchronisation des mots de passe. Si vous souhaitez une rétro-compatibilité avec la version 1.0, vous devez ajouter des stratégies aux fichiers de configuration des pilotes. Sans stratégie, la version 1.0 de la synchronisation des mots de passe fonctionne pour les comptes existants, mais pas pour des comptes nouveaux ou renommés.

13 Cliquez sur *Oui* pour créer un raccourci sur le bureau pour la console du chargeur distant. Si vous ne souhaitez pas de raccourci, cliquez sur *Non*.

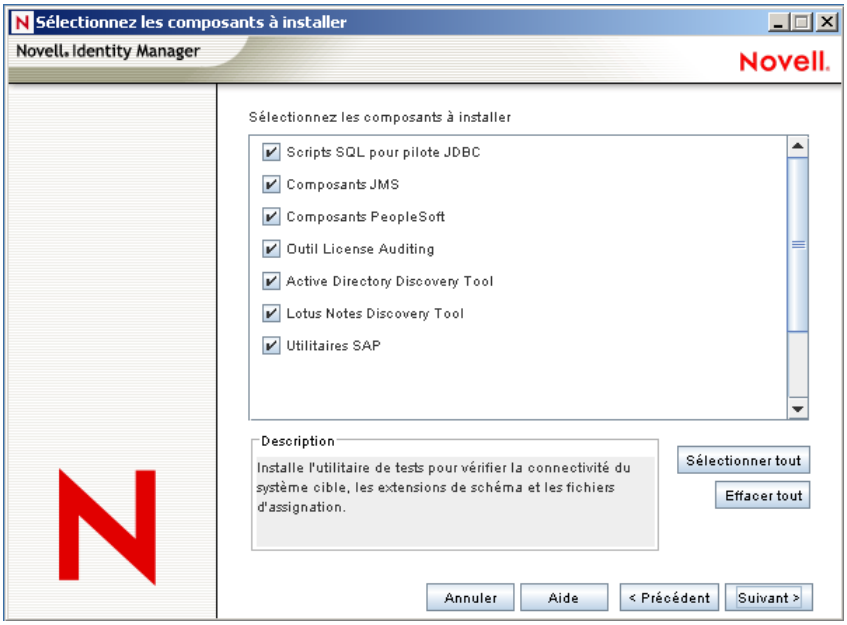
Dans la page Sélectionnez les composants à installer, *Enregistrer les composants du système Novell Audit pour Identity Manager* est sélectionné si vous avez installé une version valide d'eDirectory et du serveur de consignation Novell Audit dans l'arborescence. Sinon, ils ne sont pas sélectionnés. La sélection de *Composants de l'application* installe des composants pour les systèmes d'applications tels que JDBC et PeopleSoft.

La sélection de *Client Login Extension pour Novell Identity Manager* copie le programme d'installation de Client Login Extension dans votre système de fichiers. Pour plus d'informations sur Client Login Extension pour Novell Identity Manager, reportez-vous à « Client Login Extension pour Novell Identity Manager 3.5.1 » dans le *Guide d'administration de Novell Identity Manager*.

14 Sélectionnez les composants à installer et cliquez sur *Suivant*.

15 Cliquez sur *Suivant* pour accepter le chemin d'installation par défaut des utilitaires Identity Manager (`C:\Novell\NDS\DirXMLUtilities`).

16 Sélectionnez les composants pilotes et utilitaires à installer, puis cliquez sur *Suivant*.



17 Si vous avez choisi de copier le programme d'installation de Client Login Extension pour Novell Identity Manager sur votre système de fichiers, sélectionnez un chemin d'installation ou utilisez le chemin par défaut `C:\Novell\NDS\DirXMLUtilities\cle`. Cliquez sur *Suivant*.

18 Examinez les éléments indiqués sur la page Résumé. Si vous approuvez, cliquez sur *Terminer* pour installer les composants.

19 Cliquez sur *Fermer* pour quitter le programme d'installation.

4.6 Installation d'Identity Manager par l'interface utilisateur graphique sur les plates-formes UNIX/Linux

Avant de commencer, assurez-vous que votre système a la configuration requise indiquée dans Section 4.2, « Configuration système requise et composants Identity Manager », page 67.

1 Téléchargez Identity Manager. Fichier d'image `iso` dont vous avez besoin. Vous pouvez télécharger Identity Manager. Fichiers d'images `iso` du Site de téléchargement Novell (http://download.novell.com).

L'installation Linux pour Identity Manager se trouve dans `Identity_Manager_3_5_1_Linux.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`, tandis que AIX et Solaris se trouvent dans `Identity_Manager_3_5_1_Unix.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`.

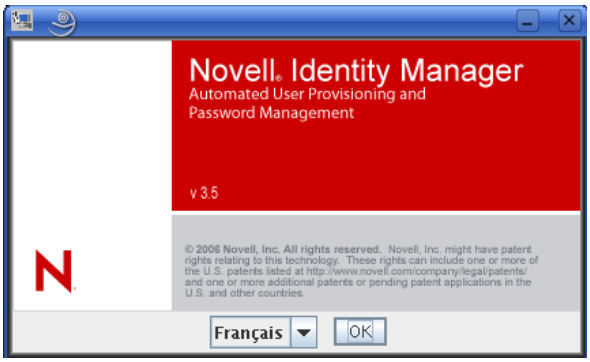
2 Sur l'ordinateur hôte, loguez-vous en tant qu'utilisateur `root`.

3 Pour exécuter l'installation de l'interface utilisateur graphique sous Linux, cliquez sur le fichier `install.bin` dans le répertoire racine. Vous êtes invité à indiquer si vous souhaitez exécuter le fichier d'installation au mode terminal ou au mode affichage. Sélectionnez *Terminal*. Le fichier `install.bin` vérifie la présence de Xwindows, et, dans cas, fait apparaître le programme d'installation de l'interface utilisateur graphique d'Identity Manager pour Linux.

Remarque : si cliquer sur `install.bin` ne lance pas le programme d'installation de l'interface utilisateur graphique, ouvrez une fenêtre de terminal et exécutez `install.bin` manuellement. Si vous avez un serveur Solaris exécutant eDirectory 8.8.x, exécutez le programme d'installation Identity Manager sans l'interface utilisateur graphique. Reportez-vous à Section 4.7, « Utilisation de la console pour installer Identity Manager sur les plates-formes UNIX/Linux », page 88.

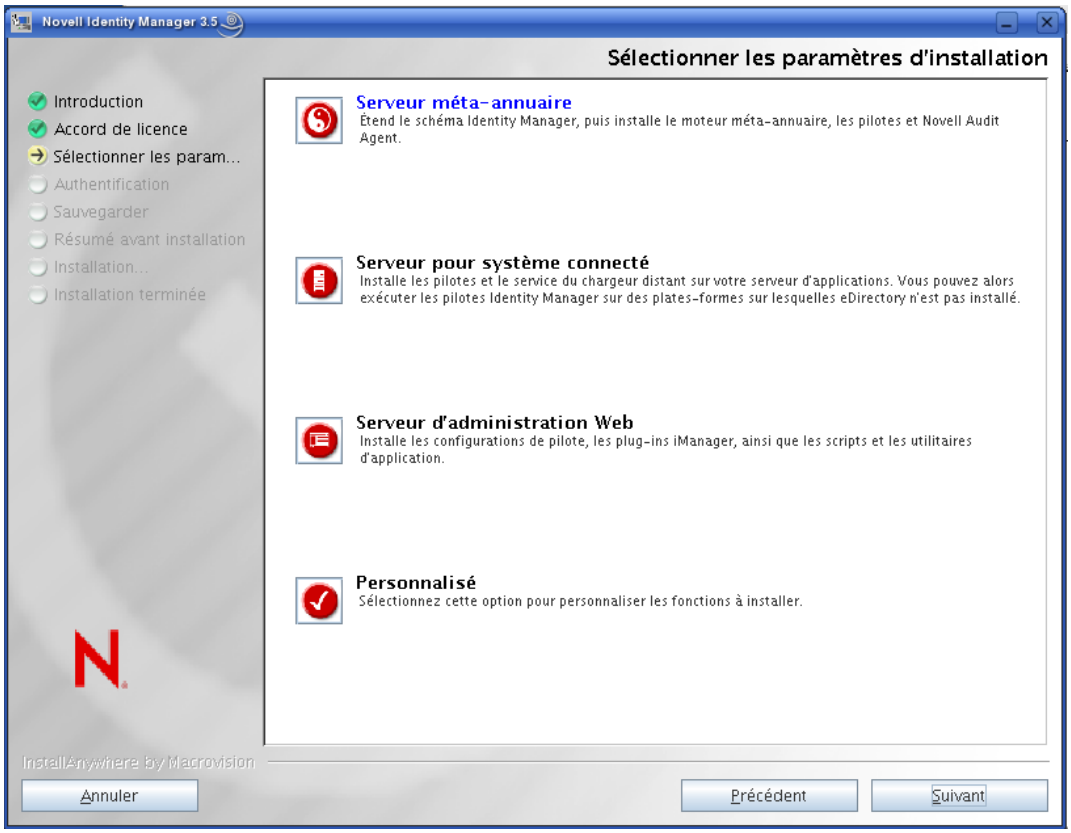
---

4 Sélectionnez la langue dans laquelle vous souhaitez exécuter le programme d'installation, ou utilisez la langue par défaut (anglais). Cliquez sur *OK*.



5 Lisez les informations sur l'écran d'accueil, puis cliquez sur *Suivant* pour poursuivre l'installation.

6 Lisez l'accord de licence, cliquez sur *J'accepte les termes de l'accord de licence,* puis cliquez sur *Suivant*.



7 Indiquez l'ensemble d'installation que vous souhaitez installer. Les ensembles d'installation contiennent les composants suivants :

- **Serveur méta-annuaire :** installe le moteur méta-annuaire et les pilotes de services, les pilotes Identity Manager, l'agent Novell Audit et étend le schéma eDirectory.

  Novell eDirectory 8.7.3.6 ou ultérieur et Security Services 2.0.5 (NMAS 3.1.3) avec les supports packs les plus récents doivent être installés avant de pouvoir installer cette option. Le processus d'installation Identity Manager s'arrête si ces éléments ne sont pas installés.

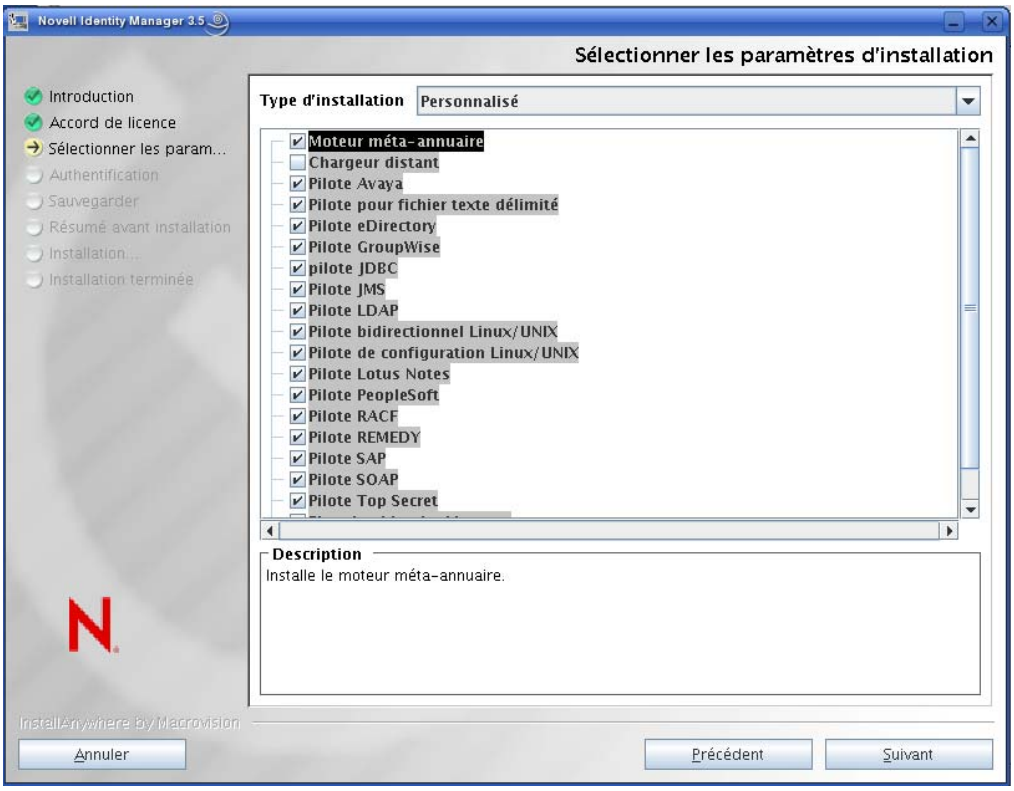
- **Serveur de systèmes connecté :** installe le chargeur distant et les pilotes suivants : Avaya, Delimited Text, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Linux/UNIX Bidirectional, Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret et Bon de travail. Choisissez l'option Serveur de systèmes connecté lorsque vous ne souhaitez pas mettre la surcharge des services eDirectory et le moteur méta-annuaire sur un serveur d'applications.

- **Service d'administration basé sur le Web :** installe les plug-ins Identity Manager et les stratégies de pilote Identity Manager.

  Novell iManager doit être installé avant de pouvoir installer cette option.

  Par défaut, les utilitaires de pilote Identity Manager ne sont pas installés sur les installations Linux/UNIX. Vous devez copier manuellement les utilitaires depuis le CD d'installation d'Identity Manager sur le serveur Identity Manager. Tous les utilitaires se trouvent sous le répertoire *de la plate-forme* `\setup\utilities`.

- **Personnaliser :** installe les composants spécifiques que vous sélectionnez à partir d'une liste de tous les composants.

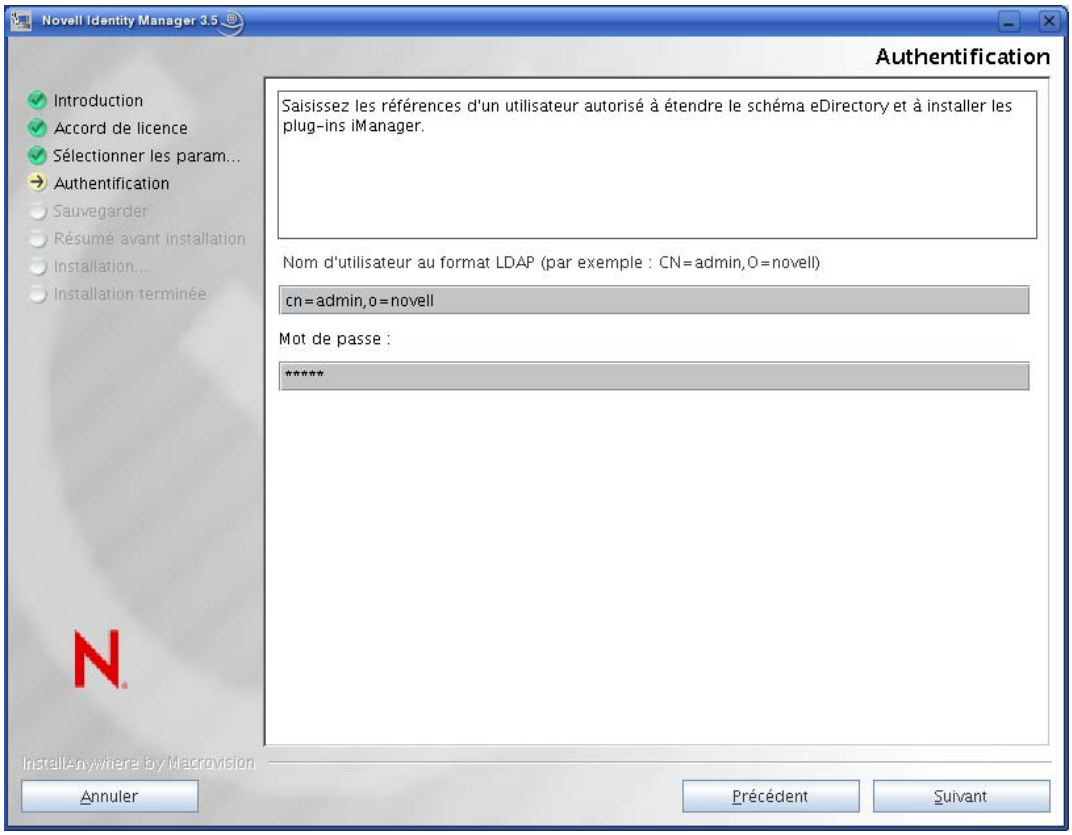


Vous pouvez sélectionner *Précédent* pour retourner aux menus précédents et modifier vos options d'installation.

8 (Facultatif) Selon l'option que vous choisissez (par exemple le serveur de méta-annuaire) et si vous exécutez eDirectory v8.8, vous êtes invité à configurer la variable d'environnement LD_LIBRARY_PATH. Pour ce faire, exécutez le script `/opt/novell/eDirectory/bin/ndspath` ; saisissez pour cela `./opt/novell/eDirectory/bin/ndspath`, puis réexécutez l'installation.

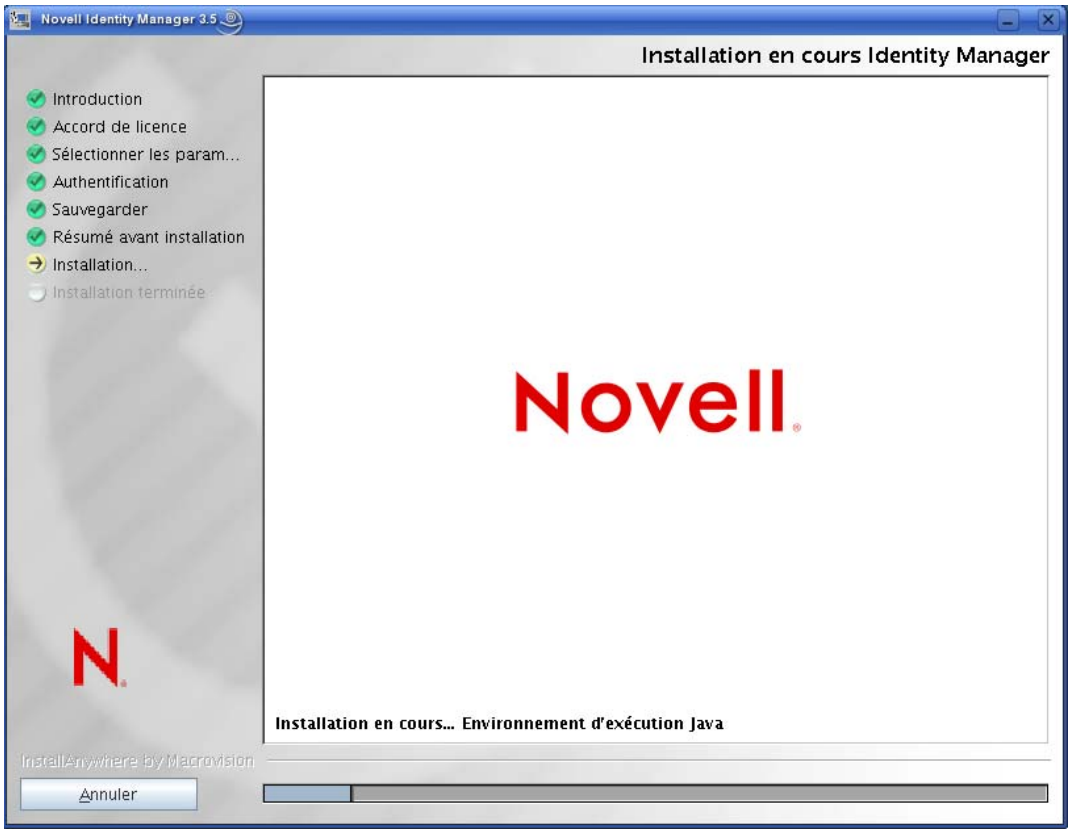
9 Si vous sélectionnez l'installation du serveur méta-annuaire, vous êtes invité à saisir le nom d'utilisateur LDAP (CN=admin,O=novell) et le mot de passe. Sélectionnez un utilisateur qui a

suffisamment de droits pour développer le schéma eDirectory (quelqu'un qui dispose des droits de superviseur à la racine de l'arborescence, comme un administrateur).



Important : (installations Solaris uniquement) si vous installez votre serveur d'administration basé sur le Web sur le même serveur qu'eDirectory, remplacez la valeur par défaut par celle d'un port libre, par exemple le port 8443, lorsque vous êtes invité à saisir le port sécurisé du serveur Web.

10 Vérifiez que les informations contenues dans la page Résumé avant installation sont correctes, puis cliquez sur *Installer* pour démarrer l'installation des packages.



eDirectory s'arrête temporairement lors de l'installation du moteur méta-annuaire et des fichiers de schémas. Par défaut, tous les pilotes disponibles étant installés, vous n'avez pas besoin d'exécuter le programme d'installation par la suite si vous souhaitez un autre pilote. Les fichiers de pilotes ne sont pas utilisés avant qu'un pilote soit configuré avec iManager ou le concepteur, puis déployé.

11 Lorsque vous voyez l'écran Installation terminée, appuyez sur *Terminé* pour fermer le programme d'installation.

4.7 Utilisation de la console pour installer Identity Manager sur les plates-formes UNIX/Linux

Avant de commencer, assurez-vous que votre système a la configuration requise indiquée dans Tableau 1-3 page 29.

1 Téléchargez Identity Manager. Fichier d'image `iso` dont vous avez besoin. Vous pouvez télécharger Identity Manager. Fichiers d'images `iso` du Site de téléchargement Novell (http://download.novell.com).

L'installation Linux pour Identity Manager se trouve dans `Identity_Manager_3_5_1_Linux.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`, tandis que AIX et Solaris se trouvent dans

`Identity_Manager_3_5_1_Unix.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`.

2 Sur l'ordinateur hôte, loguez-vous en tant qu'utilisateur `root`.

3 Exécutez le fichier `.bin` du répertoire d'installation.

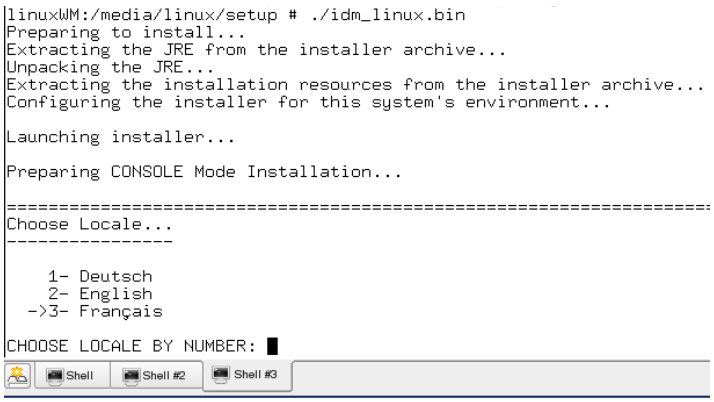
Changez le répertoire de travail actuel et passez au répertoire d'installation, dans lequel se trouve l'installation. Saisissez ensuite l'une des commandes suivantes pour exécuter l'installation.

Plate-forme	Exemple de chemin d'accès	Fichier d'installation
Linux	`linux/setup/`	`idm_linux.bin`
Solaris	`solaris/setup/`	`idm_solaris.bin`
AIX	`aix/setup/`	`idm_aix.bin`

Ces chemins d'accès sont liés à la racine de l'image d'installation, qui peut se trouver n'importe où vous l'avez développée ou là où vous avez installé le CD. Cela dépend également de l'image ISO que vous avez téléchargée. Par exemple, Linux se trouve dans `Identity_Manager_3_5_1_Linux.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`, alors que AIX et Solaris se trouvent dans `Identity_Manager_3_5_1_Unix.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`.

Le programme d'installation ne trouve pas les packages à installer à moins que le répertoire de travail soit là où se trouve le programme d'installation.

4 Sélectionnez la langue dans laquelle vous souhaitez exécuter le programme d'installation, ou utilisez la langue par défaut (anglais). Saisissez un numéro et appuyez sur Entrée.



5 Lisez les informations de l'écran d'accueil, puis appuyez sur Entrée pour poursuivre l'installation.

```
CHOOSE LOCALE BY NUMBER: 3
===============================================================================
==========
Identity Manager                  (created with InstallAnywhere by Ma
crovision)
-------------------------------------------------------------------------------
----------



===============================================================================
==========
Introduction
------------

Bienvenue dans l'installation de Novell Identity Manager 3.5.

Selon la configuration de votre système, il se peut que vous deviez e
xécuter ce
programme d'installation plusieurs fois pour installer les composants

d'Identity Manager sur les systèmes appropriés. Par exemple, il se pe
ut que
vous installiez des composants sur les systèmes suivants :

* Serveur méta-annuaire
* Serveur de système connecté
* Serveur d'administration basé sur le Web


Pour continuer, appuyez sur <Entrée>.: 
```

6 Appuyez sur Entrée pour passer à l'accord de licence, puis saisissez `Y` si vous acceptez les conditions d'utilisation. Si vous ne les acceptez pas, saisissez `N` pour quitter le programme d'installation.

```
===============================================================================
=
Sélectionner les paramètres d'installation
------------------------------------------

Sélectionnez le type d'installation requis.

  ->1- Serveur méta-annuaire
    2- Serveur pour système connecté
    3- Serveur d'administration Web

    4- Personnaliser...

Tapez le numéro du type d'installation requis, ou appuyez sur <Entrée> pour
   accepter la configuration par défaut.
   : 1
```

7 Indiquez le numéro approprié (1-4) de l'ensemble d'installation que vous souhaitez installer. Les ensembles d'installation contiennent les composants suivants :

- **1- Serveur méta-annuaire :** installe le moteur méta-annuaire et les pilotes de services, les pilotes Identity Manager, l'agent Novell Audit et étend le schéma eDirectory.

  Novell eDirectory 8.7.3.6 ou 8.8 et Security Services 2.0.5 (NMAS 3.1.3) avec les supports packs les plus récents doivent être installés avant de pouvoir installer cette option. Le processus d'installation Identity Manager s'arrêtera si ces éléments ne sont pas installés.

- **2- Serveur de systèmes connecté :** installe le chargeur distant et les pilotes suivants : Avaya, Delimited Text, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Linux/UNIX Bidirectional, Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret et Bon de travail. Vous pouvez choisir l'option *Serveur de systèmes connecté* lorsque vous ne souhaitez pas mettre la surcharge des services eDirectory et le moteur méta-annuaire sur un serveur d'applications.

- **3- Serveur administratif basé sur le Web :** installe les plug-ins Identity Manager et les stratégies de pilote Identity Manager.

  Novell iManager doit être installé avant de pouvoir installer cette option.

Par défaut, les utilitaires de pilote Identity Manager ne sont pas installés sur les installations Linux/UNIX. Vous devez copier manuellement les utilitaires depuis le CD d'installation d'Identity Manager sur le serveur Identity Manager. Tous les utilitaires se trouvent sous le répertoire *de la plate-forme* `\setup\utilities`.

- **4- Personnaliser :** installe les composants spécifiques que vous sélectionnez à partir d'une liste de tous les composants.

```
Type d'installation
    Serveur méta-annuaire

Composants de l'application :
    Pilote SAP,
    Pilote eDirectory,
    Pilote LDAP,
    Moteur méta-annuaire,
    pilote JDBC,
    Pilote pour fichier texte délimité,
    Pilote Lotus Notes,
    Pilote GroupWise,
    Pilote Avaya,
    Pilote SOAP,
    Pilote REMEDY,
    Pilote PeopleSoft,
    Pilote JMS,
    Pilote bidirectionnel Linux/UNIX,
    Pilote de configuration Linux/UNIX,
    Pilote RACF,
    Pilote Top Secret


Pour continuer, appuyez sur <Entrée>.:
```

Vous pouvez saisir `préc.` pour retourner aux menus précédents et modifier vos options d'installation.

8 (Facultatif) Selon l'option que vous choisissez (par exemple le serveur de méta-annuaire) et si vous exécutez eDirectory v8.8, vous êtes invité à configurer la variable d'environnement LD_LIBRARY_PATH. Pour ce faire, exécutez le script `/opt/novell/eDirectory/bin/ndspath` en saisissant `.`/`opt/novell/eDirectory/bin/dspath`, puis réexécutez l'installation.

9 Si vous sélectionnez l'installation du serveur méta-annuaire, vous êtes invité à saisir le nom d'utilisateur LDAP (CN=admin,O=novell) et le mot de passe. Sélectionnez un utilisateur qui a suffisamment de droits pour développer le schéma eDirectory (quelqu'un qui dispose des droits de superviseur à la racine de l'arborescence, comme un administrateur).

Important : (installations Solaris uniquement) si vous installez votre serveur d'administration basé sur le Web sur le même serveur qu'eDirectory, remplacez la valeur par défaut par celle d'un port libre, par exemple le port 8443, lorsque vous êtes invité à saisir le port sécurisé du serveur Web.

---

10 Vérifiez que les informations contenues dans le résumé sont correctes et appuyez sur Entrée pour démarrer l'installation des packages.

eDirectory s'arrête temporairement lors de l'installation du moteur méta-annuaire et des fichiers de schémas. Par défaut, tous les pilotes disponibles étant installés, vous n'avez pas besoin d'exécuter le programme d'installation par la suite si vous souhaitez un autre pilote. Les fichiers de pilotes ne sont pas utilisés avant qu'un pilote soit configuré avec iManager ou le concepteur, puis déployé.

11 Lorsque vous voyez l'écran Installation terminée, appuyez sur Entrée pour fermer le programme d'installation.

4.8 Utilisation de la console pour installer l'option Système connecté sous UNIX/Linux

Section 4.7, « Utilisation de la console pour installer Identity Manager sur les plates-formes UNIX/Linux », page 88 a couvert l'installation du serveur méta-annuaire, des composants Web et des utilitaires sur les plates-formes UNIX. De plus, les serveurs UNIX ou Linux peuvent utiliser l'option Système connecté.

Utilisez l'option Système connecté lorsque vous ne souhaitez pas mettre la surcharge des services eDirectory et le moteur méta-annuaire sur un serveur d'applications. Le chargeur distant permet la synchronisation désirée avec Identity Manager sans avoir à charger des applications accessibles ailleurs.

Avant de commencer, assurez-vous que votre système a la configuration requise indiquée dans Tableau 1-3 page 29.

1 Téléchargez Identity Manager. Fichier d'image `iso` dont vous avez besoin. Vous pouvez télécharger Identity Manager. Fichiers d'images `iso` du Site de téléchargement Novell (http://download.novell.com).

L'installation Linux pour Identity Manager se trouve dans `Identity_Manager_3_5_1_Linux.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`, tandis que AIX et Solaris se trouvent dans `Identity_Manager_3_5_1_Unix.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`.

2 Sur l'ordinateur hôte, loguez-vous en tant qu'utilisateur `root`.

3 Exécutez le fichier `. bin` du répertoire d'installation.

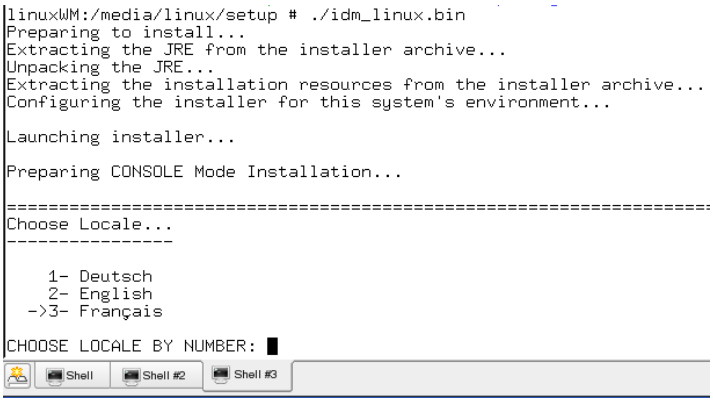
Changez le répertoire de travail actuel et passez au répertoire d'installation, dans lequel se trouve l'installation. Saisissez ensuite l'une des commandes suivantes pour exécuter l'installation :

Plate-forme	Exemple de chemin d'accès	Fichier d'installation
Linux	`linux/setup/`	`idm_linux.bin`
Solaris	`solaris/setup/`	`idm_solaris.bin`
AIX	`aix/setup/`	`idm_aix.bin`

Ces chemins d'accès sont liés à la racine de l'image d'installation, qui peut se trouver n'importe où vous l'avez développée ou là où vous avez installé le CD.

Le programme d'installation ne trouve pas les packages à installer à moins que le répertoire de travail soit là où se trouve le programme d'installation.

4 Sélectionnez la langue dans laquelle vous souhaitez exécuter le programme d'installation, ou utilisez la langue par défaut (anglais). Saisissez un numéro et appuyez sur Entrée.



5 Lisez les informations de l'écran d'accueil, puis appuyez sur Entrée pour poursuivre l'installation.

6 Appuyez sur Entrée pour passer à l'accord de licence, puis saisissez `Y` si vous acceptez les conditions d'utilisation. Si vous ne les acceptez pas, saisissez `N` pour quitter le programme d'installation.

7 Indiquez numéro 2 pour installer le serveur de systèmes connectés.

L'ensemble d'installation contient le chargeur distant et les pilotes suivantes : Avaya, Delimited Text, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Linux/UNIX Bidirectional, Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret et Bon de travail.

```
Type d'installation
    Serveur pour système connecté

Composants de l'application :
    Pilote LDAP,
    Pilote SAP,
    pilote JDBC,
    Pilote pour fichier texte délimité,
    Pilote Lotus Notes,
    Chargeur distant,
    Pilote GroupWise,
    Pilote Avaya,
    Pilote SOAP,
    Pilote REMEDY,
    Pilote PeopleSoft,
    Pilote JMS,
    Pilote bidirectionnel Linux/UNIX,
    Pilote de configuration Linux/UNIX,
    Pilote RACF,
    Pilote Top Secret


Pour continuer, appuyez sur <Entrée>.: 
```

8 Reportez-vous aux éléments indiqués sur l'écran Résumé avant installation. Appuyez sur Entrée pour installer les composants.

```
================================================================================
=
Installation en cours...
------------------------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------entered Wrap_
createNMASMethodCheckVersion
------------]



================================================================================
=
Installation terminée
---------------------

Félicitations. Novell Identity Manager 3.5 a été installé avec succès sur votr
e
système.

Si vous avez installé les plug-ins Identity Manager, redémarrez votre serveur
d'applications.

Pour abandonner l'installation, appuyez sur <Entrée>.: 
```

Par défaut, tous les pilotes disponibles étant installés, vous n'avez pas besoin d'exécuter le programme d'installation par la suite si vous souhaitez un autre pilote. Les fichiers de pilotes ne sont pas utilisés avant qu'un pilote soit configuré avec iManager ou le concepteur, puis déployé.

Par défaut, les utilitaires de pilote Identity Manager ne sont pas installés sur les installations Linux/Unix. Vous devez copier manuellement les utilitaires depuis le CD d'installation Identity Manager sur le serveur Identity Manager. Tous les utilitaires se trouvent sous le répertoire *de la plate-forme* `\setup\utilities`.

9 Lorsque vous voyez l'écran Installation terminée, appuyez sur Entrée pour fermer le programme d'installation.

4.9 Installation non-root d'Identity Manager

Cette version d'Identity Manager permet d'installer le moteur méta-annuaire d'Identity Manager dans une installation non-root d'eDirectory.

Novell Security Services 2.0.4 (NMAS 3.1.3) et eDirectory 8.8 non-root avec les correctifs actuels doivent être installés avant de pouvoir installer cette option. Pour plus d'informations sur

l'installation de NICI en tant qu'utilisateur non-root, reportez-vous à la sous-section *« Installation de NICI »* de *« Installation de 3.0 ou mise à niveau de Novell eDirectory sur Linux »* dans le Guide d'installation de Novell eDirectory 8.8 (http://www.novell.com/documentation/edir88/index.html).

Lorsque NICI est installé, suivez les instructions d'installation pour eDirectory 8.8 non-root qui se trouve dans la sous-section *« Installation de eDirectory 8.8 pour un utilisateur non-root »* de *« Installation de 3.0 ou mise à niveau de Novell eDirectory sur Linux »* dans le Guide d'installation de Novell eDirectory 8.8 (http://www.novell.com/documentation/edir88/index.html).

1. Téléchargez Identity Manager. Fichier d'image `iso` dont vous avez besoin. Vous pouvez télécharger Identity Manager. Fichier `iso` du Site de téléchargement Novell (http://download.novell.com).

   Linux se trouve dans `Identity_Manager_3_5_1_Linux.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`, alors que AIX et Solaris se trouvent dans `Identity_Manager_3_5_1_Unix.iso` ou dans `Identity_Manager_3_5_1_DVD.iso`. Le programme d'installation non-root est inclus dans l'image . `iso`.

2. Sur l'ordinateur hôte, loguez-vous avec les droits en écriture sur le répertoire dans lequel vous avez installé eDirectory non-root.

3. Exécutez le fichier `idm-nonroot-install` à partir du répertoire `/setup/`. Pour ce faire, changez le répertoire de travail actuel pour le répertoire `setup`, puis entrez la commande suivante pour exécuter l'installation non-root :

   ```
   ./idm-nonroot-install
   ```

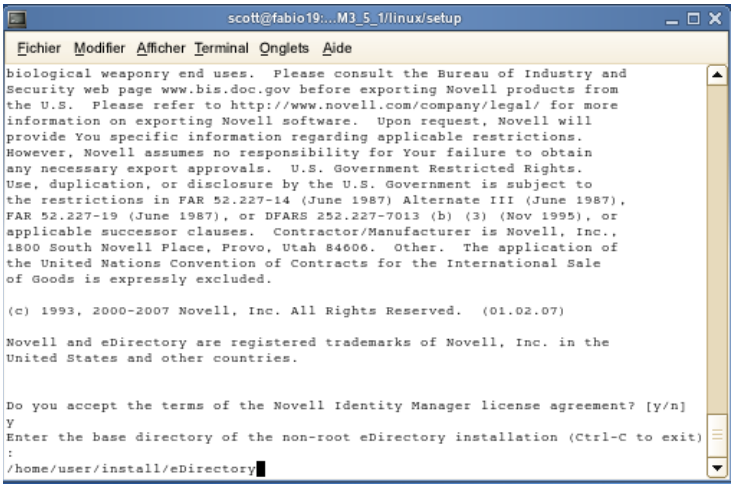
Plate-forme	Exemple de chemin d'accès	Fichier d'installation
Linux	`linux/setup/`	`idm-nonroot-install`
Solaris	`solaris/setup/`	`idm-nonroot-install`
AIX	`aix/setup/`	`idm-nonroot-install`

   Ces chemins sont relatifs à la racine de l'image `iso` et le programme d'installation ne trouve pas les packages à installer à moins que le répertoire de travail soit là où se trouve le programme d'installation.

4. Appuyez sur Entrer pour ouvrir l'accord de licence de l'utilisateur final, puis sur la barre d'espace pour faire défiler le texte de l'accord. Saisissez `Y` si vous acceptez les conditions d'utilisation. Si vous ne les acceptez pas, saisissez `N` pour quitter le programme d'installation.

5. Entrez le chemin d'accès pointant vers l'emplacement où se trouve l'eDirectory non-root. Par exemple :

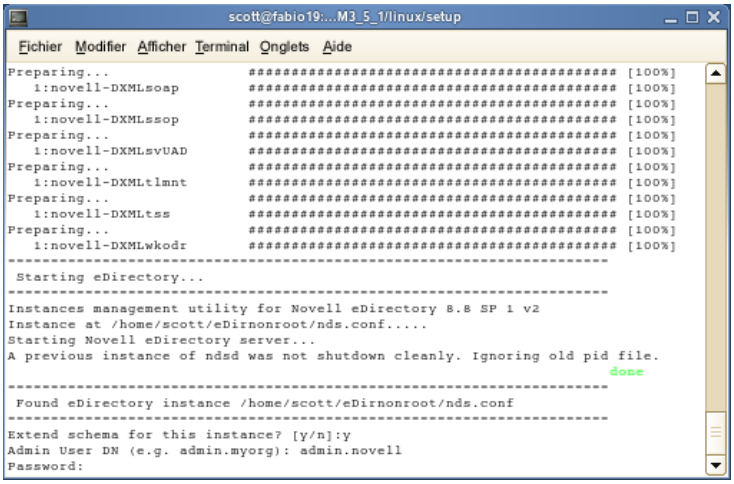
/home/user/installed/eDirectory



Le script d'installation installe ensuite Identity Manager avec les pilotes suivants : Avaya, Texte délimité, GroupWise, JDBC, JMS, LDAP, Paramètres Linux/UNIX, Linux/UNIX Bidirectionnel, Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret et Bon de travail.

6 Il vous est ensuite demandé d'étendre le schéma pour chaque instance d'eDirectory détenue par l'utilisateur logué. Pour chaque instance, entrez `O` pour étendre son schéma, ou `N` si vous ne voulez pas l'étendre.

7 Si vous choisissez d'étendre le schéma, saisissez le nom distinctif (DN) de la personne possédant les droits d'extension du schéma (par exemple admin.novell). Sélectionnez un utilisateur qui a suffisamment de droits pour développer le schéma eDirectory (quelqu'un qui dispose des droits de superviseur à la racine de l'arborescence, comme un administrateur).



8 Saisissez le mot de passe et appuyez sur Entrée. Vous devez effectuer les étapes 7 et 8 pour chaque instance d'eDirectory que vous étendez.

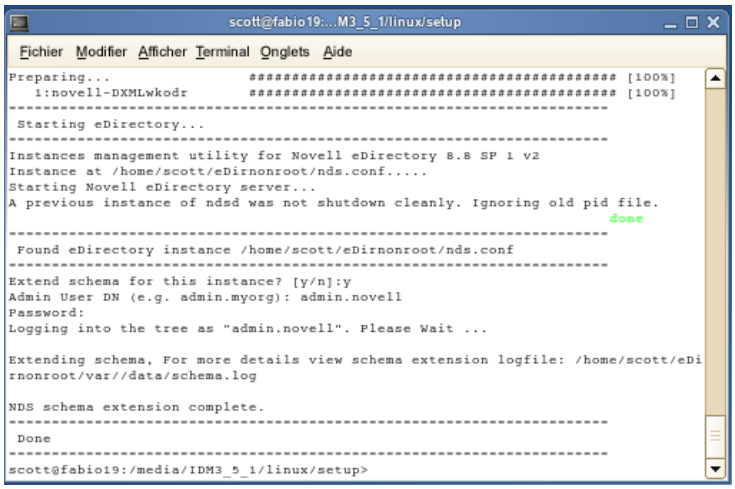
Si, ultérieurement, vous voulez étendre le schéma pour d'autres instances d'eDirectory, exécutez le script `idm-nonroot-install` dans le sous-répertoire `opt/novell/eDirectory/bin` de l'installation eDirectory non-root. Exécutez le script en étant logué en tant que propriétaire de l'instance eDirectory que vous voulez étendre.

Le script d'installation se logue à l'arborescence eDirectory et étend le schéma. Si vous souhaitez davantage de détails sur le processus d'extension du schéma, ouvrez le fichier `/home/user/eDirnonroot/var/data/schema.log`.

Par défaut, tous les pilotes disponibles étant installés, vous n'avez pas besoin d'exécuter le programme d'installation par la suite si vous souhaitez un autre pilote. Les fichiers de pilotes ne sont pas utilisés avant qu'un pilote soit configuré avec iManager ou le concepteur, puis déployé.

Par défaut, les utilitaires de pilote Identity Manager ne sont pas installés sur les installations Linux/UNIX. Vous devez copier manuellement les utilitaires depuis le CD d'installation d'Identity Manager sur le serveur Identity Manager. Tous les utilitaires se trouvent sous le répertoire *de la plate-forme* `\setup\utilities`.

9 Lorsque l'extension du schéma est terminée, Identity Manager est installé.



4.10 Tâches post-installation

Vous n'avez pas besoin de charger ou de décharger manuellement Identity Manager, car le module Identity Manager se charge lorsqu'un pilote Identity Manager démarre. Si l'un des paramètres de pilote est configuré à Autostart (démarrage automatique) et si le pilote et eDirectory sont exécutés, le pilote lance automatiquement le module Identity Manager. Si l'un des paramètres de pilote est configuré sur Manuel, le module Identity Manager se charge lorsque vous démarrez un pilote Identity Manager.

Après avoir installé Identity Manager, vous devez configurer les pilotes que vous avez installés pour mettre en oeuvre les stratégies et conditions que vous définissez comme processus métier. Les tâches post-installation comprennent généralement les éléments suivants :

- Configurer un système connecté. Reportez-vous à la documentation des pilotes Identity Manager (http://www.novell.com/documentation/dirxmldrivers) pour obtenir des instructions de configuration spécifiques au pilote.
- Créer et configurer un pilote. Utilisez iManager ou le concepteur pour créer un pilote ou pour configurer un pilote existant. Reportez-vous à « Importation d'un fichier de configuration des pilotes » dans le guide *Designer 2.1 pour Identity Manager 3.5.1*.
- Définir des stratégies. Utilisez iManager ou le concepteur pour définir des stratégies pour que les pilotes répondent à vos besoins. Reportez-vous à « Création d'une stratégie » dans le guide *Stratégies dans Designer 2.1* ou au guide *Présentation des stratégies d'Identity Manager 3.5.1*.

- Démarrer, arrêter ou redémarrer un pilote. Utilisez iManager ou le concepteur pour gérer les activités d'un pilote. Reportez-vous à « Importation d'un fichier de configuration des pilotes » dans le guide *Designer 2.1 pour Identity Manager 3.5.1*.
- Activer Identity Manager. Reportez-vous à Chapitre 6, « Activation des produits Novell Identity Manager », page 189.

4.11 Installation d'un pilote personnalisé

Un pilote personnalisé peut comprendre ce qui suit :

- Un ensemble de fichiers `jar` ou native (`. dll`, `. nlm`, ou `. so`)
- Des fichiers de règles XML pour la configuration du pilote
- Documentation

Pour plus d'informations sur la création ou l'installation de pilote personnalisé, reportez-vous au Novell Developer Kit (Kit du développeur Novell) (http://developer.novell.com/ndk/dirxml-index.htm). Reportez-vous également à « Édition des fichiers de configuration des pilotes » dans le *Guide d'administration de Novell Identity Manager 3.5.1*.

Installation de l'application utilisateur

5

Cette section décrit comment installer l'application utilisateur Identity Manager. Les thèmes incluent :

5.1 Conditions préalables à l'installation

Avant d'installer l'application utilisateur Identity Manager , vérifiez que les conditions suivantes sont satisfaites :

Tableau 5-1 *Conditions préalables à l'installation*

Conditions préalables liées à l'environnement	Description

Kit de développement Java*	Téléchargez et installez le kit de développement 5.0 édition standard de la plate-forme 2 de Java. Utilisez la version 1.5.0_10 de JRE. Avec WebSphere, utilisez IBM* JDK* en appliquant les fichiers de stratégies sans limitation.
	
	Définissez la variable d'environnement JAVA_HOME de façon à ce qu'elle pointe vers le JDK à utiliser avec l'application utilisateur. Vous pouvez également indiquer manuellement le chemin d'accès lors de l'installation de l'application utilisateur pour remplacer JAVA_HOME.
	
	◆ À l'invite de commande Linux ou Solaris, entrez `echo $JAVA_HOME`. Pour créer ou modifier JAVA_HOME, créez ou modifiez `~/.profile` (sous SUSE® Linux) :
	
	`#Java Home`
	
	`export JAVA_HOME=/usr/java/jdk1.5.0_10`
	
	`#JRE HOME`
	
	`export JRE_HOME=$JAVA_HOME/jre`
	
	◆ Sous Windows, reportez-vous à *Panneau de configuration* > *Système* > *Avancé* > *Variables d'environnement* > *Variables système*.

Serveur d'applications JBoss	Si vous utilisez JBoss, téléchargez et installez le serveur d'applications JBoss 4.2.0. (Démarrez ce serveur après avoir installé l'application utilisateur. Reportez-vous à Section 5.9, « Tâches post-installation », page 183). **RAM:** une RAM minimale de 512 Mo est recommandée pour le serveur d'applications JBoss lors de l'exécution de l'application utilisateur. **Port :** prenez note du port que votre serveur d'applications utilise. (La valeur par défaut du serveur d'applications est 8080.) **SSL:** si vous prévoyez d'utiliser une gestion des mots de passe externe, activez SSL sur les serveurs JBoss sur lesquels vous déployez l'application utilisateur et le fichier `IDMPwdMgt.war` . Reportez-vous à votre documentation JBoss pour obtenir des instructions. Assurez-vous également que le port SSL est ouvert sur votre pare-feu. Pour plus d'informations sur le `fichier IDMPwdMgt.war` , reportez-vous à Section 5.9.4, « Accès au WAR de mots de passe externe », page 185 ainsi qu'au *Guide d'administration de l'application utilisateur IDM 3.5.1* (http://www.novell.com/documentation/idm35/index.html).
Serveur d'applications WebSphere	Si vous utilisez WebSphere, téléchargez et installez le serveur d'applications WebSphere 6.1.
Activer le logout iChain	Activer logout ICS de l'application utilisateur Identity Manager en activant l'option Cookie Forward dans Novell Access Manager™ ou iChain®.

Conditions préalables liées à l'environnement	Description
Base de données	Installez votre base de données et votre pilote de base de données et créez une base de données ou une instance de base de données. Notez l'hôte et le port ; vous les utiliserez dans Section 5.5.7, « Indiquer l'hôte et le port de la base de données », page 122. Notez le nom de la base de données, le nom utilisateur et le mot de passe utilisateur ; vous les utiliserez dans Section 5.5.8, « Indiquer le nom de la base de données et l'utilisateur privilégié », page 123. Un fichier de source de données doit pointer vers la base de données. Cela est géré différemment selon votre serveur d'applications. Pour JBoss, le programme d'installation de l'application utilisateur crée un fichier source de données du serveur d'applications qui pointe vers la base de données et nomme le fichier selon le fichier WAR de l'application utilisateur. Pour WebSphere, configurez la source de données manuellement avant l'installation. Les bases de données doivent être compatibles UTF-8. Que vous installiez MySQL par l'utilitaire de l'application utilisateur IDM ou par vous-même, lisez Section 5.1.3, « Configuration de votre base de données MySQL », page 106. **Remarque :** si vous prévoyez migrer une base de données, démarrez cette base de données avant de sélectionner l'option de migration dans le programme d'installation. Si vous ne migrez pas de base de données, celle-ci n'a pas besoin d'être exécutée pendant l'installation de l'application utilisateur. Ne la démarrez que juste avant de démarrer le serveur d'applications.
En cas d'installation de l'application utilisateur IDM 3.5.1 sous Linux ou Solaris	L'emplacement d'installation par défaut est `/opt/novell/idm`. Vous pouvez sélectionner un autre répertoire d'installation par défaut lors de la procédure d'installation. Assurez-vous que le répertoire existe et qu'il est inscriptible par un utilisateur non-`root`.
En cas d'installation de l'application utilisateur IDM 3.5.1 sous Windows	**Répertoire d'installation:** l'emplacement d'installation par défaut est `C:\Novell\IDM`. Assurez-vous que ce répertoire existe et qu'il est inscriptible. Vous pouvez sélectionner un autre répertoire d'installation par défaut lors de la procédure d'installation.
Identity Manager 3.5.1	Le serveur de méta-annuaire Identity Manager 3.5.1 doit être installé avant de pouvoir créer un pilote d'application utilisateur et installer l'application utilisateur.
Pilote d'application utilisateur	Le pilote d'application utilisateur doit déjà exister (mais ne doit pas être activé) avant d'installer l'application utilisateur.
Accès au coffre-fort d'identité	L'application utilisateur requiert un utilisateur ayant un accès administrateur au contexte dans lequel se trouveront les utilisateurs de l'application utilisateur.
Stockage de l'application utilisateur IDM	L'ordinateur sur lequel vous installez l'application utilisateur doit avoir 320 Mo d'espace de stockage disponible.

Après avoir vérifié tous les prérequis, suivez les instructions d'installation aux sections suivantes :

- Section 5.1.1, « Installation du serveur d'applications JBoss et de la base de données MySQL », page 102

- Section 5.1.2, « Installation du serveur d'applications JBoss en tant que service », page 105
- Section 5.1.3, « Configuration de votre base de données MySQL », page 106

5.1.1 Installation du serveur d'applications JBoss et de la base de données MySQL

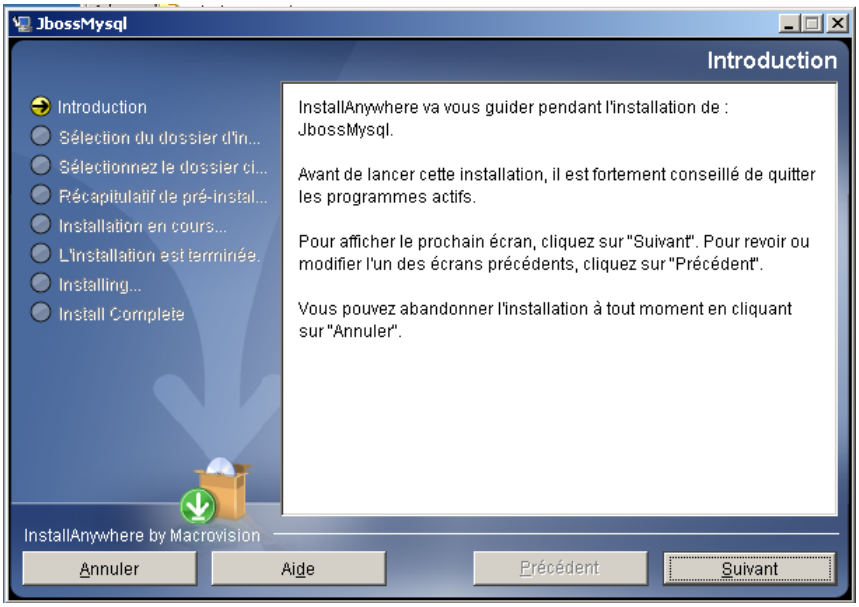
Utilisez l'utilitaire JbossMysql pour installer un serveur d'applications JBoss et MySql sur votre système.

Cet utilitaire n'installe pas le serveur d'applications JBoss en tant que service Windows. Pour installer le serveur d'applications JBoss en tant que service sur un système Windows, reportez-vous à Section 5.1.2, « Installation du serveur d'applications JBoss en tant que service », page 105.

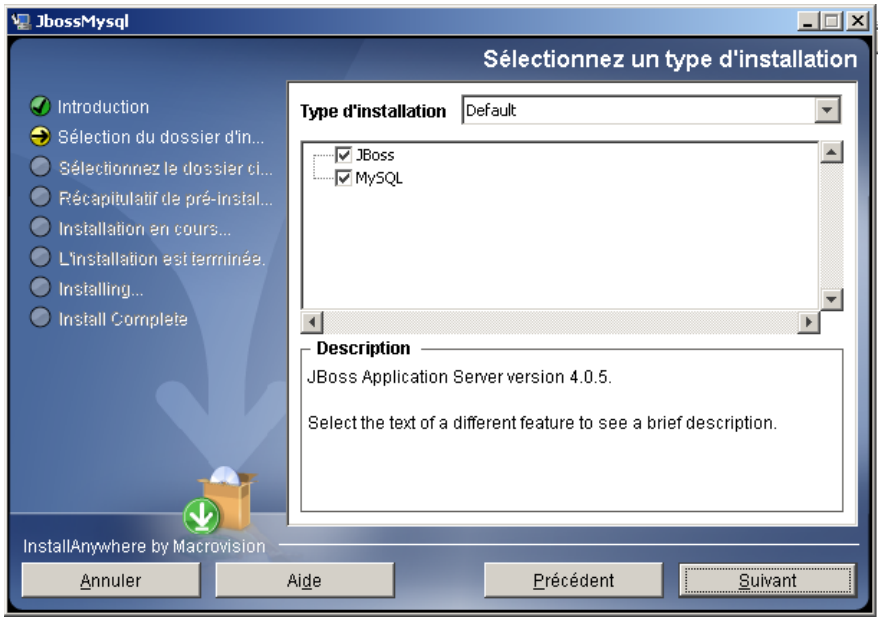
1. Localisez et exécutez `JbossMysql.bin` ou `JbossMysql.exe`. Cet utilitaire est fourni avec le programme d'installation de l'application utilisateur dans

   `/linux/user_application` (Linux)
   `/nt/user_application` (Windows)

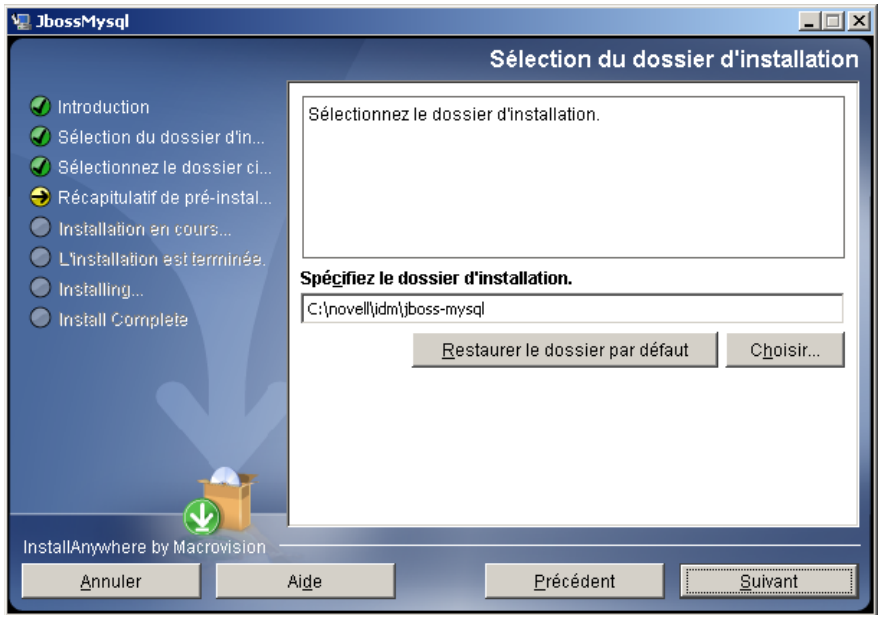
   Cet utilitaire n'est pas disponible avec Solaris.
2. Sélectionnez votre emplacement.
3. Lisez la page d'introduction, puis cliquez sur *Suivant*.



4 Sélectionnez les produits que vous voulez installer, puis cliquez sur *Suivant*.

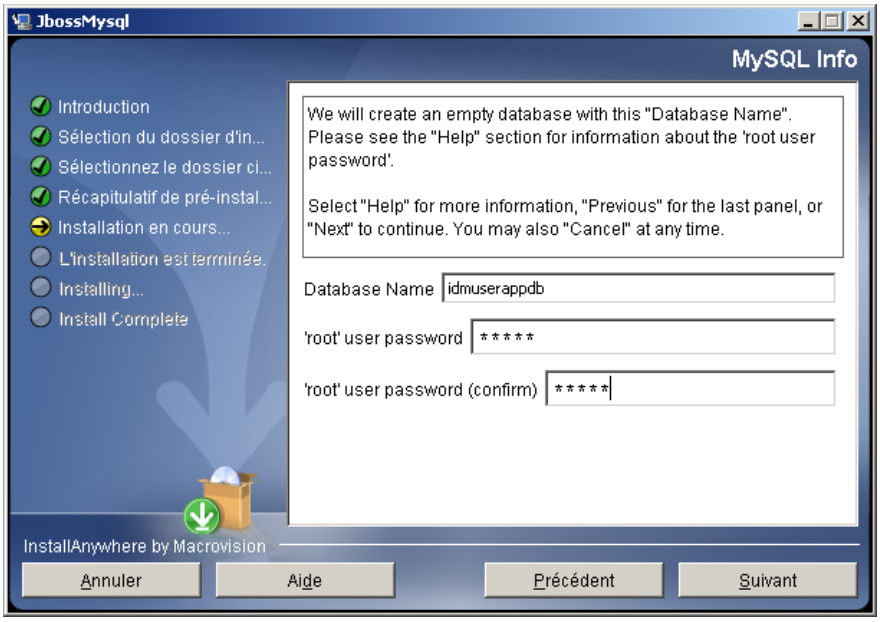


5 Cliquez sur *Choisir* pour sélectionner le dossier de base dans lequel installer les produits sélectionnés, puis cliquez sur *Suivant*.



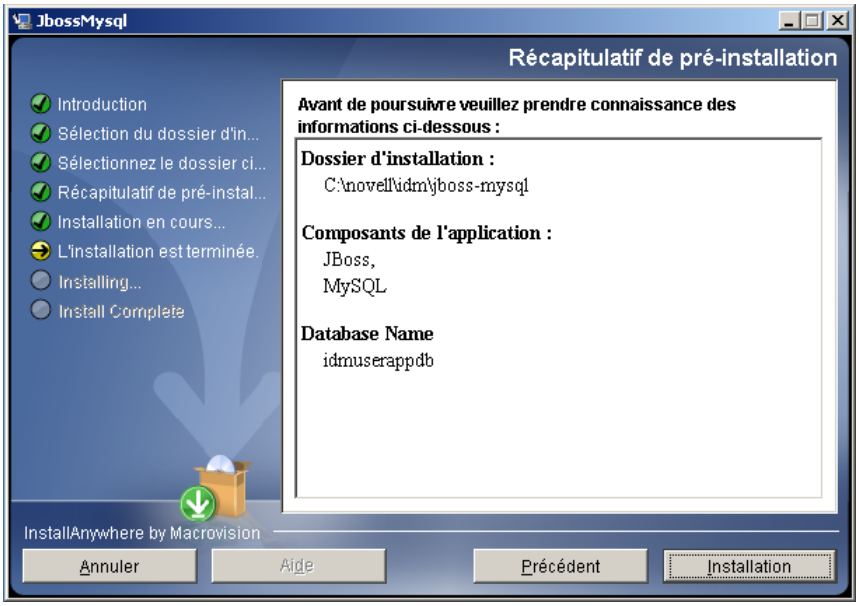
6 Nommez votre base de données. L'installation de l'application utilisateur exige ce nom.

7 Indiquez le mot de passe utilisateur `root` de la base de données.



8 Cliquez sur *Suivant*.

9 Examinez vos spécifications dans le Résumé avant installation, puis cliquez sur *Installer*.



L'utilitaire affiche un message de réussite dès qu'il a installé les produits que vous avez sélectionnés. Si vous avez installé la base de données MySQL, passez à Section 5.1.3, « Configuration de votre base de données MySQL », page 106.

5.1.2 Installation du serveur d'applications JBoss en tant que service

Pour exécuter le serveur d'applications JBoss comme un service, utilisez un wrapper de service Java ou un utilitaire tiers. Reportez-vous aux recommandations de JBoss à l'adresse http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows (http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows).

- « Utilisation d'un wrapper de service Java » page 105
- « Utilisation d'un utilitaire tiers » page 105

Utilisation d'un wrapper de service Java

Vous pouvez utiliser un wrapper de service Java pour installer, démarrer et arrêter le serveur d'applications JBoss comme service Windows ou processus daemon Linux ou UNIX. Recherchez sur Internet les utilitaires et sites de téléchargement disponibles.

L'un de ces wrappers se trouve dans http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html) : vous pouvez le gérer par JMX (reportez-vous à http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss)). Les exemples de fichiers de configuration sont les suivants :

```
wrapper.conf :
wrapper.java.command=%JAVA_HOME%/bin/java
wrapper.java.mainclass=org.tanukisoftware.wrapper.WrapperSimpleApp
wrapper.java.classpath.1=%JBOSS_HOME%/server/default/lib/
 wrapper.jar
wrapper.java.classpath.2=%JAVA_HOME%/lib/tools.jar
 wrapper.java.classpath.3=./run.jar
wrapper.java.library.path.1=%JBOSS_HOME%/server/default/lib
 wrapper.java.additional.1=-server
 wrapper.app.parameter.1=org.jboss.Main
 wrapper.logfile=%JBOSS_HOME%/server/default/log/wrapper.log
 wrapper.ntservice.name=JBoss wrapper.ntservice.displayname=JBoss
 Server
```

Avertissement : vous devez définir correctement votre variable d'environnement JBOSS_HOME. Le wrapper ne définit pas cela par lui-même.

```
java-service-wrapper-service.xml : <Xxml version="1.0"
encoding="UTF-8"?><!DOCTYPE server><server> <mbean
code="org.tanukisoftware.wrapper.jmx.WrapperManager"
name="JavaServiceWrapper:service=WrapperManager"/> <mbean
code="org.tanukisoftware.wrapper.jmx.WrapperManagerTesting"
name="JavaServiceWrapper:service=WrapperManagerTesting"/></server
```

Utilisation d'un utilitaire tiers

Pour les versions précédentes, vous pouvez utiliser un utilitaire tiers tel que JavaService pour installer, démarrer et arrêter le serveur d'applications JBoss en tant que service Windows.

Avertissement : JBoss ne recommande plus d'utiliser JavaService. Pour plus de détails, reportez-vous à http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService (http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService).

5.1.3 Configuration de votre base de données MySQL

Vos paramètres de configuration MySQL doivent être définis de façon à ce que MySQL et Identity Manager 3.5.1 fonctionnent ensemble. Si vous installez MySQL vous-même, vous devez définir les paramètres vous-même. Si vous installez MySQL à l'aide de l'utilitaire JbossMysql, celui-ci définit les valeurs qui vous conviennent, mais vous devez connaître les valeurs à maintenir pour ce qui suit :

- « Ensemble de caractères » page 106
- « Moteur de stockage et types de tables INNODB » page 106
- « Distinction de la casse » page 106

Ensemble de caractères

Indiquez UTF-8 comme ensemble de caractères pour l'ensemble du serveur ou simplement pour une base de données. Indiquez UTF-8 sur l'ensemble du serveur en incluant l'option suivante dans `my.cnf` (Linux ou Solaris) ou `my.ini` (Windows) :

`character-set-server=utf8` ou

Indiquez l'ensemble de caractères d'une base de données au moment de la création de la base de données, à l'aide de la commande suivante :

```
create database databasename character set utf8 collate utf8_bin;
```

Si vous configurez l'ensemble de caractères pour la base de données, vous devez également indiquer l'ensemble de caractères de l'URL JDBC dans le fichier `IDM-ds.xml`, comme dans :

```
<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&amp;characterEncoding
```

Moteur de stockage et types de tables INNODB

L'application utilisateur se sert du moteur de stockage INNODB, ce qui permet de choisir des types de tables INNODB pour MySQL. Si vous créez une table MySQL sans indiquer son type, la table sera de type MyISAM par défaut. Si vous choisissez d'installer MySQL à partir de la procédure d'installation d'Identity Manager, le MySQL fourni avec cette procédure contient le type de table INNODB indiqué. Pour vous assurer que votre serveur MySQL utilise INNODB, vérifiez que `my.cnf` (Linux ou Solaris) ou `my.ini` (Windows) contient l'option suivante :

`default-table-type=innodb`

Il ne doit pas contenir l'option `skip-innodb`.

Distinction de la casse

Assurez-vous que la distinction de la casse est cohérente sur les serveurs et plates-formes si vous prévoyez sauvegarder et restaurer des données sur des serveurs ou des plates-formes. Pour assurer cette cohérence, indiquez la même valeur (0 ou 1) pour les `noms_tables_minuscules` de tous vos fichiers `my.cnf` (Linux ou Solaris) ou `my.ini` (Windows), au lieu d'accepter la valeur par

défaut (valeurs par défaut Windows à 0 et valeurs par défaut Linux à 1.) Indiquez cette valeur avant de créer la base de données qui contiendra les tables Identity Manager. Vous pouvez par exemple spécifier

```
lower_case_table_names=1
```

dans les fichiers `my.cnf` et `my.ini` pour toutes les plates-formes sur lesquelles vous souhaitez sauvegarder et restaurer une base de données.

5.2 Installation et configuration

1. Créez le pilote de l'application utilisateur et laissez-le désactivé.

   Cette étape permet de créer de nouveaux objets dans le coffre-fort d'identité. Certains auront des valeurs de données par défaut. Pour plus d'informations, reportez-vous à Section 5.3, « Création du pilote d'application utilisateur », page 107.

2. Exécutez le programme d'installation de l'application utilisateur.

   Pour plus d'informations, reportez-vous à la Section 5.5, « Installation de l'application utilisateur sur un serveur d'applications JBoss à partir de l'interface utilisateur d'installation », page 114 ou à la Section 5.6, « Installation de l'application utilisateur sur un serveur d'applications WebSphere », page 146.

   Les utilisateurs de WebSphere doivent déployer manuellement le fichier WAR.

Important : l'installation de l'application utilisateur Identity Manager requiert que le pilote de l'application utilisateur existe déjà avant d'installer l'application. Vous devez toutefois démarrer le pilote *après* avoir installé l'application utilisateur Identity Manager, sinon le pilote de l'application utilisateur peut renvoyer des erreurs.

5.3 Création du pilote d'application utilisateur

Vous devez créer un pilote d'application utilisateur séparé pour chaque application utilisateur, sauf pour les applications utilisateur d'une grappe. Les applications utilisateur qui font partie de la même grappe doivent partager un seul pilote d'application utilisateur. Pour des informations sur l'exécution de l'application utilisateur dans une grappe, reportez-vous au *Guide d'administration de l'application utilisateur Identity Manager 3.5.1* (http://www.novell.com/documentation/idm35/index.html).

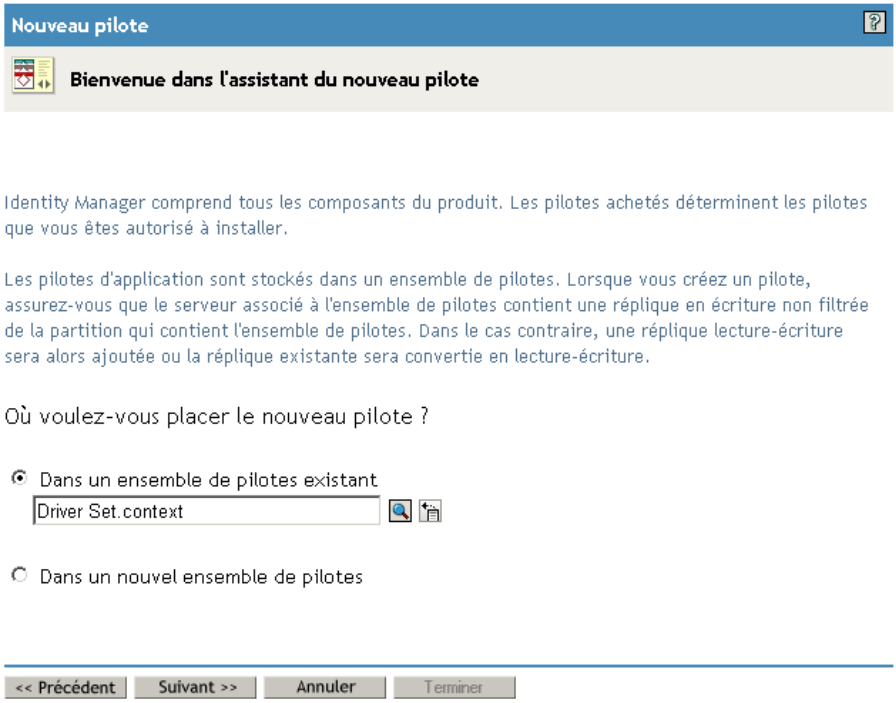
L'application utilisateur stocke des données spécifiques à l'application dans le pilote pour contrôler et configurer l'environnement de l'application. Cela inclut les informations de la grappe de serveurs d'application et la configuration du moteur de workflow.

Important : configurer un ensemble d'applications utilisateur non mises en grappe pour partager un seul pilote crée une ambiguïté et une configuration incorrecte d'un ou de plusieurs composants exécutés dans l'application utilisateur. La source des problèmes conséquents est difficile à détecter.

Pour créer un pilote de l'application utilisateur et l'associer à un ensemble de pilotes :

1. Loguez-vous au coffre-fort d'identité avec iManager (si vous ne l'avez pas déjà fait).

2 Allez à *Rôles et tâches* > *Utilitaires Identity Manager* et sélectionnez *Nouveau pilote* pour lancer l'assistant de création de pilote.

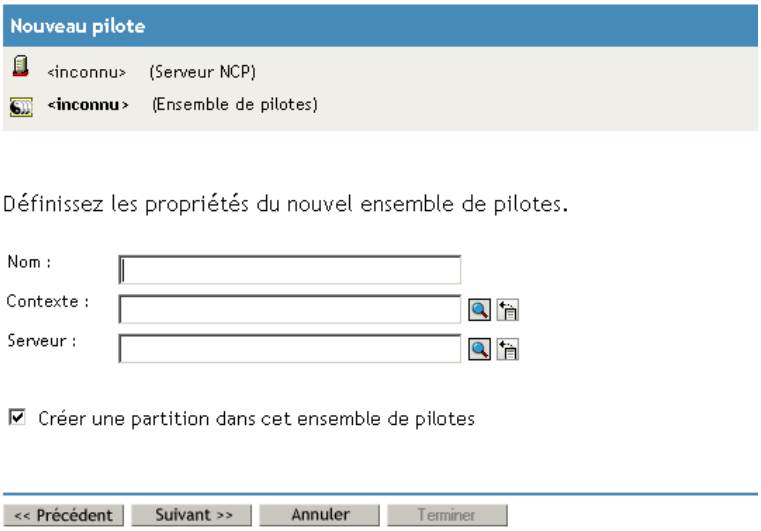


3 Pour créer le pilote dans un ensemble de pilotes existant, sélectionnez *Dans un ensemble de pilotes existant*, cliquez sur l'icône de sélection d'objet, sélectionnez un objet Ensemble de pilotes, cliquez sur *Suivant* et passez à Étape 4.

ou

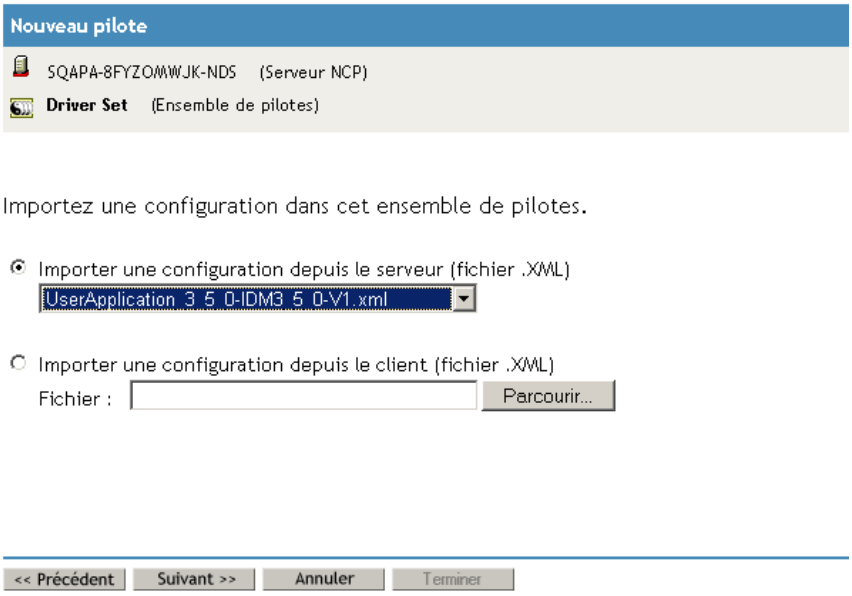
Si vous devez créer un nouvel ensemble de pilotes (par exemple, si vous placez le pilote de l'application utilisateur sur un serveur différent de vos autres pilotes), sélectionnez *Dans un nouvel ensemble de pilotes*, cliquez sur *Suivant*, puis définissez les propriétés du nouvel ensemble de pilotes.

3a Indiquez un nom, un contexte et un serveur pour le nouvel ensemble de pilotes.



3b Cliquez sur *Suivant*.

4 Cliquez sur *Importer une configuration de pilote depuis le serveur (fichier .XML)*.



5 Sélectionnez *UserApplication.xml* dans la liste déroulante.

Il s'agit du fichier de configuration de votre nouveau pilote.

6 Cliquez sur *Suivant*.

Si *UserApplication.xml* ne figure pas dans cette liste déroulante, vous n'avez probablement pas exécuté la portion du serveur d'administration basé sur le Web de l'installation d'Identity Manager 3.5.1.

7 Vous êtes invité à saisir les paramètres de votre pilote. (Faites défiler pour afficher tout.) Prenez note des paramètres ; vous en avez besoin lorsque vous installez l'application utilisateur.

Champ	Description
Nom du pilote	Le nom du pilote que vous créez.
ID d'authentification	Le nom distinctif de l'administrateur de l'application utilisateur. Il s'agit d'un administrateur de l'application utilisateur à qui vous donnez les droits d'administrer le portail de l'application utilisateur. Utilisez le format eDirectory™, par exemple admin.orgunit.novell, ou recherchez l'utilisateur. Ce champ est obligatoire.
Mot de passe	Mot de passe de l'administrateur de l'application utilisateur indiqué dans l'ID d'authentification.
Contexte de l'application	Le contexte de l'application utilisateur. Il s'agit de la portion de contexte de l'URL du fichier WAR de l'application utilisateur. La valeur par défaut est : IDM.
Hôte	Le nom d'hôte ou l'adresse IP du serveur d'applications où l'application utilisateur Identity Manager est déployée. En cas d'exécution dans une grappe, saisissez le nom d'hôte ou l'adresse IP du répartiteur.
Port	Le port de l'hôte indiqué ci-dessus.
Autoriser l'initiateur de remplacement : (les valeurs sont Non/Oui)	Sélectionnez *Oui* pour autoriser l'administrateur du Provisioning à démarrer des workflows au nom de la personne pour qui l'administrateur du provisioning est désigné comme proxy.

8 Cliquez sur *Suivant*.

9 Cliquez sur *Définir les équivalents de sécurité* pour ouvrir la fenêtre Équivalents de sécurité. Recherchez et sélectionnez un objet administrateur ou autre superviseur, puis cliquez sur *Ajouter*.

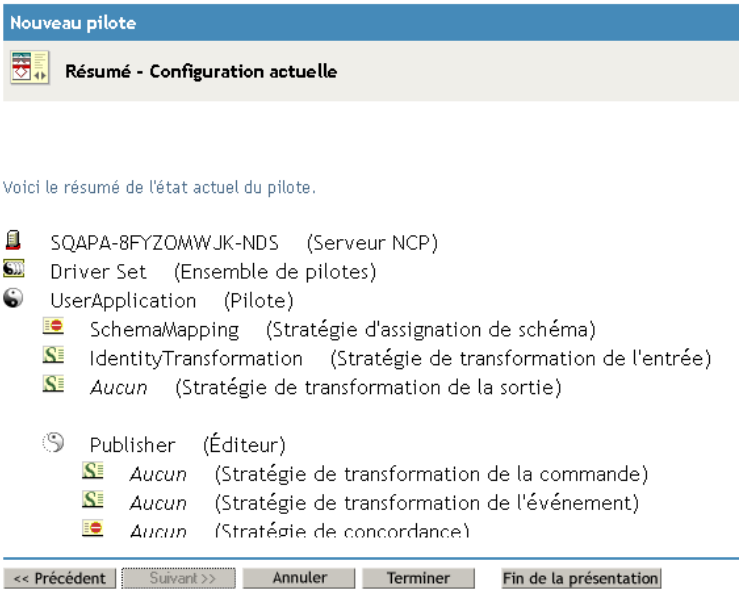
Cette étape donne au pilote les autorisations de sécurité dont il a besoin. Des détails sur le sens de cette étape se trouvent dans votre documentation Identity Manager.

10 (Facultatif, mais recommandé) Cliquez sur *Exclure les rôles administratifs*.

11 Cliquez sur *Ajouter*, puis sélectionnez les utilisateurs que vous souhaitez exclure des actions de pilote (les rôles administratifs, par exemple).

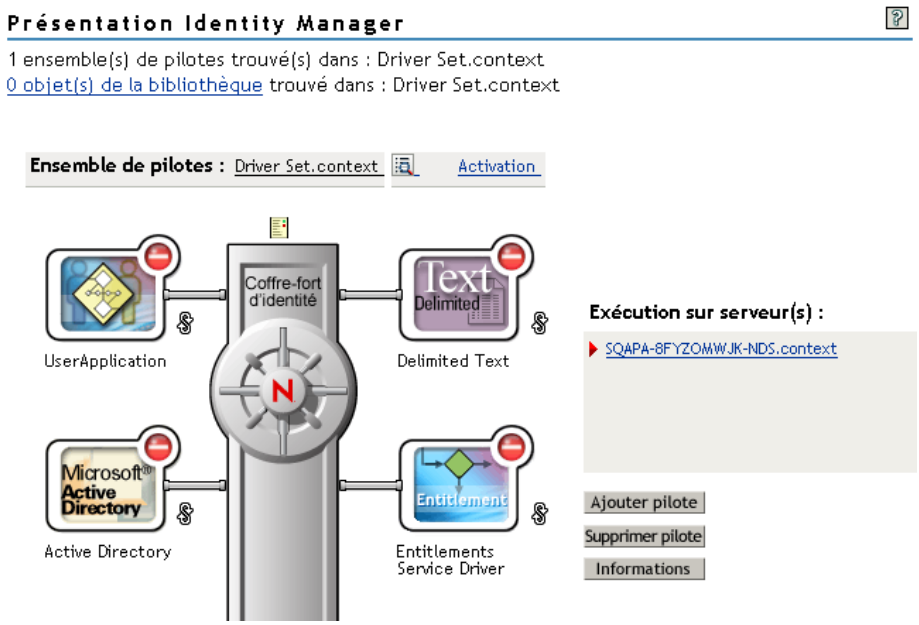
12 Cliquez deux fois sur *OK*, puis sur *Suivant*.

13 Cliquez sur *OK* pour fermer la fenêtre Équivalents de sécurité et afficher la page de résumé.



14 Si les informations sont correctes, cliquez sur *Terminer* ou *Terminer avec présentation.*

Important : le pilote est désactivé par défaut. Laissez le pilote désactivé jusqu'à ce que l'application utilisateur soit installée.



5.4 À propos du programme d'installation

Le programme d'installation de l'application utilisateur effectue ce qui suit :

- Désigne une version existante d'un serveur d'applications à utiliser.
- Désigne une version existante d'une base de données à utiliser, par exemple MySQL, Oracle ou Microsoft SQL Server. La base de données stocke les données de l'application utilisateur et les informations de configuration de l'application utilisateur.
- Configure le fichier des certificats de JDK pour que l'application utilisateur (exécutée sur le serveur d'applications) puisse communiquer avec le coffre-fort d'identité et le pilote de l'application utilisateur de façon sécurisée.
- Configure et déploie le fichier (WAR) d'archive de l'application Web Java (WAR) pour l'application utilisateur Novell Identity Manager sur le serveur d'applications JBoss.
- Active la consignation Novell Audit si vous la sélectionnez.
- Permet d'importer une clé maîtresse existante pour restaurer une installation particulière de l'application utilisateur et pour prendre des grappes en charge.

- Section 5.4.1, « Scripts et exécutables d'installation », page 112
- Section 5.4.2, « Valeurs requises à l'installation », page 113

Vous pouvez lancer le programme d'installation en trois modes :

- Interface Utilisateur Graphique. Reportez-vous à Section 5.5, « Installation de l'application utilisateur sur un serveur d'applications JBoss à partir de l'interface utilisateur d'installation », page 114)
- Interface de console (ligne de commande). Reportez-vous à Section 5.7, « Installation de l'application utilisateur à partir d'une interface de console », page 175)
- Installation en mode silencieux. Reportez-vous à Section 5.8, « Installation de l'application utilisateur avec une seule commande », page 176.

5.4.1 Scripts et exécutables d'installation

Vous pouvez obtenir les fichiers d'installation Identity Manager 3.5.1 de l'une des méthodes suivantes :

- Téléchargez l'image `.iso` ou le fichier `.zip` de l'application utilisateur qui convient à votre système : `Identity_Manager_3_5_1_User_Application.iso` ou `Identity_Manager_3_5_1_User_Application_Provisioning.iso`. Les téléchargements sont disponibles depuis Téléchargements Novell (http://download.novell.com/index.jsp).
- Téléchargez le DVD du produit, `Identity_Manager_3_5_1_DVD.iso`, de Novell, Inc.

Tableau 5-2 répertorie les fichiers et les scripts dont vous avez besoin pour installer l'application utilisateur Identity Manager 3.5.1.

Tableau 5-2 *Fichiers et scripts requis pour l'installation de l'application utilisateur Identity Manager 3.5.1*

Fichier	Description
WAR de l'application utilisateur	Choisissez-en un : **IDM.war.** Comprend l'application utilisateur Identity Manager 3.5.1 avec les fonctions Identity Self-Service. **IDMProv.war.** Comprend l'application utilisateur Identity Manager 3.5.1 avec les fonctions Identity Self-Service et le module Provisioning.

Les fichiers WAR de votre système, ainsi que les fichiers `IdmUserApp.jar` et `silent.properties`, sont disponibles initialement dans le répertoire du CD approprié à votre système :

`/linux/user_application` (Linux)
`/nt/user_application` (Windows)
`/solaris/user_application` (Solaris)

5.4.2 Valeurs requises à l'installation

Tableau 5-3 est une feuille de calcul pour noter les valeurs des paramètres d'installation que vous prévoyez d'utiliser lors de l'installation de JBoss. Les paramètres de configuration de l'application utilisateur peuvent également être définis à l'installation ; reportez-vous à Section 5.5.14, « Configuration de l'application utilisateur », page 130.

Tableau 5-3 *Feuille de calcul des paramètres d'installation pour JBoss*

Paramètre	Valeur exemple	Votre valeur
Dossier d'installation	C:\IDM\IDMinstalllocation	
Plate-forme de base de données	MySQL	
Hôte de base de données	localhost	
port de base de données	3306	
Nom ou sid de la base de données	IDM	
Utilisateur de base de données	`root`	
Mot de passe utilisateur de base de données		
Dossier racine Java	C:\Java\jdk1.5.0_10\	
Dossier de base (JBoss)	C:\jboss	
Hôte JBoss	localhost	
Port JBoss	8080	

Paramètre	Valeur exemple	Votre valeur
L'ID de moteur de workflow (pour les installations de grappes. Doit être unique pour chaque membre de la grappe.)		
Nom de l'application (contexte URL)	IDM	
Serveur Novell Audit	[nom ou adresse IP]	
Clé maîtresse codée. Reportez-vous à Section 5.5.13, « Indiquer une clé maîtresse », page 128.	_+FEJEefMAglH0A= =:3VRmp04lub21Y3GpdaXCY)LG qS1nBaL/	

5.5 Installation de l'application utilisateur sur un serveur d'applications JBoss à partir de l'interface utilisateur d'installation

Cette section décrit comment installer l'application utilisateur Identity Manager sur un serveur d'applications JBoss via la version de l'interface utilisateur graphique du programme d'installation.

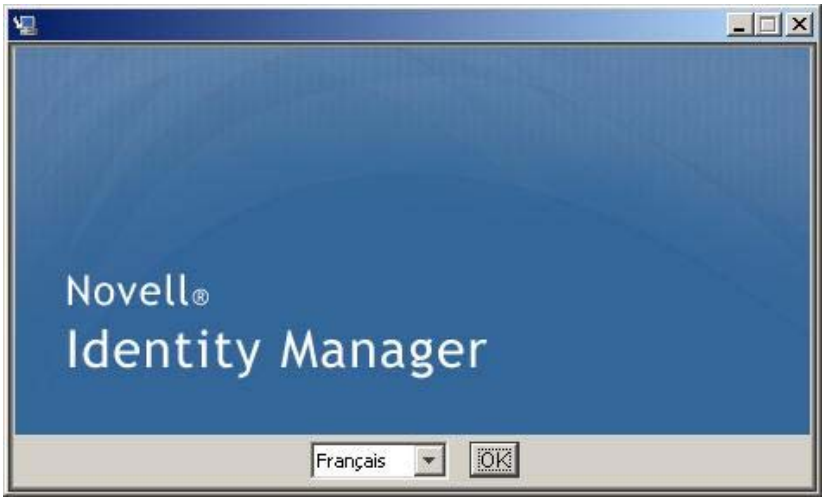
5.5.1 Lancer l'interface utilisateur graphique du programme d'installation

1 Naviguez jusqu'au répertoire contenant vos fichiers d'installation, indiqué dans Tableau 5-2 page 113.

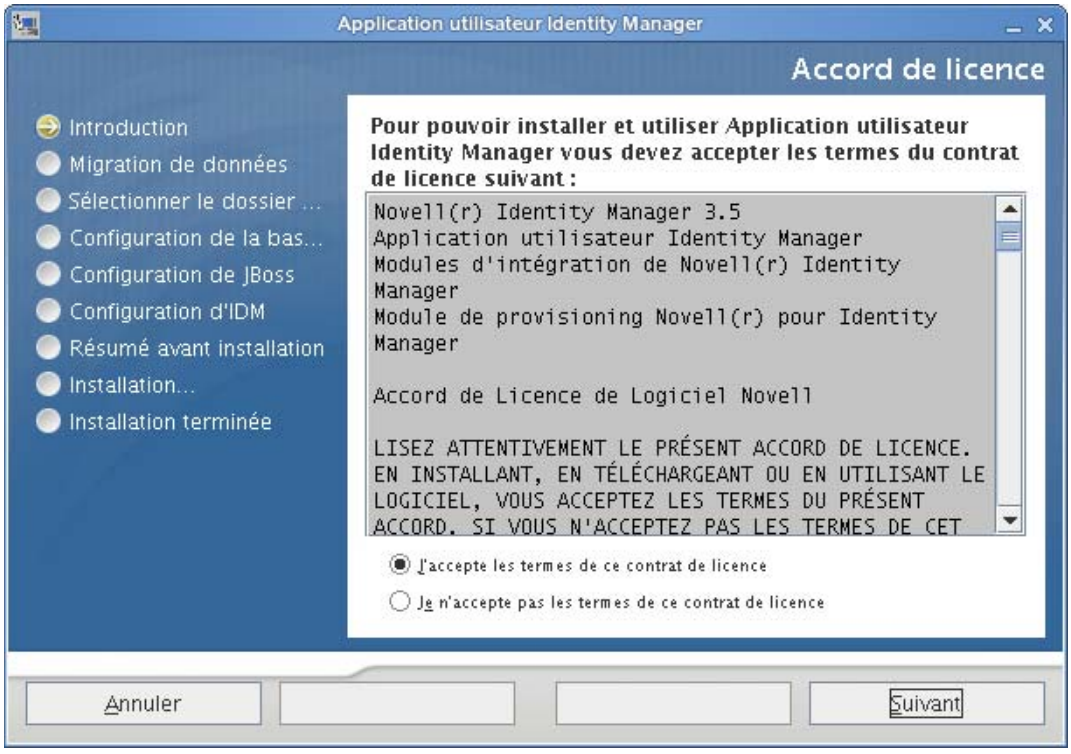
2 Lancez le programme d'installation correspondant à votre plate-forme à partir de la ligne de commande :

```
java -jar IdmUserApp.jar
```

3 Sélectionnez une langue dans le menu déroulant, puis cliquez sur *OK*.



4 Lisez l'accord de licence, cliquez sur *J'accepte les termes de l'accord de licence,* puis cliquez sur *Suivant*.

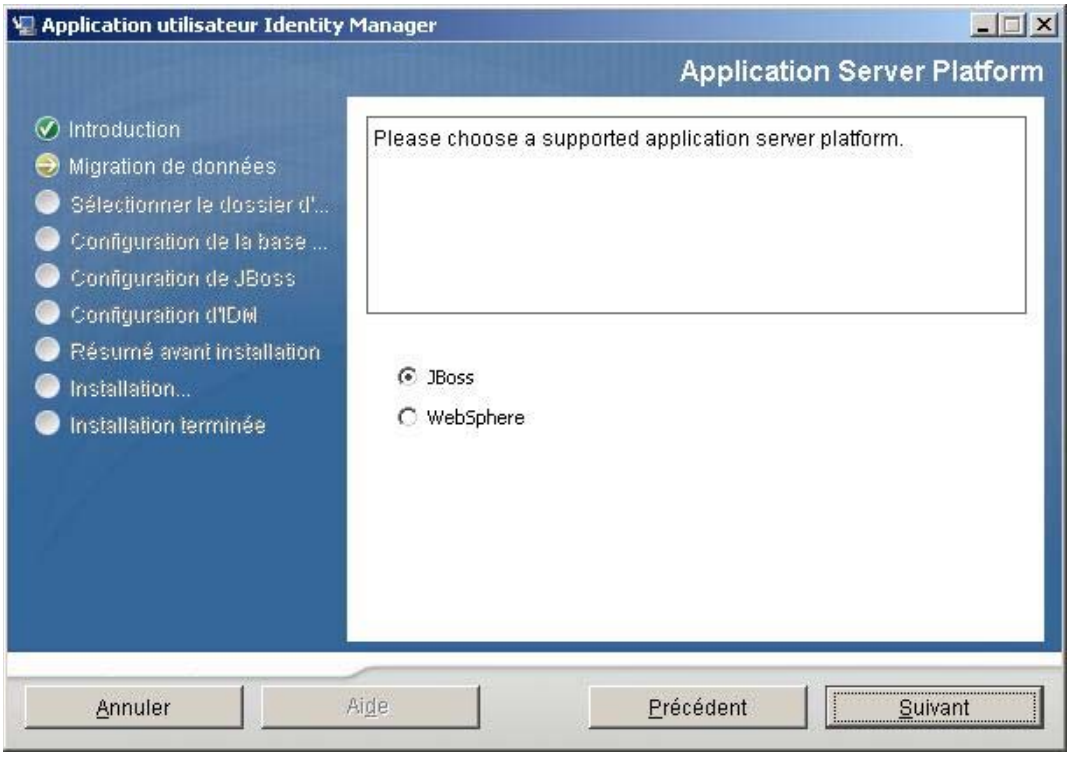


5 Lisez la page d'introduction de l'assistant d'installation, puis cliquez sur *Suivant*.

6 Passez à Section 5.5.2, « Choix d'une plate-forme de serveur d'applications », page 116.

5.5.2 Choix d'une plate-forme de serveur d'applications

1 Choisissez la plate-forme de serveur d'applications JBoss et cliquez sur *Suivant*.



5.5.3 Migration de votre base de données

Si vous ne souhaitez pas faire migrer une base de données, cliquez sur *Suivant* et passez à Section 5.5.4, « Indiquer l'emplacement du WAR », page 118.

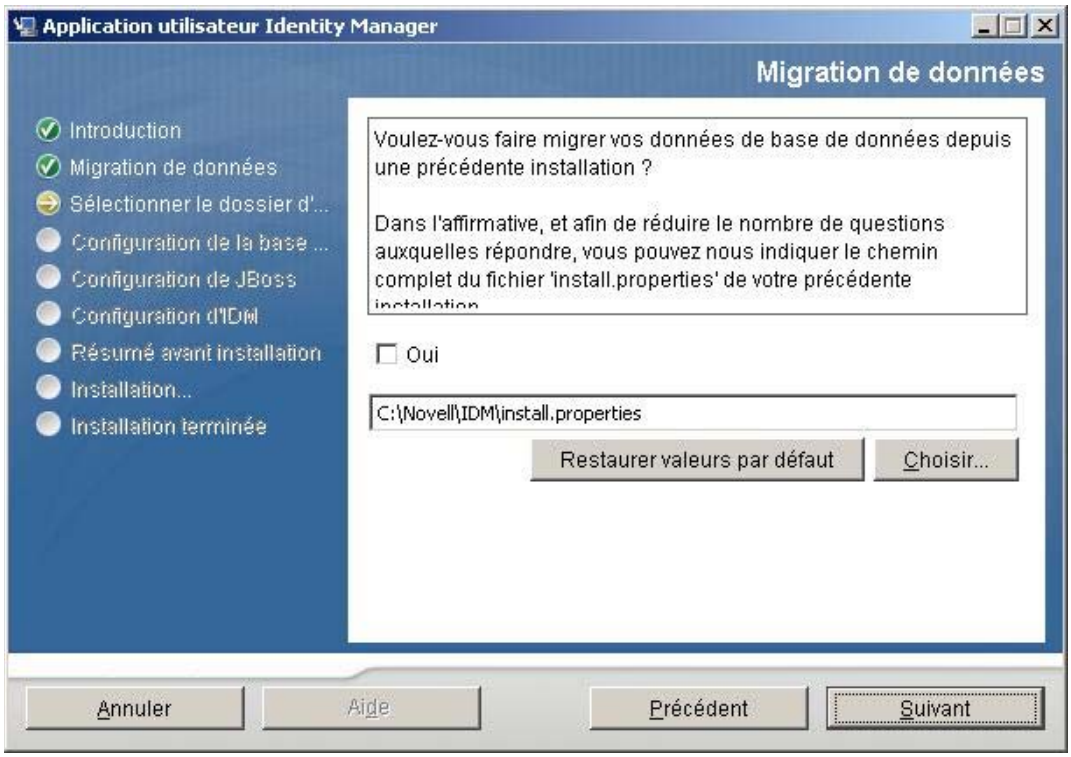
Si vous souhaitez utiliser une base de données existante depuis votre version 3.0 ou version 3.01 de l'application utilisateur, vous devez migrer la base de données.

1 Vérifiez que vous avez démarré la base de données que vous souhaitez migrer.

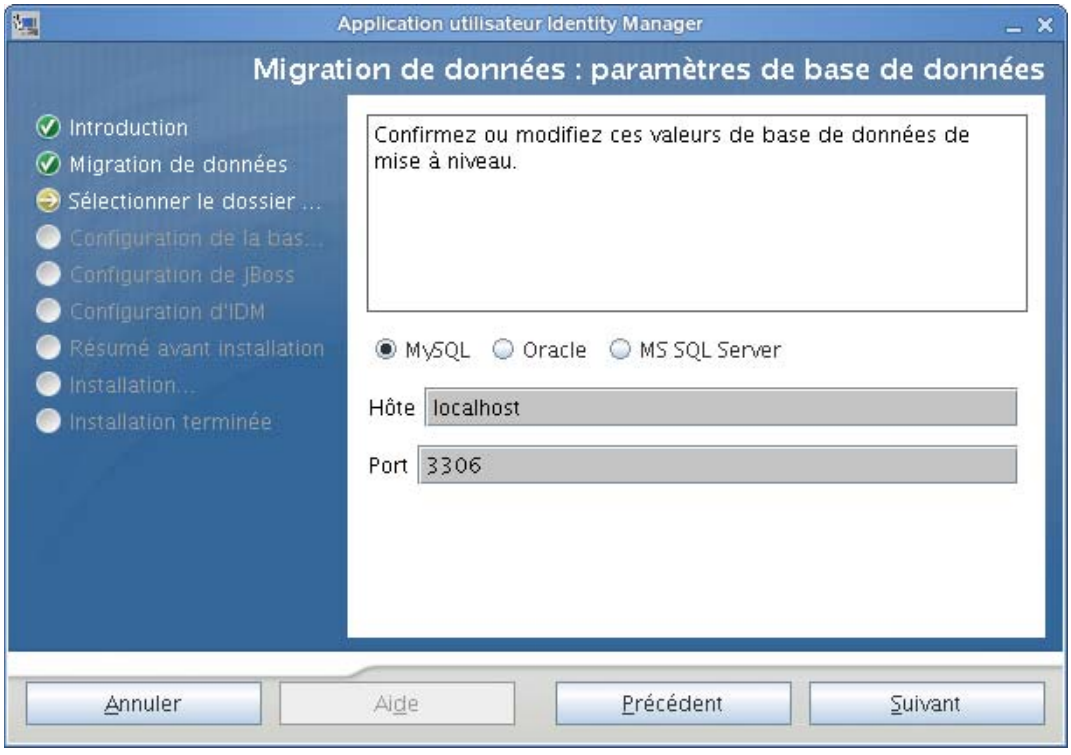
2 Cliquez sur *Oui* sur la page Migration de données du programme d'installation.

3 Cliquez sur *Choisir* pour trouver le fichier `install.properties` dans le répertoire d'installation de l'application utilisateur Identity Manager 3.0 ou 3.01.

Indiquer l'emplacement du fichier `install.properties` depuis votre installation précédente réduit le nombre d'éléments que vous devez indiquer aux pages suivantes.



4 Il vous est demandé de confirmer le type de base de données, le nom d'hôte et le port. Faites-le, puis cliquez sur *Suivant*.



5 Cliquez sur *Suivant* et passez à Section 5.5.4, « Indiquer l'emplacement du WAR », page 118 ou à Section 5.5.5, « Choix d'un dossier d'installation », page 118.

Le programme d'installation de l'application utilisateur met à jour votre application utilisateur et migre les données de la base de données version 3.0 ou 3.0.1 vers la base de données utilisée pour la version 3.5.1. Pour plus d'informations et des étapes supplémentaires sur la migration de votre base de données, reportez-vous au *Guide de migration de l'application utilisateur Identity Manager* (http://www.novell.com/documentation/idm35/index.html).

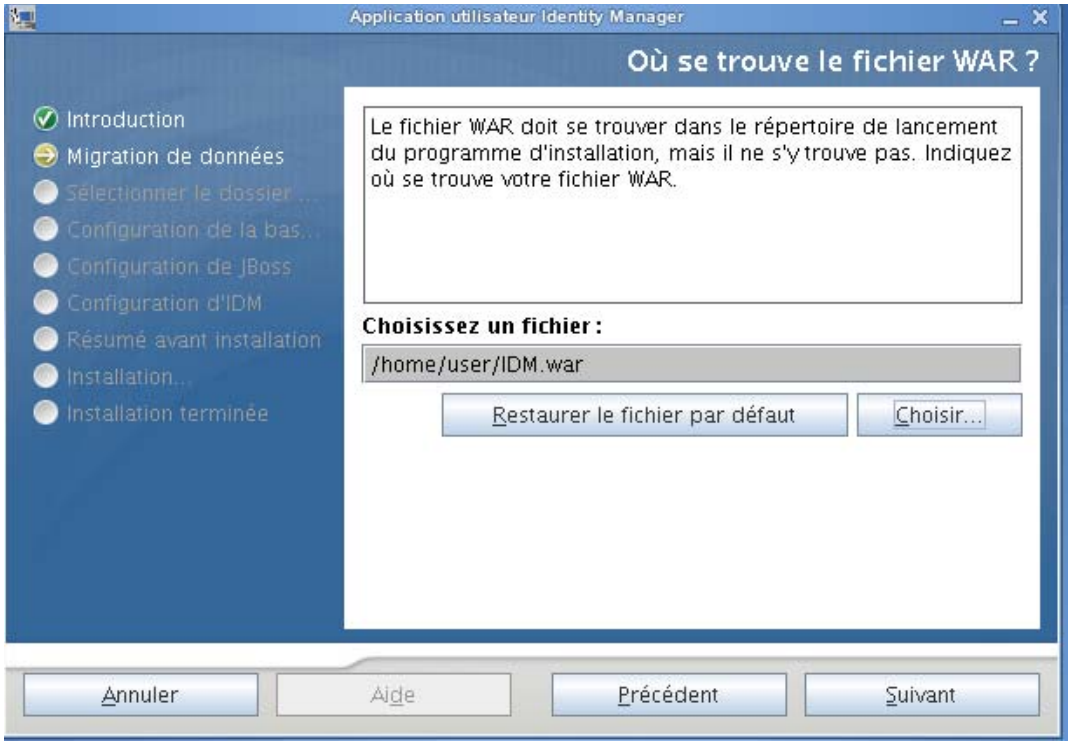
5.5.4 Indiquer l'emplacement du WAR

Si le fichier WAR de l'application utilisateur Identity Manager est dans un répertoire différent du programme d'installation, ce dernier vous invite à saisir le chemin d'accès au WAR.

1 Si le fichier WAR se trouve à l'emplacement par défaut, cliquez sur *Restaurer le dossier par défaut*.

Ou, pour spécifier l'emplacement du fichier WAR, cliquez sur *Choisir* et sélectionnez un emplacement.

2 Cliquez sur *Suivant*, puis passez à Section 5.5.5, « Choix d'un dossier d'installation », page 118.



5.5.5 Choix d'un dossier d'installation

1 Sur la page Choisir un dossier d'installation, sélectionnez l'emplacement où installer l'application utilisateur. Si vous devez vous rappeler et utiliser l'emplacement par défaut, cliquez sur *Restaurer le dossier par défaut*, ou si vous souhaitez choisir un autre emplacement pour les fichiers d'installations, cliquez sur *Choisir* et trouvez un emplacement.

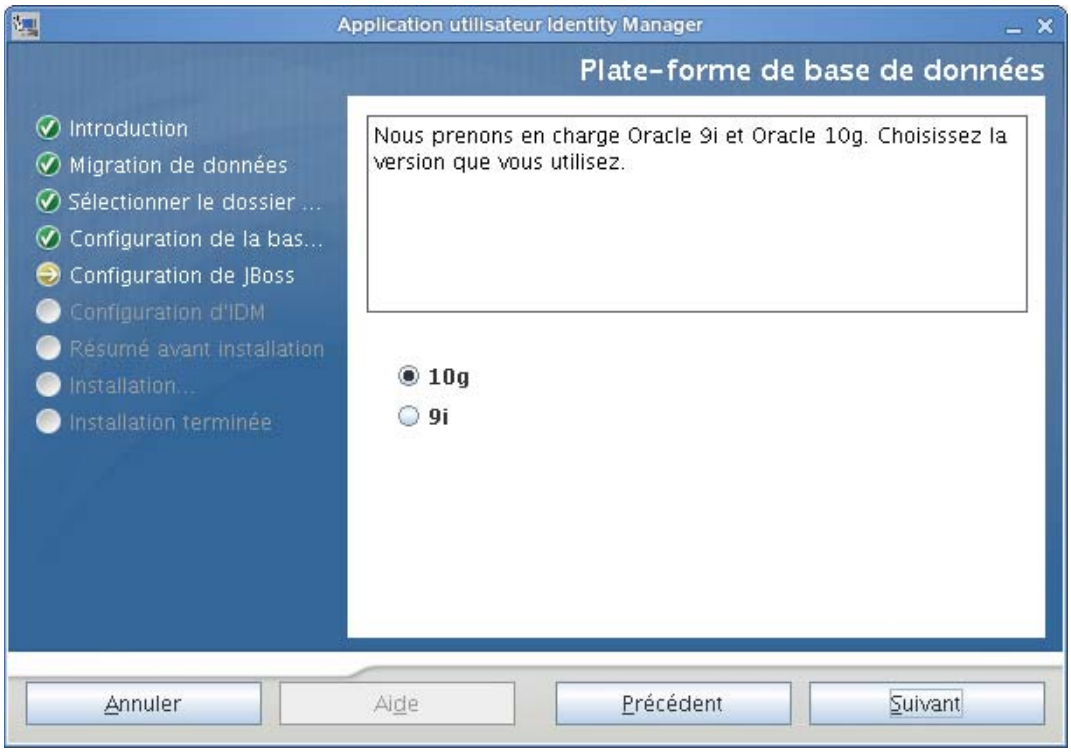
2 Cliquez sur *Suivant*, puis passez à Section 5.5.6, « Choix d'une plate-forme de base de données », page 120.

5.5.6 Choix d'une plate-forme de base de données

1 Sélectionnez la plate-forme de base de données à utiliser.

2 Si vous utilisez une base de données Oracle, passez à Étape 3. Sinon, passez à l'Étape 4.

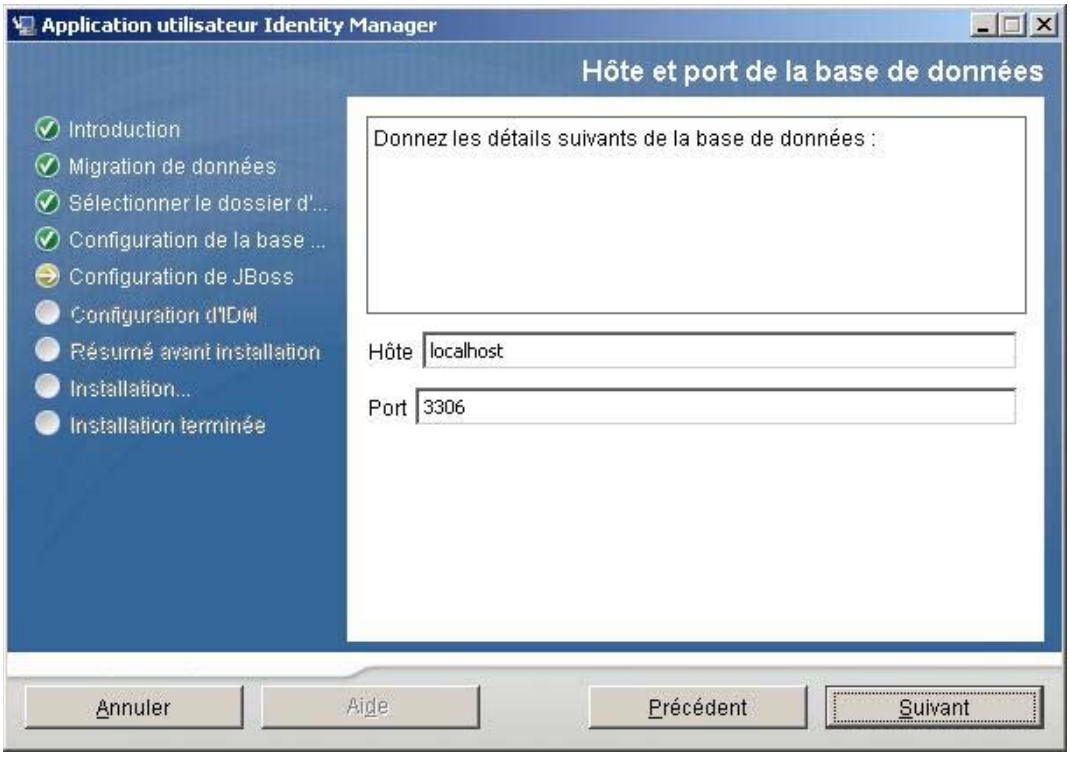
3 Si vous utilisez une base de données Oracle, le programme d'installation demande quelle version vous utilisez. Choisissez votre version.



4 Cliquez sur *Suivant*, puis passez à Section 5.5.7, « Indiquer l'hôte et le port de la base de données », page 122.

5.5.7 Indiquer l'hôte et le port de la base de données

1 Remplissez les champs suivants :

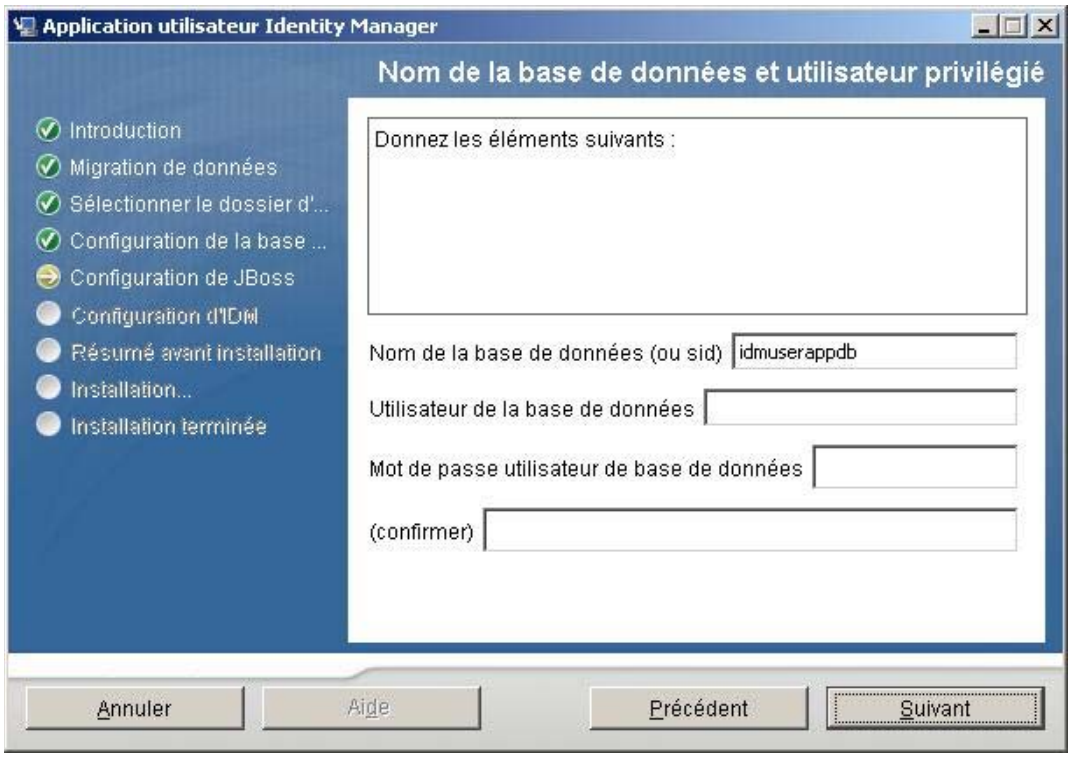


Champ	Description
Hôte	Indiquez le nom d'hôte ou l'adresse IP du serveur de bases de données. Pour une grappe, indiquez le même nom d'hôte ou la même adresse IP pour chaque membre de la grappe.
Port	Indiquez le numéro du port d'écoute de la base de données. Pour une grappe, indiquez le même port pour chaque membre de la grappe.

2 Cliquez sur *Suivant*, puis passez à Section 5.5.8, « Indiquer le nom de la base de données et l'utilisateur privilégié », page 123.

5.5.8 Indiquer le nom de la base de données et l'utilisateur privilégié

1 Remplissez les champs suivants :

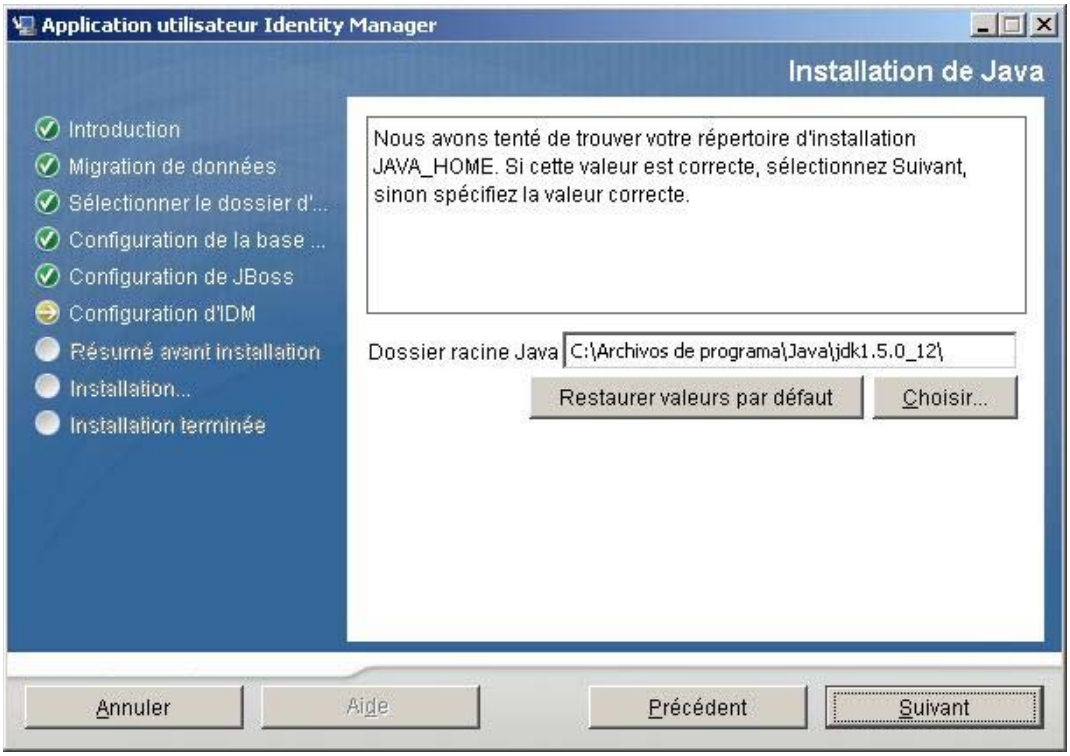


Champ	Description
Nom ou sid de la base de données	Pour le serveur MySQL ou MS SQL, donnez le nom de votre base de données préconfigurée. Pour Oracle, donnez l'identificateur système Oracle (SID) que vous avez créé précédemment. Pour une grappe, indiquez le même nom ou SID de base de données pour chaque membre de la grappe.
Utilisateur de base de données	Indiquez l'utilisateur associé à la base de données. Pour une grappe, indiquez le même utilisateur de base de données pour chaque membre de la grappe.
Mot de passe base de données/Confirmer mot de passe	Indiquez le mot de passe associé à la base de données. Pour une grappe, indiquez le même mot de passe de base de données pour chaque membre de la grappe.

2 Cliquez sur *Suivant,* puis passez à Section 5.5.9, « Indiquer le répertoire racine Java », page 124.

5.5.9 Indiquer le répertoire racine Java

1 Cliquez sur *Choisir* pour trouver votre dossier racine Java. Pour utiliser l'emplacement par défaut, cliquez sur *Restaurer les valeurs par défaut*.



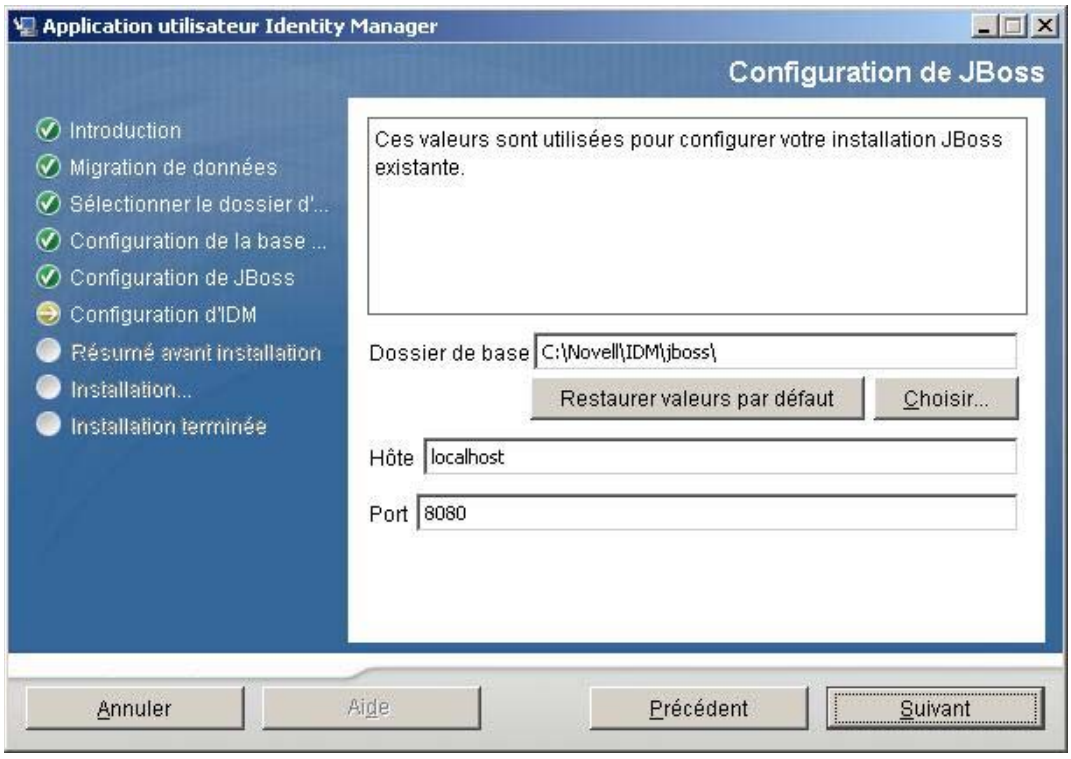
2 Cliquez sur *Suivant*, puis passez à Section 5.5.10, « Indiquer les paramètres du serveur d'applications JBoss », page 124.

5.5.10 Indiquer les paramètres du serveur d'applications JBoss

Sur cette page, indiquez à l'application utilisateur où trouver le serveur d'applications JBoss.

La procédure d'installation n'installe pas le serveur d'applications JBoss : pour obtenir des directives sur l'installation du serveur d'applications JBoss, reportez-vous à Section 5.1.1, « Installation du serveur d'applications JBoss et de la base de données MySQL », page 102.

1 Fournissez le dossier de base, l'hôte et le port :

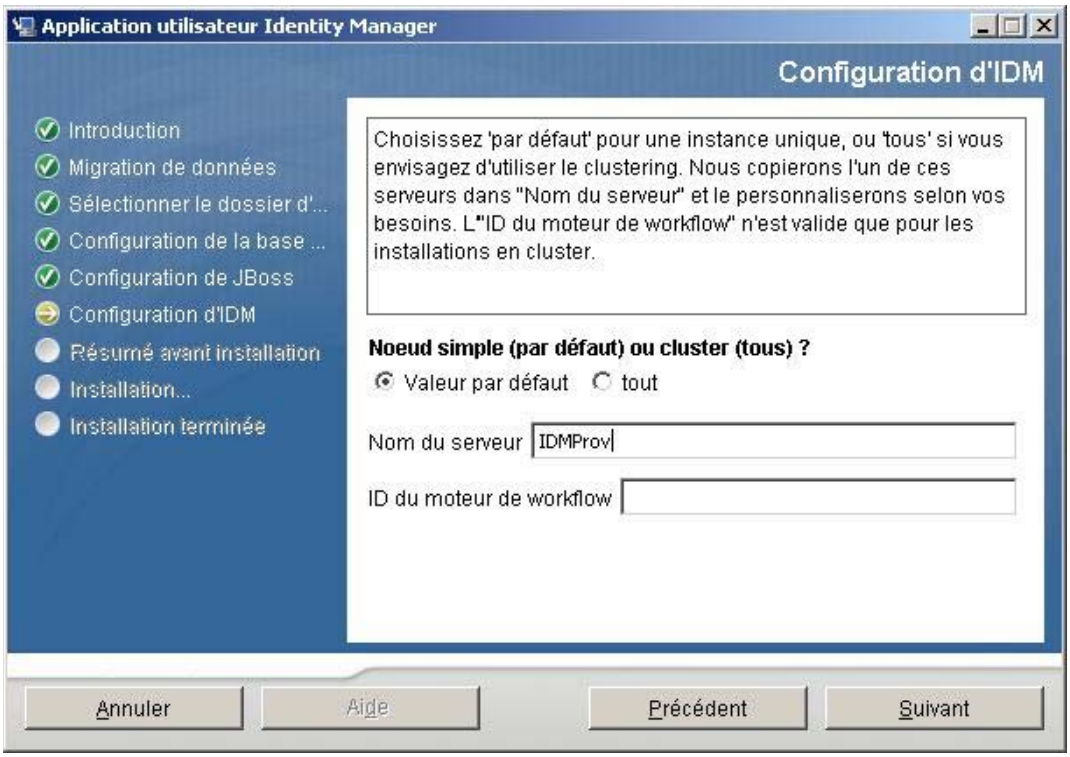


Champ	Description
Dossier de base	Indiquez l'emplacement du serveur d'applications.
Hôte	Indiquez le nom d'hôte ou l'adresse IP du serveur d'applications
Port	Indiquez le numéro de port d'écoute du serveur d'applications. Le port JBoss par défaut est 8080.

2 Cliquez sur *Suivant*, puis passez à Section 5.5.11, « Choix du type de configuration du serveur d'applications », page 126.

5.5.11 Choix du type de configuration du serveur d'applications

1 Remplissez les champs suivants :



Option	Description
Simple (par défaut) ou *mise en grappe* (tous)	Sélectionnez le type de configuration du serveur d'applications : ◆ Sélectionnez *tous* si cette installation fait partie d'une grappe ◆ Sélectionnez *par défaut* si cette installation est sur un noeud simple qui ne fait pas partie d'une grappe
Nom de serveur	Définissez le nom du serveur. Le nom du serveur est le nom de la configuration du serveur d'applications, le nom du fichier WAR de l'application et le nom du contexte de l'URL. Le script d'installation crée une configuration serveur et par défaut nomme la configuration en fonction du *Nom de l'application*. Notez le nom de l'application et ajoutez-le dans l'URL lorsque vous démarrez l'application utilisateur Identity Manager à partir d'un navigateur.

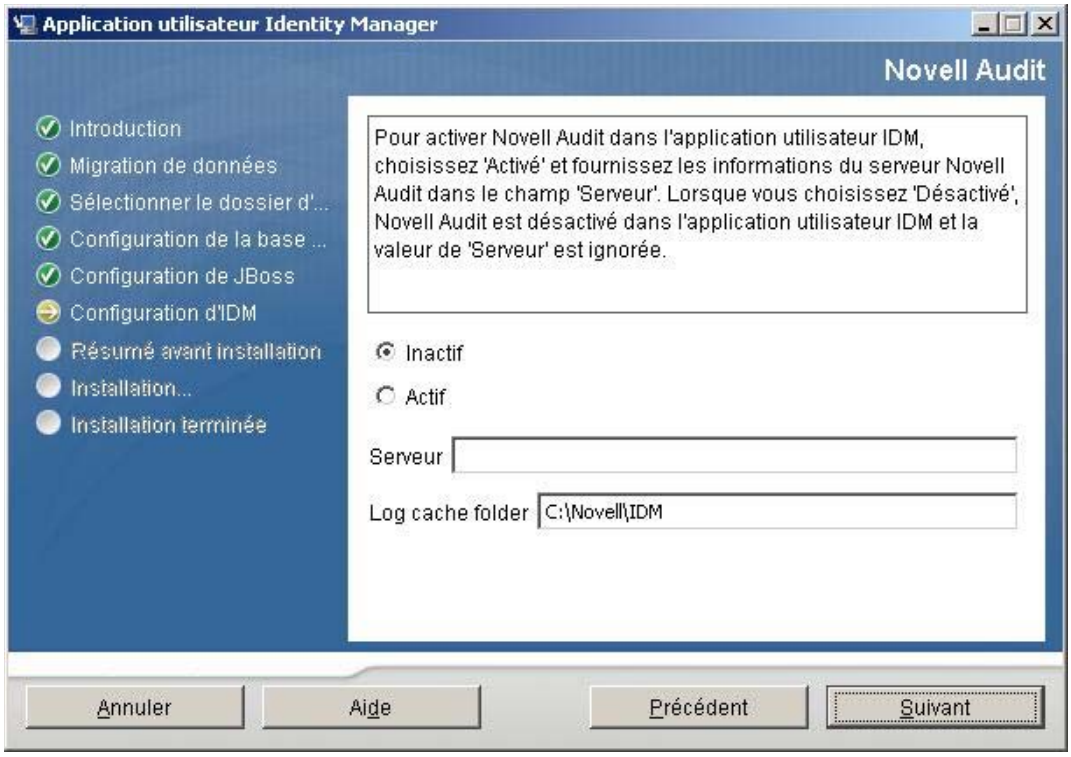
Option	Description
ID de moteur de workflow	Chaque serveur d'une grappe doit avoir un ID de moteur de workflow unique. Les ID de moteur de workflow sont décrits dans le *Guide d'administration de l'application utilisateur Identity Manager* à la section 3.5.4, « Configuration de workflows pour la mise en grappe ».

2 Cliquez sur *Suivant*, puis passez à Section 5.5.12, « Activation de la consignation Novell Audit », page 127.

5.5.12 Activation de la consignation Novell Audit

(Facultatif) Pour activer la consignation Novell Audit de l'application utilisateur :

1 Remplissez les champs suivants :



Option	Description
Actif	Active la consignation Novell Audit de l'application utilisateur. Pour plus d'informations sur la configuration de la consignation Novell Audit, reportez-vous au *Guide d'administration de l'application utilisateur Identity Manager*.

Option	Description
Inactif	Désactive la consignation Novell Audit de l'application utilisateur. Vous pouvez l'activer plus tard via l'onglet *Administration* de l'application utilisateur. Pour plus d'informations sur l'activation de la consignation Novell Audit, reportez-vous au *Guide d'administration de l'application utilisateur Identity Manager.*
Serveur	Si vous activez la consignation Novell Audit, indiquez le nom d'hôte ou l'adresse IP du serveur Novell Audit. Si vous désactivez la consignation, cette valeur est ignorée.

2 Cliquez sur *Suivant*, puis passez à Section 5.5.14, « Configuration de l'application utilisateur », page 130.

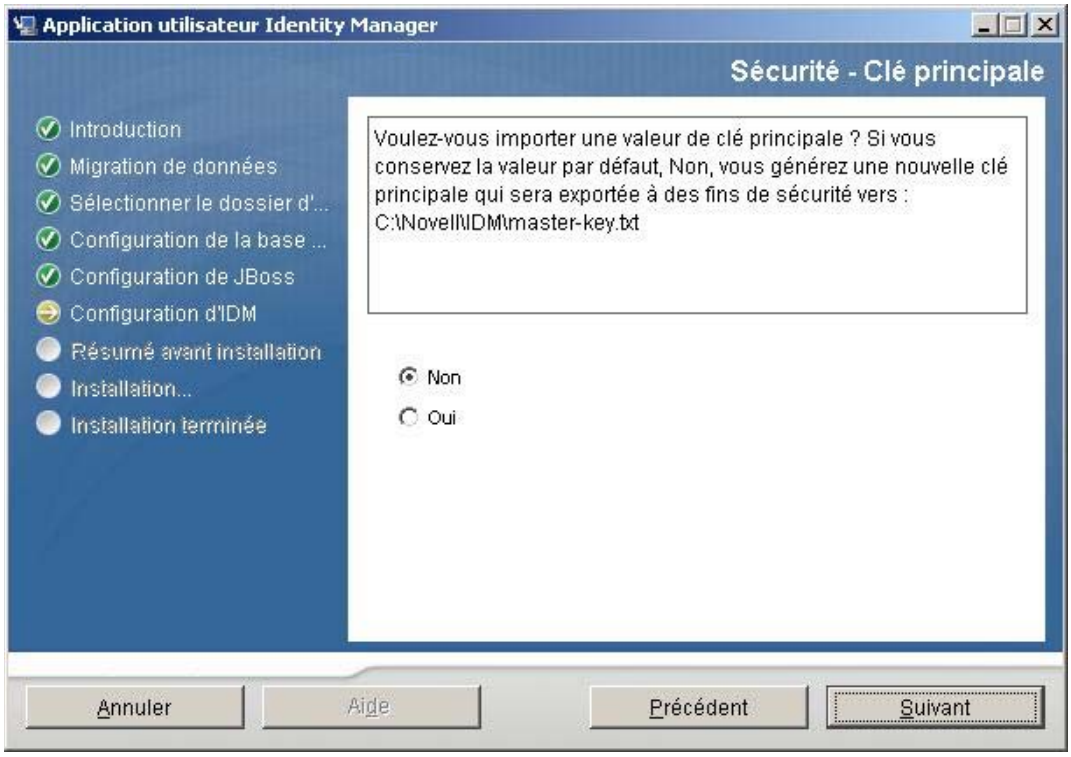
5.5.13 Indiquer une clé maîtresse

Indiquez si vous souhaitez importer une clé maîtresse existante ou en créer une nouvelle. Voici des exemples de raisons d'importer une clé maîtresse existante :

- Vous déplacez votre installation d'un système provisoire à un système de production et vous souhaitez conserver l'accès à la base de données que vous avez utilisée avec le système provisoire.
- Vous avez installé l'application utilisateur sur le premier membre d'une grappe JBoss et vous l'installez maintenant sur de nouveaux membres de la grappe (qui requièrent la même clé maîtresse).

- En raison d'un disque défectueux, vous devez restaurer votre application utilisateur. Vous devez réinstaller l'application utilisateur et indiquer la même clé maîtresse codée que celle qu'utilisait l'installation précédente. Cela vous donne accès aux données codées stockées précédemment.

1 Cliquez sur *Oui* pour importer une clé maîtresse existante ou sur *Non* pour en créer une nouvelle.



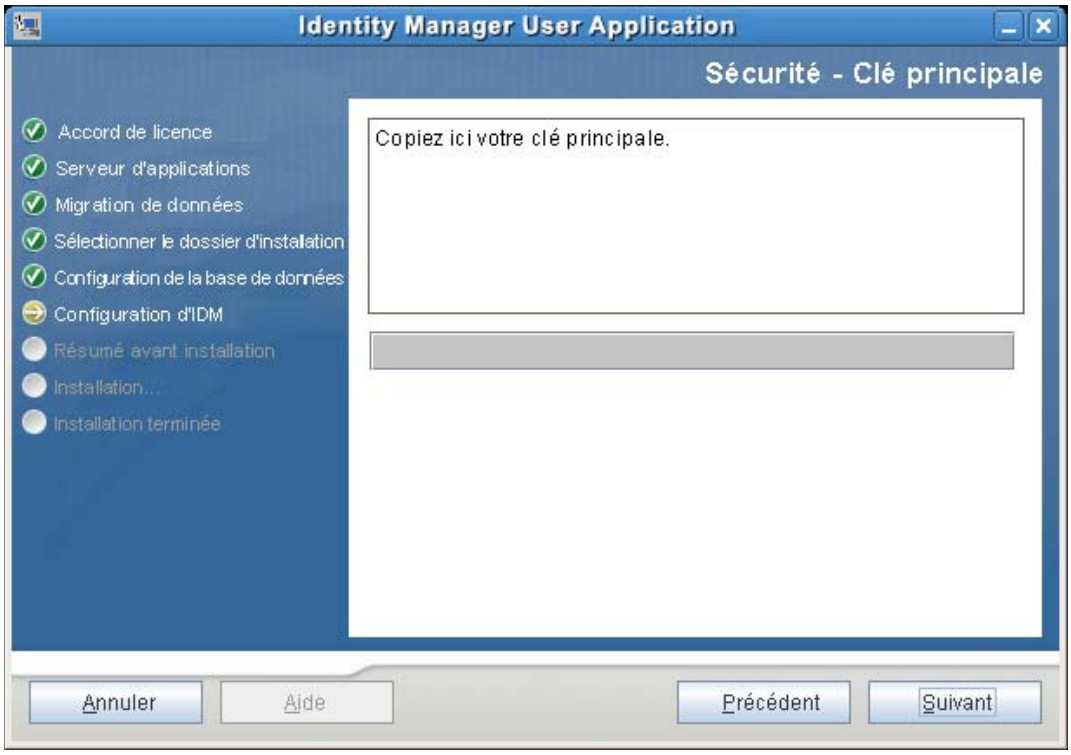
2 Cliquez sur *Suivant*.

La procédure d'installation inscrit la clé maîtresse codée dans le fichier `master-key.txt` dans le répertoire d'installation.

Si vous sélectionnez *Non*, passez à Section 5.5.14, « Configuration de l'application utilisateur », page 130. Une fois l'installation terminée, vous devez enregistrer manuellement la clé maîtresse tel que décrit dans Section 5.9.1, « Enregistrement de la clé maîtresse », page 184.

Si vous sélectionnez *Oui*, passez à Étape 3.

3 Si vous choisissez d'importer une clé maîtresse codée existante, coupez et collez la clé dans la fenêtre de procédure d'installation.



4 Cliquez sur *Suivant*, puis passez à Section 5.5.14, « Configuration de l'application utilisateur », page 130.

5.5.14 Configuration de l'application utilisateur

Le programme d'installation de l'application utilisateur permet de configurer les paramètres de configuration de l'application utilisateur. La plupart de ces paramètres sont également éditables avec `configupdate.sh` ou `configupdate.bat` après l'installation ; les exceptions sont notées dans les descriptions des paramètres.

Pour une grappe, indiquez les paramètres de configuration identiques de l'application utilisateur pour chaque membre de la grappe.

1 Définissez les paramètres de configuration de base de l'application utilisateur décrits dans Tableau 5-4, puis passez à Étape 2.

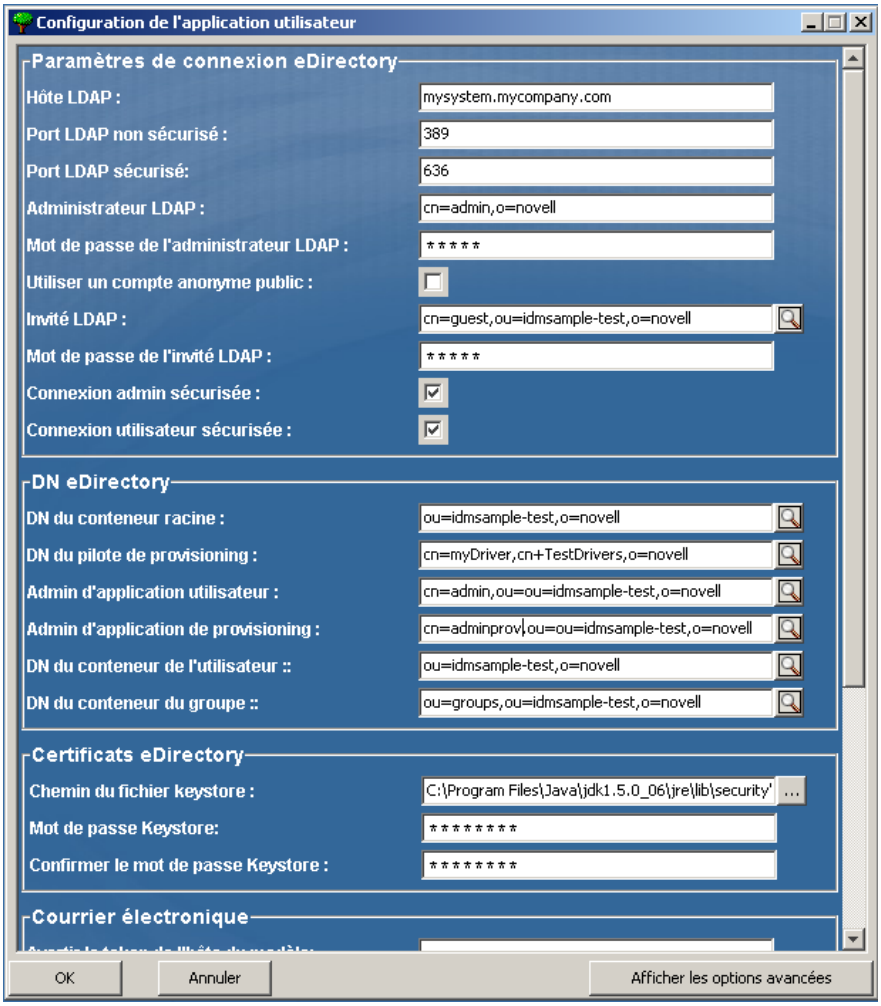


Tableau 5-4 *Configuration de l'application utilisateur : paramètres de base*

Type de paramètre	Champ	Description
Paramètres de login eDirectory	*Hôte LDAP*	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP et son port sécurisé. Par exemple : `myLDAPhost`
	Port non sécurisé LDAP	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	Port sécurisé LDAP	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	Administrateur LDAP	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer un login administratif au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
	Mot de passe administrateur LDAP	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
	Utiliser le compte anonyme public	Permet aux utilisateurs non logués d'accéder au compte anonyme public LDAP.
	Guest LDAP	Permet aux utilisateurs non logués d'accéder à des portlets autorisés. Ce compte utilisateur doit déjà exister dans le coffre-fort d'identité. Pour activer Guest LDAP, vous devez désélectionner *Utiliser le compte anonyme public*. Pour désactiver l'utilisateur Guest, sélectionnez *Utiliser le compte anonyme public*.
	Mot de passe Guest LDAP	Indiquez le mot de passe Guest LDAP.
	Login admin sécurisé	Sélectionnez cette option pour exiger que toutes les communications utilisant le compte admin. soient effectuées à l'aide d'un socket sécurisé (cette option peut avoir des implications néfastes sur la performance).
	Login utilisateur sécurisé	Sélectionnez cette option pour exiger que toutes les communications utilisant le compte de l'utilisateur logué soient effectuées à l'aide d'un socket sécurisé (cette option peut avoir des implications néfastes sur la performance).

Type de paramètre	Champ	Description
DN eDirectory	*DN du conteneur racine*	Requis. Indiquez le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire.
	DN du pilote de provisioning	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur que vous avez créé auparavant dans Section 5.3, « Création du pilote d'application utilisateur », page 107. Par exemple, si votre pilote est UserApplicationDriver et si votre ensemble de pilotes est appelé myDriverSet, et si l'ensemble de pilotes est dans un contexte de o=myCompany, vous saisiriez une valeur de : `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Admin. application utilisateur	Requis. Un utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs de l'application utilisateur spécifié. Cet utilisateur peut utiliser l'onglet *Administration* de l'application utilisateur pour administrer le portail. Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, le concepteur Novell pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), vous devez accorder à cet administrateur des droits d'ayant droit sur les instances d'objets contenues dans le pilote de l'application utilisateur. Reportez-vous au *Guide d'administration de l'application utilisateur IDM* pour en savoir plus. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.
	Admin. application provisioning	Ce rôle est disponible dans la version de provisioning d'Identity Manager 3.5.1. L'administrateur de l'application de provisioning utilise l'onglet *Provisioning* (sous l'onglet *Administration*) pour gérer les fonctions de workflow du provisioning. Ces fonctions sont accessibles aux utilisateurs en passant par l'onglet *Requêtes et approbations* de l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur de l'application Provisioning. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.

Type de paramètre	Champ	Description
DN eDirectory (suite)	*DN du conteneur d'utilisateurs*	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur utilisateur. Cela définit l'étendue de recherche d'utilisateurs et de groupes. Les utilisateurs de ce conteneur (et en-dessous) sont autorisés à se loguer à l'application utilisateur. **Important :** assurez-vous que l'administrateur de l'application utilisateur spécifié lors de la configuration des pilotes de l'application utilisateur existe dans ce conteneur si vous souhaitez que cet utilisateur soit en mesure d'exécuter les workflows.
	DN de conteneur de groupes	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur de groupes. Utilisé par les définitions d'entités au sein de la couche d'abstraction d'annuaire.
Certificats eDirectory	*Chemin d'accès au Keystore*	Requis. Indiquez le chemin d'accès complet au fichier (`cacerts`) de votre keystore du JDK que le serveur d'applications utilise pour fonctionner, ou bien cliquez sur le petit bouton du navigateur pour trouver le fichier `cacerts`. Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier.
	Mot de passe Keystore/ Confirmer mot de passe Keystore	Requis. Indiquez le mot de passe `cacerts`. L'unité par défaut est `changeit`.

Type de paramètre	Champ	Description
Courrier électronique	*Jeton de l'hôte du modèle de notification*	Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple : `myapplication serverServer` Cette valeur remplace le jeton $HOST$ des modèles de courrier électronique. L'URL construite est la liaison aux tâches de requête de provisioning et aux notifications d'approbation.
	Jeton du port du modèle de notification	Utilisé pour remplacer le jeton $PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Jeton du port sécurisé du modèle de notification	Utilisé pour remplacer le jeton $SECURE_PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Notification SMTP - Expéditeur du courrier électronique :	Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
	Notification SMTP - destinataire du courrier électronique :	Indiquez l'utilisateur destinataire du courrier électronique dans le message de provisioning. Il peut s'agir d'une adresse IP ou d'un nom DNS.
Gestion des mots de passe	*Utiliser le WAR de mots de passe externe*	Cette fonction permet d'indiquer une page Mot de passe oublié qui réside dans un WAR Mot de passe oublié externe et une URL que le WAR Mot de passe oublié externe utilise pour rappeler l'application utilisateur grâce à un service Web. Si vous cochez *Utiliser le WAR de mot de passe externe*, vous devez fournir des valeurs pour *Lien Mot de passe oublié* et *Lien Retour mot de passe oublié*. Si vous ne sélectionnez pas *Utiliser le·WAR de mots de passe externe*, IDM utilise la fonction de gestion des mots de passe interne par défaut. `/jsps/pwdmgt/ForgotPassword.jsf` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.

Type de paramètre	Champ	Description
	Liaison Mot de passe oublié	Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier `ForgotPassword.jsf` dans un WAR de gestion des mots de passe externe ou interne. Pour plus de détails, reportez-vous à « Utilisation des WAR de mots de passe » page 144.
	Liaison de retour Mot de passe oublié	Si vous utilisez un WAR de gestion des mots de passe externe, indiquez le chemin d'accès que le WAR de gestion des mots de passe externe utilise pour rappeler l'application utilisateur par des services Web, par exemple `https://idmhost:sslport/idm`.

2 Si vous souhaitez définir d'autres paramètres de configuration de l'application utilisateur, cliquez sur *Afficher les options avancées*. (Faites défiler pour afficher tout le panneau.) Tableau 5-5 décrit les paramètres des options avancées.

Si vous ne souhaitez pas définir d'autres paramètres décrits dans cette étape, passez à Étape 3.

Tableau 5-5 *Configuration de l'application utilisateur : tous les paramètres*

Type de paramètre	Champ	Description
Paramètres de login eDirectory	*Hôte LDAP*	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP. Par exemple : myLDAPhost
	Port non sécurisé LDAP	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	Port sécurisé LDAP	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	Administrateur LDAP	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer un login administratif au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
	Mot de passe administrateur LDAP	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
	Utiliser le compte anonyme public	Permet aux utilisateurs non logués d'accéder au compte anonyme public LDAP.
	Guest LDAP	Permet aux utilisateurs non logués d'accéder à des portlets autorisés. Ce compte utilisateur doit déjà exister dans le coffre-fort d'identité. Pour activer Guest LDAP, vous devez désélectionner *Utiliser le compte anonyme public*. Pour désactiver l'utilisateur Guest, sélectionnez *Utiliser le compte anonyme public*.
	Mot de passe Guest LDAP	Indiquez le mot de passe Guest LDAP.
	Login admin sécurisé	Sélectionnez cette option pour exiger que toutes les communications utilisant le compte admin. soient effectuées à l'aide d'un socket sécurisé (cette option peut avoir des implications néfastes sur la performance).
	Login utilisateur sécurisé	Sélectionnez cette option pour exiger que toutes les communications sur le compte de l'utilisateur logué soient effectuées à l'aide d'un socket sécurisé (cette option peut avoir des implications néfastes graves sur la performance).

Type de paramètre	Champ	Description
DN eDirectory	*DN du conteneur racine*	Requis. Indiquez le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire.
	DN du pilote de provisioning	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur que vous avez créé auparavant dans Section 5.3, « Création du pilote d'application utilisateur », page 107. Par exemple, si votre pilote est UserApplicationDriver et si votre ensemble de pilotes est appelé myDriverSet, et si l'ensemble de pilotes est dans un contexte de o=myCompany, vous saisissez une valeur de : `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Admin. application utilisateur	Requis. Un utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs de l'application utilisateur spécifié. Cet utilisateur peut utiliser l'onglet *Administration* de l'application utilisateur pour administrer le portail. Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, le concepteur Novell pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), vous devez accorder à cet administrateur des droits d'ayant droit sur les instances d'objets contenues dans le pilote de l'application utilisateur. Reportez-vous au *Guide d'administration de l'application utilisateur IDM* pour en savoir plus. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.
	Admin. application provisioning	Ce rôle est disponible dans la version de provisioning d'Identity Manager 3.5.1. L'administration de l'application de provisioning gère les fonctions de workflow du provisioning accessibles par l'onglet *Requêtes et approbations* de l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur de l'application Provisioning. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.

Type de paramètre	Champ	Description
Identité utilisateur du méta-annuaire	*DN du conteneur d'utilisateurs*	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur d'utilisateurs. Cela définit l'étendue de recherche d'utilisateurs et de groupes. Les utilisateurs de ce conteneur (et en-dessous) sont autorisés à se loguer à l'application utilisateur. **Important :** assurez-vous que l'administrateur de l'application utilisateur spécifié lors de la configuration des pilotes de l'application utilisateur existe dans ce conteneur si vous souhaitez que cet utilisateur soit en mesure d'exécuter les workflows.
	Classe d'objets Utilisateur	La classe d'objets utilisateur LDAP (généralement inetOrgPerson).
	Attribut de login	L'attribut LDAP (par exemple, CN) qui représente le nom de login de l'utilisateur.
	Attribut de nom	L'attribut LDAP utilisé comme identifiant lors de la consultation d'utilisateurs ou de groupes. Il est différent de l'attribut de login, qui n'est utilisé que lors du login, et non pas lors des recherches d'utilisateurs/de groupes.
	Attribut de l'adhésion utilisateur	Facultatif. L'attribut LDAP qui représente l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.
Groupes d'utilisateurs du méta-annuaire	*DN de conteneur de groupes*	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur de groupes. Utilisé par les définitions d'entités au sein de la couche d'abstraction d'annuaire.
	Classe d'objets Groupe	La classe d'objets Groupe LDAP (généralement groupofNames).
	Attribut d'adhésion à un groupe	L'attribut qui représente l'adhésion d'un utilisateur à un groupe. N'utilisez pas d'espaces pour le nom.
	Utiliser des groupes dynamiques	Sélectionnez cette option si vous souhaitez utiliser des groupes dynamiques.
	Classe d'objets Groupe dynamique	La classe d'objets Groupe dynamique LDAP (généralement dynamicGroup).

Type de paramètre	Champ	Description
Certificats eDirectory	*Chemin d'accès au Keystore*	Requis. Indiquez le chemin d'accès complet au fichier (`cacerts`) de votre keystore du JRE que le serveur d'applications utilise pour fonctionner, ou bien cliquez sur le bouton du navigateur pour trouver le fichier `cacerts`. L'installation de l'application utilisateur modifie le fichier keystore. Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier.
	Mot de passe Keystore *Confirmer le mot de passe Keystore*	Requis. Indiquez le mot de passe `cacerts`. L'unité par défaut est `changeit`.
Keystore privé	*Chemin d'accès au keystore privé*	Le keystore privé contient la clé privée et les certificats de l'application utilisateur. Réservé. Si vous laissez ce champ vierge, ce chemin d'accès est `/jre/lib/security/cacerts` par défaut.
	Mot de passe Keystore privé	Ce mot de passe est `changeit`, à moins d'indication contraire. Ce mot de passe est codé, en fonction de la clé maîtresse.
	Alias de clé privée	Cet alias est `novellIDMUserApp`, à moins d'indication contraire.
	Mot de passe de la clé privée	Ce mot de passe est `novellIDM`, à moins d'indication contraire. Ce mot de passe est codé, en fonction de la clé maîtresse.
Banque de clés approuvée	*Chemin d'accès à la banque approuvée*	La banque de clés approuvées contient tous les certificats approuvés des signataires utilisés pour valider les signatures numériques. Si ce chemin est vide, l'application utilisateur obtient le chemin à partir de la propriété Système `javax.net.ssl.trustStore`. Si le chemin n'y est pas, il est supposé être `jre/lib/security/cacerts`.
	Mot de passe de la banque approuvée	Si ce champ est vierge, l'application utilisateur obtient le mot de passe à partir de la propriété système `javax.net.ssl.trustStorePassword`. S'il n'y a aucune valeur, `changeit` est utilisé. Ce mot de passe est codé, en fonction de la clé maîtresse.
Clé de certificat et signature numérique Novell Audit		Contient le certificat et la clé de signature numérique Novell Audit.
	Certificat de signature numérique Novell Audit	Affiche le certificat de signature numérique.

Type de paramètre	Champ	Description
	Clé privée de signature numérique Novell Audit	Affiche la clé privée de signature numérique. Cette clé est codée, en fonction de la clé maîtresse.
Paramètres iChain	*Logout ICS activé*	Si cette option est sélectionnée, l'application utilisateur prend en charge le logout simultané de l'application utilisateur ainsi que iChain ou Novell Access Manager. L'application utilisateur recherche un cookie iChain ou Novell Access Manager au logout et, en cas de présence du cookie, redirige l'utilisateur vers la page de logout ICS.
	Page de logout ICS	L'URL vers la page de logout de Ichain ou Novell Access Manager, où l'URL est un nom d'hôte auquel Ichain ou Novell Access Manager s'attend. Si le login à ICS est activée et si un utilisateur se délogue de l'application utilisateur, il est redirigé vers cette page.

Type de paramètre	Champ	Description
Courrier électronique	*Jeton de l'hôte du modèle de notification*	Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple : `myapplication serverServer` Cette valeur remplace le jeton $HOST$ des modèles de courrier électronique. L'URL construite est la liaison aux tâches de requête de provisioning et aux notifications d'approbation.
	Jeton du port du modèle de notification	Utilisé pour remplacer le jeton $PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Jeton du port sécurisé du modèle de notification	Utilisé pour remplacer le jeton $SECURE_PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Jeton PROTOCOLE du modèle de notification	Se rapporte à un protocole non sécurisé, HTTP. Utilisé pour remplacer le jeton $PROTOCOL$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Jeton PROTOCOLE SÉCURISÉ du modèle de notification	Se rapporte à un protocole sécurisé, HTTPS. Utilisé pour remplacer le jeton $SECURE_PROTOCOL$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Notification SMTP - Expéditeur du courrier électronique :	Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
	Notification SMTP - destinataire du courrier électronique :	Indiquez l'utilisateur destinataire du courrier électronique dans le message de provisioning. Il peut s'agir d'une adresse IP ou d'un nom DNS.

Type de paramètre	Champ	Description
Gestion des mots de passe		
	Utiliser le WAR de mots de passe externe	Cette fonction permet d'indiquer une page Mot de passe oublié qui réside dans un WAR Mot de passe oublié externe et une URL que le WAR Mot de passe oublié externe utilise pour rappeler l'application utilisateur grâce à un service Web. Si vous sélectionnez *Utiliser le WAR de mot de passe externe*, vous devez fournir des valeurs pour *Lien Mot de passe oublié* et *Lien Retour mot de passe oublié*. Si vous ne sélectionnez pas *Utiliser le WAR de mots de passe externe*, IDM utilise la fonction de gestion des mots de passe interne par défaut. `/jsps/pwdmgt/ForgotPassword.jsf` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.
	Liaison Mot de passe oublié	Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier `ForgotPassword.jsf` dans un WAR de gestion des mots de passe externe ou interne. Pour plus de détails, reportez-vous à « Utilisation des WAR de mots de passe » page 144.
	Liaison de retour Mot de passe oublié	Si vous utilisez un WAR de gestion des mots de passe externe, indiquez le chemin d'accès que le WAR de gestion des mots de passe externe utilise pour rappeler l'application utilisateur par des services Web, par exemple `https://idmhost:sslport/idm`.
Divers	*Timeout de session*	Le timeout de session de l'application.
	OCSP URI	Si l'installation client utilise le protocole OCSP (protocole de propriété d'état de certificat en ligne), fournissez un identificateur de ressource uniforme (URI). Par exemple, le format est http://host:port/ocspLocal. L'URI OCSP met à jour le statut des certificats approuvés en ligne.
	Chemin de configuration d'autorisation	Nom complet du fichier de configuration de l'autorisation.

Type de paramètre	Champ	Description
Objet Conteneur	*Sélectionné*	Sélectionnez chaque type d'objet Conteneur à utiliser.
	Type d'objet Conteneur	Sélectionnez parmi les conteneurs standard suivants : lieu, pays, unité organisationnelle, organisation et domaine. Vous pouvez également définir vos propres conteneurs dans iManager et les ajouter sous *Ajouter un nouvel objet Conteneur*.
	Nom de l'attribut Conteneur	Indique le nom de type d'attribut associé au type d'objet Conteneur.
	Ajouter un nouvel objet Conteneur : type d'objet Conteneur	Indiquez le nom LDAP d'une classe d'objets du coffre-fort d'identité qui peut servir de conteneur. Pour plus d'informations sur les conteneurs, reportez-vous au *Guide d'administration de Novell iManager 2.6 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*.
	Ajouter un nouvel objet Conteneur : nom d'attribut Conteneur	Donnez le nom d'attribut de l'objet Conteneur.

Remarque : vous pouvez modifier la plupart des paramètres de ce fichier après l'installation. Pour ce faire, exécutez le script `configupdate.sh` ou le fichier Windows `configupdate.bat` qui se trouve dans votre sous-répertoire d'installation. N'oubliez pas que dans une grappe, les paramètres de ce fichier doivent être identiques pour tous les membres de la grappe.

3 Une fois les paramètres configurés, cliquez sur *OK*, puis passez à Section 5.5.15, « Vérification des choix et installation », page 145.

Utilisation des WAR de mots de passe

Utilisez le paramètre de configuration *Liaison Mot de passe oublié* pour indiquer l'emplacement d'un WAR contenant la fonction Mot de passe oublié. Vous pouvez indiquer un WAR qui est externe ou interne à l'application utilisateur.

Spécification d'un WAR de gestion des mots de passe externe

1 Utilisez la procédure d'installation ou l'utilitaire configupdate.

2 Dans les paramètres de configuration de l'application utilisateur, cochez la case du paramètre de configuration *Utiliser le WAR de mot de passe externe*.

3 Pour le paramètre de configuration *Liaison Mot de passe oublié*, indiquez l'emplacement du WAR de mots de passe externe.

Indiquez l'hôte et le port, par exemple `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`. Un WAR de mots de passe externe peut être en-dehors du pare-feu qui protège l'application utilisateur.

4 Pour la *Liaison de retour Mot de passe oublié*, indiquez le chemin d'accès que WAR de gestion des mots de passe externe utilise pour rappeler l'application utilisateur grâce à des services Web, par exemple `https://idmhost:sslport/idm`.

   La liaison de retour doit utiliser SSL pour assurer une communication sécurisée des services Web vers l'application utilisateur. Reportez-vous également à Section 5.9.3, « Configuration de communication SSL entre serveurs JBoss », page 184.

5 Si vous utilisez le programme d'installation, lisez les informations de cette étape et passez à Étape 6.

   Si vous utilisez l'utilitaire configupdate pour mettre à jour le WAR de mots de passe externe dans le répertoire racine d'installation, lisez cette étape et renommez manuellement le WAR comme le premier répertoire que vous avez indiqué dans *Liaison Mot de passe oublié*. Passez ensuite à Étape 6.

   Avant la fin de l'installation, le programme d'installation renomme `IDMPwdMgt.war` (regroupé avec le programme d'installation) et lui donne le nom du premier répertoire que vous avez indiqué. Le fichier renommé `IDMPwdMgt.war` devient votre WAR de mots de passe externe. Par exemple, si vous indiquez `http://www.idmpwdmgthost.com/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`, le programme d'installation renomme `IDMPwdMgt.war` qui devient `ExternalPwd.war`. Le programme d'installation déplace le WAR renommé dans le répertoire racine d'installation.

6 Copiez manuellement `ExternalPwd.war` dans le répertoire de déploiement du serveur distant JBoss qui exécute la fonction WAR de mots de passe externe.

Spécification d'un WAR de gestion des mots de passe interne

1 Ne sélectionnez pas *Utiliser le WAR de mot de passe externe*.

2 Acceptez l'emplacement par défaut de la *liaison Mot de passe oublié* ou fournissez une URL pour un autre WAR de mots de passe.

3 Acceptez la valeur par défaut de la *liaison de retour Mot de passe oublié*.

5.5.15 Vérification des choix et installation

1 Lisez la page Résumé avant installation pour vérifier vos choix de paramètres d'installation.

2 Si nécessaire, utilisez *Retour* pour retourner aux pages d'installation précédentes et modifier les paramètres d'installation.

   La page de configuration de l'application utilisateur ne sauvegarde pas de valeur. Une fois les pages précédentes de l'installation à nouveau spécifiées, vous devez saisir à nouveau les valeurs de configuration de l'application utilisateur.

3 Lorsque vous êtes satisfait de vos paramètres d'installation et de configuration, retournez à la page Résumé avant installation, puis cliquez sur *Installer*.

5.5.16 Affichage des fichiers journaux

1 Si votre installation s'est terminée sans erreur, passez à Section 5.9, « Tâches post-installation », page 183.

2 Si l'installation a émis des messages d'erreur ou d'avertissement, examinez les fichiers journaux pour déterminer les problèmes :

- `Identity_Manager_User_Application_InstallLog.log` contient les résultats des tâches d'installation de base
- `Novell-Custom-Install.log` contient des informations sur la configuration de l'application utilisateur effectuée lors de l'installation

Pour obtenir de l'aide et résoudre les problèmes, reportez-vous à Section 5.11, « Dépannage », page 187.

5.6 Installation de l'application utilisateur sur un serveur d'applications WebSphere

Cette section décrit comment installer l'application utilisateur Identity Manager sur un serveur d'applications WebSphere via la version de l'interface utilisateur graphique du programme d'installation.

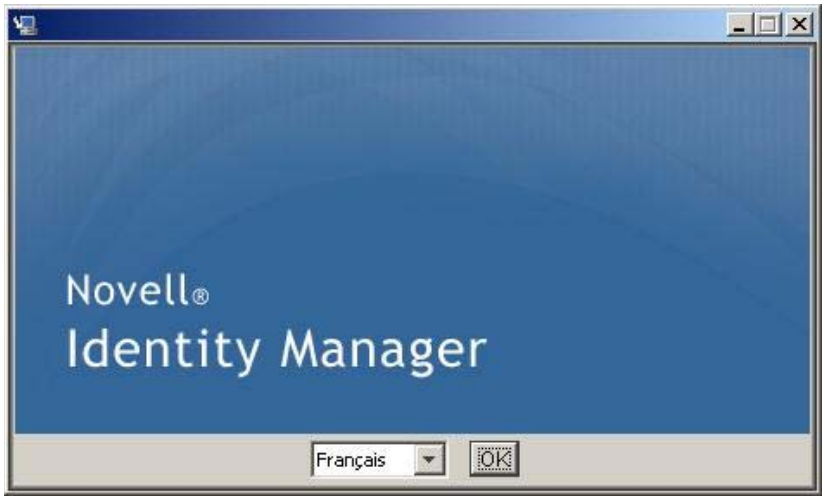
5.6.1 Lancer l'interface utilisateur graphique du programme d'installation

1 Naviguez jusqu'au répertoire contenant vos fichiers d'installation.

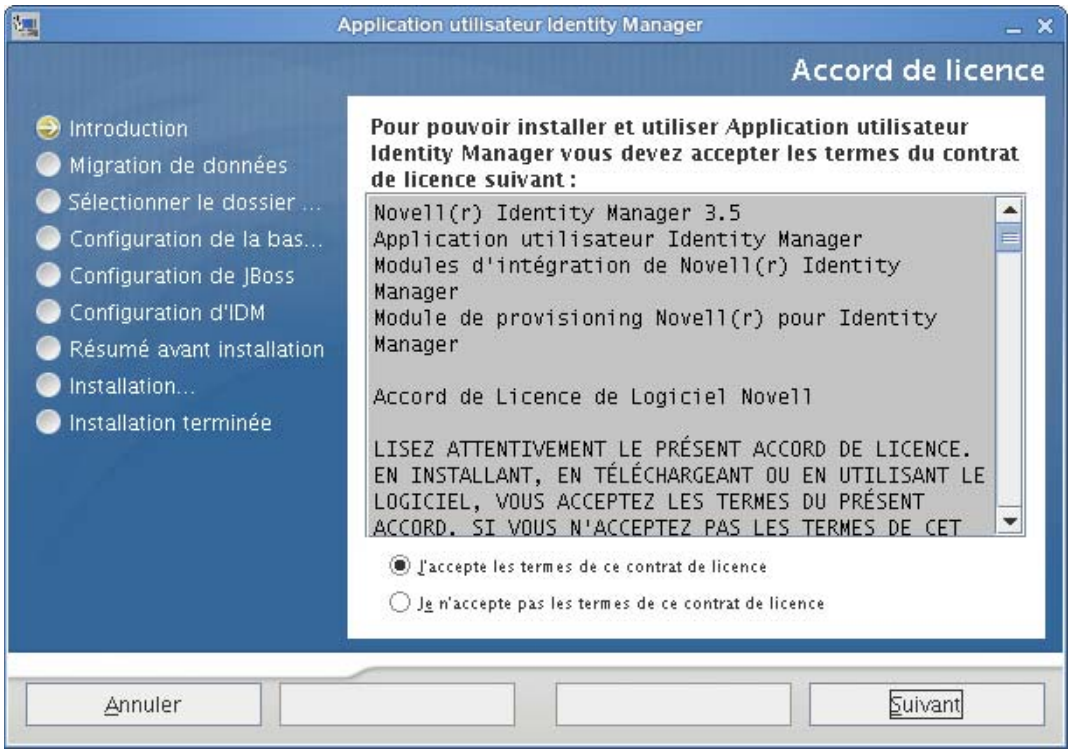
2 Lancez le programme d'installation :

```
java -jar IdmUserApp.jar
```

3 Sélectionnez une langue dans le menu déroulant, puis cliquez sur OK.



4 Lisez l'accord de licence, cliquez sur *J'accepte les termes de l'accord de licence,* puis cliquez sur *Suivant*.



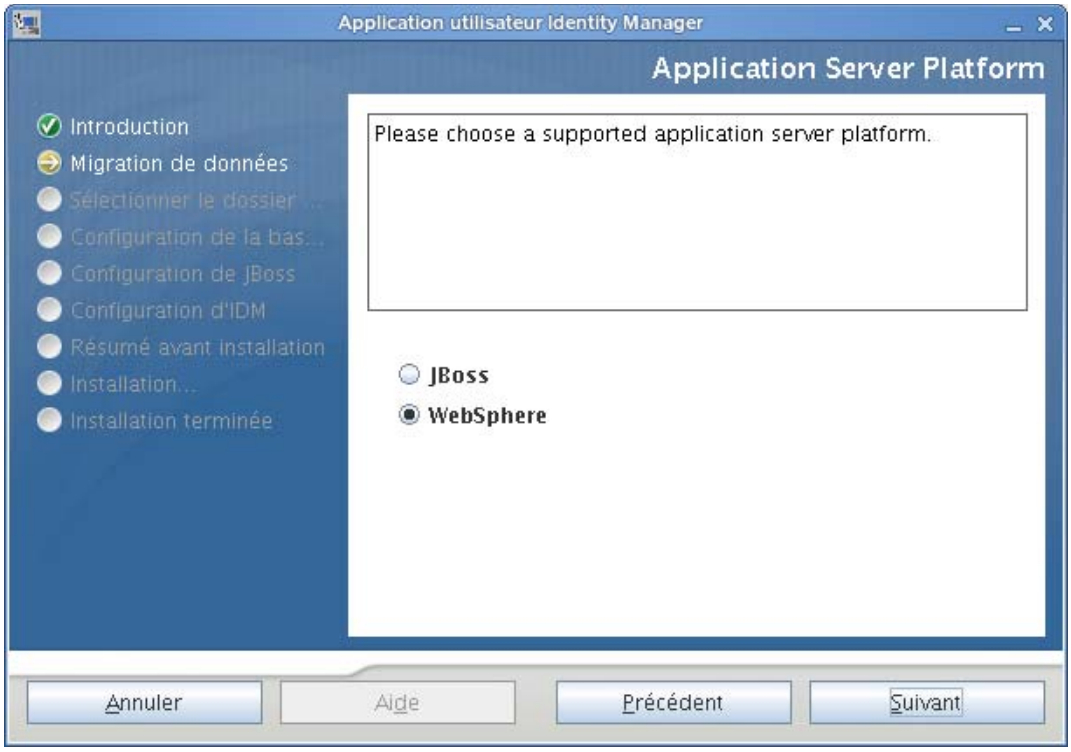
5 Lisez la page d'introduction de l'assistant d'installation, puis cliquez sur *Suivant*.

6 Passez à Section 5.6.2, « Choix d'une plate-forme de serveur d'applications », page 148.

5.6.2 Choix d'une plate-forme de serveur d'applications

1 Dans la fenêtre de la plate-forme du serveur d'applications, sélectionnez la plate-forme du serveur d'applications WebSphere.

2 Cliquez sur *Suivant*. Puis passez à l'étape Section 5.6.3, « Indiquer l'emplacement du WAR », page 148.

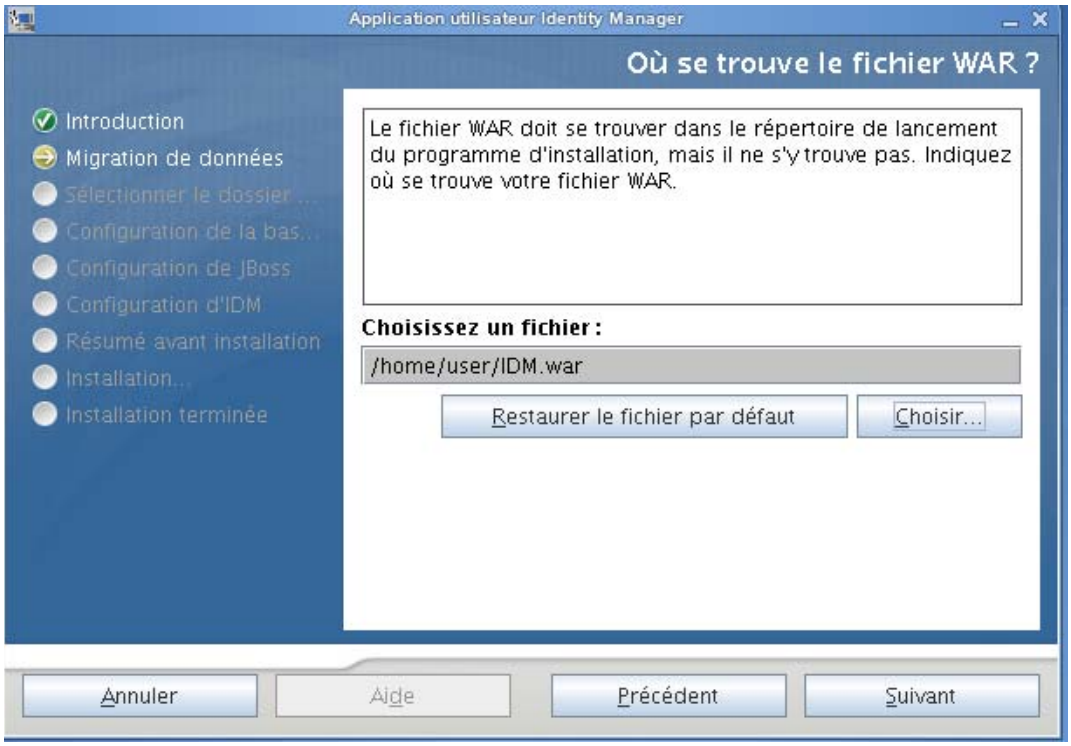


5.6.3 Indiquer l'emplacement du WAR

Si le fichier WAR de l'application utilisateur Identity Manager est dans un répertoire différent du programme d'installation, ce dernier vous invite à saisir le chemin d'accès au WAR.

1 Si le fichier WAR se trouve à l'emplacement par défaut, vous pouvez cliquez sur *Restaurer le dossier par défaut*.

Ou, pour spécifier l'emplacement du fichier WAR, cliquez sur *Choisir* et sélectionnez un emplacement.



2 Cliquez sur *Suivant*, puis passez à Section 5.6.4, « Choix d'un dossier d'installation », page 149.

5.6.4 Choix d'un dossier d'installation

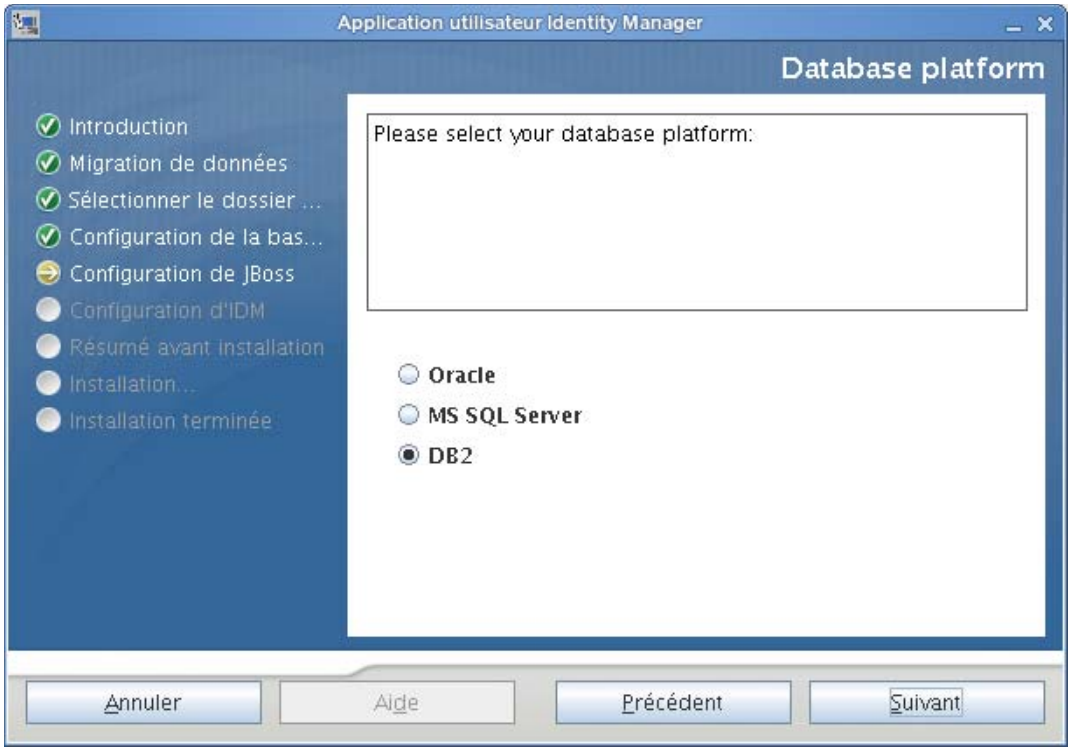
1 Sur la page Choisir un dossier d'installation, sélectionnez l'emplacement où installer l'application utilisateur. Si vous voulez utiliser l'emplacement par défaut, cliquez sur *Restaurer*

le dossier par défaut, ou si vous souhaitez choisir un autre emplacement pour les fichiers d'installation, cliquez sur *Choisir* et trouvez un emplacement.

2 Cliquez sur *Suivant*, puis passez à Section 5.6.5, « Choix d'une plate-forme de base de données », page 151.

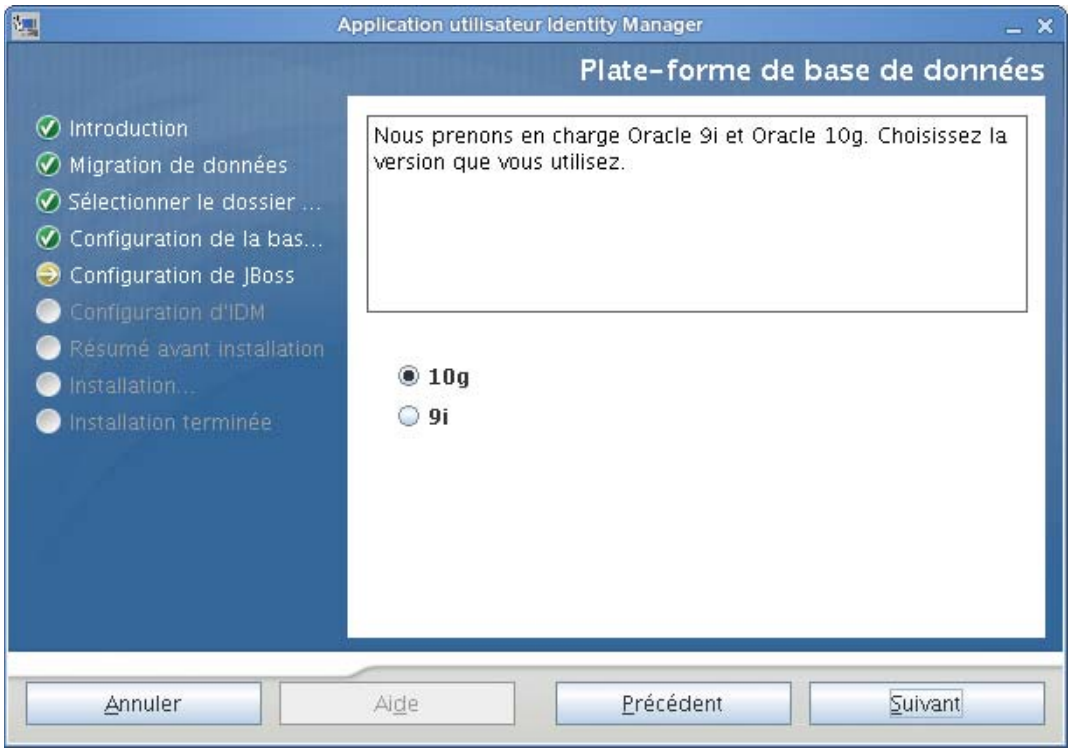
5.6.5 Choix d'une plate-forme de base de données

1 Sélectionnez la plate-forme de base de données à utiliser.



2 Si vous utilisez une base de données Oracle, passez à Étape 3. Sinon, passez à l'Étape 4.

3 Si vous utilisez une base de données Oracle, le programme d'installation demande quelle version vous utilisez. Choisissez votre version.

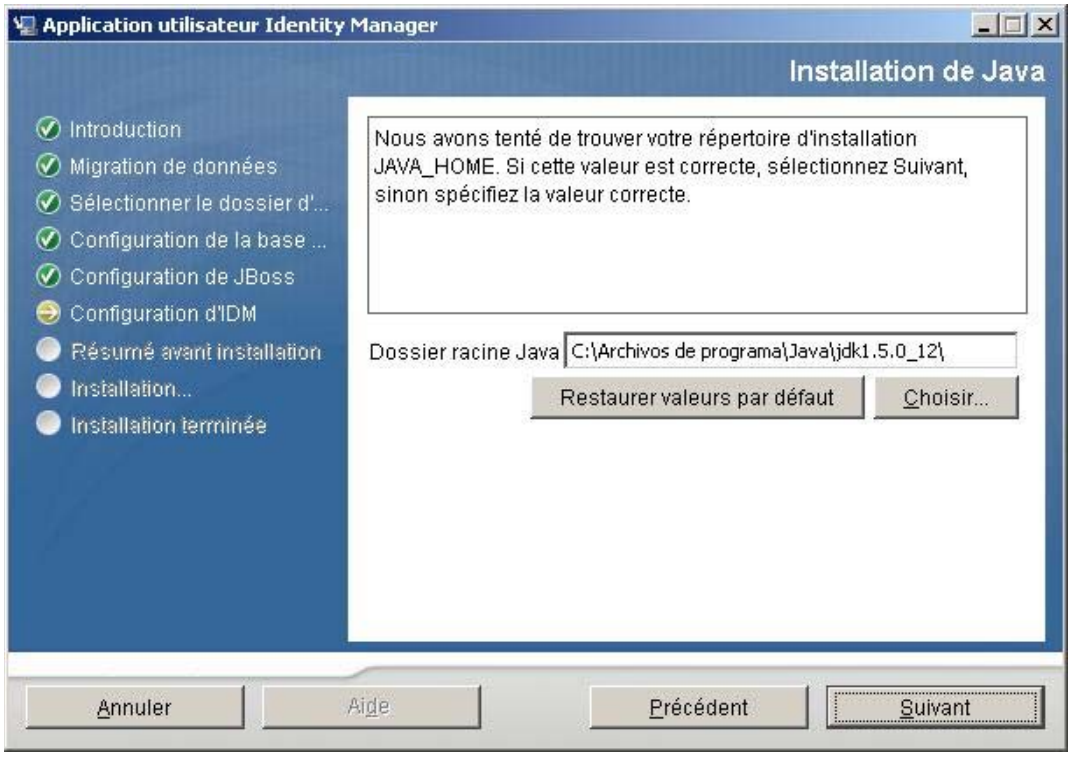


4 Cliquez sur *Suivant*, puis passez à Section 5.6.6, « Indiquer le répertoire racine Java », page 153.

5.6.6 Indiquer le répertoire racine Java

Remarque : avec WebSphere, utilisez IBM JDK en appliquant les fichiers de stratégies sans limitation.

1 Cliquez sur *Choisir* pour trouver votre dossier racine Java. Pour utiliser l'emplacement par défaut, cliquez sur *Restaurer les valeurs par défaut*.

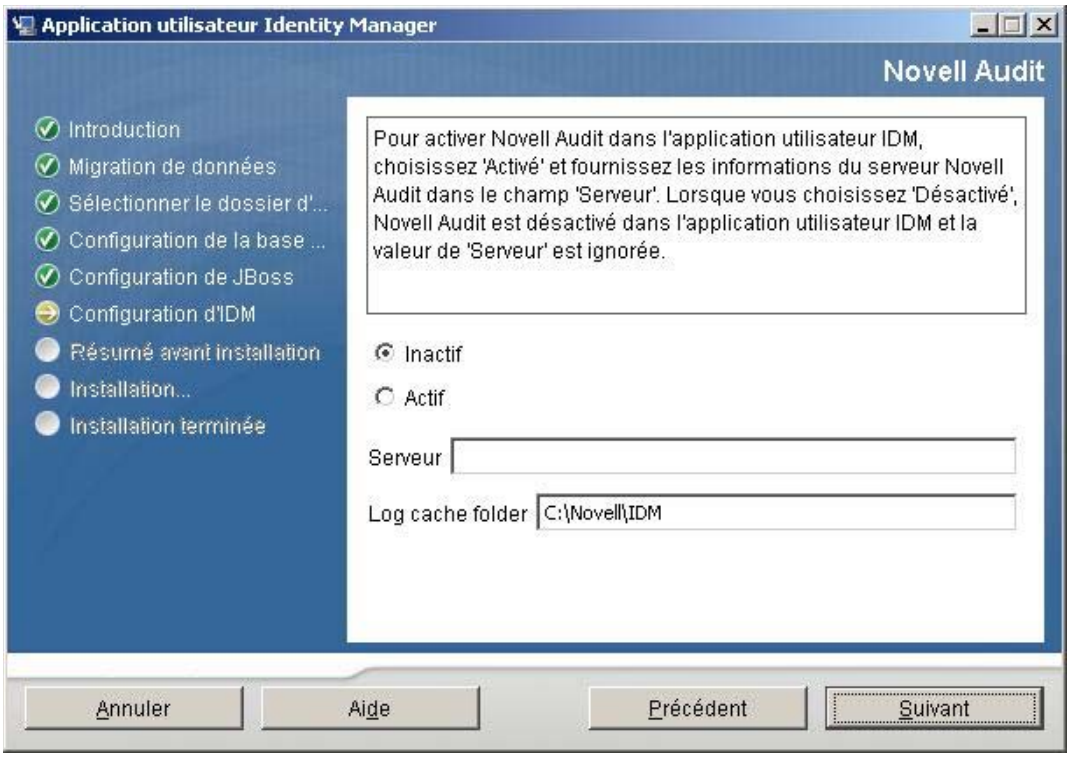


2 Cliquez sur *Suivant*, puis passez à Section 5.6.7, « Activation de la consignation Novell Audit », page 154.

5.6.7 Activation de la consignation Novell Audit

Pour activer la consignation Novell Audit (facultatif) de l'application utilisateur :

1 Renseignez les champs suivants :



Option	Description
Inactif	Désactive la consignation Novell Audit de l'application utilisateur. Vous pouvez l'activer plus tard via l'onglet *Administration* de l'application utilisateur. Pour plus d'informations sur l'activation de la consignation Novell Audit, reportez-vous au *Guide d'administration de l'application utilisateur Identity Manager*.
Actif	Active la consignation Novell Audit de l'application utilisateur. Pour plus d'informations sur la configuration de la consignation Novell Audit, reportez-vous au *Guide d'administration de l'application utilisateur Identity Manager*.
Serveur	Si vous activez la consignation Novell Audit, indiquez le nom d'hôte ou l'adresse IP du serveur Novell Audit. Si vous désactivez la consignation, cette valeur est ignorée.
Dossier du cache des fichiers journaux	Indiquez le répertoire du cache de consignation.

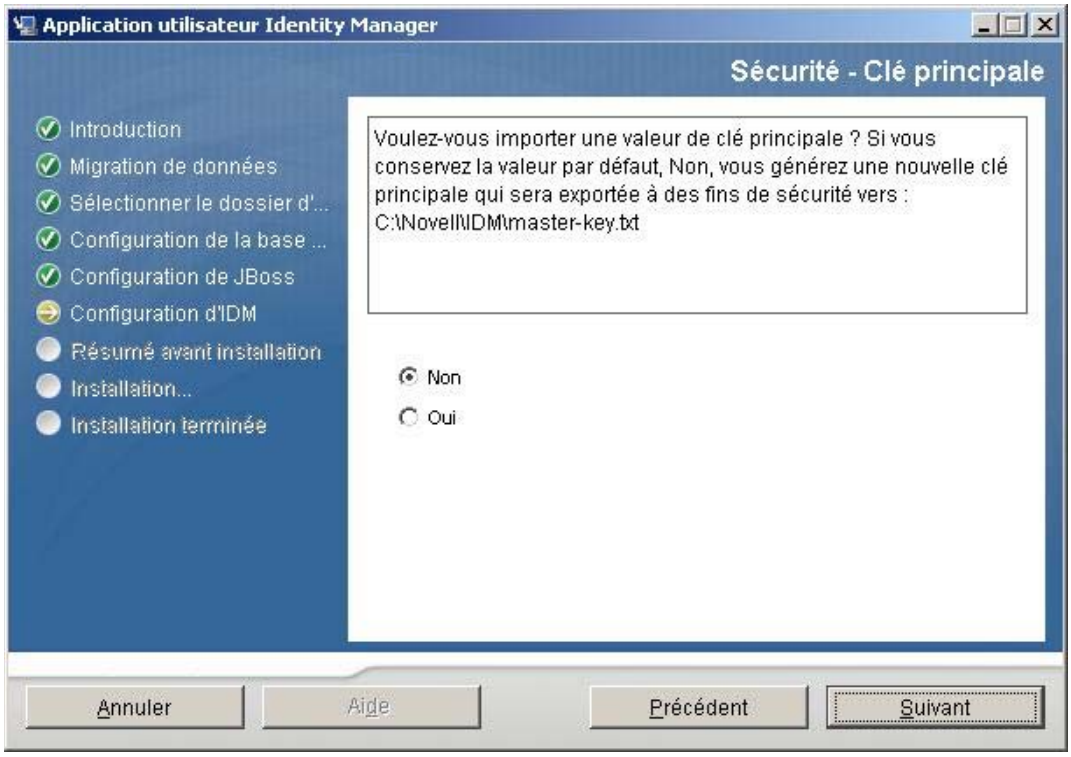
2 Cliquez sur *Suivant*, puis passez à Section 5.6.8, « Indiquer une clé maîtresse », page 155.

5.6.8 Indiquer une clé maîtresse

Indiquez si vous souhaitez importer une clé maîtresse existante ou en créer une nouvelle. Voici des exemples de raisons d'importer une clé maîtresse existante :

- Vous déplacez votre installation d'un système provisoire à un système de production et vous souhaitez conserver l'accès à la base de données que vous avez utilisée avec le système provisoire.
- Vous avez installé l'application utilisateur sur le premier membre d'une grappe et vous l'installez maintenant sur de nouveaux membres de la grappe (qui requièrent la même clé maîtresse).
- En raison d'un disque défectueux, vous devez restaurer votre application utilisateur. Vous devez réinstaller l'application utilisateur et indiquer la même clé maîtresse codée que celle qu'utilisait l'installation précédente. Cela vous donne accès aux données codées stockées précédemment.

1 Cliquez sur *Oui* pour importer une clé maîtresse existante ou sur *Non* pour en créer une nouvelle.

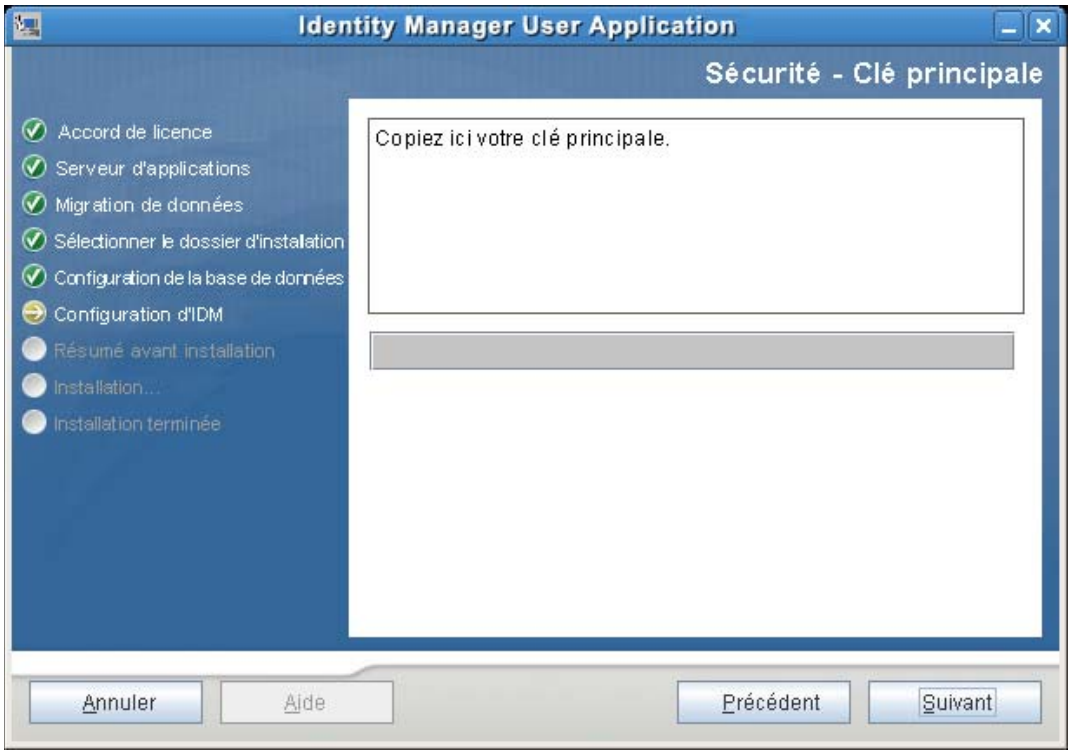


2 Cliquez sur *Suivant*.

La procédure d'installation inscrit la clé maîtresse codée dans le fichier `master-key.txt` dans le répertoire d'installation.

Si vous sélectionnez *Non*, passez à Section 5.6.9, « Configuration de l'application utilisateur », page 156. Une fois l'installation terminée, vous devez enregistrer manuellement la clé maîtresse. Si vous choisissez *Oui*, continuez avec Étape 3.

3 Si vous choisissez d'importer une clé maîtresse codée existante, coupez et collez la clé dans la fenêtre de procédure d'installation.



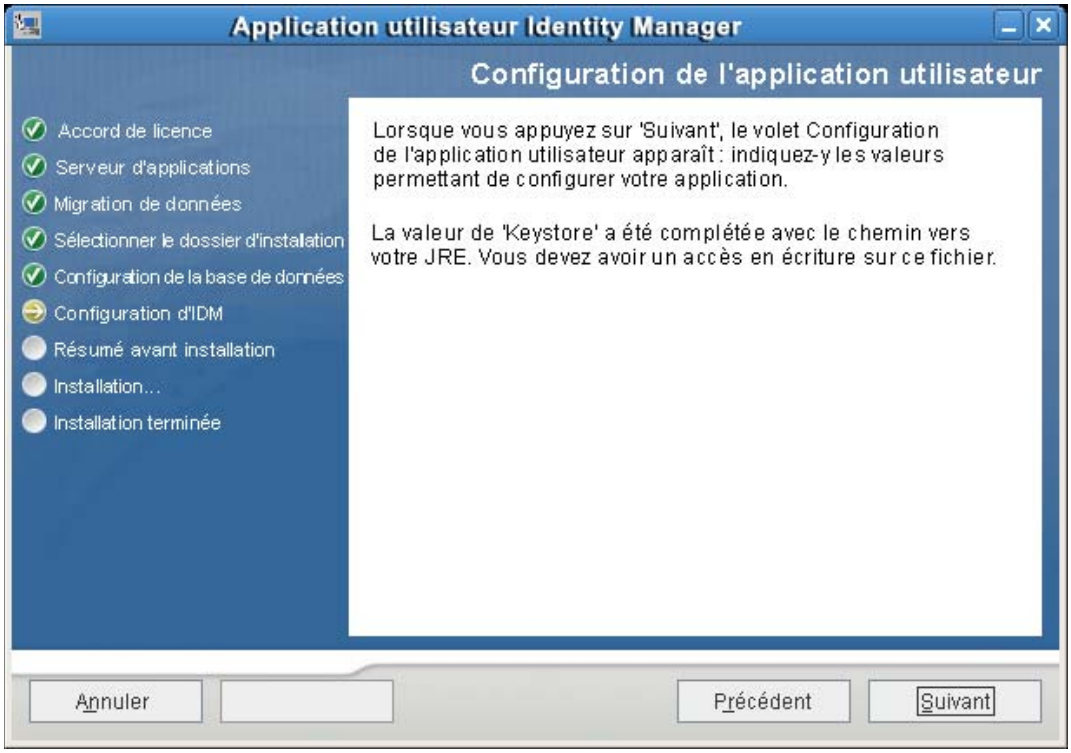
4 Cliquez sur *Suivant*, puis passez à Section 5.6.9, « Configuration de l'application utilisateur », page 156.

5.6.9 Configuration de l'application utilisateur

Le programme d'installation de l'application utilisateur permet de configurer les paramètres de configuration de l'application utilisateur. La plupart de ces paramètres sont également éditables avec `configupdate.sh` ou `configupdate.bat` après l'installation ; les exceptions sont notées

dans les descriptions des paramètres. Pour une grappe, indiquez les paramètres de configuration identiques de l'application utilisateur pour chaque membre de la grappe.

1 Cliquez sur *Suivant* jusqu'à la première page de configuration de l'application utilisateur.



2 Définissez les paramètres de configuration de base de l'application utilisateur décrits dans Tableau 5-6 page 159, puis passez à Étape 3.

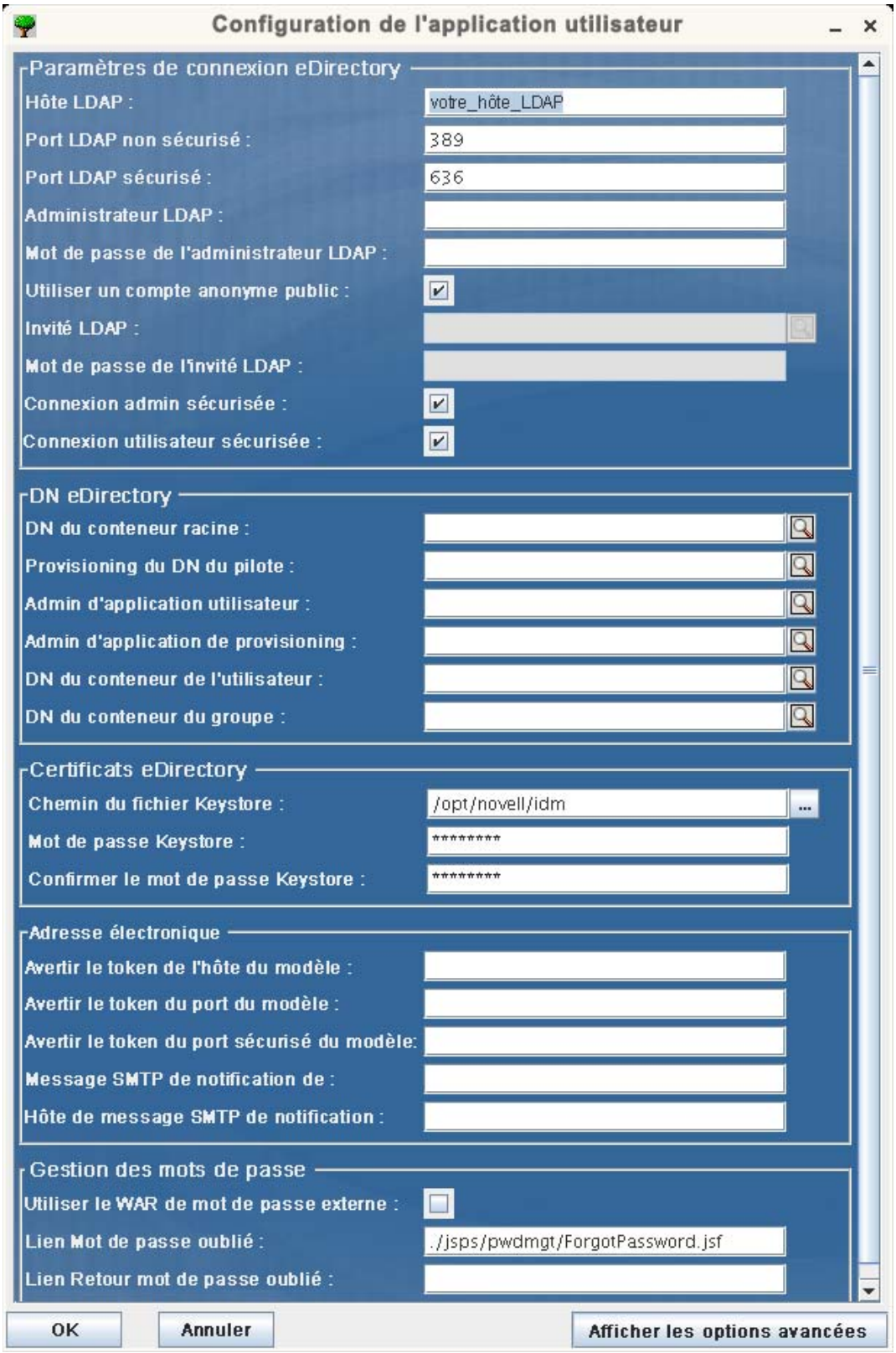


Tableau 5-6 *Configuration de l'application utilisateur : paramètres de base*

Type de paramètre	Champ	Description
Paramètres de login eDirectory	*Hôte LDAP*	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP et son port sécurisé. Par exemple : `myLDAPhost`
	Port non sécurisé LDAP	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	Port sécurisé LDAP	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	Administrateur LDAP	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer un login administratif au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
	Mot de passe administrateur LDAP	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
	Utiliser le compte anonyme public	Permet aux utilisateurs non logués d'accéder au compte anonyme public LDAP.
	Guest LDAP	Permet aux utilisateurs non logués d'accéder à des portlets autorisés. Ce compte utilisateur doit déjà exister dans le coffre-fort d'identité. Pour activer Guest LDAP, vous devez désélectionner *Utiliser le compte anonyme public*. Pour désactiver l'utilisateur Guest, sélectionnez *Utiliser le compte anonyme public*.
	Mot de passe Guest LDAP	Indiquez le mot de passe Guest LDAP.
	Login admin sécurisé	Sélectionnez cette option pour exiger que toutes les communications utilisant le compte admin. soient effectuées à l'aide d'un socket sécurisé (cette option peut avoir des implications néfastes sur la performance).
	Login utilisateur sécurisé	Sélectionnez cette option pour exiger que toutes les communications utilisant le compte de l'utilisateur logué soient effectuées à l'aide d'un socket sécurisé (cette option peut avoir des implications néfastes sur la performance).

Type de paramètre	Champ	Description
DN eDirectory	*DN du conteneur racine*	Requis. Indiquez le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire.
	DN du pilote de provisioning	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur. Par exemple, si votre pilote est UserApplicationDriver et si votre ensemble de pilotes est appelé myDriverSet, et si l'ensemble de pilotes est dans un contexte de o=myCompany, vous saisiriez une valeur de : `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Admin. application utilisateur	Requis. Un utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs de l'application utilisateur spécifié. Cet utilisateur peut utiliser l'onglet *Administration* de l'application utilisateur pour administrer le portail. Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, le concepteur Novell pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), vous devez accorder à cet administrateur des droits d'ayant droit sur les instances d'objets contenues dans le pilote de l'application utilisateur. Reportez-vous au *Guide d'administration de l'application utilisateur IDM* pour en savoir plus. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.
	Admin. application provisioning	Ce rôle est disponible dans la version de provisioning d'Identity Manager 3.5.1. L'administrateur de l'application de provisioning utilise l'onglet *Provisioning* (sous l'onglet *Administration*) pour gérer les fonctions de workflow du provisioning. Ces fonctions sont accessibles aux utilisateurs en passant par l'onglet *Requêtes et approbations* de l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur de l'application Provisioning. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.

Type de paramètre	Champ	Description
DN eDirectory (suite)	*DN du conteneur d'utilisateurs*	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur utilisateur. Cela définit l'étendue de recherche d'utilisateurs et de groupes. Les utilisateurs de ce conteneur (et en-dessous) sont autorisés à se loguer à l'application utilisateur. **Important :** assurez-vous que l'administrateur de l'application utilisateur spécifié lors de la configuration des pilotes de l'application utilisateur existe dans ce conteneur si vous souhaitez que cet utilisateur soit en mesure d'exécuter les workflows.
	DN de conteneur de groupes	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur de groupes. Utilisé par les définitions d'entités au sein de la couche d'abstraction d'annuaire.
Certificats eDirectory	*Chemin d'accès au Keystore*	Requis. Indiquez le chemin d'accès complet au fichier (`cacerts`) de votre keystore du JDK que le serveur d'applications utilise pour fonctionner, ou bien cliquez sur le petit bouton du navigateur pour trouver le fichier `cacerts`. Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier.
	Mot de passe Keystore/ Confirmer mot de passe Keystore	Requis. Indiquez le mot de passe `cacerts`. L'unité par défaut est `changeit`.

Type de paramètre	Champ	Description
Courrier électronique	*Jeton de l'hôte du modèle de notification*	Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple : `myapplication serverServer` Cette valeur remplace le jeton $HOST$ des modèles de courrier électronique. L'URL construite est la liaison aux tâches de requête de provisioning et aux notifications d'approbation.
	Jeton du port du modèle de notification	Utilisé pour remplacer le jeton $PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Jeton du port sécurisé du modèle de notification	Utilisé pour remplacer le jeton $SECURE_PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Notification SMTP - Expéditeur du courrier électronique :	Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
	Notification SMTP - destinataire du courrier électronique :	Indiquez l'utilisateur destinataire du courrier électronique dans le message de provisioning. Il peut s'agir d'une adresse IP ou d'un nom DNS.
Gestion des mots de passe	*Utiliser le WAR de mots de passe externe*	Cette fonction permet d'indiquer une page Mot de passe oublié qui réside dans un WAR Mot de passe oublié externe et une URL que le WAR Mot de passe oublié externe utilise pour rappeler l'application utilisateur grâce à un service Web. Si vous sélectionnez *Utiliser le WAR de mot de passe externe*, vous devez fournir des valeurs pour *Lien Mot de passe oublié* et *Lien Retour mot de passe oublié*. Si vous ne sélectionnez pas *Utiliser le·WAR de mots de passe externe*, IDM utilise la fonction de gestion des mots de passe interne par défaut. `/jsps/pwdmgt/ForgotPassword.jsf` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.
	Liaison Mot de passe oublié	Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier `ForgotPassword.jsf` dans un WAR de gestion des mots de passe externe ou interne.

Type de paramètre	Champ	Description
	Liaison de retour Mot de passe oublié	Si vous utilisez un WAR de gestion des mots de passe externe, indiquez le chemin d'accès que le WAR de gestion des mots de passe externe utilise pour rappeler l'application utilisateur par des services Web, par exemple `https://idmhost:sslport/idm`.

3 Si vous souhaitez définir d'autres paramètres de configuration de l'application utilisateur, cliquez sur *Afficher les options avancées*. (Faites défiler pour afficher tout le panneau.) Le tableau Tableau 5-7 page 164 décrit les paramètres des options avancées. Si vous ne souhaitez pas définir d'autres paramètres décrits dans cette étape, passez à Étape 4.

Tableau 5-7 *Configuration de l'application utilisateur : tous les paramètres*

Type de paramètre	Champ	Description
Paramètres de login eDirectory	*Hôte LDAP*	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP. Par exemple : myLDAPhost
	Port non sécurisé LDAP	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	Port sécurisé LDAP	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	Administrateur LDAP	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer un login administratif au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
	Mot de passe administrateur LDAP	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
	Utiliser le compte anonyme public	Permet aux utilisateurs non logués d'accéder au compte anonyme public LDAP.
	Guest LDAP	Permet aux utilisateurs non logués d'accéder à des portlets autorisés. Ce compte utilisateur doit déjà exister dans le coffre-fort d'identité. Pour activer Guest LDAP, vous devez désélectionner *Utiliser le compte anonyme public*. Pour désactiver l'utilisateur Guest, sélectionnez *Utiliser le compte anonyme public*.
	Mot de passe Guest LDAP	Indiquez le mot de passe Guest LDAP.
	Login admin sécurisé	Sélectionnez cette option pour exiger que toutes les communications utilisant le compte admin. soient effectuées à l'aide d'un socket sécurisé (cette option peut avoir des implications néfastes sur la performance).
	Login utilisateur sécurisé	Sélectionnez cette option pour exiger que toutes les communications sur le compte de l'utilisateur logué soient effectuées à l'aide d'un socket sécurisé (cette option peut avoir des implications néfastes graves sur la performance).

Type de paramètre	Champ	Description
DN eDirectory	*DN du conteneur racine*	Requis. Indiquez le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire.
	DN du pilote de provisioning	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur. Par exemple, si votre pilote est UserApplicationDriver et si votre ensemble de pilotes est appelé myDriverSet, et si l'ensemble de pilotes est dans un contexte de o=myCompany, vous saisissez une valeur de : `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Admin. application utilisateur	Requis. Un utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs de l'application utilisateur spécifié. Cet utilisateur peut utiliser l'onglet *Administration* de l'application utilisateur pour administrer le portail. Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, le concepteur Novell pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), vous devez accorder à cet administrateur des droits d'ayant droit sur les instances d'objets contenues dans le pilote de l'application utilisateur. Reportez-vous au *Guide d'administration de l'application utilisateur IDM* pour en savoir plus. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.
	Admin. application provisioning	Ce rôle est disponible dans la version de provisioning d'Identity Manager 3.5.1. L'administration de l'application de provisioning gère les fonctions de workflow du provisioning accessibles par l'onglet *Requêtes et approbations* de l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur de l'application Provisioning. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.

Type de paramètre	Champ	Description
Identité utilisateur du méta-annuaire	*DN du conteneur d'utilisateurs*	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur d'utilisateurs. Cela définit l'étendue de recherche d'utilisateurs et de groupes. Les utilisateurs de ce conteneur (et en-dessous) sont autorisés à se loguer à l'application utilisateur. **Important :** assurez-vous que l'administrateur de l'application utilisateur spécifié lors de la configuration des pilotes de l'application utilisateur existe dans ce conteneur si vous souhaitez que cet utilisateur soit en mesure d'exécuter les workflows.
	Classe d'objets Utilisateur	La classe d'objets utilisateur LDAP (généralement inetOrgPerson).
	Attribut de login	L'attribut LDAP (par exemple, CN) qui représente le nom de login de l'utilisateur.
	Attribut de nom	L'attribut LDAP utilisé comme identifiant lors de la consultation d'utilisateurs ou de groupes. Il est différent de l'attribut de login, qui n'est utilisé que lors du login, et non pas lors des recherches d'utilisateurs/de groupes.
	Attribut de l'adhésion utilisateur	Facultatif. L'attribut LDAP qui représente l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.
Groupes d'utilisateurs du méta-annuaire	*DN de conteneur de groupes*	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur de groupes. Utilisé par les définitions d'entités au sein de la couche d'abstraction d'annuaire.
	Classe d'objets Groupe	La classe d'objets Groupe LDAP (généralement groupofNames).
	Attribut d'adhésion à un groupe	L'attribut qui représente l'adhésion d'un utilisateur à un groupe. N'utilisez pas d'espaces pour le nom.
	Utiliser des groupes dynamiques	Sélectionnez cette option si vous souhaitez utiliser des groupes dynamiques.
	Classe d'objets Groupe dynamique	La classe d'objets Groupe dynamique LDAP (généralement dynamicGroup).

Type de paramètre	Champ	Description
Certificats eDirectory	*Chemin d'accès au Keystore*	Requis. Indiquez le chemin d'accès complet au fichier (`cacerts`) de votre keystore du JRE que le serveur d'applications utilise pour fonctionner, ou bien cliquez sur le petit bouton du navigateur pour trouver le fichier `cacerts`. L'installation de l'application utilisateur modifie le fichier keystore. Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier.
	Mot de passe Keystore *Confirmer le mot de passe Keystore*	Requis. Indiquez le mot de passe `cacerts`. L'unité par défaut est `changeit`.
Keystore privé	*Chemin d'accès au keystore privé*	Le keystore privé contient la clé privée et les certificats de l'application utilisateur. Réservé. Si vous laissez ce champ vierge, ce chemin d'accès est `/jre/lib/security/cacerts` par défaut.
	Mot de passe Keystore privé	Ce mot de passe est `changeit`, à moins d'indication contraire. Ce mot de passe est codé, en fonction de la clé maîtresse.
	Alias de clé privée	Cet alias est `novellIDMUserApp`, à moins d'indication contraire.
	Mot de passe de la clé privée	Ce mot de passe est `novellIDM`, à moins d'indication contraire. Ce mot de passe est codé, en fonction de la clé maîtresse.
Banque de clés approuvée	*Chemin d'accès à la banque approuvée*	La banque de clés approuvées contient tous les certificats approuvés des signataires utilisés pour valider les signatures numériques. Si ce chemin est vide, l'application utilisateur obtient le chemin à partir de la propriété Système `javax.net.ssl.trustStore`. Si le chemin n'y est pas, il est supposé être `jre/lib/security/cacerts`.
	Mot de passe de la banque approuvée	Si ce champ est vierge, l'application utilisateur obtient le mot de passe à partir de la propriété système `javax.net.ssl.trustStorePassword`. S'il n'y a aucune valeur, `changeit` est utilisé. Ce mot de passe est codé, en fonction de la clé maîtresse.
Clé de certificat et signature numérique Novell Audit		Contient le certificat et la clé de signature numérique Novell Audit.
	Certificat de signature numérique Novell Audit	Affiche le certificat de signature numérique.

Type de paramètre	Champ	Description
	Clé privée de signature numérique Novell Audit	Affiche la clé privée de signature numérique. Cette clé est codée, en fonction de la clé maîtresse.
Paramètres iChain	*Logout ICS activé*	Si cette option est sélectionnée, l'application utilisateur prend en charge le logout simultané de l'application utilisateur ainsi que iChain ou Novell Access Manager. L'application utilisateur recherche un cookie iChain ou Novell Access Manager au logout et, en cas de présence du cookie, redirige l'utilisateur vers la page de logout ICS.
	Page de logout ICS	L'URL vers la page de logout de Ichain ou Novell Access Manager, où l'URL est un nom d'hôte auquel Ichain ou Novell Access Manager s'attend. Si le login à ICS est activée et si un utilisateur se délogue de l'application utilisateur, il est redirigé vers cette page.

Type de paramètre	Champ	Description
Courrier électronique	*Jeton HÔTE du modèle de notification*	Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple : `myapplication serverServer` Cette valeur remplace le jeton $HOST$ des modèles de courrier électronique. L'URL construite est la liaison aux tâches de requête de provisioning et aux notifications d'approbation.
	Jeton du port du modèle de notification	Utilisé pour remplacer le jeton $PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Jeton du port sécurisé du modèle de notification	Utilisé pour remplacer le jeton $SECURE_PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Jeton PROTOCOLE du modèle de notification	Se rapporte à un protocole non sécurisé, HTTP. Utilisé pour remplacer le jeton $PROTOCOL$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Jeton PROTOCOLE SÉCURISÉ du modèle de notification	Se rapporte à un protocole sécurisé, HTTPS. Utilisé pour remplacer le jeton $SECURE_PROTOCOL$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Notification SMTP - Expéditeur du courrier électronique :	Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
	Notification SMTP - destinataire du courrier électronique :	Indiquez l'utilisateur destinataire du courrier électronique dans le message de provisioning. Il peut s'agir d'une adresse IP ou d'un nom DNS.

Type de paramètre	Champ	Description
Gestion des mots de passe		
	Utiliser le WAR de mots de passe externe	Cette fonction permet d'indiquer une page Mot de passe oublié qui réside dans un WAR Mot de passe oublié externe et une URL que le WAR Mot de passe oublié externe utilise pour rappeler l'application utilisateur grâce à un service Web. Si vous sélectionnez *Utiliser le WAR de mot de passe externe*, vous devez fournir des valeurs pour *Lien Mot de passe oublié* et *Lien Retour mot de passe oublié*. Si vous ne sélectionnez pas *Utiliser le·WAR de mots de passe externe*, IDM utilise la fonction de gestion des mots de passe interne par défaut. `/jsps/pwdmgt/ForgotPassword.jsf` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.
	Liaison Mot de passe oublié	Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier `ForgotPassword.jsf` dans un WAR de gestion des mots de passe externe ou interne.
	Liaison de retour Mot de passe oublié	Si vous utilisez un WAR de gestion des mots de passe externe, indiquez le chemin d'accès que le WAR de gestion des mots de passe externe utilise pour rappeler l'application utilisateur par des services Web, par exemple `https://idmhost:sslport/idm`.
Divers	*Timeout de session*	Le timeout de session de l'application.
	OCSP URI	Si l'installation client utilise le protocole OCSP (protocole de propriété d'état de certificat en ligne), fournissez un identificateur de ressource uniforme (URI). Par exemple, le format est http://host:port/ocspLocal. L'URI OCSP met à jour le statut des certificats approuvés en ligne.
	Chemin de configuration d'autorisation	Nom complet du fichier de configuration de l'autorisation.
	Créer un index eDirectory	
	DN du serveur	

Type de paramètre	Champ	Description
Objet Conteneur	*Sélectionné*	Sélectionnez chaque type d'objet Conteneur à utiliser.
	Type d'objet Conteneur	Sélectionnez parmi les conteneurs standard suivants : lieu, pays, unité organisationnelle, organisation et domaine. Vous pouvez également définir vos propres conteneurs dans iManager et les ajouter sous *Ajouter un nouvel objet Conteneur*.
	Nom de l'attribut Conteneur	Indique le nom de type d'attribut associé au type d'objet Conteneur.
	Ajouter un nouvel objet Conteneur : type d'objet Conteneur	Indiquez le nom LDAP d'une classe d'objets du coffre-fort d'identité qui peut servir de conteneur. Pour plus d'informations sur les conteneurs, reportez-vous au *Guide d'administration de Novell iManager 2.6 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*.
	Ajouter un nouvel objet Conteneur : nom d'attribut Conteneur	Donnez le nom d'attribut de l'objet Conteneur.

4 Une fois les paramètres configurés, cliquez sur *OK*, puis passez à Section 5.6.10, « Vérification des choix et installation », page 171.

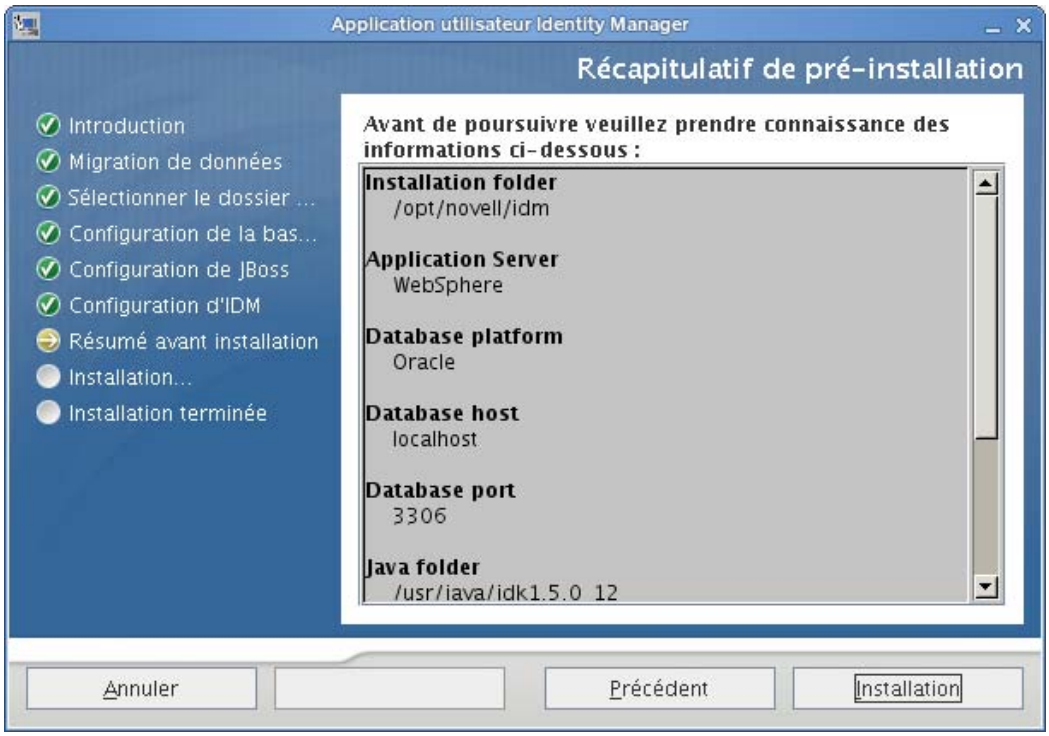
5.6.10 Vérification des choix et installation

1 Lisez la page Résumé avant installation pour vérifier vos choix de paramètres d'installation.

2 Si nécessaire, utilisez *Retour* pour retourner aux pages d'installation précédentes et modifier les paramètres d'installation.

La page de configuration de l'application utilisateur ne sauvegarde pas de valeur. Une fois les pages précédentes de l'installation à nouveau spécifiées, vous devez saisir à nouveau les valeurs de configuration de l'application utilisateur.

3 Lorsque vous êtes satisfait de vos paramètres d'installation et de configuration, retournez à la page Résumé avant installation, puis cliquez sur *Installer*. Passez à Section 5.6.11, « Affichage des fichiers journaux », page 172.



5.6.11 Affichage des fichiers journaux

Si votre installation s'est terminée sans erreur, passez à Section 5.6.12, « Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM », page 172.

Si l'installation a émis des messages d'erreur ou d'avertissement, examinez les fichiers journaux pour déterminer les problèmes :

- `Identity_Manager_User_Application_InstallLog.log` contient les résultats des tâches d'installation de base
- `Novell-Custom-Install.log` contient des informations sur la configuration de l'application utilisateur effectuée lors de l'installation

5.6.12 Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM

1. Copiez le fichier `sys-configuration-xmldata.xml` du répertoire d'installation de l'application utilisateur dans un répertoire de la machine hébergeant le serveur WebSphere, par exemple `/UserAppConfigFiles`. Le répertoire d'installation de l'application utilisateur est celui dans lequel vous avez installé l'application utilisateur.
2. Définissez le chemin d'accès du fichier `sys-configuration-xmldata.xml` dans les propriétés du système JVM. Loguez-vous à la console d'administration WebSphere en tant qu'utilisateur administrateur pour ce faire.
3. Dans le tableau de bord de gauche, accédez à *Serveurs* > *Serveurs d'application*.
4. Cliquez sur le nom du serveur dans la liste des serveurs, par exemple serveur1.

5 Dans la liste des paramètre de droite, accédez à *Java et Gestion de processus* sous *Infrastructure de serveur*.

6 Développez le lien et sélectionnez *Définition du processus*.

7 Sous la liste des *Propriétés supplémentaires*, sélectionnez *Machine virtuelle Java*.

8 Sélectionnez *Propriétés personnalisées* sous le titre *Propriétés supplémentaires* de la page JVM.

9 Cliquez sur *Nouveau* pour ajouter une nouvelle propriété du système JVM.

9a Pour le *Nom*, indiquez `extend.local.config.dir`.

9b Pour la *Valeur*, indiquez le répertoire, par exemple `/UserAppConfigFiles`, dans lequel vous avez copié le fichier `sys-configuration-xmldata.xml`.

9c Pour la *Description*, indiquez la description de la propriété, par exemple `le chemin vers sys-configuration-xmldata.xml`.

9d Cliquez sur *OK* pour enregistrer la propriété.

10 Cliquez sur *Nouveau* pour ajouter une autre propriété nouvelle du système JVM.

10a Pour le *Nom*, indiquez `idmuserapp.logging.config.dir`.

10b Pour la *Valeur*, indiquez le répertoire, par exemple `/UserAppConfigFiles`, dans lequel vous avez copié le fichier `sys-configuration-xmldata.xml`.

10c Pour la *Description*, indiquez la description de la propriété, par exemple `le chemin vers sys-configuration-xmldata.xml`.

10d Cliquez sur *OK* pour enregistrer la propriété.

Remarque : le fichier `idmuserapp-logging.xml` n'existe pas dans ce répertoire. Il est créé lorsque des changements sont apportés à la configuration de la consignation.

---

11 Passez à la section Section 5.6.13, « Importation de la racine approuvée d'eDirectory dans la zone de stockage des clés WebSphere », page 173.

5.6.13 Importation de la racine approuvée d'eDirectory dans la zone de stockage des clés WebSphere

1 La procédure d'installation de l'application utilisateur exporte les certificats de la racine approuvée d'eDirectory dans le répertoire dans lequel vous avez installé l'application utilisateur. Copiez ces certificats sur la machine qui héberge le serveur WebSphere.

2 Importez les certificats dans la zone de stockage de clés WebSphere. Vous pouvez le faire en utilisant la console de l'administrateur WebSphere (« Importation de certificats avec la console de l'administrateur WebSphere » page 173) ou par l'intermédiaire de la ligne de commande (« Importation de certificats avec la ligne de commande » page 174).

3 Après avoir importé les certificats, passez à Section 5.6.14, « Déploiement du fichier WAR IDM », page 174.

Importation de certificats avec la console de l'administrateur WebSphere

1 Loguez-vous à la console d'administration WebSphere en tant qu'utilisateur administrateur.

2 Dans le tableau de bord de gauche, accédez à *Sécurité* > *Gestion des certificats SSL et des clés*

3 Dans la liste des paramètre de droite, accédez à *Zone se stockage des clés et des certificats* sous *Propriétés supplémentaires*.

4 Sélectionnez *NodeDefaultTrustStore* (ou la zone de stockage fiable que vous utilisez).

5 Sous *Propriétés supplémentaires*, sur la droite, sélectionnez *Certificats du signataire*.

6 Cliquez sur *Ajouter*.

7 Saisissez le nom de l'alias et le chemin d'accès complet au fichier de certificat.

8 Changez le type de donnée dans la liste de déroulante pour *Données DER binaires*.

9 Cliquez sur *OK*. À présent, le certificat doit apparaître dans la liste des certificats du signataire.

Importation de certificats avec la ligne de commande

1 Dans la ligne de commande de la machine qui héberge le serveur WebSphere, exécutez l'outil clé pour importer le certificat dans la zone de stockage de clés de WebSphere.

Remarque : vous devez utiliser l'outil clé de WebSphere, sinon, cela·ne fonctionnera pas. Vérifiez en outre que la zone de stockage est de type PKCS12.

L'outil clé WebSphere se trouve dans `/IBM/WebSphere/AppServer/java/bin`.

Exemple de commande d'outil clé

```
keytool -import -trustcacerts -file servercert.der -alias
myserveralias -keystore trust.p12 -storetype PKCS12
```

Si votre système contient plusieurs fichiers `trust.p12`, il se peut que vous deviez indiquer le chemin complet du fichier.

5.6.14 Déploiement du fichier WAR IDM

1 Loguez-vous à la console d'administration WebSphere en tant qu'utilisateur administrateur.

2 Dans le tableau de bord de gauche, accédez à *Applications* > *Installer une nouvelle application*

3 Recherchez l'emplacement du fichier WAR IDM. (Le fichier WAR IDM est configuré au cours de l'installation de l'application utilisateur. Il se trouve dans le répertoire d'installation de l'application utilisateur que vous avez spécifié au cours de l'installation de l'application utilisateur.)

4 Saisissez la racine du contexte de l'application, par exemple `IDMProv`. Il s'agira du chemin de l'URL.

5 Assurez-vous que *Me demander uniquement lorsque des informations supplémentaires sont requises* est sélectionné, puis cliquez sur *Suivant* pour ouvrir la page *Sélectionner des options d'installation*.

6 Acceptez les valeurs par défaut de cette page et cliquez sur *Suivant* pour passer à l'écran *Mapper les modules sur les serveurs*.

7 Laissez toutes les valeurs par défaut de cette page et cliquez sur *Suivant* pour passer à la page *Mapper les références des ressources sur les ressources*.

8 Pour la méthode d'authentification, cochez la case *Méthode de l'utilisateur par défaut*. Ensuite, dans la liste déroulante *Entrée des données d'authentification*, sélectionnez l'alias que vos avez créé précédemment, par exemple `MyServerNode01/MyAlias`.

9 Dans le tableau ci-dessous des paramètres d'authentification, recherchez le module que vous déployez. Sous la colonne intitulée `Nom JNDI de la ressource cible`, cliquez sur le bouton Parcourir pour indiquer un nom JNDI. Cela doit ouvrir la liste des ressources. Sélectionnez la source de données que vous avez créée précédemment et cliquez sur le bouton *Appliquer* pour revenir à la page `Mapper les références des ressources sur les ressources`, par exemple `MyDataSource`.

10 Sélectionnez *Suivant* pour accéder à la page *Mapper des hôtes virtuels pour les modules Web*.

11 Acceptez les valeurs par défaut de cette page et cliquez sur *Suivant* pour accéder à la page *Résumé*.

12 Cliquez sur *Terminer* pour achever le déploiement.

13 Une fois·le déploiement terminé, cliquez sur *Enregistrer* pour enregistrer les changements.

14 Passez à Section 5.6.15, « Démarrage de l'application », page 175.

5.6.15 Démarrage de l'application

1 Loguez-vous à la console d'administrateur WebSphere en tant qu'utilisateur administrateur.

2 Dans le tableau de bord de gauche, accédez à *Applications* > *Applications d'entreprise*.

3 Cochez la case en regard de l'application que vous voulez démarrer, puis cliquez sur *Démarrer*.

Une fois l'application démarrée, la colonne *État de l'application* affiche une flèche verte.

5.6.16 Accès au portail de l'application utilisateur

1 Accédez au portail en utilisant le contexte que vous avez spécifié au cours du déploiement.

Le port par défaut du conteneur Web sur WebSphere est 9080, ou 9443 pour le port sécurisé. Le format de l'URL est le suivant :

`http://<serveur>:9080/IDMProv`

5.7 Installation de l'application utilisateur à partir d'une interface de console

Cette section décrit comment installer l'application utilisateur Identity Manager via la version de console (ligne de commande) du programme d'installation.

1 Obtenez les fichiers d'installation appropriés décrits dans Tableau 5-2 page 113.

2 Loguez-vous et ouvrez une session de terminal.

3 Lancez le programme d'installation correspondant à votre plate-forme avec Java en utilisant la commande suivante :

```
java -jar IdmUserApp.jar -i console
```

4 Suivez les mêmes étapes que pour l'interface utilisateur graphique sous Section 5.5, « Installation de l'application utilisateur sur un serveur d'applications JBoss à partir de l'interface utilisateur d'installation », page 114 : lisez les invites sur la ligne de commande et saisissez les réponses sur la ligne de commande, grâce aux étapes d'importation ou de création de la clé maîtresse.

5 Pour configurer les paramètres de configuration de l'application utilisateur, vous devez lancer manuellement l'utilitaire configupdate. Sur une ligne de commande, saisissez `configupdate.sh` (Linux ou Solaris) ou `configupdate.bat` (Windows), puis renseignez les valeurs telles que décrites dans Section 5.5.14, « Configuration de l'application utilisateur », page 130.

6 Si vous utilisez un WAR·de gestion des mots de passe externe, copiez-le manuellement dans le répertoire d'installation et dans le répertoire de déploiement du serveur distant JBoss qui exécute la fonction WAR de mot de passe externe.

7 Passez à Section 5.9, « Tâches post-installation », page 183.

5.8 Installation de l'application utilisateur avec une seule commande

Cette section décrit comment effectuer une installation en mode silencieux. Une installation en mode silencieux ne requiert aucune interaction lors de l'installation et peut faire gagner du temps, en particulier lors d'une installation sur plusieurs systèmes. L'installation en mode silencieux est prise en charge sous Linux et Solaris.

1 Obtenez les fichiers d'installation appropriés indiqués dans Tableau 5-2 page 113.

2 Loguez-vous et ouvrez une session de terminal.

3 Localisez le fichier de propriétés IDM, `silent.properties`, qui se trouve avec les fichiers d'installation. Si vous travaillez à partir d'un CD, faites une copie locale de ce fichier.

4 Modifiez `silent.properties` pour fournir vos paramètres d'installation et les paramètres de configuration de l'application utilisateur.

   Reportez-vous au fichier `silent.properties` pour afficher un exemple de chaque paramètre d'installation. Les paramètres d'installation correspondent aux paramètres d'installation que vous avez configurés dans les procédures d'installation de l'interface utilisateur graphique ou de la console.

   Reportez-vous à Tableau 5-8 pour obtenir une description de chaque paramètre de configuration de l'application utilisateur. Les paramètres de configuration de l'application utilisateur sont les mêmes que ceux que vous pouvez configurer dans les procédures d'installation de l'interface utilisateur graphique ou de la console ou avec l'utilitaire configupdate.

5 Lancez l'installation silencieuse de la façon suivante :

   ```
   java -jar IdmUserApp.jar -i silent -f / yourdirectorypath/
   silent.properties
   ```

   Saisissez le chemin d'accès complet à `silent.properties` si ce fichier est dans un répertoire différent du script du programme d'installation. Le script décondense les fichiers nécessaires vers un répertoire temporaire et lance l'installation en mode silencieux.

Tableau 5-8 *Paramètres de configuration de l'application utilisateur pour l'installation en mode silencieux*

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur et description
NOVL_CONFIG_LDAPHOST=	Paramètres de login eDirectory : hôte LDAP. Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP.
NOVL_CONFIG_LDAPADMIN=	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer un login administratif au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
NOVL_CONFIG_LDAPADMINPASS=	Paramètres de login eDirectory : mot de passe administrateur LDAP. Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
NOVL_CONFIG_ROOTCONTAINERNAME=	DN eDirectory : DN du conteneur racine. Requis. Indiquez le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire.
NOVL_CONFIG_PROVISIONROOT=	DN eDirectory : DN du pilote de provisioning. Requis. Indiquez le nom distinctif du pilote de l'application utilisateur que vous avez créé auparavant dans Section 5.3, « Création du pilote d'application utilisateur », page 107. Par exemple, si votre pilote est UserApplicationDriver et si votre ensemble de pilotes est appelé myDriverSet, et si l'ensemble de pilotes est dans un contexte de o=myCompany, vous saisissez une valeur de : `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur et description
NOVL_CONFIG_LOCKSMITH=	DN eDirectory : admin. de l'application utilisateur. Requis. Un utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs de l'application utilisateur spécifié. Cet utilisateur peut utiliser l'onglet *Administration* de l'application utilisateur pour administrer le portail. Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, le concepteur Novell pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), vous devez accorder à cet administrateur des droits d'ayant droit sur les instances d'objets contenues dans le pilote de l'application utilisateur. Reportez-vous au *Guide d'administration de l'application utilisateur IDM* pour en savoir plus. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.
NOVL_CONFIG_PROVLOCKSMITH=	DN eDirectory : admin. de l'application de provisioning. Ce rôle est disponible dans la version de provisioning d'Identity Manager 3.5.1. L'administrateur de l'application de provisioning utilise l'onglet *Provisioning* (sous l'onglet *Administration*) pour gérer les fonctions de workflow du provisioning. Ces fonctions sont accessibles aux utilisateurs en passant par l'onglet *Requêtes et approbations* de l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur de l'application Provisioning. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.
NOVL_CONFIG_USERCONTAINERDN=	Identité utilisateur du méta-annuaire : DN du conteneur utilisateur. Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur utilisateur. Cela définit l'étendue de recherche d'utilisateurs et de groupes. Les utilisateurs de ce conteneur (et en-dessous) sont autorisés à se loguer à l'application utilisateur. **Important :** assurez-vous que l'administrateur de l'application utilisateur spécifié lors de la configuration des pilotes de l'application utilisateur existe dans ce conteneur si vous souhaitez que cet utilisateur soit en mesure d'exécuter les workflows.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur et description
NOVL_CONFIG_GROUPCONTAINERDN=	Groupes d'utilisateurs du méta-annuaire : DN du conteneur de groupes. Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur de groupes. Utilisé par les définitions d'entités au sein de la couche d'abstraction d'annuaire.
NOVL_CONFIG_KEYSTOREPATH=	Certificats eDirectory : chemin d'accès au keystore. Requis. Indiquez le chemin d'accès complet au fichier (`cacerts`) de votre keystore du JRE que le serveur d'applications utilise. L'installation de l'application utilisateur modifie le fichier keystore. Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier.
NOVL_CONFIG_KEYSTOREPASSWORD=	Certificats eDirectory : mot de passe du keystore. Requis. Indiquez le mot de passe `cacerts`. L'unité par défaut est `changeit`.
NOVL_CONFIG_SECUREADMINCONNECTION=	Paramètres de login eDirectory : login admin sécurisé. Indiquez Vrai pour exiger que toutes les communications utilisant le compte admin. soient effectuées à l'aide d'un socket sécurisé (cette option peut avoir des implications néfastes sur la performance). Indiquez Faux si le compte admin. n'utilise pas de communication à socket sécurisé.
NOVL_CONFIG_SECUREUSERCONNECTION=	Paramètres de login eDirectory : login·utilisateur sécurisé. Indiquez Vrai pour exiger que toutes les communications sur le compte de l'utilisateur logué soient effectuées via un socket sécurisé (cette option peut avoir de graves implications sur la performance). Indiquez Faux si le compte utilisateur n'utilise pas de communication par socket sécurisé.
NOVL_CONFIG_SESSIONTIMEOUT=	Divers : timeout de session. Indiquez un intervalle de timeout de session d'application.
NOVL_CONFIG_LDAPPLAINPORT=	Paramètres de login eDirectory : port non sécurisé LDAP. Indiquez le port non sécurisé de votre serveur LDAP, par exemple 389.
NOVL_CONFIG_LDAPSECUREPORT=	Paramètres de login eDirectory : port sécurisé LDAP. Indiquez le port sécurisé de votre serveur LDAP, par exemple 636.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur et description
NOVL_CONFIG_ANONYMOUS=	Paramètres de login eDirectory : utiliser un compte anonyme public. Indiquez vrai pour permettre aux utilisateurs non logués d'accéder au compte anonyme public LDAP. Indiquez Faux pour activer NOVL_CONFIG_GUEST à la place.
NOVL_CONFIG_GUEST=	Paramètres de login eDirectory : guest LDAP. Permet aux utilisateurs non logués d'accéder à des portlets autorisés. Vous devez également désélectionner *Utiliser un compte anonyme public*. Le compte utilisateur Guest doit déjà exister dans le coffre-fort d'identité. Pour désactiver l'utilisateur Guest, sélectionnez *Utiliser un compte anonyme public*.
NOVL_CONFIG_GUESTPASS=	Paramètres de login eDirectory : mot de passe Guest LDAP.
NOVL_CONFIG_EMAILNOTIFYHOST=	Courrier électronique : jeton HÔTE du modèle de notification. Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple : `myapplication serverServer` Cette valeur remplace le jeton $HOST$ des modèles de courrier électronique. L'URL construite est la liaison aux tâches de requête de provisioning et aux notifications d'approbation.
NOVL_CONFIG_EMAILNOTIFYPORT=	Courrier électronique : jeton du port du modèle de notification. Utilisé pour remplacer le jeton $PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	Courrier électronique : jeton du port sécurisé du modèle de notification. Utilisé pour remplacer le jeton $SECURE_PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
NOVL_CONFIG_NOTFSMTPEMAILFROM=	Courrier électronique : notification SMTP - expéditeur du courrier électronique. Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
NOVL_CONFIG_NOTFSMTPEMAILHOST=	Courrier électronique : notification SMTP - destinataire du courrier électronique. Indiquez l'utilisateur destinataire du courrier électronique SMTP que le message de provisioning utilise. Il peut s'agir d'une adresse IP ou d'un nom DNS.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur et description
NOVL_CONFIG_USEEXTPWDWAR=	Gestion des mots de passe : utiliser un WAR de mots de passe externe. Indiquez Vrai si vous utilisez un WAR de gestion de mots de passe externe. Si vous indiquez Vrai, vous devez également fournir des valeurs pour *NOVL_CONFIG_EXTPWDWARPTH* et *NOVL_CONFIG_EXTPWDWARRTNPATH*. Indiquez Faux pour utiliser la fonction de gestion des mots de passe interne par défaut. `/jsps/pwdmgt/ForgotPassword.jsf` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.
NOVL_CONFIG_EXTPWDWARPATH=	Gestion des mots de passe : liaison Mot de passe oublié. Indiquez l'URL de la page de la fonction Mot de passe oublié, `ForgotPassword.jsf`, dans un WAR de gestion de mots de passe externe ou interne. Vous pouvez également accepter le WAR de gestion des mots de passe interne par défaut. Pour plus de détails, reportez-vous à « Utilisation des WAR de mots de passe » page 144.
NOVL_CONFIG_EXTPWDWARRTNPATH=	Gestion des mots de passe : liaison de retour Mot de passe oublié. Si vous utilisez un WAR de gestion des mots de passe externe, indiquez le chemin d'accès que le WAR de gestion des mots de passe externe utilise pour rappeler l'application utilisateur par des services Web, par exemple `https://idmhost:sslport/idm`.
NOVL_CONFIG_USEROBJECTATTRIBUTE=	Identité utilisateur du méta-annuaire : classe d'objets utilisateur. La classe d'objets utilisateur LDAP (généralement inetOrgPerson).
NOVL_CONFIG_LOGINATTRIBUTE=	Identité utilisateur du méta-annuaire : attribut de login. L'attribut LDAP (par exemple, CN) qui représente le nom de login de l'utilisateur.
NOVL_CONFIG_NAMINGATTRIBUTE=	Identité utilisateur du méta-annuaire : attribut d'assignation de nom. L'attribut LDAP utilisé comme identifiant lors de la consultation d'utilisateurs ou de groupes. Il est différent de l'attribut de login, qui n'est utilisé que lors du login, et non pas lors des recherches d'utilisateurs/de groupes.
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	Identité utilisateur du méta-annuaire : attribut d'adhésion utilisateur. Facultatif. L'attribut LDAP qui représente l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur et description
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	Groupes d'utilisateurs du méta-annuaire : classe d'objets Groupe. La classe d'objets Groupe LDAP (généralement groupofNames).
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	Groupes d'utilisateurs du méta-annuaire : attribut d'adhésion à un groupe. Indiquez l'attribut représentant l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.
NOVL_CONFIG_USEDYNAMICGROUPS=	Groupes d'utilisateurs du méta-annuaire : utiliser des groupes dynamiques. Indiquez Vrai pour l'utilisation de groupes dynamiques. Sinon, indiquez Faux.
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	Groupes d'utilisateurs du méta-annuaire : classe d'objets de groupe dynamique. Indiquez la classe d'objets de groupe dynamique LDAP (généralement dynamicGroup).
NOVL_CONFIG_PRIVATESTOREPATH=	Keystore privé : chemin du keystore privé. Indiquez le chemin d'accès au keystore privé qui contient la clé privée et les certificats de l'application utilisateur. Réservé. Si vous laissez ce champ vierge, ce chemin d'accès est `/jre/lib/security/cacerts` par défaut.
NOVL_CONFIG_PRIVATESTOREPASSWORD=	Keystore privé : mot de passe du keystore privé.
NOVL_CONFIG_PRIVATEKEYALIAS=	Keystore privé : alias de clé privée. Cet alias est `novellIDMUserApp` à moins d'indication contraire.
NOVL_CONFIG_PRIVATEKEYPASSWORD=	Keystore privé : mot de passe de clé privée.
NOVL_CONFIG_TRUSTEDSTOREPATH=	Keystore approuvé : chemin de keystore approuvé. Le keystore approuvé contient tous les certificats approuvés des signataires utilisés pour valider les signatures numériques. Si ce chemin est vide, l'application utilisateur obtient le chemin à partir de la propriété Système `javax.net.ssl.trustStore`. Si le chemin n'y est pas, il est supposé être `jre/lib/security/cacerts`.
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	Keystore approuvé : mot de passe du keystore approuvé.
NOVL_CONFIG_AUDITCERT=	Certificat de signature numérique Novell Audit.
NOVL_CONFIG_AUDITKEYFILEPATH=	Chemin de fichier du keystore privé de signatures numériques Novell Audit.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur et description
NOVL_CONFIG_ICSLOGOUTENABLED=	Paramètres iChain : logout ICS activé. Indiquez Vrai pour activer le logout simultané de l'application utilisateur et de iChain ou de Novell Access Manager. L'application utilisateur recherche un cookie iChain ou Novell Access Manager au logout et, en cas de présence du cookie, réachemine l'utilisateur vers la page de logout ICS. Indiquez Faux pour désactiver le logout simultané.
NOVL_CONFIG_ICSLOGOUTPAGE=	Paramètres iChain : page de logout ICS. Indiquez l'URL vers la page de logout de iChain ou Novell Access Manager, où l'URL est un nom d'hôte auquel iChain ou Novell Access Manager s'attend. Si le login à ICS est activée et si un utilisateur se délogue de l'application utilisateur, il est réacheminé vers cette page.
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	Courrier électronique : jeton PROTOCOLE du modèle de notification. Se rapporte à un protocole non sécurisé, HTTP. Utilisé pour remplacer le jeton $PROTOCOL$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	Courrier électronique : jeton du port sécurisé du modèle de notification.
NOVL_CONFIG_OCSPURI=	Divers : OCSP URI. Si l'installation client utilise le protocole OCSP (protocole de propriété d'état de certificat en ligne), fournissez un identificateur de ressource uniforme (URI). Par exemple, le format est http://hstport/ocspLocal. L'URI OCSP met à jour le statut des certificats approuvés en ligne.
NOVL_CONFIG_AUTHCONFIGPATH=	Divers : chemin de configuration d'autorisation. Le nom complet du fichier de configuration de l'autorisation.

5.9 Tâches post-installation

Une fois l'application utilisateur installée et configurée, passez aux tâches post-installation.

- Section 5.9.8, « Configuration de votre équipe de provisioning et de ses requêtes », page 186
- Section 5.9.9, « Création d'index dans eDirectory », page 186

5.9.1 Enregistrement de la clé maîtresse

Immédiatement après l'installation, copiez la clé maîtresse codée et enregistrez-la en lieu sûr.

1. Ouvrez le fichier `master-key.txt` dans le répertoire d'installation.
2. Copiez la clé maîtresse codée dans un emplacement sûr accessible en cas de défaillance système.

Avertissement : conservez toujours une copie de la clé maîtresse codée. Vous avez besoin de la clé maîtresse codée pour accéder à nouveau aux données codées en cas de perte de la clé maîtresse, par exemple en raison d'une défaillance de l'équipement.

Si cette installation est sur le premier membre d'une grappe , utilisez cette clé maîtresse codée lors de l'installation de l'application utilisateur sur d'autres membres de la grappe.

Pour plus d'informations sur la clé maîtresse, reportez-vous aux sections du *Guide d'administration de l'application utilisateur Identity Manager* (http://www.novell.com/documentation/idm35/index.html) sur le *Codage des données sensibles de l'application utilisateur* et la *mise en grappe JBoss*.

5.9.2 Vérification de vos installations de grappes

Vérifiez vos installations de grappes. Vérifiez que chaque serveur JBoss d'une grappe JBoss possède :

- Un nom de partition unique (nom de partition)
- Un UDP de partition unique (partition.udpGroup)
- Un ID de moteur de workflow unique
- le même fichier WAR (identique). Le WAR est inscrit par l'installation dans le répertoire `jboss\server\IDM\deploy` par défaut.

Vérifiez que chaque serveur d'une grappe WebSphere a un ID de moteur de workflow unique.

Pour plus d'informations, reportez-vous à la section sur la mise en grappe au chapitre 4 du *Guide d'administration de l'application utilisateur Identity Manager* (http://www.novell.com/documentation/idm35/index.html).

5.9.3 Configuration de communication SSL entre serveurs JBoss

Si vous sélectionnez *Utiliser le WAR de mot de passe externe* dans le fichier de configuration de l'application utilisateur lors de l'installation, vous devez configurer la communication SSL entre les serveurs JBoss sur lesquels vous déployez le WAR de l'application utilisateur et le fichier `IDMPwdMgt.war`. Reportez-vous à votre documentation JBoss pour obtenir des directives.

5.9.4 Accès au WAR de mots de passe externe

Si vous avez un WAR de mots de passe externe et si vous souhaitez tester la fonction Mot de passe oublié, vous pouvez y accéder dans deux emplacements :

- Dans un navigateur. Allez sur la page Mot de passe oublié dans le WAR de mots de passe externe, par exemple `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`.
- Dans la page de login de l'application utilisateur, cliquez sur le lien *Mot de passe oublié*.

5.9.5 Mise à jour des paramètres Mot de passe oublié

Vous pouvez modifier les valeurs de la *liaison Mot de passe oublié* et de la *liaison retour Mot de passe oublié* après l'installation. Utilisez l'utilitaire configupdate ou l'application utilisateur.

Utilisation de l'utilitaire configupdate: sur une ligne de commande, naviguez jusqu'au répertoire d'installation et entrez `configupdate.sh` (Linux ou Solaris) ou `configupdate.bat` (Windows). Si vous créez ou modifiez un WAR de gestion de mots de passe externe, vous devez alors renommer manuellement le WAR avant de le copier sur le serveur distant JBoss.

Utilisation de l'application utilisateur: loguez-vous en tant qu'administrateur de l'application utilisateur et allez dans *Administration* > *Configuration application* > *Configuration module mot de passe* > *Login*. Modifiez les champs suivants :

- *Liaison Mot de passe oublié* (par exemple : `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`)
- *Liaison retour Mot de passe oublié* (par exemple : `https://idmhost:sslport/idm`)

5.9.6 Configuration de la notification par message électronique

Pour mettre en oeuvre les fonctions de notification par message électronique Mot de passe oublié et Workflow :

1. Dans iManager, sous Rôles et tâches, sélectionnez *Administration du workflow*, puis sélectionnez *Options du serveur de messagerie*.
2. Spécifiez votre nom de serveur SMTP sous *Nom d'hôte*.
3. Près de *De*, indiquez une adresse électronique (par exemple, *noreply@novell.com*), puis cliquez sur *OK*.

5.9.7 Tester l'installation sur le serveur d'applications JBoss

1. Démarrez votre base de données. Reportez-vous à la documentation de votre base de données pour obtenir des directives.
2. Démarrez le serveur de l'application utilisateur (JBoss). Sur la ligne de commande, faites du répertoire d'installation votre répertoire de travail et exécutez le script suivant (fourni par l'installation de l'application utilisateur) :

   `start-jboss.sh` (Linux et Solaris)

   `start-jboss.bat` (Windows)

Si vous devez interrompre le serveur d'applications, utilisez `stop-jboss.sh` ou `stop-jboss.bat`, ou fermez la fenêtre dans laquelle `start-jboss.sh` ou `start-jboss.bat` est exécuté.

3 Démarrez le pilote d'application utilisateur. Cela active la communication vers le pilote de l'application utilisateur.

3a Loguez-vous à iManager.

3b Sur l'écran des Rôles et tâches dans la trame de navigation de gauche, sélectionnez *Présentation Identity Manager* sous *Identity Manager*.

3c Sur l'affichage du contenu, spécifiez l'ensemble de pilotes qui contient le pilote de l'application utilisateur, puis cliquez sur *Rechercher*. Un graphique s'affiche, indiquant l'ensemble de pilotes avec ses pilotes associés.

3d Cliquez sur l'icône rouge et blanche sur le pilote.

3e Sélectionnez *Démarrer le pilote*. Le statut du pilote change et passe au symbole du yin et du yang, indiquant que le pilote est démarré.

Le pilote, au démarrage, tente une « reconnaissance mutuelle » avec l'application utilisateur. Si votre serveur d'applications n'est pas en cours d'exécution ou si le WAR n'a pas été correctement déployé, le pilote renvoie une erreur.

4 Pour lancer et se loguer à l'application utilisateur, utilisez votre navigateur Web pour aller sur l'URL suivante :

http:// *nomhôte*:*port*/ *NomApplication*

Là où *nomhôte*:*port* est le nom d'hôte du serveur d'applications (par exemple, myserver.domain.com) et le port est le port de votre serveur d'applications (par exemple, 8080 par défaut sur JBoss). *NomApplication* est IDM par défaut. Vous avez spécifié le nom de l'application lors de l'installation lorsque vous avez fourni les informations de configuration du serveur d'applications.

La page de renvoi de l'application utilisateur Novell Identity Manager doit s'afficher.

5 Dans le coin supérieur droit de cette page, cliquez sur *Login* pour vous loguer à l'application utilisateur.

Si la page de l'application utilisateur Identity Manager ne s'affiche pas dans votre navigateur à la suite de ces étapes, vérifiez l'absence de messages d'erreur sur la console du terminal et reportez-vous à Section 5.11, « Dépannage », page 187.

5.9.8 Configuration de votre équipe de provisioning et de ses requêtes

Configurez votre équipe de provisioning et les requêtes de votre équipe de provisioning pour permettre les tâches de workflow. Pour obtenir des directives, reportez-vous au *Guide d'administration de l'application utilisateur Identity Manager 3.5.1* (http://www.novell.com/documentation/idm35/index.html).

5.9.9 Création d'index dans eDirectory

Pour une meilleure performance de l'application utilisateur IDM, l'administrateur eDirectory doit créer des index pour les attributs manager, ismanager et srvprvUUID. Sans index pour ces attributs, les utilisateurs de l'application utilisateur peuvent connaître la performance de l'application utilisateur se réduire, en particulier dans un environnement à grappes. Reportez-vous au *Guide*

d'administration Novell eDirectory (http://www.novell.com/documentation) pour obtenir des directives sur l'utilisation du Gestionnaire d'index pour créer des index.

5.10 Reconfiguration du fichier WAR IDM après l'installation

1. Exécutez l'utilitaire ConfigUpdate dans le répertoire d'installation de l'application utilisateur en exécutant `configupdate.sh` ou `configupdate.bat`. Cela permet de mettre à jour le fichier WAR dans le répertoire d'installation.

   Pour plus d'informations sur les paramètres de l'utilitaire ConfigUpdate, reportez-vous à Section 5.5.14, « Configuration de l'application utilisateur », page 130 ou à Section 5.6.9, « Configuration de l'application utilisateur », page 156.

2. Déployez le nouveau fichier WAR sur votre serveur d'applications.

5.11 Dépannage

Votre représentant Novell passera en revue tout problème de configuration avec vous. En attendant, voici quelques points à vérifier en cas de problème.

Tableau 5-9 *Dépannage de l'application utilisateur*

Point	Actions suggérées

Vous souhaitez modifier les paramètres de configuration de l'application utilisateur définis lors de l'installation. Cela comprend la configuration des éléments suivants par exemple :
◆ Logins·et certificats du coffre-fort d'identité
◆ Paramètres de messagerie électronique
◆ Identité utilisateur du méta-annuaire, groupes d'utilisateurs
◆ Paramètres iChain
	Vous pouvez exécuter l'utilitaire de configuration indépendamment du programme d'installation.
	Sous Linux et Solaris, exécutez la commande suivante depuis le répertoire d'installation (par défaut, `/opt/novell/idm`):
	`configupdate.sh`
	Sous Windows, exécutez la commande suivante depuis le répertoire d'installation (par défaut, `c:\opt\novell\idm`) :
	`configupdate.bat`

Des exceptions apparaissent lorsque le serveur d'application démarre, avec un message de journal `port 8080 déjà en cours d'utilisation.`	Arrêter toute instance de Tomcat (ou autre logiciel de serveur) qui pourrait déjà être en cours d'exécution. Si vous décidez de reconfigurer le serveur d'applications de façon à ce qu'il utilise un port autre que 8080, n'oubliez pas de modifier les paramètres `config` pour le pilote de l'application utilisateur dans iManager.
Au démarrage du serveur d'applications, un message s'affiche indiquant qu'aucun certificat approuvé n'a été trouvé.	Assurez-vous de démarrer le serveur d'applications via le JDK spécifié dans l'installation de l'application utilisateur.
Vous ne pouvez pas vous loguer à la page d'administration du portail.	Assurez-vous que le compte administrateur de l'application utilisateur existe. Ne le confondez pas avec votre compte administrateur iManager. Il s'agit de deux objets admin. différents (normalement).

Point	Actions suggérées
Vous pouvez vous loguer en tant qu'administrateur, mais vous ne pouvez pas créer de nouveaux utilisateurs.	L'administrateur de l'application utilisateur doit être un ayant droit du conteneur maître et doit avoir des droits de superviseur. En attendant, vous pouvez essayer de configurer les droits administrateur de l'application utilisateur équivalents aux droits administrateur LDAP (via iManager).
Au démarrage du serveur d'applications, il y a des erreurs de login à MySQL.	N'exécutez rien en tant qu'utilisateur `root`. (Ce problème est cependant improbable si vous exécutez la version de MySQL fournie avec IDM.) Assurez-vous que MySQL fonctionne (et que la copie correcte est exécutée). Détruisez toute autre instance de MySQL. Exécutez `/idm/mysql/start-mysql.sh`, puis `/idm/start-jboss.sh`. Examinez `/idm/mysql/setup-mysql.sh` dans un éditeur de texte et corrigez toute valeur qui semble suspecte. Exécutez ensuite le script, puis `/idm/start-jboss.sh`.
Vous rencontrez des erreurs de keystore lors du démarrage du serveur d'applications.	Votre serveur d'applications n'exécute pas le JDK spécifié à l'installation de l'application utilisateur. Utilisez la commande `keytool` pour importer le fichier de certificat : `keytool -import -trustcacerts -alias` *`aliasName`* `-file` *`certFile`* `-keystore ..\lib\security\cacerts -storepass changeit` ◆ Remplacez *aliasName* par un nom unique de votre choix pour ce certificat. ◆ Remplacez *certFile* par le chemin complet et le nom de votre fichier de certificat. ◆ Le mot de passe du keystore par défaut est `changeit` (si vous avez un mot de passe différent, indiquez-le).

Aucune notification n'a été envoyée par courrier électronique.	Exécutez l'utilitaire configupdate pour vérifier si vous avez fourni les valeurs des paramètres de configuration de l'expéditeur du courrier électronique et de l'hôte de courrier électronique de l'application utilisateur.
	
	Sous Linux et Solaris, exécutez la commande suivante depuis le répertoire d'installation (par défaut, `/opt/novell/idm`) :
	`configupdate.sh`
	
	Sous Windows, exécutez la commande suivante depuis le répertoire d'installation (par défaut, `c:\opt\novell\idm`) :
	`configupdate.bat`

Activation des produits Novell Identity Manager

6

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

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

- Achat d'une licence de produit Identity Manager
- Activation des produits Identity Manager à l'aide d'une référence
- Installation d'une référence d'activation de produit
- Affichage des activations de produits pour Identity Manager et les pilotes

6.1 Achat d'une licence de produit Identity Manager

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

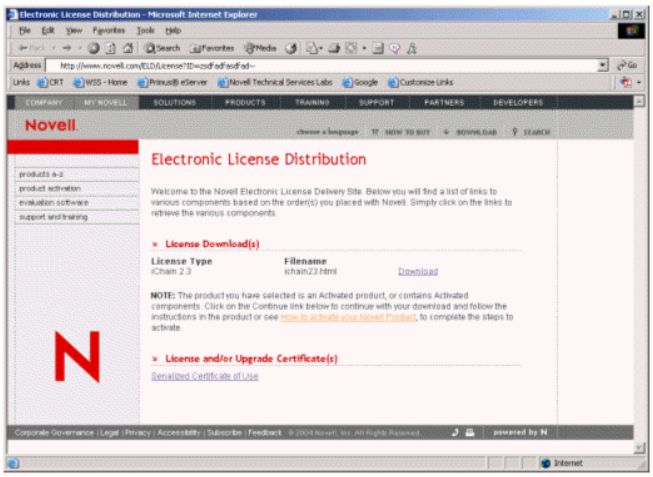
Une fois la licence de produit achetée, Novell vous envoie votre ID client par courrier électronique. Le courrier électronique contient également une URL vers le site Novell sur lequel vous pouvez obtenir une référence. Si vous ne vous en souvenez pas ou si vous ne recevez pas votre ID client, appelez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

6.2 Activation des produits Identity Manager à l'aide d'une référence

1 Une fois la licence achetée, Novell vous envoie un courrier électronique avec votre ID client. Ce courrier électronique contient également un lien sous la section Détail de la commande vers le site sur lequel vous pouvez obtenir votre référence. Cliquez sur le lien pour aller sur le site.

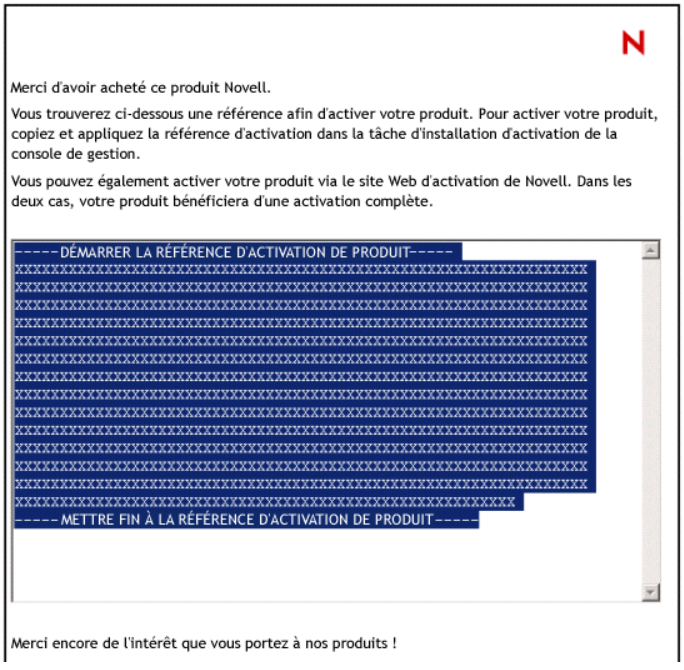
Important : ce courrier électronique n'est pas nécessaire pour activer le produit. Si le courrier électronique a été envoyé à quelqu'un d'autre dans votre entreprise, contactez le centre d'activation Novell pour plus d'informations.

Après avoir cliqué sur le lien, une page similaire à celle qui suit doit s'afficher :



2 Cliquez sur le lien de téléchargement de la licence pour enregistrer (télécharger) ou ouvrir le fichier `html`.

Le fichier que vous ouvrez doit présenter le même contenu que celui illustré ci-dessous :



3 Passez à Section 6.3, « Installation d'une référence d'activation de produit », page 191 pour obtenir des instructions sur l'activation des composants Identity Manager.

6.3 Installation d'une référence d'activation de produit

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

1. Ouvrez le message électronique de Novell qui contient la référence d'activation du produit.
2. Effectuez l'une des opérations suivantes :
   - Enregistrez le fichier de référence d'activation du produit.

     ou

   - Ouvrez le fichier de référence d'activation du produit, puis copiez son contenu dans le Presse-papiers. Copiez attentivement le contenu et veillez à n'inclure aucune ligne ni aucun espace supplémentaire. Vous devez commencer la copie à partir du premier tiret (-) de la référence (----DÉBUT DE LA RÉFÉRENCE D'ACTIVATION DU PRODUIT) jusqu'au dernier tiret (-) de la référence (FIN DE LA RÉFÉRENCE D'ACTIVATION DU PRODUIT-----).
3. Ouvrez iManager.
4. Sélectionnez *Identity Manager > Présentation d'Identity Manager*.
5. Sélectionnez l'ensemble de pilotes requis ou recherchez-en un autre, puis cliquez sur *Suivant*.
6. Sur la page de présentation d'Identity Manager, localisez l'ensemble de pilotes, cliquez sur le lien *Activation requise par* en rouge, puis cliquez sur *Installer l'activation*.
7. Sélectionnez l'ensemble de pilotes sur lequel vous voulez activer un composant Identity Manager.
8. 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*.
9. 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.

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

Pour chacun de vos ensembles de pilotes, vous pouvez afficher les références d'activation des produits que vous avez installés pour le moteur méta-annuaire et les pilotes Identity Manager. Pour afficher les références d'activation de produit :

1. Ouvrez iManager.
2. Cliquez sur *Identity Manager > Présentation d'Identity Manager.*
3. Dans le champ Nom de l'objet, indiquez le nom de l'ensemble de pilotes ou du pilote dont vous voulez afficher les informations d'activation.

ou

Recherchez et sélectionnez l'ensemble de pilotes ou le pilote pour lequel vous souhaitez afficher les informations d'activation.

4. Localisez l'ensemble de pilotes pour lequel vous souhaitez afficher les informations d'activation, puis cliquez sur le nom de l'ensemble de pilotes.
5. Sélectionnez l'onglet *Activation*.

   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.
