

# Novell

## Module de provisioning basé sur les rôles Identity Manager

3.6

[www.novell.com](http://www.novell.com)

21 janvier 2008

GUIDE D'INSTALLATION DE  
L'APPLICATION UTILISATEUR



Novell®

## Mentions légales

Novell, Inc. n'accorde aucune garantie, explicite ou implicite, quant au contenu et à l'utilisation de cette documentation, y compris toute garantie de bonne qualité marchande ou d'aptitude à un usage particulier. Novell se réserve en outre le droit de réviser cette publication à tout moment et sans préavis de ces modifications à quiconque.

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 préavis de ces modifications à quiconque.

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

Copyright © 2008 Novell, Inc. Tous droits réservés. Cette publication ne peut être reproduite, photocopiée, stockée sur un système de recherche documentaire ou transmise, même en partie, sans le consentement écrit explicite préalable de l'éditeur.

Novell, Inc. dispose de droits de propriété intellectuelle sur la technologie intégrée dans le 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 Novell relatif aux mentions légales \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) (en anglais) et un ou plusieurs brevets supplémentaires ou en cours d'homologation aux États-Unis et dans d'autres pays.

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
États-Unis  
[www.novell.com](http://www.novell.com)

*Documentation en ligne* : pour accéder à la documentation en ligne la plus récente de ce produit et des autres produits Novell ou pour obtenir des mises à jour, reportez-vous au site Novell de documentation (<http://www.novell.com/documentation>).

## **Marques de Novell**

Pour connaître les marques commerciales de Novell, reportez-vous à la [liste des marques commerciales et des marques de service de Novell \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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

<b>À propos de ce guide</b>	<b>7</b>
<b>1 Présentation</b>	<b>9</b>
1.1 Présentation de l'installation	9
1.2 À propos du programme d'installation	10
1.3 Configuration système requise	10
<b>2 Conditions préalables à l'installation</b>	<b>19</b>
2.1 Kit de développement Java	19
2.2 Installation du méta-annuaire Identity Manager	20
2.3 Installation du serveur d'applications JBoss	20
2.3.1 Installation du serveur d'applications JBoss et de la base de données MySQL	21
2.3.2 Installation du serveur d'applications JBoss en tant que service	24
2.4 Installation du serveur d'applications WebSphere	25
2.5 Bases de données	25
2.5.1 Installation de MySQL	25
2.5.2 Configuration de votre base de données MySQL	26
2.6 Conditions préalables de la sécurité	27
2.7 Téléchargement du produit	27
2.8 Installation du contenu du fichier prerequisitefiles.zip	28
2.8.1 Extension du schéma eDirectory de la version 3.6 du module de provisioning basé sur les rôles d'Identity Manager	29
2.8.2 Copie du fichier JAR du pilote de service de rôle	30
2.8.3 Copie du fichier de configuration du pilote de service de rôle	31
2.8.4 Copie du fichier de configuration du pilote d'application utilisateur	31
2.8.5 Copie du fichier dirxml.lsc	31
2.9 Installation des icônes iManager destinées aux rôles	32
<b>3 Création de pilotes</b>	<b>33</b>
3.1 Création du pilote d'application utilisateur dans iManager	33
3.2 Création du pilote de service de rôle dans iManager	37
<b>4 Installation de JBoss depuis une interface graphique</b>	<b>39</b>
4.1 Lancement de l'interface utilisateur graphique du programme d'installation	39
4.2 Choix d'une plate-forme de serveur d'applications	40
4.3 Migration de votre base de données	41
4.4 Emplacement du WAR	43
4.5 Choix d'un dossier d'installation	43
4.6 Choix d'une plate-forme de base de données	44
4.7 Spécification de l'hôte et du port de la base de données	45
4.8 Spécification du nom de la base de données et de l'utilisateur privilégié	46
4.9 Spécification du répertoire racine Java	47
4.10 Choix du type de configuration du serveur d'applications	48
4.11 Spécification des paramètres du serveur d'applications JBoss	50
4.12 Activation de la consigne Novell Audit	50

4.13	Spécification d'une clé maîtresse . . . . .	52
4.14	Configuration de l'application utilisateur . . . . .	53
4.15	Utilisation des WAR de mots de passe . . . . .	67
4.15.1	Spécification d'un WAR de gestion des mots de passe externe . . . . .	67
4.15.2	Spécification d'un WAR de mot de passe interne . . . . .	68
4.16	Vérification des choix et installation . . . . .	68
4.17	Affichage des fichiers journaux. . . . .	69
<b>5</b>	<b>Installation depuis la console ou à l'aide d'une commande unique</b>	<b>71</b>
5.1	Installation de l'application utilisateur à partir de la console . . . . .	71
5.2	Installation de l'application utilisateur avec une seule commande . . . . .	71
<b>6</b>	<b>Installation sur un serveur d'applications WebSphere</b>	<b>81</b>
6.1	Lancement de l'interface utilisateur graphique du programme d'installation . . . . .	81
6.2	Choix d'une plate-forme de serveur d'applications. . . . .	82
6.3	Emplacement du WAR . . . . .	83
6.4	Choix d'un dossier d'installation . . . . .	84
6.5	Choix d'une plate-forme de base de données . . . . .	85
6.6	Spécification du répertoire racine Java . . . . .	86
6.7	Activation de la consignment Novell Audit . . . . .	87
6.8	Spécification d'une clé maîtresse . . . . .	89
6.9	Configuration de l'application utilisateur . . . . .	90
6.10	Vérification des choix et installation . . . . .	105
6.11	Affichage des fichiers journaux. . . . .	106
6.12	Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM . . . . .	106
6.13	Importation de la racine approuvée d'eDirectory dans la zone de stockage des clés WebSphere. . . . .	107
6.13.1	Importation de certificats avec la console de l'administrateur WebSphere . . . . .	108
6.13.2	Importation de certificats avec la ligne de commande . . . . .	108
6.14	Déploiement du fichier WAR IDM. . . . .	108
6.15	Démarrage de l'application. . . . .	109
6.16	Accès au portail de l'application utilisateur . . . . .	109
<b>7</b>	<b>Tâches post-installation</b>	<b>111</b>
7.1	Enregistrement de la clé maîtresse . . . . .	111
7.2	Configuration de post-installation . . . . .	111
7.3	Vérification de vos installations de grappes . . . . .	112
7.4	Configuration de la communication SSL entre serveurs JBoss . . . . .	112
7.5	Accès au WAR de mots de passe externe . . . . .	112
7.6	Mise à jour des paramètres Mot de passe oublié. . . . .	112
7.7	Configuration de la notification par message électronique. . . . .	113
7.8	Tester l'installation sur le serveur d'applications JBoss . . . . .	113
7.9	Configuration de votre équipe de provisioning et de ses requêtes. . . . .	114
7.10	Création d'index dans eDirectory . . . . .	114
7.11	Reconfiguration du fichier WAR IDM après l'installation . . . . .	115
7.12	Dépannage . . . . .	115

# À propos de ce guide

La version 3.6 du module de provisioning basé sur les rôles d'Identity Manager (Identity Manager Roles Based Provisioning Module 3.6) de Novell® comprend une application utilisateur Identity Manager de provisioning basé sur les rôles. Le présent guide décrit l'installation de la version 3.6 de ce module et aborde les points suivants :

- ♦ [Chapitre 1, « Présentation », page 9](#)
- ♦ [Chapitre 2, « Conditions préalables à l'installation », page 19](#)
- ♦ [Chapitre 3, « Création de pilotes », page 33](#)
- ♦ [Chapitre 4, « Installation de JBoss depuis une interface graphique », page 39](#)
- ♦ [Chapitre 5, « Installation depuis la console ou à l'aide d'une commande unique », page 71](#)
- ♦ [Chapitre 6, « Installation sur un serveur d'applications WebSphere », page 81](#)
- ♦ [Chapitre 7, « Tâches post-installation », page 111](#)

## Public

Ce guide s'adresse aux administrateurs et aux consultants qui planifieront et mettront en oeuvre le module de provisioning basé sur les rôles d'Identity Manager.

## Commentaires

Nous souhaiterions connaître vos commentaires et suggestions sur ce guide et les autres documentations fournies avec ce produit. Utilisez la fonction Commentaires des utilisateurs au bas de chaque page de la documentation en ligne ou saisissez vos commentaires dans la page [www.novell.com/documentation/feedback.html](http://www.novell.com/documentation/feedback.html).

## Documentation supplémentaire

Pour plus d'informations sur le module de provisioning basé sur les rôles d'Identity Manager, reportez-vous au [site Web de documentation d'Identity Manager \(http://www.novell.com/documentation/lg/dirxml/drivers/index.html\)](http://www.novell.com/documentation/lg/dirxml/drivers/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 requièrent une barre oblique normale, comme Linux\* ou UNIX\*, doivent utiliser ces barres obliques comme l'exige leur logiciel.





# Présentation

# 1

Cette section présente l'installation du produit et décrit la configuration système requise. Les rubriques incluent :

- ♦ [Section 1.1, « Présentation de l'installation », page 9](#)
- ♦ [Section 1.2, « À propos du programme d'installation », page 10](#)
- ♦ [Section 1.3, « Configuration système requise », page 10](#)

## 1.1 Présentation de l'installation

La procédure d'installation du module Provisioning d'Identity Manager basé sur les rôles de Novell® installe une application utilisateur prenant en charge les rôles et le module de provisioning basé sur les rôles. Les étapes de l'installation sont les suivantes :

- 1 Si vous migrez vers le module Provisioning d'Identity Manager basé sur les rôles, consultez le manuel *Guide de migration de l'application utilisateur Identity Manager* (<http://www.novell.com/documentation/idmrbpm36/pdfdoc/migration/migration.pdf>).
- 2 Vérifiez que votre système répond aux exigences de configuration. Reportez-vous à [Section 1.3, « Configuration système requise », page 10](#).
- 3 Installez le méta-annuaire Identity Manager. Pour obtenir les instructions associées à cette procédure, reportez-vous au *Guide d'installation d'Identity Manager 3.5.1* (<http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf>). Vous devez avoir installé le serveur de méta-annuaire Identity Manager pour pouvoir créer les pilotes requis et installer l'application utilisateur et le module Provisioning basé sur les rôles.
- 4 Respectez les conditions requises à l'installation. Reportez-vous à [Chapitre 2, « Conditions préalables à l'installation », page 19](#).
- 5 Recherchez le fichier `prerequisitefiles.zip` dans le répertoire de téléchargement et dézippez-le. Installez ou appliquez manuellement les fichiers dézippés.
- 6 Si vous souhaitez utiliser Designer pour créer et configurer les pilotes, installez Designer 2.1.1. Reportez-vous à la rubrique consacrée à l'installation de Designer ([http://www.novell.com/documentation/designer21/admin\\_guide/index.html?page=/documentation/designer21/admin\\_guide/data/ginstall.html](http://www.novell.com/documentation/designer21/admin_guide/index.html?page=/documentation/designer21/admin_guide/data/ginstall.html)).
- 7 Créez le pilote d'application utilisateur sous iManager ou Designer 2.1.1. Les instructions de création sous iManager figurent dans [Section 3.1, « Création du pilote d'application utilisateur dans iManager », page 33](#).  
Le pilote d'application utilisateur doit déjà exister (sans être activé) avant d'installer l'application utilisateur et le module Provisioning basé sur les rôles de Novell Identity Manager.
- 8 Créez le pilote de service de rôle sous iManager ou Designer 2.1.1. Les instructions de création sous iManager figurent dans [Section 3.2, « Création du pilote de service de rôle dans iManager », page 37](#).  
Le pilote de service de rôle doit déjà exister (sans être activé) avant d'installer l'application utilisateur Novell Identity Manager et le module Provisioning basé sur les rôles.

9 Installez et configurez l'application utilisateur et le module Provisioning basé sur les rôles de Novell Identity Manager. Reportez-vous à :

- ♦ [Chapitre 4, « Installation de JBoss depuis une interface graphique », page 39](#)
- ♦ [Chapitre 5, « Installation depuis la console ou à l'aide d'une commande unique », page 71](#)
- ♦ [Chapitre 6, « Installation sur un serveur d'applications WebSphere », page 81](#)

---

**Remarque :** si vous utilisez WebSphere\*, vous devez déployer le fichier WAR manuellement.

---

10 Exécutez les tâches de post-installation.

## 1.2 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\*, DB2\*, 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 d'archive de l'application Web Java\* (fichier WAR ) pour l'application utilisateur Novell Identity Manager sur le serveur d'applications. Si vous utilisez WebSphere, vous devez déployer le fichier WAR manuellement.
- ♦ Active la consignment Novell Audit si vous la sélectionnez.
- ♦ Permet d'importer une clé maîtresse existante pour restaurer une installation particulière de module Provisioning basé sur les rôles et pour prendre des grappes en charge.

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

- ♦ Interface Utilisateur Graphique. Reportez-vous à [Chapitre 4, « Installation de JBoss depuis une interface graphique », page 39](#) ou à [Chapitre 6, « Installation sur un serveur d'applications WebSphere », page 81](#).
- ♦ Interface de console (ligne de commande). Reportez-vous à [Section 5.1, « Installation de l'application utilisateur à partir de la console », page 71](#).
- ♦ Installation en mode silencieux. Reportez-vous à [Section 5.2, « Installation de l'application utilisateur avec une seule commande », page 71](#).

## 1.3 Configuration système requise

Vous ne pouvez utiliser la version 3.6 du module de provisioning basé sur les rôles d'Identity Manager que si vous avez installé chacun des composants requis indiqués au [Tableau 1-1](#).

**Tableau 1-1** Configuration système requise

Composant système requis	Configuration système requise	Remarques
<p>Système méta-annuaire (Identity Manager 3.5.1)</p> <ul style="list-style-type: none"> <li>◆ Moteur méta-annuaire</li> <li>◆ L'agent Novell Audit</li> <li>◆ Pilotes de service</li> <li>◆ Pilotes Identity Manager</li> <li>◆ Utilitaires (dont les outils d'application et l'outil de configuration Novell Audit)</li> </ul>	<p>L'un des systèmes d'exploitation suivants :</p> <ul style="list-style-type: none"> <li>◆ NetWare® 6.5 SP6</li> <li>◆ Novell Open Enterprise Server (OES) 1.0 avec le dernier Support Pack</li> <li>◆ Novell Open Enterprise Server (OES) 2.0</li> <li>◆ Windows* 2000 Server avec le dernier Service Pack (32 bits)</li> <li>◆ Windows Server 2003 avec le dernier Service Pack (32 bits)</li> <li>◆ Red Hat Linux 3.0, 4.0 ou 5.0 ES et AS (les versions 32 bits et 64 bits sont prises en charge)</li> <li>◆ SUSE Linux Enterprise Server 9 et 10 avec le dernier Support Pack (prise en charge 32 bits et 64 bits)</li> <li>◆ Solaris* 9 ou 10</li> <li>◆ AIX* 5.2L, versions 5.2 ou 5.3</li> </ul> <p>L'une des versions suivantes d'eDirectory™ :</p> <ul style="list-style-type: none"> <li>◆ eDirectory 8.7.3.10</li> <li>◆ eDirectory 8.8.1 ou 8.8.2</li> </ul> <p>Security Services 2.0.5 (NMASTM 3.1.3)</p>	<p>L'utilisation de VMware* dans votre mise en oeuvre est prise en charge si vous utilisez une plate-forme de système méta-annuaire.</p> <p>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. Sauf indication contraire, les plates-formes OES, NetWare, Windows et Linux (Red Hat* et SUSE®) prennent en charge tous les processeurs dans le mode 32 bits :</p> <ul style="list-style-type: none"> <li>◆ Intel* x86-32</li> <li>◆ AMD* x86-32</li> <li>◆ Intel EM64T</li> <li>◆ AMD Athlon64* et Opteron*</li> </ul> <p>Identity Manager prend en charge ces fonctions d'eDirectory 8.8 :</p> <ul style="list-style-type: none"> <li>◆ Instances multiples d'eDirectory sur le même serveur</li> <li>◆ Attributs codés</li> </ul> <p>eDirectory 8.8 prend en charge Red Hat Linux 4.0 64 bits.</p> <p>Une version 64 bits de la synchronisation des mots de passe sur Windows Server 2003 est disponible.</p> <p>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.</p> <p>La virtualisation Xen* est désormais prise en charge sur SUSE Linux Enterprise Server 10 lorsque la machine virtuelle (VM) Xen exécute SLES 10 comme système d'exploitation invité en mode paravirtualisé. Un correctif Xen pour SLES 10 est nécessaire (reportez-vous à TID n° 3915180 (<a href="http://www.novell.com/support/search.do?cmd=displayKC&amp;docType=kc&amp;externalId=3915180&amp;sliceId=SAL_Public&amp;dialogId=52670386&amp;stateId=1%20%204926187">http://www.novell.com/support/search.do?cmd=displayKC&amp;docType=kc&amp;externalId=3915180&amp;sliceId=SAL_Public&amp;dialogId=52670386&amp;stateId=1%20%204926187</a>)).</p>

Composant système requis	Configuration système requise	Remarques
Serveur d'administration basé sur le Web	<p>L'un des systèmes d'exploitation suivants :</p> <ul style="list-style-type: none"> <li>◆ Novell Open Enterprise Server (OES) 1.0 sous NetWare avec le dernier Support Pack</li> <li>◆ Novell Open Enterprise Server (OES) 2.0</li> <li>◆ NetWare 6.5 avec le dernier Support Pack</li> <li>◆ Windows 2000 Server avec le dernier Service Pack (32 bits)</li> <li>◆ Windows Server 2003 avec le dernier Service Pack (32 bits)</li> <li>◆ Microsoft Windows Vista*</li> <li>◆ Red Hat Linux 3.0, 4.0 ou 5.0 ES et AS (prise en charge 32 bits et 64 bits)</li> <li>◆ Solaris* 9 ou 10 avec le dernier Support Pack</li> <li>◆ SUSE Linux Enterprise Server 9 ou 10 avec le dernier Support Pack (prise en charge 32 bits et 64 bits)</li> </ul> <p>Systèmes d'exploitation pris en charge via le poste de travail iManager :</p> <ul style="list-style-type: none"> <li>◆ Windows 2000 Professional avec le dernier Service Pack</li> <li>◆ Windows XP avec SP2</li> <li>◆ SUSE Linux Enterprise Desktop 10</li> <li>◆ SUSE Linux 10.1</li> </ul> <p>Le logiciel suivant :</p> <ul style="list-style-type: none"> <li>◆ Novell iManager 2.6 ou 2.7 avec les derniers Support Pack et plug-ins</li> </ul>	<p>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 :</p> <ul style="list-style-type: none"> <li>◆ Intel x86</li> <li>◆ AMD x86</li> <li>◆ Intel EM64T</li> <li>◆ AMD Athlon64 et Opteron</li> <li>◆ La prise en charge du navigateur est déterminée par iManager 2.6. Cette liste comprend actuellement : <ul style="list-style-type: none"> <li>◆ Internet Explorer* 6, SP1 et versions supérieures</li> <li>◆ Internet Explorer 7</li> <li>◆ Firefox* 2.0 et versions supérieures</li> </ul> </li> <li>◆ Vous devez passer par l'assistant de configuration iManager ou le concepteur pour installer ou déployer le contenu du portail dans eDirectory.</li> <li>◆ (Windows) Le logiciel Novell Client™ 4.9 est disponible sur le <a href="http://download.novell.com/index.jsp">site de téléchargement de logiciels Novell (http://download.novell.com/index.jsp)</a>.</li> <li>◆ 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.</li> <li>◆ Seul l'agent de synchronisation des mots de passe est pris en charge sous Windows 2003 64 bits.</li> </ul>

Composant système requis	Configuration système requise	Remarques
Service de consignation sécurisée	Pour le serveur de consignation sécurisée, un des systèmes d'exploitation suivants :	Les plates-formes OES, NetWare, Windows et Linux (Red Hat et SUSE) prennent en charge tous les processeurs suivants au mode 32 bits :
<ul style="list-style-type: none"> <li>◆ Le serveur de consignation sécurisée</li> <li>◆ L'agent de plate-forme (composant client)</li> <li>◆ Novell Audit 2.0.2 ou Sentinel™ 5.1.3</li> </ul>	<ul style="list-style-type: none"> <li>◆ Novell Open Enterprise Server (OES) 1.0 ou 2.0 avec le dernier Support Pack</li> <li>◆ NetWare 6.5 avec le dernier Support Pack</li> <li>◆ Windows 2000 Server avec le dernier Service Pack (32 bits)</li> <li>◆ Windows Server 2003 avec le dernier Service Pack (32 bits)</li> <li>◆ Red Hat Linux 3.0, 4.0 ou 5.0 AS et ES (32 bits ou 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits)</li> <li>◆ Solaris 9 ou 10 avec le dernier Support Pack</li> <li>◆ SUSE Linux Enterprise Server 9 ou 10 (32 bits ou 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits) avec le dernier Support Pack</li> <li>◆ 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)</li> </ul>	<ul style="list-style-type: none"> <li>◆ Intel x86</li> <li>◆ AMD x86</li> <li>◆ Intel EM64T</li> <li>◆ AMD Athlon64 et Opteron</li> </ul>
	Pour l'agent de plate-forme, un des systèmes d'exploitation suivants :	La configuration minimum requise pour le serveur sécurisé comprend :
	<ul style="list-style-type: none"> <li>◆ Novell Open Enterprise Server (OES) 1.0 SP1 ou le dernier Support Pack</li> <li>◆ NetWare 6.5 avec le dernier Support Pack</li> <li>◆ Serveur Windows 2000 ou 2000, XP ou Windows Server 2003 avec le dernier Service Pack (32 bits)</li> <li>◆ Red Hat Linux 3 ou 4 AS ou ES (32 bits ou 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits)</li> <li>◆ Solaris 8, 9 ou 10</li> <li>◆ SUSE Linux Enterprise Server 9 ou 10 (32 bits ou 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits)</li> </ul>	<ul style="list-style-type: none"> <li>◆ Ordinateur monoprocesseur de type serveur avec Pentium II 400 MHz</li> <li>◆ Un minimum de 40 Mo d'espace disque</li> <li>◆ 512 Mo de RAM</li> </ul>
		L'instrumentation eDirectory, qui permet la consignation d'événements eDirectory, prend en charge les versions suivantes d'eDirectory :
		<ul style="list-style-type: none"> <li>◆ eDirectory 8.7.3 (NetWare, Windows, Linux et Solaris)</li> <li>◆ eDirectory 8.8 avec le support pack le plus récent</li> </ul>
		L'instrumentation NetWare, qui permet la consignation d'événements NetWare, prend en charge les versions suivantes de NetWare :
		<ul style="list-style-type: none"> <li>◆ NetWare 5.1 avec le dernier Support Pack</li> <li>◆ NetWare 6.0 avec le dernier Support Pack</li> <li>◆ NetWare 6.5 ou NetWare 6.5 avec le dernier Support Pack</li> <li>◆ Novell Open Enterprise Server (OES) avec le dernier Support Pack</li> </ul>
	iManager 2.6 ou 2.7 avec le Support Pack et les plug-ins les plus récents	

Composant système requis	Configuration système requise	Remarques
Serveur d'applications de l'application utilisateur	<p>L'application utilisateur fonctionne sous JBoss* et WebSphere (voir ci-dessous).</p> <p>JBoss 4.0.5 GA est pris en charge sous :</p> <ul style="list-style-type: none"> <li>◆ Novell Open Enterprise Server (OES) 1.0 SP2 ou le dernier Support Pack (Linux uniquement)</li> <li>◆ SUSE Linux Enterprise Server 9 SP2 (inclus dans OES 1.0 SP2) ou 10.1.x (JVM* 64 bits;)</li> <li>◆ Windows 2000 Server avec SP4 (32 bits)</li> <li>◆ Windows 2003 Server avec SP1 (32 bits)</li> <li>◆ Solaris 10 support pack daté du 6/06</li> </ul> <p>WebSphere 6.1 est pris en charge sur :</p> <ul style="list-style-type: none"> <li>◆ Solaris 10 (64 bits)</li> <li>◆ Windows 2003 SP1</li> </ul> <p>L'application utilisateur requiert JRE* 1,5.0_14.</p>	<p>SUSE Linux Enterprise Server prend en charge les processeurs suivants au mode 32 bits :</p> <ul style="list-style-type: none"> <li>◆ Intel x86</li> <li>◆ AMD x86</li> <li>◆ Intel EM64T</li> <li>◆ AMD Athlon64 et Opteron</li> </ul> <p>SUSE Linux Enterprise Server fonctionnera au mode 64 bits sur les processeurs suivants :</p> <ul style="list-style-type: none"> <li>◆ Intel EM64T</li> <li>◆ AMD Athlon64</li> <li>◆ AMD Opteron</li> <li>◆ Sun* SPARC*</li> </ul> <p>La virtualisation Xen* est désormais prise en charge sur SUSE Linux Enterprise Server 10 lorsque la machine virtuelle (VM) Xen exécute SLES 10 comme système d'exploitation invité en mode paravirtualisé. Un correctif Xen pour SLES 10 est nécessaire (reportez-vous au TID n° (<a href="http://www.novell.com/support/search.do?cmd=displayKC&amp;docType=kc&amp;externalId=3915180&amp;sliceId=SAL_Public&amp;dialogID=52670386&amp;stateId=1%200%204926187">http://www.novell.com/support/search.do?cmd=displayKC&amp;docType=kc&amp;externalId=3915180&amp;sliceId=SAL_Public&amp;dialogID=52670386&amp;stateId=1%200%204926187</a>)).</p>

Composant système requis	Configuration système requise	Remarques
<p>Navigateur de l'application utilisateur</p>	<p>L'application utilisateur prend en charge Firefox et Internet Explorer, comme indiqué ci-dessous.</p> <p>Firefox 2 est pris en charge sur :</p> <ul style="list-style-type: none"> <li>◆ Windows 2000 Professionnel avec SP4</li> <li>◆ Windows XP avec SP2</li> <li>◆ Red Hat Enterprise Linux WS 4.0</li> <li>◆ Novell Linux Desktop 9</li> <li>◆ SUSE Linux 10.1</li> <li>◆ SUSE Linux Enterprise Desktop 10</li> </ul> <p>Internet Explorer 7 est pris en charge sur :</p> <ul style="list-style-type: none"> <li>◆ Windows 2000 Professionnel avec SP4</li> <li>◆ Windows XP avec SP2</li> <li>◆ Windows Vista Enterprise version 6</li> </ul> <p>Internet Explorer 6 SP1 est pris en charge sous :</p> <ul style="list-style-type: none"> <li>◆ Windows 2000 Professionnel avec SP4</li> <li>◆ Windows XP avec SP2</li> </ul>	
<p>Serveur de base de données pour l'application utilisateur</p> <ul style="list-style-type: none"> <li>◆ MySQL</li> <li>◆ Oracle</li> <li>◆ MS SQL</li> <li>◆ DB2</li> </ul>	<p>Les bases de données suivantes sont prises en charge avec JBoss :</p> <ul style="list-style-type: none"> <li>◆ MySQL version 5.0.27</li> <li>◆ Oracle 9i (9.2.0.1.4)</li> </ul> <p>Les bases de données suivantes sont prises en charge avec WebSphere :</p> <ul style="list-style-type: none"> <li>◆ Oracle 10g version 2 (10.2.0.1.0)</li> <li>◆ MS SQL 2005 avec SP1</li> <li>◆ Oracle 10g version 2 (10.2.0)</li> <li>◆ MS SQL 2005 avec SP1</li> <li>◆ DB2 DV2 v9.1.0.0</li> </ul>	<p>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.</p> <p>Le service de consignation sécurisée et le provisioning de l'application utilisateur et de workflow nécessitent une base de données. Vous pouvez configurer une base de données pour servir les deux applications, ou des bases de données indépendantes pour chacune. Le service de consignation sécurisée ne comprend pas de base de données spécifique.</p> <p>Oracle est pris en charge avec le pilote du client léger et le pilote du client OCI.</p>

Composant système requis	Configuration système requise	Remarques
Postes de travail	Le concepteur a été testé sur les plateformes suivantes :	Le concepteur utilise Eclipse comme plateforme de développement. Reportez-vous au <a href="http://www.eclipse.org">site Web d'Eclipse (http://www.eclipse.org)</a> pour obtenir des informations spécifiques à la plate-forme.
<ul style="list-style-type: none"> <li>◆ Designer 2.1.1 Windows : pour Identity Manager 3.5.1</li> <li>◆ Accès en ligne à iManager</li> </ul>	<ul style="list-style-type: none"> <li>◆ Windows 2000 Professional avec le dernier Service Pack</li> <li>◆ Windows XP SP2</li> <li>◆ Microsoft Windows Vista</li> </ul> <p>Linux :</p> <ul style="list-style-type: none"> <li>◆ SUSE Linux Enterprise Server 10 (concepteur uniquement)</li> <li>◆ SUSE Linux 10.1</li> <li>◆ SUSE Linux Enterprise Desktop 10</li> <li>◆ Red Hat Enterprise Linux WS 4.0 (pour Designer uniquement), Gnome* par défaut</li> <li>◆ Red Hat Fedora Core 5 (pour Designer uniquement), Gnome* par défaut</li> <li>◆ Novell Linux Desktop 9, KDE par défaut</li> </ul>	<p>Configuration matérielle minimum et recommandée pour le concepteur :</p> <ul style="list-style-type: none"> <li>◆ 1 GHz minimum ; 2 GHz ou plus recommandés</li> <li>◆ 512 Mo de RAM minimum ; 1 Go de RAM ou plus recommandé</li> <li>◆ Résolution minimum 1024 x 768 ; 1280 x 1024 recommandé</li> </ul> <p>Logiciels prérequis :</p> <ul style="list-style-type: none"> <li>◆ Microsoft Internet Explorer 6.0 avec SP1</li> <li>◆ Microsoft Internet Explorer 7</li> <li>◆ ou Mozilla* Firefox 2.0</li> </ul>



Composant système requis	Configuration système requise	Remarques
<p>Serveur de système connecté (hôte sur un serveur séparé exécutant le chargeur distant)</p> <ul style="list-style-type: none"> <li>◆ Chargeur distant</li> <li>◆ Outil de configuration du chargeur distant (Windows uniquement)</li> <li>◆ L'agent Novell Audit</li> <li>◆ Agent de synchronisation des mots de passe</li> <li>◆ Un module d'interface pilote pour le système connecté</li> <li>◆ Outils pour le système connecté</li> </ul>	<p>Chaque pilote exige que le système connecté soit disponible et les API pertinentes fournies.</p> <p>Reportez-vous à la <a href="http://www.novell.com/documentation/idm35drivers">documentation sur les pilotes Identity Manager (http://www.novell.com/documentation/idm35drivers)</a> pour connaître les exigences de système d'exploitation et de système connecté spécifiques à chaque système.</p>	<p>Chaque application connectée exige des connaissances spécifiques à l'application et une responsabilité des individus.</p> <p>Système de chargeur distant :</p> <ul style="list-style-type: none"> <li>◆ Windows NT* 4.0, Windows 2000 Server ou Windows Server 2003 avec le s derniers Support Packs</li> <li>◆ Windows Server* 2003 (64 bits) avec le dernier Service Pack</li> <li>◆ L'agent de synchronisation des mots de passe est pris en charge sous Windows Server 2003 (64 bits).</li> <li>◆ Red Hat Linux 3.0, 4.0 ou 5.0 ES ou AS</li> <li>◆ SUSE Linux Enterprise Server 9 ou 10</li> <li>◆ AIX 5.2L version 5.2 ou 5.3</li> </ul> <p>Système de chargeur distant Java :</p> <ul style="list-style-type: none"> <li>◆ HP-UX* 11i</li> <li>◆ OS/400</li> <li>◆ xOS*</li> <li>◆ L'utilisation devrait être possible sur tout système équipé de JVM 1.4.2 ou version supérieure</li> </ul>
Audit	Novell Audit 2.0.2	
Intégration SSO de l'application utilisateur	Nécessite Novell Access Manager 3.0.1.	Contient une version de saslsaml.jar générée avec JDK* 1.5.



# Conditions préalables à l'installation

# 2

La présente rubrique décrit les prérequis nécessaires à l'installation du module Provisioning d'Identity Manager basé sur les rôles. Les rubriques incluent :

- ♦ [Section 2.1, « Kit de développement Java », page 19](#)
- ♦ [Section 2.2, « Installation du méta-annuaire Identity Manager », page 20](#)
- ♦ [Section 2.3, « Installation du serveur d'applications JBoss », page 20](#)
- ♦ [Section 2.4, « Installation du serveur d'applications WebSphere », page 25](#)
- ♦ [Section 2.5, « Bases de données », page 25](#)
- ♦ [Section 2.6, « Conditions préalables de la sécurité », page 27](#)
- ♦ [Section 2.7, « Téléchargement du produit », page 27](#)
- ♦ [Section 2.8, « Installation du contenu du fichier prerequisitefiles.zip. », page 28](#)
- ♦ [Section 2.9, « Installation des icônes iManager destinées aux rôles », page 32](#)

## 2.1 Kit de développement Java

JBoss, WebSphere et le coffre-fort d'identité ont chacun des exigences particulières concernant le kit de développement Java.

**Serveurs d'applications JBoss :** sur les serveurs d'applications JBoss, utilisez le kit de développement 1.5.0\_14 édition Standard de la plate-forme Java 2.

Utilisez cette version du JDK de Sun pour démarrer le programme d'installation du module de provisioning basé sur les rôles en procédant comme suit :

Linux/Solaris :

```
$ /opt/jdk1.5.0_10/bin/java -jar IdmUserApp.jar
```

Windows :

```
C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.5.0_10\bin\java.exe" -jar IdmUserApp.jar
```

Lorsque le programme d'installation vous invite à saisir le chemin complet de l'installation Java, indiquez le chemin racine de Sun JDK. Voici un exemple de chemin racine sous Linux

```
/opt/jdk1.5.0_10
```

---

**Remarque :** les utilisateurs SLES ne doivent pas se servir du JDK d'IBM fourni avec SLES. Cette version n'est en effet pas compatible avec certaines parties de l'installation.

---

**Serveurs d'applications WebSphere :** sur les serveurs d'applications WebSphere\*, utilisez le JDK d'IBM livré avec WebSphere Application Server 6.1.0.9 et appliquez les fichiers de stratégies accessibles. Appliquez le jeu de correctifs JDK pour WAS version 6.1.0.9.

**Programme d'installation du coffre-fort d'identité (méta-annuaire) :** le programme d'installation du coffre-fort d'identité (méta-annuaire) installe sa propre copie de JVM sur toutes les plates-formes à l'exception de NetWare<sup>®</sup>. Sous NetWare, le coffre-fort d'identité utilise la version de Java installée sur le système.

## 2.2 Installation du méta-annuaire Identity Manager

Installez le méta-annuaire Identity Manager 3.5.1. Pour obtenir des instructions, reportez-vous au *Guide d'installation de Novell Identity Manager 3.5.1* (<http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf>).

Donnez accès au coffre-fort d'identité à un administrateur de module Provisioning d'Identity Manager basé sur les rôles. Pour cela, affectez un accès administrateur dans iManager au contexte qui hébergera les utilisateurs du module Provisioning d'Identity Manager basé sur les rôles.

## 2.3 Installation du serveur d'applications JBoss

Si vous envisagez d'utiliser le serveur d'applications JBoss\*, procédez selon l'une des méthodes suivantes:

- ♦ Téléchargez et installez le serveur d'applications JBoss 4.2.0 en vous conformant aux instructions du fabricant.
- ♦ Utilisez l'utilitaire JbossMysql fourni lors du téléchargement de module Provisioning basé sur les rôles pour installer un serveur d'applications JBoss (et MySQL le cas échéant). Pour plus d'informations, reportez-vous à [Section 2.3.1, « Installation du serveur d'applications JBoss et de la base de données MySQL »](#), page 21.

Attendez la fin de l'installation du module Provisioning d'Identity Manager basé sur les rôles avant de démarrer le serveur JBoss : le démarrage du serveur JBoss constitue en effet une tâche de post-installation.

**Mémoire vive :** la mémoire vive minimale recommandée pour le serveur d'applications JBoss lors de l'exécution du module de provisioning basé sur les rôles d'Identity Manager est de 512 Mo.

**Port :** notez le port que votre serveur d'applications utilise ; le programme d'installation du module de provisioning basé sur les rôles vous demande cette information. (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 le module de provisioning basé sur les rôles d'Identity Manager et le fichier `IDMPwdMgt.war`. Reportez-vous à votre documentation JBoss pour activer SSL. Assurez-vous également que le port SSL est ouvert dans votre pare-feu. Pour plus d'informations sur le fichier `IDMPwdMgt.war`, reportez-vous à [Section 7.5, « Accès au WAR de mots de passe externe »](#), page 112 ainsi qu'au manuel *Identity Manager User Application: Administration Guide* (*Guide d'administration de l'application utilisateur Identity Manager 3.5.1*) (<http://www.novell.com/documentation/idmrpbm36/index.html>).

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

L'utilitaire JbossMysql permet d'installer un serveur d'applications JBoss et MySQL sur votre système.

---

**Remarque :** 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 2.3.2, « Installation du serveur d'applications JBoss en tant que service », page 24.](#)

---

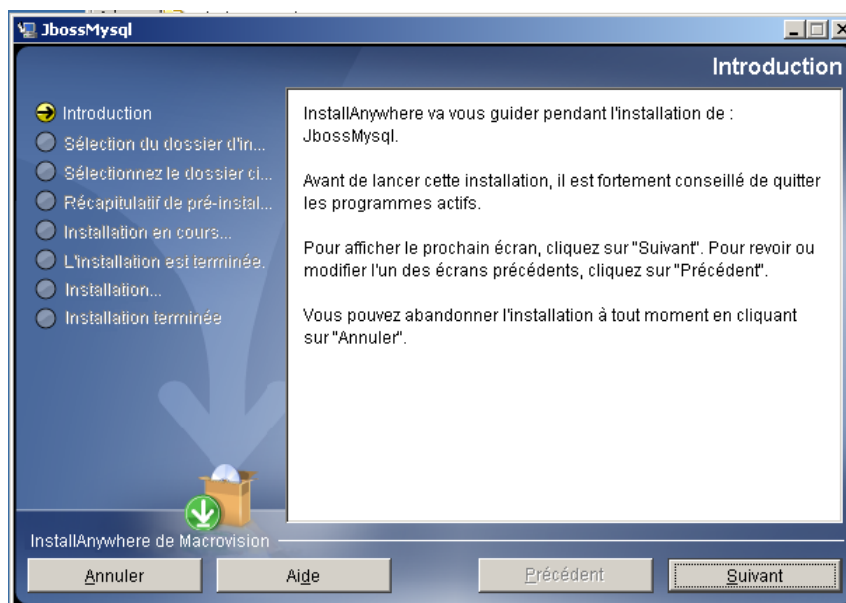
- 1 Localisez et exécutez `JbossMysql.bin` ou `JbossMysql.exe`. Cet utilitaire est fourni avec le programme d'installation de l'application utilisateur dans

`/linux/user_application` (Linux)

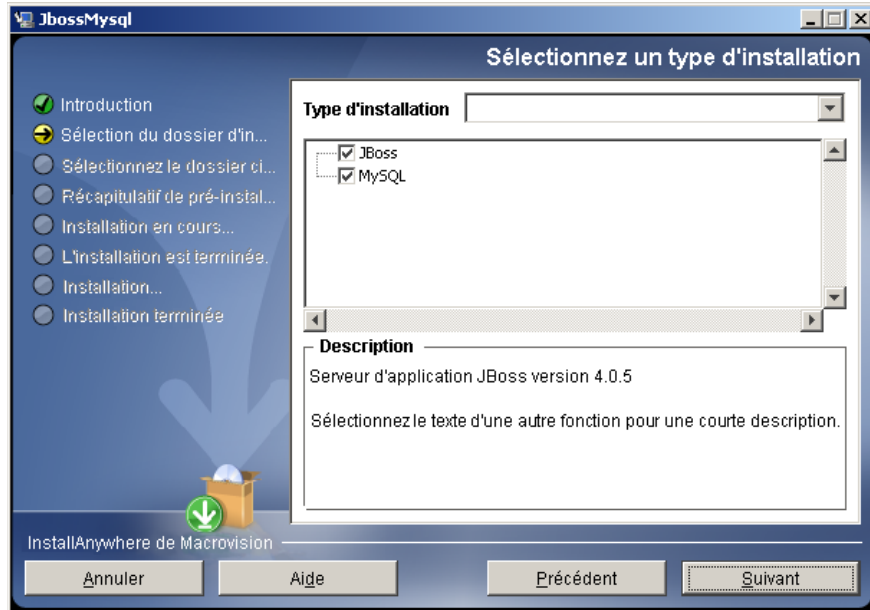
`/nt/user_application` (Windows)

Cet utilitaire n'est pas disponible avec Solaris.

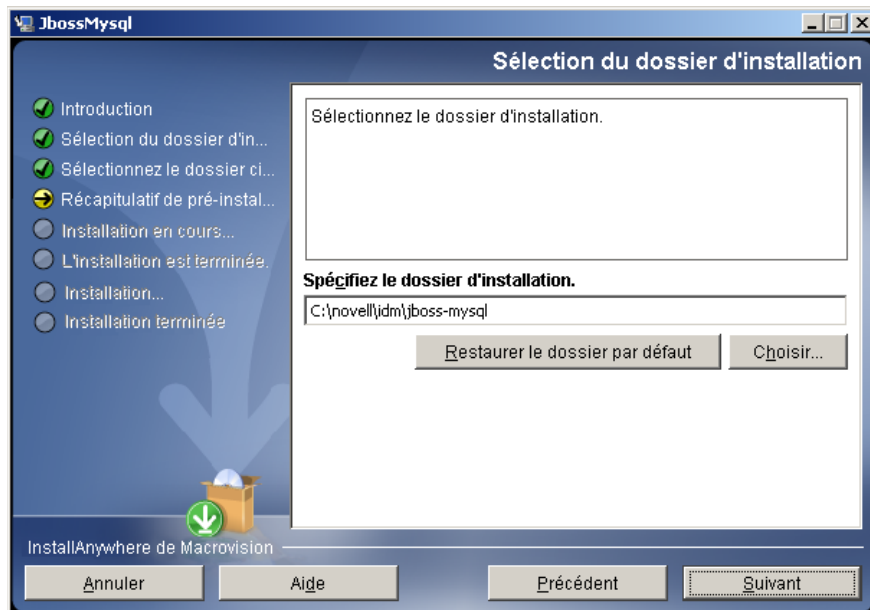
- 2 Sélectionnez votre emplacement.
- 3 Lisez la page d'introduction, puis cliquez sur *Suivant*.



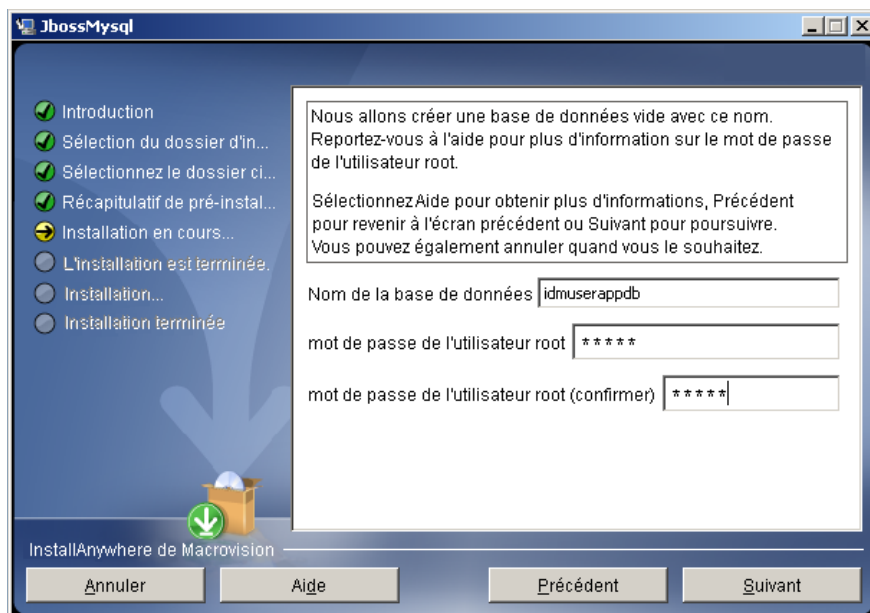
- 4 Sélectionnez les produits que vous voulez installer, puis cliquez sur *Suivant*.



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

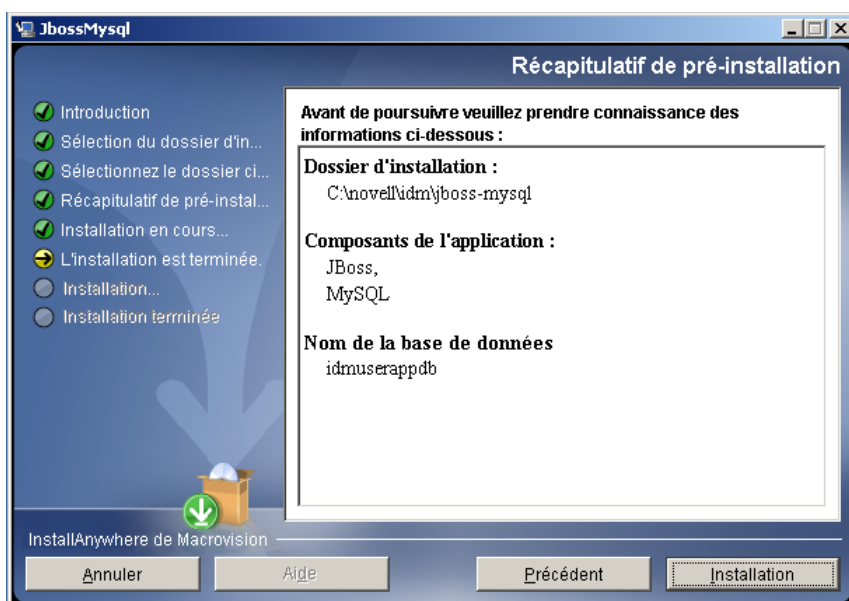


- 6 Nommez votre base de données. L'installation de l'application utilisateur exige ce nom.
- 7 Indiquez le mot de passe utilisateur `root` de la base de données.



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 2.5.2, « Configuration de votre base de données MySQL »](#), page 26.

## 2.3.2 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>).

Cette rubrique aborde les points suivants :

- ◆ « Utilisation d'un wrapper de service Java » page 24
- ◆ « Utilisation d'un utilitaire tiers » page 25

### 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
```

---

**Important :** vous devez définir correctement votre variable d'environnement JBOSS\_HOME. Le wrapper ne définit pas cela par lui-même.

---

```
java-service-wrapper-service.xml : <Xml 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.

---

**Important :** 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>).

---

## 2.4 Installation du serveur d'applications WebSphere

Si vous souhaitez utiliser le serveur d'applications WebSphere, téléchargez et installez le serveur d'applications WebSphere 6.1.0.9. Appliquez le jeu de correctifs JDK pour WAS version 6.1.0.9.

## 2.5 Bases de données

Installez votre base de données et votre pilote de base de données, puis créez une base de données ou une instance de base de données. Notez les paramètres suivants de la base de données car ils serviront lors de l'installation du module Provisioning d'Identity Manager basé sur les rôles :

- ♦ hôte et port
- ♦ nom de la base de données, nom et mot de passe de l'utilisateur

Un fichier de source de données doit pointer vers la base de données. La méthode diffère selon le serveur d'applications. Dans le cas de JBoss, le programme d'installation du module de provisioning basé sur les rôles d'Identity Manager crée un fichier source de données du serveur d'applications qui pointe vers la base de données et nomme le fichier en fonction du fichier WAR du module de provisioning basé sur les rôles d'Identity Manager. Pour WebSphere, configurez la source de données manuellement avant l'installation.

Les bases de données doivent être compatibles UTF-8.

- ♦ [Section 2.5.1, « Installation de MySQL », page 25](#)
- ♦ [Section 2.5.2, « Configuration de votre base de données MySQL », page 26](#)

### 2.5.1 Installation de MySQL

Que vous installiez MySQL\* par l'utilitaire de l'application utilisateur IDM ou par vous-même, lisez [Section 2.5.2, « Configuration de votre base de données MySQL », page 26](#).

---

**Remarque :** si vous prévoyez de 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, vous n'avez pas à l'exécuter pendant l'installation du module de provisioning basé sur les rôles d'Identity Manager. Ne la démarrez que juste avant de démarrer le serveur d'applications.

---

## 2.5.2 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 :

- ♦ « Moteur de stockage et types de tables INNODB » page 26
- ♦ « Ensemble de caractères » page 26
- ♦ « Distinction de la casse » page 26

### 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`.

### Ensemble de caractères

Indiquez UTF8 comme ensemble de caractères pour l'ensemble du serveur ou simplement pour une base de données. Indiquez UTF8 sur l'ensemble du serveur en incluant l'option suivante dans `my.cnf` (Linux ou Solaris) ou `my.ini` (Windows) :

```
character-set-server=utf8
```

Pour indiquer le jeu de caractères d'une base de données au moment de la création de la base de données, utilisez la commande suivante :

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

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

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

### 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.

## 2.6 Conditions préalables de la sécurité

Pour activer le logout simultané dans le module de provisioning basé sur les rôles d'Identity Manager, activez l'option Cookie Forward (Transfert de cookies) dans Novell Access Manager™ ou iChain®. Pour obtenir des directives, reportez-vous à [Injecting into the Cookie Header \(Injection dans l'en-tête de cookie\)](http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b5pqck8.html) (<http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b5pqck8.html>) dans le *Novell Access Manager 3.0 SPI Administration Guide (Guide d'administration de Novell Access Manager 3.0 SPI)*.

## 2.7 Téléchargement du produit

Procurez-vous la version 3.6 du module de provisioning basé sur les rôles d'Identity Manager depuis la page [Téléchargements Novell](http://download.novell.com/index.jsp) (<http://download.novell.com/index.jsp>).

Téléchargez l'image `.iso` ou le fichier de l'application utilisateur qui convient à votre système : `Identity_Manager_3_6_0_User_Application_Provisioning.iso`

Le fichier `.iso` contient les dossiers de réception suivants :

```
/linux/user_application (sous Linux)
/nt/user_application (sous Windows)
/solaris/user_application (sous Solaris)
/36MetaDirSupport (contient les fichiers nécessaires à la mise à
jour du méta-annuaire d'IDM 3.5.1 en vue de la prise en charge de
l'application utilisateur IDM 3.6)
```

Le [Tableau 2-1](#) contient les fichiers et les scripts dont vous avez besoin pour installer la version 3.6 du module de provisioning basé sur les rôles d'Identity Manager.

**Tableau 2-1** Fichiers et scripts requis pour l'installation de l'application utilisateur Identity Manager 3.6

Fichier	Description
<code>IDMProv.war</code>	Fichier WAR du module de provisioning basé sur les rôles d'Identity Manager. Il contient l'application utilisateur Identity Manager 3.6 avec les fonctions Identity Self-Service et le module Provisioning basé sur les rôles.
<code>IDMUserApp.jar</code>	Programme d'installation du module de provisioning basé sur les rôles.
<code>silent.properties</code>	Ce fichier contient les paramètres requis pour une installation en mode silencieux. Ceux-ci correspondent aux paramètres d'installation que vous avez définis dans les procédures d'installation de l'interface utilisateur graphique ou de la console.
<code>prerequisitefiles.zip</code>	Fichier ZIP contenant les fichiers nécessitant une installation manuelle.

Fichier	Description
UserApplication_3_6_0- IDM3_5_1-V1.xml	Fichier de configuration du pilote d'application utilisateur.
iManager_icons_for_roles.zip	Contient les icônes iManager destinées aux objets de rôle dans eDirectory.

---

**Suggestion :** Les fichiers `iManager_icons_for_roles.zip` et `prerequisites.zip` se trouvent dans le répertoire `/36MetaDirSupport`. Les autres fichiers se trouvent dans les répertoires `<systeme_d'exploitation>/user_application`.

---

L'ordinateur sur lequel vous installez le module de provisioning basé sur les rôles d'Identity Manager doit disposer d'un espace de stockage minimal de 320 Mo.

Le répertoire d'installation par défaut est:

- ◆ Linux ou Solaris : `/opt/novell/idm`
- ◆ Windows : `C:\Novell\IDM`

Vous pouvez sélectionner un répertoire d'installation différent durant l'installation, mais celui-ci doit avoir été créé avant le démarrage de l'installation et être accessible en écriture. Sous Linux et Solaris, les utilisateurs non-`root` doivent également y avoir un accès en écriture.

## 2.8 Installation du contenu du fichier `prerequisitefiles.zip`.

Recherchez le fichier `prerequisitefiles.zip` dans le fichier image que vous avez téléchargé, puis dézippez-le. Ce fichier contient les fichiers que vous devez installer manuellement (reportez-vous au [Tableau 2-2](#)) :

**Tableau 2-2** Fichiers nécessitant une installation manuelle

Nom de fichier	Description	Instructions
nrf-extensions.sch	Schéma de fichier eDirectory™	Section 2.8.1, « Extension du schéma eDirectory de la version 3.6 du module de provisioning basé sur les rôles d'Identity Manager », page 29
nrfdriver.jar	Fichier JAR du pilote de service de rôle	Section 2.8.2, « Copie du fichier JAR du pilote de service de rôle », page 30
RoleService-IDM3_5_1-V1.xml	Fichier de configuration du pilote de service de rôle	Section 2.8.3, « Copie du fichier de configuration du pilote de service de rôle », page 31
UserApplicationn_3_6_0-IDM3_5_1-V1.xml	Fichier de configuration du pilote d'application utilisateur prenant en charge le module Provisioning basé sur les rôles	Section 2.8.4, « Copie du fichier de configuration du pilote d'application utilisateur », page 31
dirxml.lsc	Schéma de fichier de consignation des applications de consignation	Section 2.8.5, « Copie du fichier dirxml.lsc », page 31

- ♦ Section 2.8.1, « Extension du schéma eDirectory de la version 3.6 du module de provisioning basé sur les rôles d'Identity Manager », page 29
- ♦ Section 2.8.2, « Copie du fichier JAR du pilote de service de rôle », page 30
- ♦ Section 2.8.3, « Copie du fichier de configuration du pilote de service de rôle », page 31
- ♦ Section 2.8.4, « Copie du fichier de configuration du pilote d'application utilisateur », page 31
- ♦ Section 2.8.5, « Copie du fichier dirxml.lsc », page 31

## 2.8.1 Extension du schéma eDirectory de la version 3.6 du module de provisioning basé sur les rôles d'Identity Manager

Permet d'étendre le schéma eDirectory d'Identity Manager Roles Based Provisioning Module ; reportez-vous aux sections suivantes :

- ♦ « Extension du schéma sous Windows » page 29
- ♦ « Extension du schéma sous UNIX/Linux » page 30
- ♦ « Extension du schéma sous NetWare » page 30

### Extension du schéma sous Windows

NDSCons.exe permet d'étendre le schéma sur les serveurs Windows. Les fichiers de schéma (\*.sch) fournis avec eDirectory sont installés par défaut dans le répertoire C:\Novell\NDS .

- 1 Cliquez sur *Démarrer* > *Paramètres* > *Panneau de configuration* > *Novell eDirectory Services*.

- 2 Cliquez sur *install.dlm*, puis sur *Exécuter*
- 3 Cliquez sur *Installer d'autres fichiers de schéma*, puis cliquez sur *Suivant*.
- 4 Loguez-vous en tant qu'utilisateur doté de droits d'administrateur, puis cliquez sur *OK*.
- 5 Indiquez le chemin d'accès au fichier de schéma (par exemple, `c:\Novell\NDS\nrf-extensions.sch`).
- 6 Cliquez sur *Terminer*.

### Extension du schéma sous UNIX/Linux

Pour étendre le schéma eDirectory du module Provisioning basé sur les rôles sur les plates-formes UNIX/Linux, procédez comme suit :

- 1 Ajoutez le fichier de schéma du module de provisioning basé sur les rôles, `nrf-extensions.sch`. Utilisez à cet effet la commande `ndssch` depuis la ligne de commande.

```
ndssch [-h hostname[:port]] [-t tree_name] admin-FDN
schemafilename.sch
```

### Extension du schéma sous NetWare

`NWConfig.nlm` permet d'étendre le schéma sur les serveurs NetWare. Les fichiers de schéma (\*.sch) fournis avec eDirectory sont installés dans le répertoire `sys:\system\schema`.

- 1 À l'invite de la console du serveur, entrez la commande `nwconfig`.
- 2 Cliquez sur *Options de l'annuaire > Étendre le schéma*.
- 3 Loguez-vous en tant qu'utilisateur doté de droits d'administrateur.
- 4 Appuyez sur F3 pour changer de chemin, puis saisissez `sys:\system\schema` (ou le chemin d'accès à votre fichier \*.sch) et le fichier de schéma `nrf-extensions.sch`.
- 5 Appuyez sur Entrée.

## 2.8.2 Copie du fichier JAR du pilote de service de rôle

Installez manuellement le pilote de service de rôle sur le serveur du méta-annuaire. Pour ce faire, copier le fichier JAR exécutable de service de rôle `nrfdriver.jar` (il se trouve dans l'archive `prerequisitefiles.zip`) vers le répertoire approprié de votre système :

**Tableau 2-3** Emplacement du fichier JAR du pilote de service de rôle

Système d'exploitation	Répertoire
UNIX (eDirectory 8.7.x)	<code>/usr/lib/dirxml/classes</code>
UNIX (eDirectory 8.8.x)	<code>/opt/novell/eDirectory/lib/dirxml/classes</code>
Windows	<code>&lt;lecteur&gt;:\novell\nds\lib</code>
NetWare	<code>SYS:SYSTEM\LIB</code>

## 2.8.3 Copie du fichier de configuration du pilote de service de rôle

Installez manuellement le fichier de configuration du pilote de service de rôle (RoleService\_IDM3\_5\_1-V1.xml) dans le répertoire approprié de votre système :

**Tableau 2-4** Emplacement du fichier de configuration du pilote de service de rôle

Système d'exploitation	Répertoire
Linux (eDirectory 8.7.x)	/usr/lib/dirxml/classes
Linux (eDirectory 8.8)	/var/opt/novell/iManager/nps/DirXML.Drivers
Windows	C:\Program Files\Novell\tomcat\webapps\nps\Dirxml.Drivers
NetWare	SYS:\tomcat\4\webapps\nps\Dirxml.Drivers

## 2.8.4 Copie du fichier de configuration du pilote d'application utilisateur

Installez manuellement le fichier de configuration du pilote d'application utilisateur (UserApplication\_3\_6\_0-IDM3\_5\_1-V1.xml) dans le répertoire approprié de votre système :

**Tableau 2-5** Emplacement du fichier de configuration du pilote d'application utilisateur

Système d'exploitation	Répertoire
Linux (eDirectory 8.7.x)	/usr/lib/dirxml/classes
Linux (eDirectory 8.8)	/var/opt/novell/iManager/nps/DirXML.Drivers
Windows	C:\Program Files\Novell\tomcat\webapps\nps\Dirxml.Drive rs
NetWare	SYS:\tomcat\4\webapps\nps\Dirxml.Drivers

## 2.8.5 Copie du fichier dirxml.lsc

Copiez le fichier `dirxml.lsc` sur le serveur Audit en suivant les instructions décrites dans la section Setting Up Logging (Configuration de la journalisation) du manuel [Identity Manager User Application: Administration Guide \(Guide d'administration de l'application utilisateur Identity Manager 3.5.1\)](http://www.novell.com/documentation/idmrbpm36/pdfdoc/agpro/agpro.pdf) (<http://www.novell.com/documentation/idmrbpm36/pdfdoc/agpro/agpro.pdf>).

## 2.9 Installation des icônes iManager destinées aux rôles

Recherchez le fichier `iManager_icons_for_roles.zip` dans le fichier image que vous avez téléchargé, puis dézippez-le. Copiez le fichier dézippé dans le répertoire `nps/portal/modules/dev/images/dir`. Redémarrez iManager pour qu'il utilise les nouvelles icônes.



La présente rubrique décrit la création des pilotes nécessaires à l'utilisation du module de provisioning basé sur les rôles. Les rubriques incluent :

- ♦ [Section 3.1, « Création du pilote d'application utilisateur dans iManager », page 33](#)
- ♦ [Section 3.2, « Création du pilote de service de rôle dans iManager », page 37](#)

---

**Important :** vous devez créer le pilote d'application utilisateur avant de créer de pilote de service de rôle. Il est important de créer d'abord le pilote d'application utilisateur car le pilote de service de rôle y référence le conteneur du coffre de rôles (RoleConfig.AppConfig).

---

La configuration permise du pilote est la suivante :

- ♦ Vous pouvez ajouter un seul pilote de service de rôle par ensemble de pilotes dans iManager.
- ♦ Vous pouvez associer un seul pilote d'application utilisateur à un pilote de service de rôle.
- ♦ Vous pouvez associer une seule application utilisateur à un pilote d'application utilisateur.

## 3.1 Création du pilote d'application utilisateur dans iManager

Vous devez créer un pilote d'application utilisateur séparé pour chaque module de provisioning basé sur les rôles d'Identity Manager, à l'exception des modules de provisioning basés sur les rôles membres d'une grappe. Les modules de provisioning basés sur les rôles qui font partie de la même grappe doivent partager un seul pilote d'application utilisateur. Pour plus d'informations sur l'exécution du module de provisioning basé sur les rôles dans une grappe, reportez-vous au [Guide d'administration de l'application utilisateur Identity Manager](http://www.novell.com/documentation/idmrbpm36/index.html) (<http://www.novell.com/documentation/idmrbpm36/index.html>).

Le module de provisioning basé sur les rôles stocke des données spécifiques à l'application dans le pilote d'application utilisateur 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.

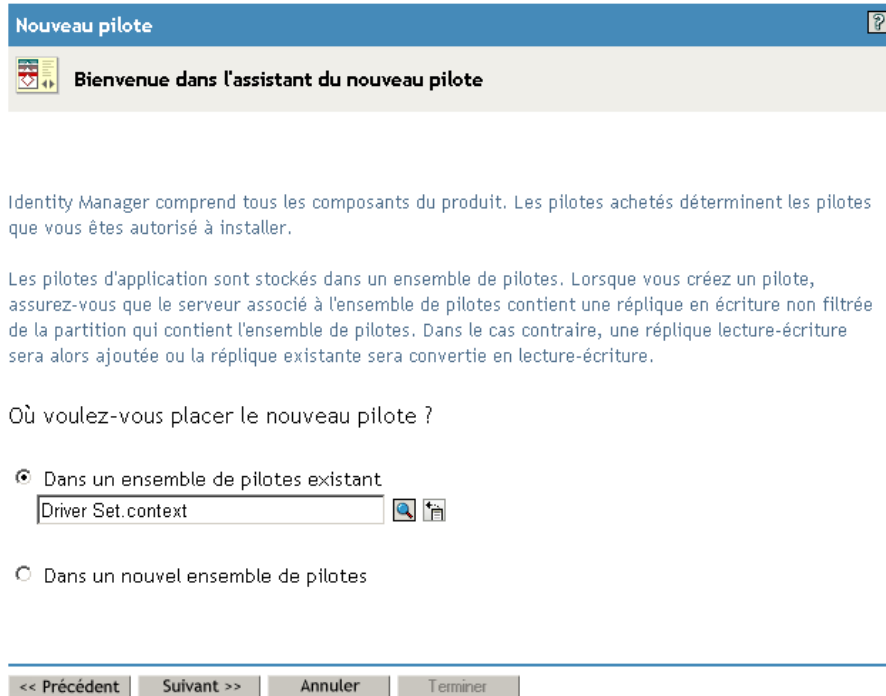
---

**Important :** la configuration d'un ensemble de modules de provisioning basés sur les rôles non mis en grappe pour partager un seul pilote crée une ambiguïté et une configuration incorrecte d'un ou plusieurs des composants exécutés dans le module de provisioning basé sur les rôles. 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 Ouvrez iManager 2.6 ou ultérieur dans votre navigateur Web.
- 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*, puis passez à l'**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. Le contexte correspond au contexte eDirectory™ dans lequel l'objet serveur se trouve.



Définissez les propriétés du nouvel ensemble de pilotes.

Nom :

Contexte :   

Serveur :   

Créer une partition dans cet ensemble de pilotes

**3b** Cliquez sur *Suivant*.

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

**5** Sélectionnez *UserApplication\_3\_6\_0-IDM3\_5\_1-V1.xml* dans la liste déroulante. Il s'agit du fichier de configuration du pilote d'application utilisateur prenant en charge le module Provisioning basé sur les rôles.

Si le fichier *UserApplication\_3\_6\_0-IDM3\_5\_1-V1.xml* ne figure pas dans la liste, vous ne l'avez pas copié au bon emplacement. Reportez-vous à [Section 2.8.4, « Copie du fichier de configuration du pilote d'application utilisateur »](#), page 31.

**6** Cliquez sur *Suivant*.

**7** Vous êtes invité à saisir les paramètres de votre pilote. (Faites défiler pour afficher tout.) Notez les paramètres ; vous en aurez besoin pour installer le module de provisioning basé sur les rôles.

Champ	Description
<i>Nom du pilote</i>	Le nom du pilote que vous créez.
<i>ID d'authentification</i>	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.
<i>Mot de passe</i>	Mot de passe de l'administrateur de l'application utilisateur indiqué dans l'ID d'authentification.
<i>Contexte de l'application</i>	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.

Champ	Description
<i>Hôte</i>	Le nom d'hôte ou l'adresse IP du serveur d'applications où l'application utilisateur Identity Manager est déployée.  Si vous exécutez l'application utilisateur dans une grappe, saisissez le nom d'hôte ou l'adresse IP du répartiteur.
<i>Port</i>	Le port de l'hôte indiqué ci-dessus.
<i>Autoriser l'initiateur de remplacement</i>  (les valeurs sont Non/Oui)	Sélectionnez <i>Oui</i> 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*.

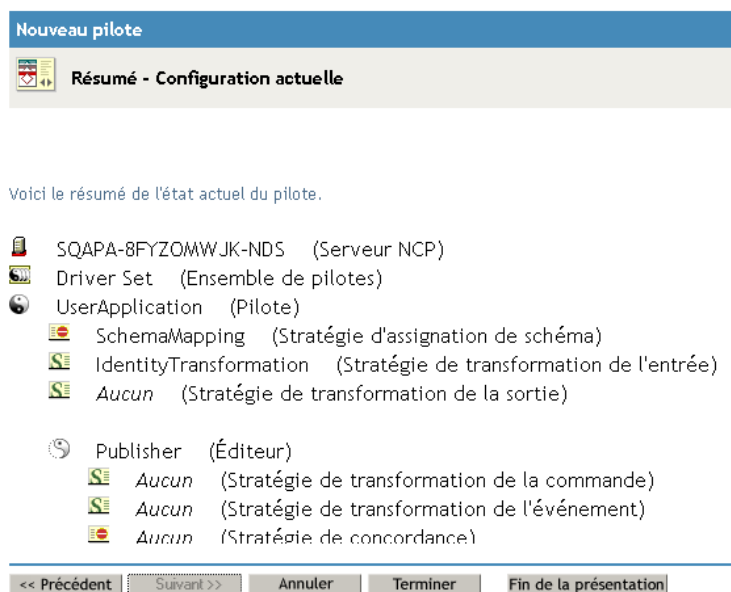
9 Cliquez sur *Définir les équivalents de sécurité* pour ouvrir la fenêtre Équivalents de sécurité. Recherchez et sélectionnez un objet administrateur ou autre superviseur, puis cliquez sur *Ajouter*.

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*, sélectionnez les utilisateurs que vous souhaitez exclure des actions de pilote (les rôles administratifs, par exemple), cliquez deux fois sur *OK*, puis cliquez sur *Suivant*.

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



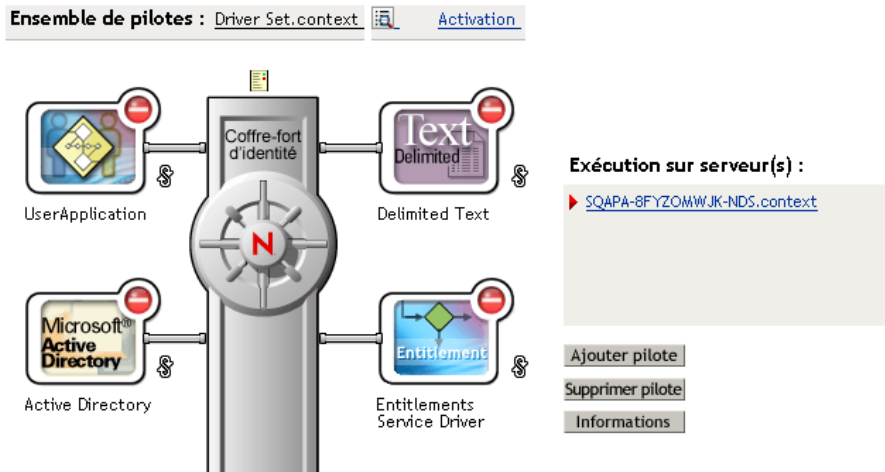
Voici le résumé de l'état actuel du pilote.

- SQAPA-8FYZOMWJK-NDS (Serveur NCP)
- Driver Set (Ensemble de pilotes)
- UserApplication (Pilote)
  - SchemaMapping (Stratégie d'assignation de schéma)
  - IdentityTransformation (Stratégie de transformation de l'entrée)
  - Aucun (Stratégie de transformation de la sortie)
- Publisher (Éditeur)
  - Aucun (Stratégie de transformation de la commande)
  - Aucun (Stratégie de transformation de l'événement)
  - Aucun (Stratégie de concordance)

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

**Important :** le pilote est désactivé par défaut. Laissez-le désactivé jusqu'à ce que le module de provisioning basé sur les rôles soit installé.

1 ensemble(s) de pilotes trouvé(s) dans : Driver Set.context  
0 objet(s) de la bibliothèque trouvé(s) dans : Driver Set.context



## 3.2 Création du pilote de service de rôle dans iManager

Pour créer et configurer le pilote de service de rôle dans iManager, procédez comme suit :

- 1 Ouvrez iManager 2.6 ou ultérieur dans votre navigateur Web.
- 2 Dans *Identity Manager* > *Présentation Identity Manager*, sélectionnez l'ensemble de pilotes dans lequel installer le pilote de service de rôle.

Installez le pilote d'application utilisateur avant le pilote de service de rôle. Utilisez la version 3.6 du pilote d'application utilisateur (*UserApplication\_3\_6\_0-IDM3\_5\_1-V1.xml*) avec le pilote de service de rôle. Le catalogue de rôles ne sera pas disponible si vous utilisez une autre version du pilote d'application utilisateur.

Les ensembles de pilotes ne peuvent contenir qu'un seul pilote de service de rôle.

- 3 Cliquez sur *Ajouter pilote*.
- 4 Dans l'assistant Nouveau pilote, conservez la valeur par défaut *Dans un ensemble de pilotes existant*. Cliquez sur *Suivant*.
- 5 Sélectionnez *RoleService-IDM3\_5\_1-V1.xml* dans la liste déroulante. Il s'agit du fichier de configuration du pilote de service de rôle prenant en charge le module de provisioning basé sur les rôles.

Si le fichier *RoleService-IDM3\_5\_1-V1.xml* ne figure pas dans la liste, vous ne l'avez pas copié au bon emplacement. Reportez-vous à [Section 2.8.3, « Copie du fichier de configuration du pilote de service de rôle », page 31](#).

Cliquez sur *Suivant*.

L'erreur suivante peut se produire lorsque vous essayez de créer le pilote :

```
The following 'Namespace Exception' occurred while trying to access the directory. (CLASS_NOT_DEFINED)
```

Dans ce cas, l'application iManager n'a pas encore récupéré votre nouveau schéma de rôles. Ce dernier est nécessaire au pilote de service de rôle. Essayez de redémarrer votre session iManager (fermez tous les navigateurs et logez-vous de nouveau dans iManager). Ou encore, essayez de redémarrer le serveur.

- 6** Renseignez les informations dans la page Informations d'importation demandées. Le tableau suivant décrit ces informations.

Option	Description
<i>Nom du pilote</i>	Indiquez le nom du pilote ou conservez le nom par défaut (Service de rôle). Si vous installez un pilote dont le nom est identique à celui d'un pilote existant, le nouveau pilote remplace la configuration de l'ancien pilote.  Le bouton <i>Parcourir</i> permet d'afficher les pilotes existants de l'ensemble sélectionné. Ce champ est obligatoire.
<i>DN du pilote de l'application utilisateur</i>	Nom distinctif de l'objet Pilote de l'application utilisateur qui héberge le système du rôle. Utilisez le format eDirectory, par exemple UserApplication.driverset.org, ou recherchez l'objet pilote. Ce champ est obligatoire.
<i>URL de l'application utilisateur</i>	URL utilisée pour se connecter à l'application utilisateur afin de lancer les workflows d'approbation. L'exemple d'URL indiqué est <i>http://hôte:port/IDM</i> . Ce champ est obligatoire.
<i>Identité de l'application utilisateur</i>	Nom distinctif de l'objet utilisé pour authentifier l'application utilisateur afin de lancer les workflows d'approbation. Il peut s'agir d'un administrateur de l'application utilisateur à qui vous avez donné le droit de gérer le portail de l'application utilisateur. Utilisez le format eDirectory, par exemple admin.department.org, ou recherchez l'utilisateur. Ce champ est obligatoire.
<i>Mot de passe de l'application utilisateur</i>	Mot de passe de l'administrateur de l'application utilisateur indiqué dans l'ID d'authentification. Mot de passe utilisé pour s'authentifier auprès de l'application utilisateur afin de lancer les workflows d'approbation. Ce champ est obligatoire.
<i>Confirmez le mot de passe</i>	Saisissez de nouveau le mot de passe de l'administrateur de l'application utilisateur.

- 7** Une fois tous les champs renseignés, cliquez sur *Terminer*.

# Installation de JBoss depuis une interface graphique

# 4

Cette section décrit l'installation du module de provisioning basé sur les rôles d'Identity Manager sur un serveur d'applications JBoss à l'aide de l'interface graphique du programme d'installation. Si vous préférez utiliser la console ou une commande unique, reportez-vous au [Chapitre 5, « Installation depuis la console ou à l'aide d'une commande unique », page 71](#).

- ♦ [Section 4.1, « Lancement de l'interface utilisateur graphique du programme d'installation », page 39](#)
- ♦ [Section 4.2, « Choix d'une plate-forme de serveur d'applications », page 40](#)
- ♦ [Section 4.3, « Migration de votre base de données », page 41](#)
- ♦ [Section 4.4, « Emplacement du WAR », page 43](#)
- ♦ [Section 4.5, « Choix d'un dossier d'installation », page 43](#)
- ♦ [Section 4.6, « Choix d'une plate-forme de base de données », page 44](#)
- ♦ [Section 4.7, « Spécification de l'hôte et du port de la base de données », page 45](#)
- ♦ [Section 4.8, « Spécification du nom de la base de données et de l'utilisateur privilégié », page 46](#)
- ♦ [Section 4.9, « Spécification du répertoire racine Java », page 47](#)
- ♦ [Section 4.10, « Choix du type de configuration du serveur d'applications », page 48](#)
- ♦ [Section 4.11, « Spécification des paramètres du serveur d'applications JBoss », page 50](#)
- ♦ [Section 4.12, « Activation de la consignment Novell Audit », page 50](#)
- ♦ [Section 4.13, « Spécification d'une clé maîtresse », page 52](#)
- ♦ [Section 4.14, « Configuration de l'application utilisateur », page 53](#)
- ♦ [Section 4.15, « Utilisation des WAR de mots de passe », page 67](#)
- ♦ [Section 4.16, « Vérification des choix et installation », page 68](#)
- ♦ [Section 4.17, « Affichage des fichiers journaux », page 69](#)

Si vous préférez utiliser la ligne de commande, reportez-vous au [Chapitre 5, « Installation depuis la console ou à l'aide d'une commande unique », page 71](#).

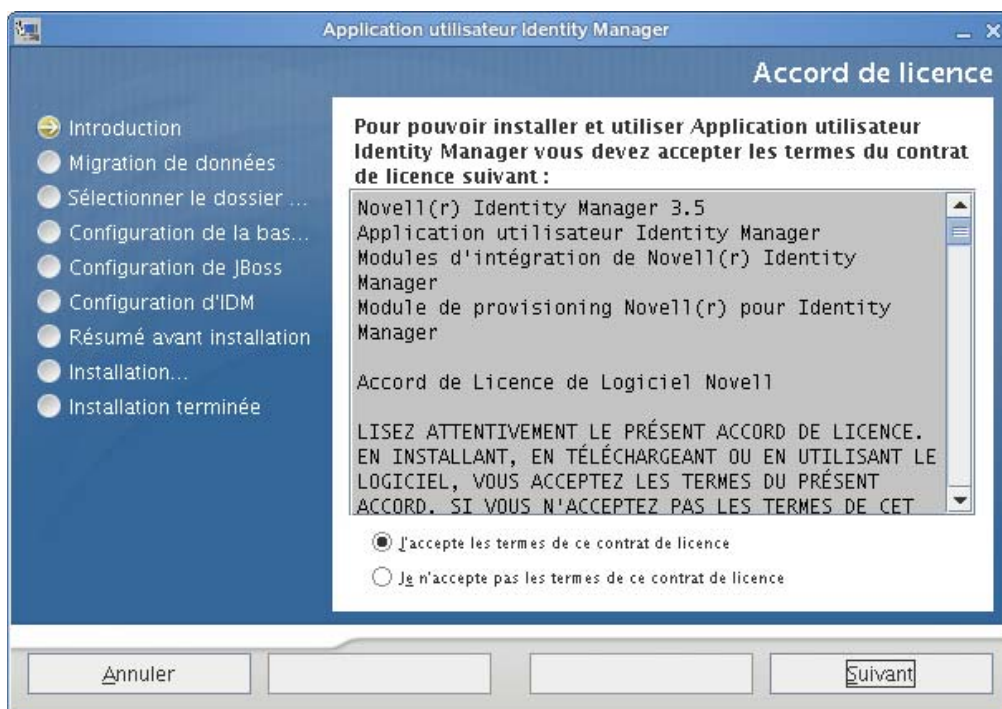
## 4.1 Lancement de l'interface utilisateur graphique du programme d'installation

- 1 Naviguez jusqu'au répertoire contenant vos fichiers d'installation, indiqué dans le [Tableau 2-1 page 27](#).
- 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 ce contrat de licence*, puis cliquez sur *Suivant*.



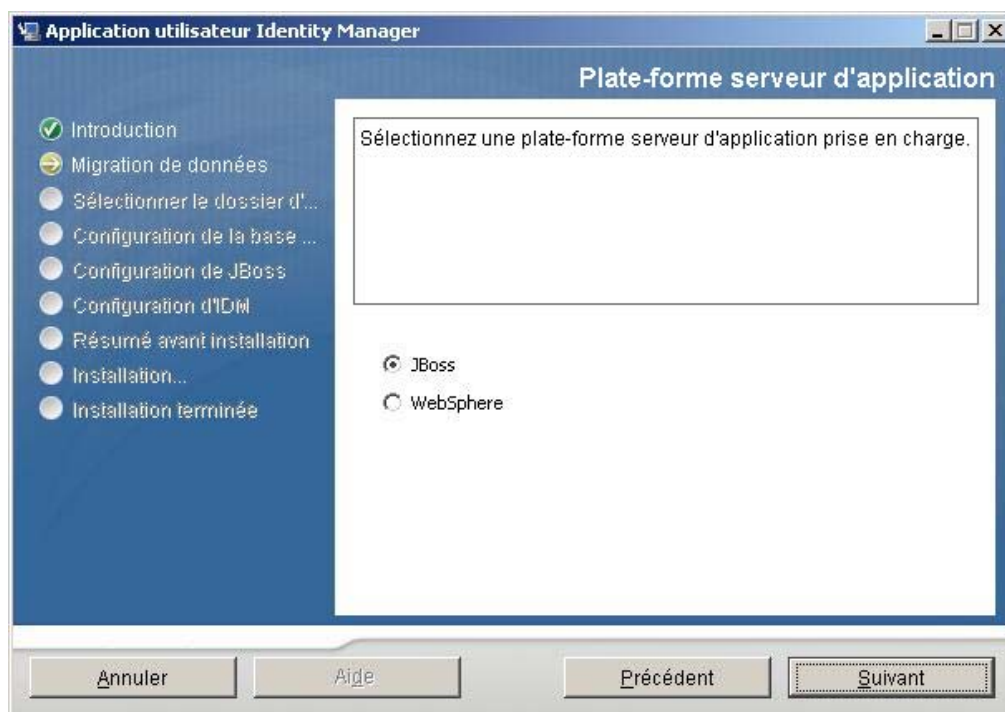
- 5 Lisez la page d'introduction de l'assistant d'installation, puis cliquez sur *Suivant*.
- 6 Passez à [Section 4.2, « Choix d'une plate-forme de serveur d'applications », page 40](#).

## 4.2 Choix d'une plate-forme de serveur d'applications

Effectuez la procédure décrite dans la [Section 4.1, « Lancement de l'interface utilisateur graphique du programme d'installation », page 39](#), puis passez aux étapes ci-dessous.



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



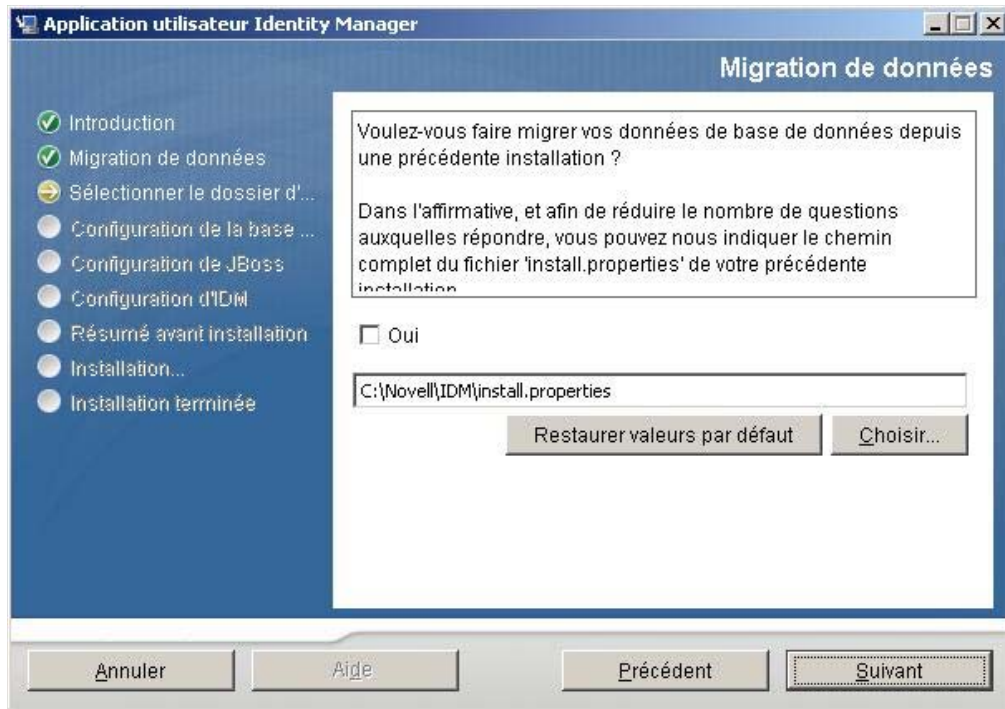
### 4.3 Migration de votre base de données

- 1 Si vous ne souhaitez pas faire migrer une base de données, cliquez sur *Suivant*, puis passez à [Section 4.4, « Emplacement du WAR », page 43](#).

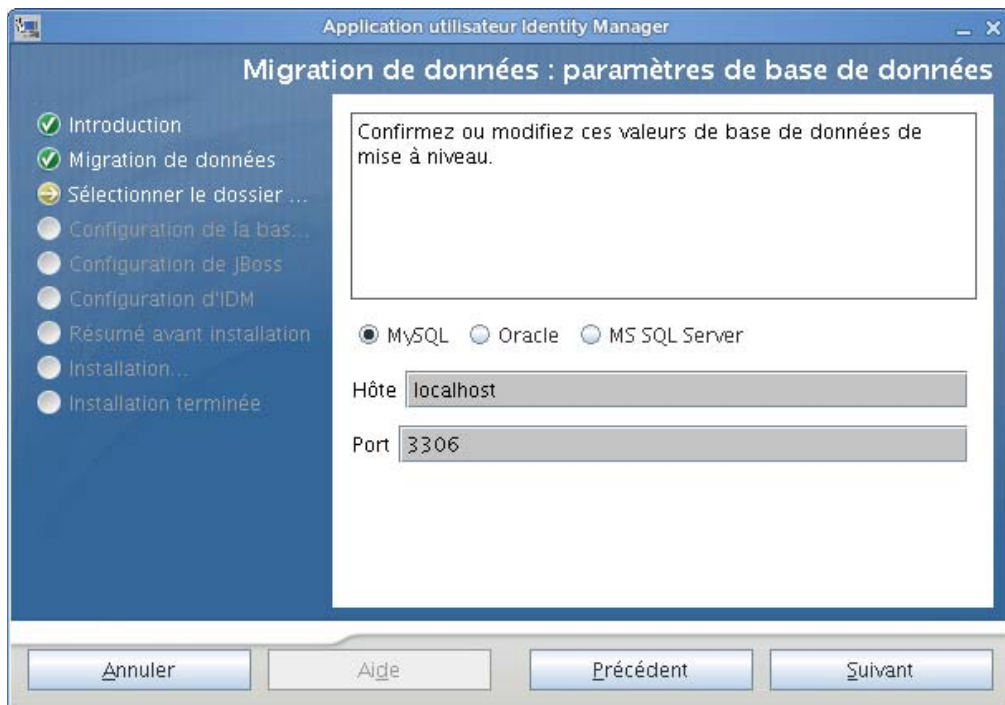
Si vous souhaitez utiliser une base de données existante depuis la version 3.0 ou version 3.01 de l'application utilisateur, vous devez migrer la base de données. Passez à l'étape suivante.

- 2 Vérifiez que vous avez démarré la base de données que vous souhaitez migrer.
- 3 Cliquez sur *Oui* sur la page Migration de données du programme d'installation.
- 4 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.

Le fait d'indiquer l'emplacement du fichier `install.properties` de votre installation précédente réduit le nombre des éléments que vous devrez indiquer aux pages suivantes.



- 5 Vous devez confirmer le type de base de données, le nom d'hôte et le port. Pour cela, cliquez sur *Suivant*.



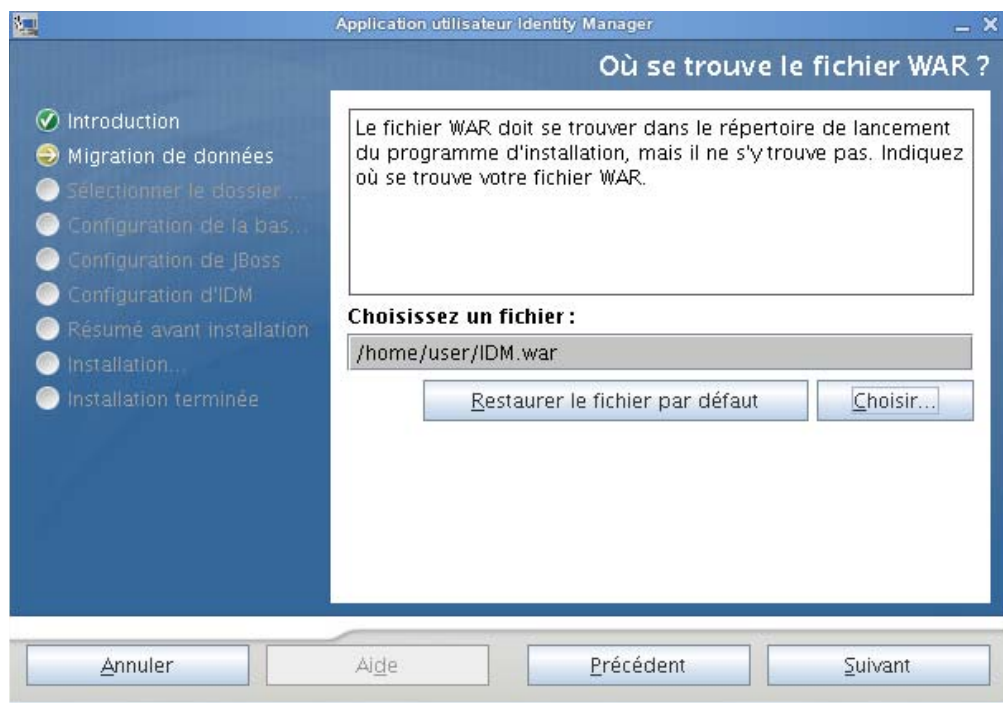
- 6 Cliquez sur *Suivant*, puis passez à [Section 4.4, « Emplacement du WAR », page 43](#) ou à [Section 4.5, « Choix d'un dossier d'installation », page 43](#).

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/idmrbpm36/index.html>).

## 4.4 Emplacement du WAR

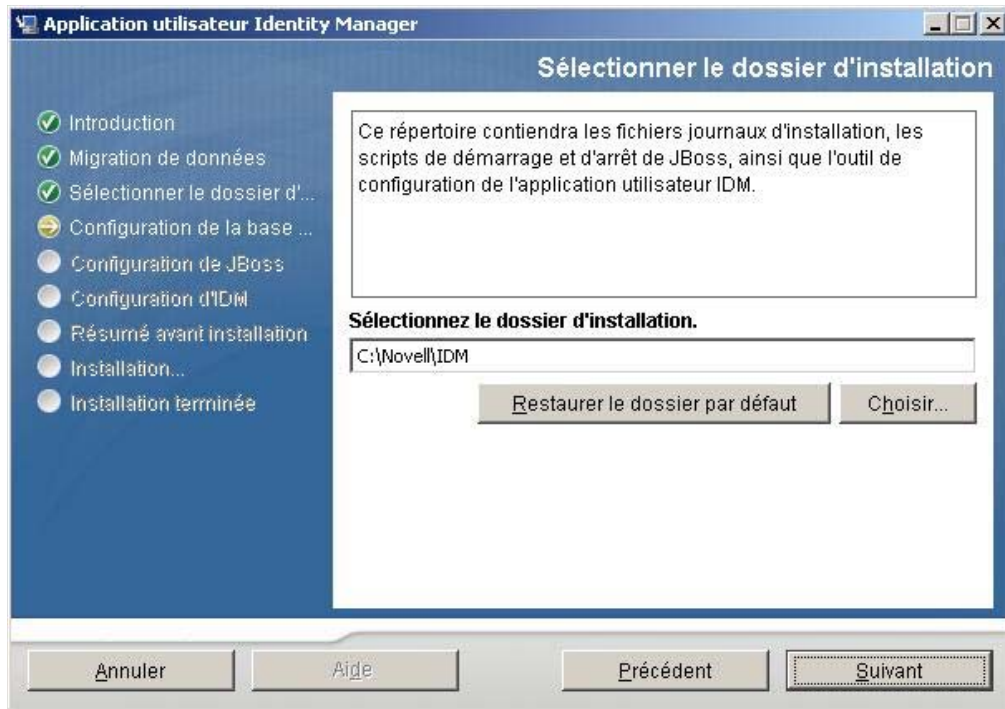
Si le fichier WAR de l'application utilisateur Identity Manager est dans un répertoire différent du programme d'installation, ce dernier vous invite à saisir le chemin d'accès au WAR.

- 1 Si le fichier WAR se trouve à l'emplacement par défaut, cliquez sur *Restaurer le fichier 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 4.5, « Choix d'un dossier d'installation », page 43.**



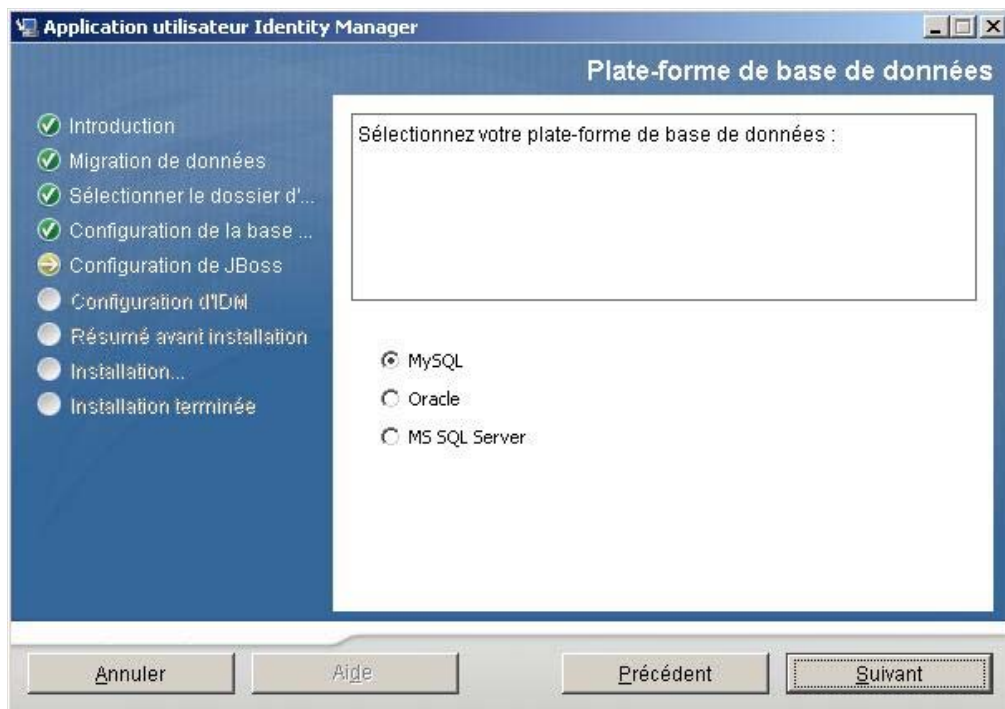
## 4.5 Choix d'un dossier d'installation

- 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 4.6, « Choix d'une plate-forme de base de données », page 44.**



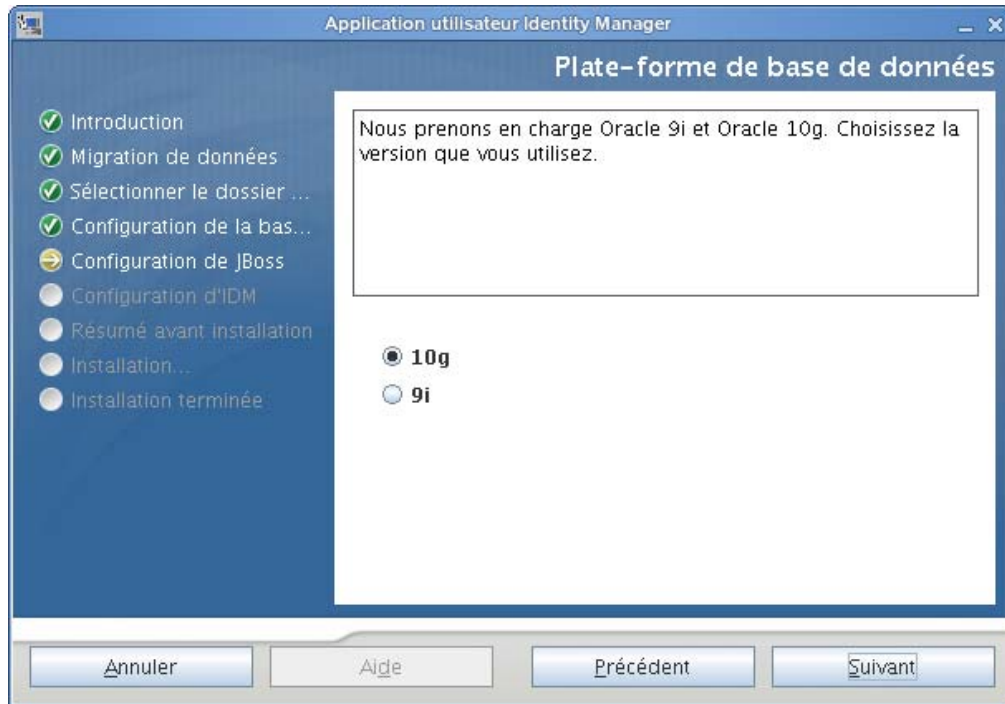
## 4.6 Choix d'une plate-forme de base de données

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



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

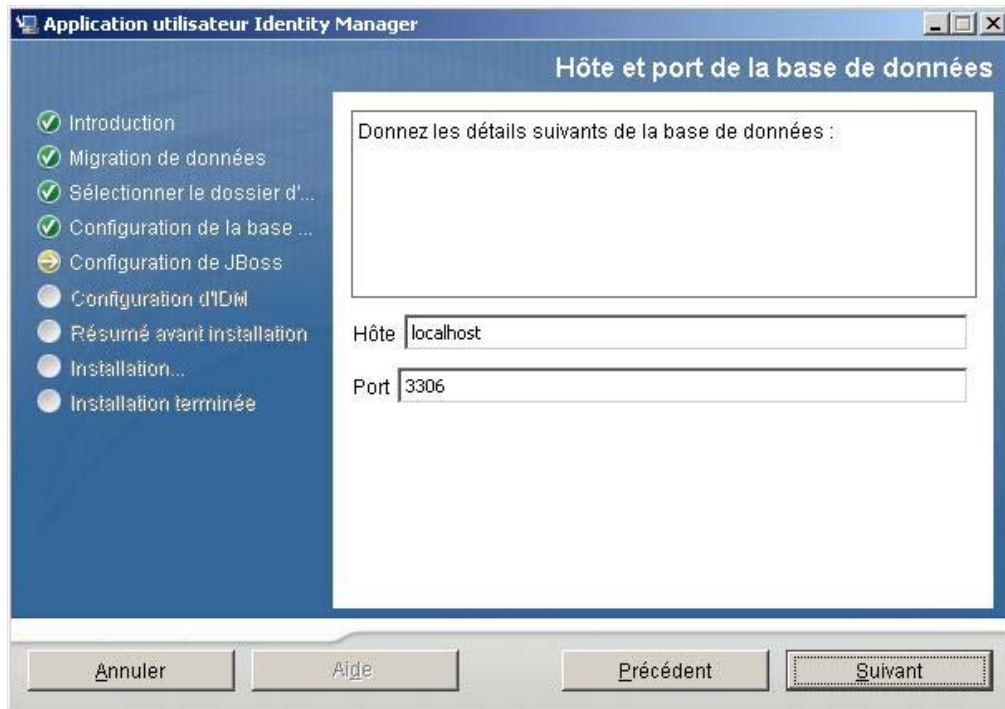
- 3 Si vous utilisez une base de données Oracle, le programme d'installation demande quelle version vous utilisez. Choisissez votre version.



- 4 Cliquez sur *Suivant*, puis passez à [Section 4.7, « Spécification de l'hôte et du port de la base de données »](#), page 45.

## 4.7 Spécification de l'hôte et du port de la base de données

- 1 Remplissez les champs suivants :

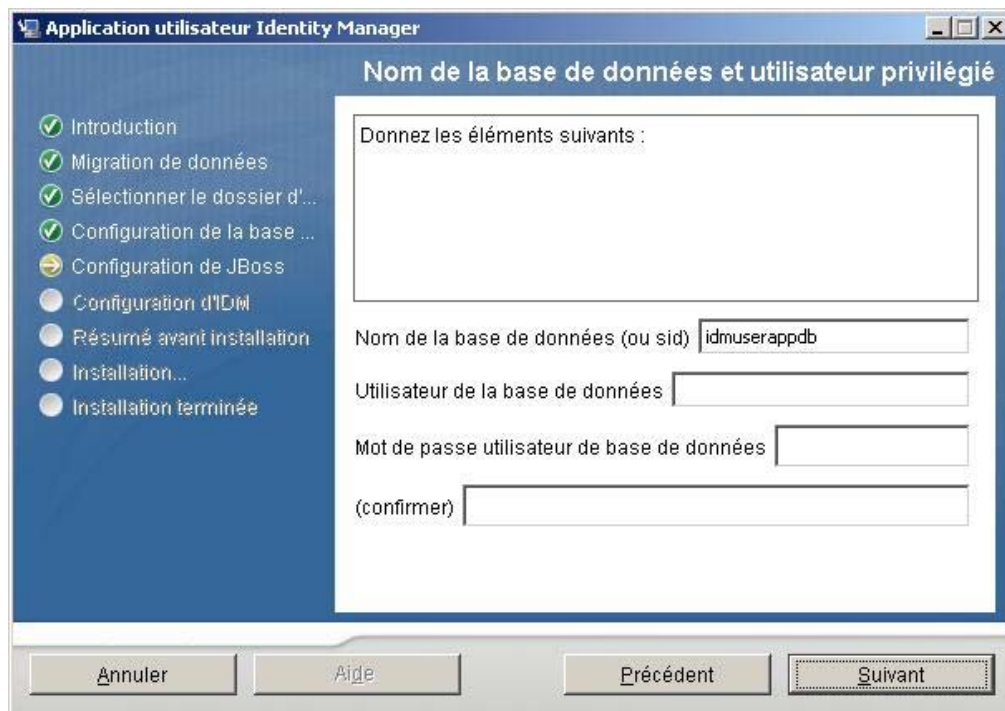


Champ	Description
<i>Hôte</i>	Indiquez le nom d'hôte ou l'adresse IP du serveur de bases de données. Pour une grappe, indiquez le même nom d'hôte ou la même adresse IP pour chaque membre de la grappe.
<i>Port</i>	Indiquez le numéro du port d'écoute de la base de données. Pour une grappe, indiquez le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

- 2 Cliquez sur *Suivant*, puis passez à [Section 4.8, « Spécification du nom de la base de données et de l'utilisateur privilégié », page 46.](#)

## 4.8 Spécification du nom de la base de données et de l'utilisateur privilégié

- 1 Remplissez les champs suivants :

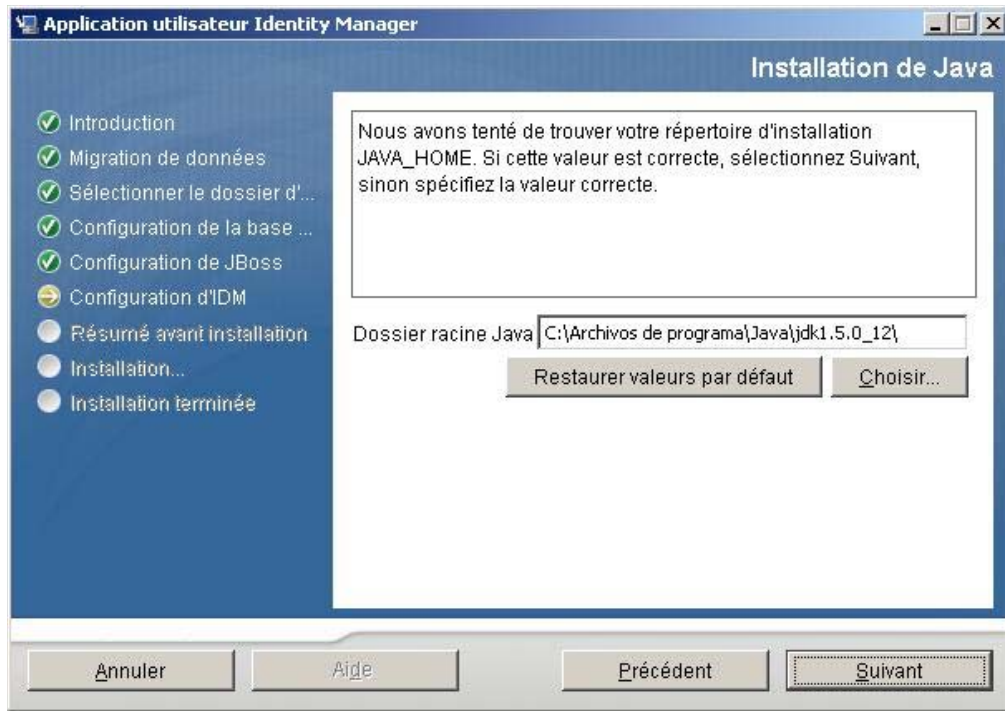


Champ	Description
<i>Nom de la base de données (ou sid)</i>	<p>Pour le serveur MySQL ou MS SQL, donnez le nom de votre base de données préconfigurée. Pour Oracle, donnez l'identificateur système Oracle (SID) que vous avez créé précédemment.</p> <p>Pour une grappe, indiquez le même nom ou SID de base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

- 2 Cliquez sur *Suivant*, puis passez à [Section 4.9, « Spécification du répertoire racine Java », page 47.](#)

## 4.9 Spécification du 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*.

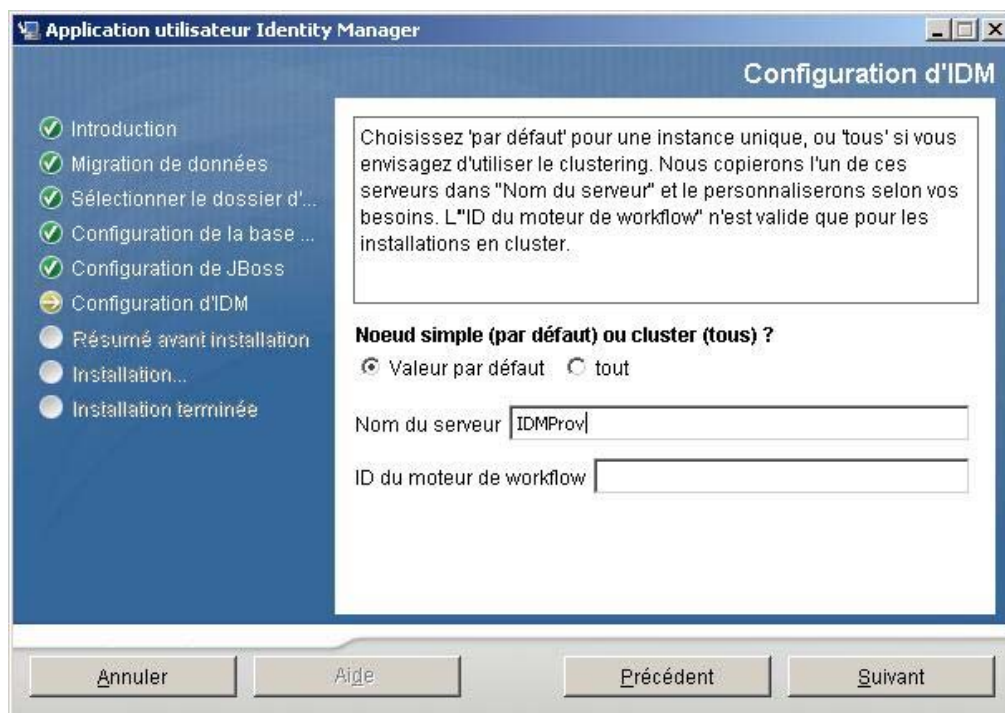


- 2 Cliquez sur *Suivant*, puis passez à [Section 4.11, « Spécification des paramètres du serveur d'applications JBoss »](#), page 50.

## 4.10 Choix du type de configuration du serveur d'applications

- 1 Remplissez les champs suivants :





Option	Description
<i>Simple</i> (par défaut) ou <i>mise en grappe</i> (tous)	<p>Sélectionnez le type de configuration du serveur d'applications :</p> <ul style="list-style-type: none"> <li>◆ Sélectionnez <i>tous</i> si cette installation fait partie d'une grappe</li> <li>◆ Sélectionnez <i>par défaut</i> si cette installation est sur un noeud simple qui ne fait pas partie d'une grappe</li> </ul>
<i>Nom du serveur</i>	<p>Définissez le nom du serveur.</p> <p>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 <i>Nom de l'application</i>.</p> <p>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.</p>
<i>ID du moteur de workflow</i>	<p>Chaque serveur d'une grappe doit avoir un ID de moteur de workflow unique. Les ID de moteur de workflow sont décrits dans le <i>Guide d'administration de l'application utilisateur Identity Manager</i> à la section 3.5.4, Configuration de workflows pour la mise en grappe.</p>

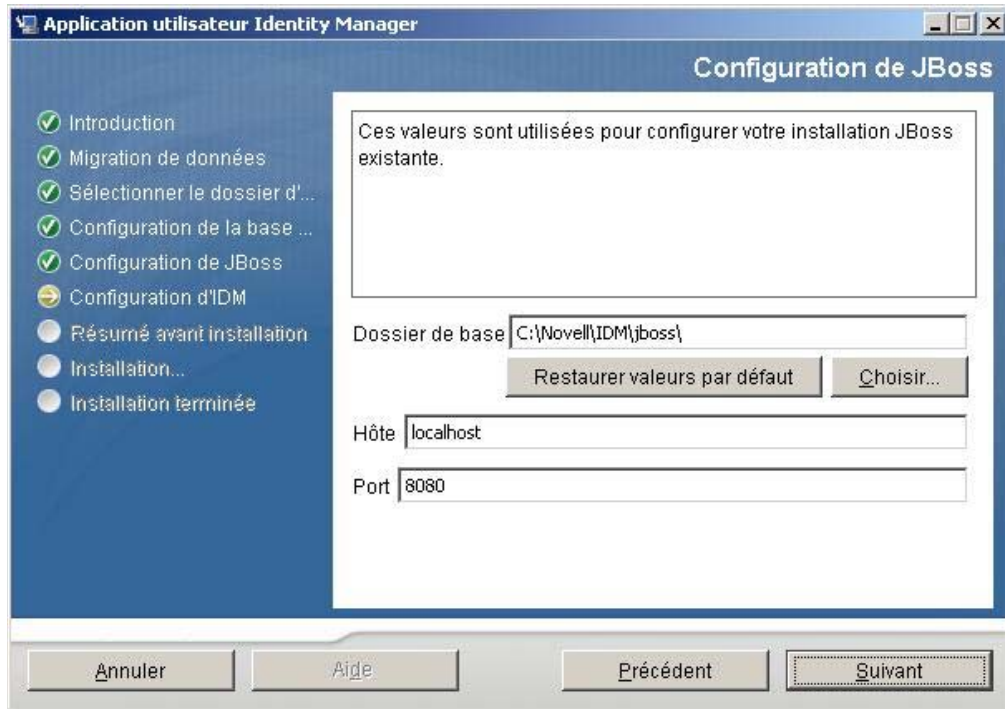
- 2 Cliquez sur *Suivant*, puis passez à [Section 4.12, « Activation de la consignment Novell Audit »](#), page 50.

## 4.11 Spécification des 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 instructions sur l'installation du serveur d'applications JBoss, reportez-vous à [Section 2.3.1, « Installation du serveur d'applications JBoss et de la base de données MySQL »](#), page 21.

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



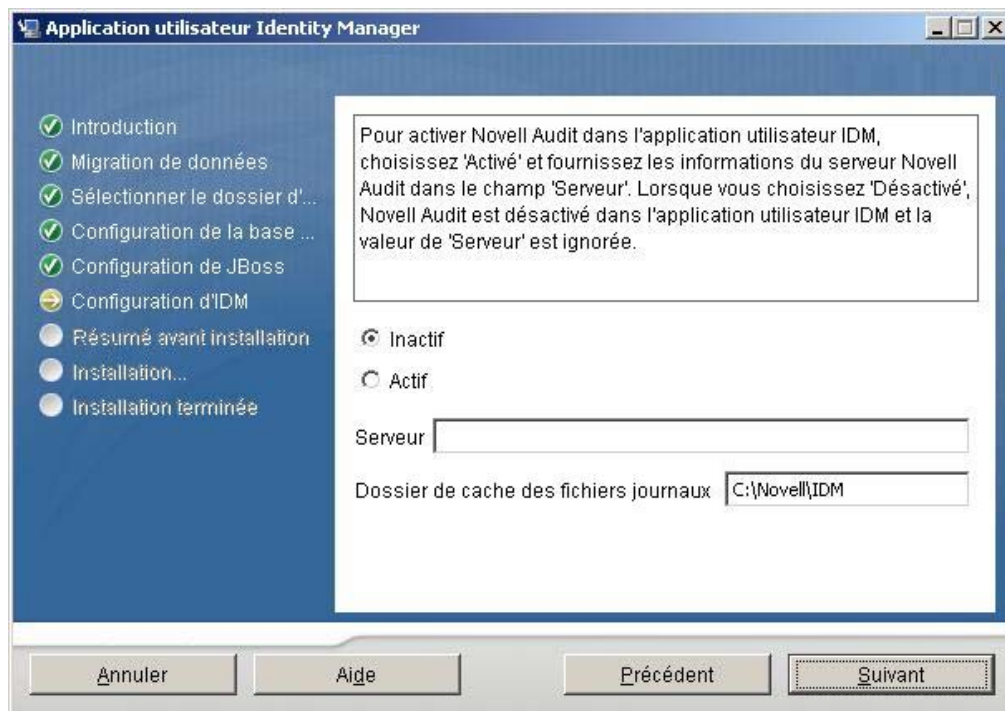
Champ	Description
<i>Dossier de base</i>	Indiquez l'emplacement du serveur d'applications.
<i>Hôte</i>	Indiquez le nom d'hôte ou l'adresse IP du serveur d'applications
<i>Port</i>	Indiquez le numéro de port d'écoute du serveur d'applications. Le port JBoss par défaut est 8080.

- 2 Cliquez sur *Suivant*, puis passez à [Section 4.10, « Choix du type de configuration du serveur d'applications »](#), page 48.

## 4.12 Activation de la consignation Novell Audit

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

- 1 Remplissez les champs suivants :



Option	Description
<i>Actif</i>	Active la consignation Novell Audit de l'application utilisateur.  Pour plus d'informations sur la configuration de la consignation Novell Audit, reportez-vous au <i>Guide d'administration de l'application utilisateur Identity Manager</i> .
<i>Inactif</i>	Désactive la consignation Novell Audit de l'application utilisateur. Vous pouvez l'activer plus tard via l'onglet <i>Administration</i> de l'application utilisateur.  Pour plus d'informations sur l'activation de la consignation Novell Audit, reportez-vous au <i>Guide d'administration de l'application utilisateur Identity Manager</i> .
<i>Serveur</i>	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.

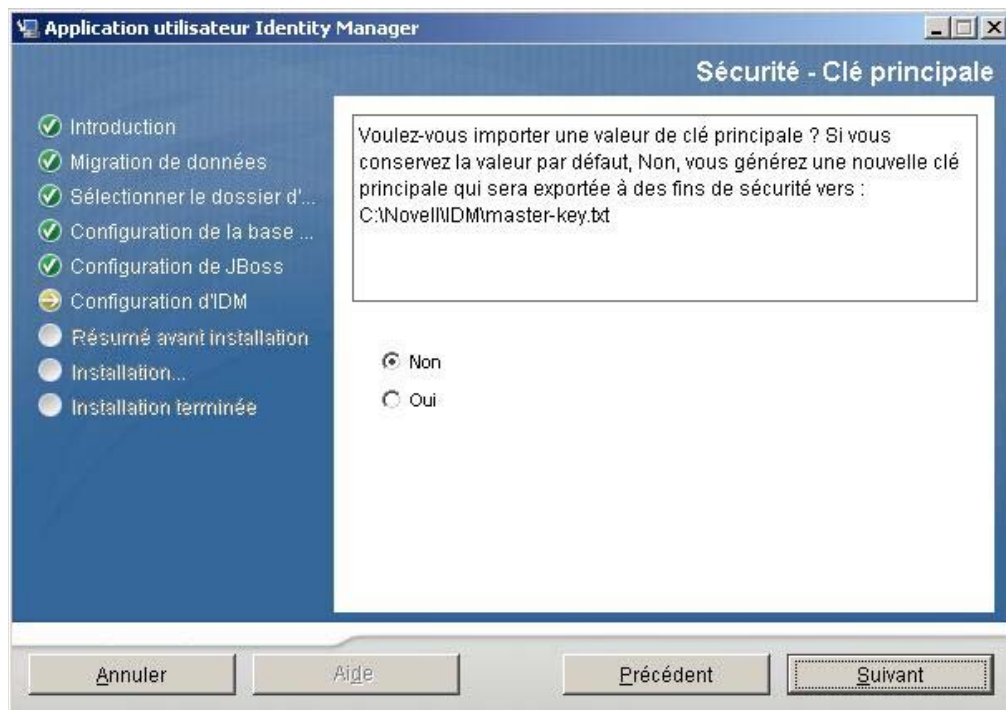
- 2 Cliquez sur *Suivant*, puis passez à [Section 4.14, « Configuration de l'application utilisateur », page 53](#).

## 4.13 Spécification d'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.



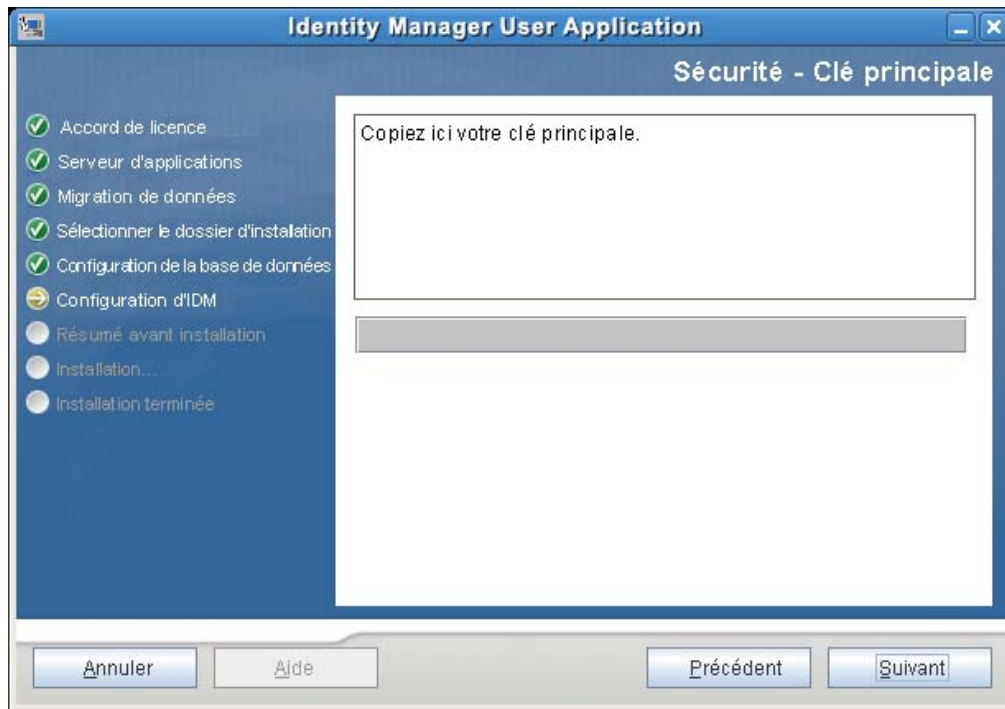
- 2 Cliquez sur *Suivant*.

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 l'[Section 4.14, « Configuration de l'application utilisateur », page 53](#). Une fois l'installation terminée, vous devez enregistrer manuellement la clé maîtresse tel que décrit dans [Section 7.1, « Enregistrement de la clé maîtresse », page 111](#).

Si vous sélectionnez *Oui*, passez à l'[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*.

## 4.14 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 le [Tableau 4-1](#), puis passez à l'[Étape 2](#).

Configuration de l'application utilisateur

**Paramètres de connexion eDirectory**

Hôte LDAP : mysystem.mycompany.com

Port LDAP non sécurisé : 389

Port LDAP sécurisé : 636

Administrateur LDAP : cn=admin,o=novell

Mot de passe de l'administrateur LDAP : \*\*\*\*\*

Utiliser un compte anonyme public :

Invité LDAP : cn=guest,ou=idmsample-test,o=novell

Mot de passe de l'invité LDAP : \*\*\*\*\*

Connexion admin sécurisée :

Connexion utilisateur sécurisée :

**DN eDirectory**

DN du conteneur racine : ou=idmsample-test,o=novell

DN du pilote de provisioning : cn=myDriver,cn=TestDrivers,o=novell

Admin d'application utilisateur : cn=admin,ou=ou=idmsample-test,o=novell

Admin d'application de provisioning : cn=adminprov,ou=ou=idmsample-test,o=novell

DN du conteneur de l'utilisateur :: ou=idmsample-test,o=novell

DN du conteneur du groupe :: ou=groups,ou=idmsample-test,o=novell

**Certificats eDirectory**

Chemin du fichier keystore : C:\Program Files\Java\jdk1.5.0\_06\lib\security' ...

Mot de passe Keystore : \*\*\*\*\*

Confirmer le mot de passe Keystore : \*\*\*\*\*

**Courrier électronique**

Adresse e-mail de l'administrateur :

OK    Annuler    Afficher les options avancées

**Tableau 4-1** Configuration de l'application utilisateur : paramètres de base

Type de paramètre	Champ	Description
Paramètres de connexion eDirectory	<i>Hôte LDAP</i>	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP et son port sécurisé. Par exemple : myLDAPhost
	<i>Port non sécurisé LDAP</i>	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	<i>Port sécurisé LDAP</i>	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	<i>Administrateur LDAP</i>	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer une connexion administrative au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
	<i>Mot de passe administrateur LDAP</i>	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
	<i>Utiliser le compte anonyme public</i>	Permet aux utilisateurs non logués d'accéder au compte anonyme public LDAP.
	<i>Guest LDAP</i>	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 l'invité LDAP, vous devez désactiver <i>Utiliser un compte anonyme public</i> . Pour désactiver l'utilisateur invité, sélectionnez <i>Utiliser un compte anonyme public</i> .
	<i>Mot de passe Guest LDAP</i>	Indiquez le mot de passe Guest LDAP.
	<i>Connexion admin. sécurisée</i>	Sélectionnez cette option pour que toutes les communications utilisant le compte administrateur soient effectuées à l'aide d'un socket sécurisé (cette option peut nuire aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.
	<i>Login utilisateur sécurisé</i>	Sélectionnez cette option pour que toutes les communications utilisant le compte de l'utilisateur logué soient effectuées à l'aide d'un socket sécurisé (cette option peut nuire aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.

Type de paramètre	Champ	Description
DN eDirectory	<i>DN du conteneur racine</i>	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.
	<i>DN du pilote de provisioning</i>	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur que vous avez créé auparavant dans <a href="#">Section 3.1, « Création du pilote d'application utilisateur dans iManager », page 33</a> . Par exemple, si votre pilote est <code>UserApplicationDriver</code> et si votre ensemble de pilotes est appelé <code>myDriverSet</code> , et si l'ensemble de pilotes est dans un contexte de <code>o=myCompany</code> , vous saisissez une valeur de : <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
	<i>Admin. application utilisateur</i>	<p>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 <i>Administration</i> de l'application utilisateur pour administrer le portail.</p> <p>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 <i>Requêtes et approbations</i>), 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 <i>Guide d'administration de l'application utilisateur IDM</i> pour en savoir plus.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration &gt; Sécurité</i> de l'application utilisateur.</p>
<i>Admin. application provisioning</i>	<p>L'administrateur de l'application de provisioning utilise l'onglet <i>Provisioning</i> (sous l'onglet <i>Administration</i>) pour gérer les fonctions de workflow du provisioning. Ces fonctions sont accessibles aux utilisateurs en passant par l'onglet <i>Requêtes et approbations</i> de l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur de l'application Provisioning.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration &gt; Sécurité</i> de l'application utilisateur.</p>	



Type de paramètre	Champ	Description
DN eDirectory (suite)	<i>Administrateur de rôles</i>	<p>Ce rôle est disponible dans le module de provisioning basé sur les rôles de Novell d'Identity Manager. Il permet aux membres de créer, de supprimer ou de modifier l'ensemble des rôles, ainsi que de révoquer les assignations de rôles des utilisateurs, des groupes ou des conteneurs. Il permet également à ses membres d'exécuter des rapports pour n'importe quel utilisateur. Par défaut, ce rôle est assigné à l'administrateur de l'application utilisateur.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page <i>Rôles &gt; Assignations de rôles</i> de l'application utilisateur.</p>
	<i>DN du conteneur d'utilisateurs</i>	<p>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.</p> <hr/> <p><b>Important :</b> 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.</p>
	<i>DN de conteneur de groupes</i>	<p>Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur de groupes.</p> <p>Utilisé par les définitions d'entités au sein de la couche d'abstraction d'annuaire.</p>
Certificats eDirectory	<i>Chemin d'accès au Keystore</i>	<p>Requis. Indiquez le chemin d'accès complet au fichier (<i>cacerts</i>) 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 <i>cacerts</i> .</p> <p>Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier.</p>
	<i>Mot de passe Keystore/ Confirmer mot de passe Keystore</i>	<p>Requis. Indiquez le mot de passe <i>cacerts</i>. L'unité par défaut est <i>changeit</i>.</p>

Type de paramètre	Champ	Description
Courrier électronique	<i>Jeton de l'hôte du modèle de notification</i>	Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple : <code>myapplication serverServer</code>  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.
	<i>Jeton du port du modèle de notification</i>	Utilisé pour remplacer le jeton \$PORT\$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	<i>Jeton du port sécurisé du modèle de notification</i>	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.
	<i>Notification SMTP - expéditeur du courrier électronique</i>	Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
	<i>Notification SMTP - destinataire du courrier électronique</i>	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	<i>Utiliser le WAR de mots de passe externe</i>	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 <i>Utiliser le WAR de mot de passe externe</i> , vous devez fournir des valeurs pour <i>Lien Mot de passe oublié</i> et <i>Lien Retour mot de passe oublié</i> .  Si vous ne sélectionnez pas <i>Utiliser le WAR de mot de passe externe</i> , IDM utilise la fonction de gestion des mots de passe interne par défaut. <code>/jsps/pwdmgt/ForgotPassword.jsf</code> (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
	<i>Liaison Mot de passe oublié</i>	Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier <code>ForgotPassword.jsf</code> dans un WAR de gestion des mots de passe externe ou interne. Pour plus de détails, reportez-vous à « <a href="#">Utilisation des WAR de mots de passe</a> » page 67.
	<i>Liaison de retour Mot de passe oublié</i>	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 <code>https:// idmhost:sslport/idm .</code>

- 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.) Le [Tableau 4-2](#) décrit les paramètres des options avancées.

Si vous ne souhaitez pas définir d'autres paramètres décrits dans cette étape, passez à l'[Étape 3](#).

**Tableau 4-2** Configuration de l'application utilisateur : tous les paramètres

Type de paramètre	Champ	Description
Paramètres de connexion eDirectory	<i>Hôte LDAP</i>	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP. Par exemple :  myLDAPhost
	<i>Port non sécurisé LDAP</i>	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	<i>Port sécurisé LDAP</i>	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	<i>Administrateur LDAP</i>	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer une connexion administrative au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
	<i>Mot de passe administrateur LDAP</i>	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
	<i>Utiliser le compte anonyme public</i>	Permet aux utilisateurs non logués d'accéder au compte anonyme public LDAP.
	<i>Guest LDAP</i>	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 <i>Utiliser le compte anonyme public</i> . Pour désactiver l'utilisateur Guest, sélectionnez <i>Utiliser le compte anonyme public</i> .
	<i>Mot de passe Guest LDAP</i>	Indiquez le mot de passe Guest LDAP.
	<i>Connexion admin. sécurisée</i>	Sélectionnez cette option pour que toutes les communications utilisant le compte administrateur soient effectuées à l'aide d'un socket sécurisé (cette option peut nuire aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.
	<i>Login utilisateur sécurisé</i>	Sélectionnez cette option pour que toutes les communications sur le compte de l'utilisateur logué soient effectuées à l'aide d'un socket sécurisé (cette option peut nuire aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.

Type de paramètre	Champ	Description
DN eDirectory	<i>DN du conteneur racine</i>	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.
	<i>DN du pilote de provisioning</i>	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur que vous avez créé auparavant dans <a href="#">Section 3.1, « Création du pilote d'application utilisateur dans iManager », page 33</a> . Par exemple, si votre pilote est <code>UserApplicationDriver</code> et si votre ensemble de pilotes est appelé <code>myDriverSet</code> , et si l'ensemble de pilotes est dans un contexte de <code>o=myCompany</code> , vous saisissez une valeur de : <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
	<i>Admin. application utilisateur</i>	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 <i>Administration</i> 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 <i>Requêtes et approbations</i> ), 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 <i>Guide d'administration de l'application utilisateur IDM</i> pour en savoir plus.  Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration &gt; Sécurité</i> de l'application utilisateur.
	<i>Admin. application provisioning</i>	L'administration de l'application de provisioning gère les fonctions de workflow du provisioning accessibles par l'onglet <i>Requêtes et approbations</i> 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 <i>Administration &gt; Sécurité</i> de l'application utilisateur.

Type de paramètre	Champ	Description
Identité utilisateur du méta-annuaire	<i>DN du conteneur d'utilisateurs</i>	<p>Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur d'utilisateurs.</p> <p>Cela définit l'étendue de recherche d'utilisateurs et de groupes.</p> <p>Les utilisateurs de ce conteneur (et en-dessous) sont autorisés à se loguer à l'application utilisateur.</p> <hr/> <p><b>Important</b> : 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.</p> <hr/>
	<i>Classe d'objets Utilisateur</i>	La classe d'objets utilisateur LDAP (généralement inetOrgPerson).
	<i>Attribut de login</i>	L'attribut LDAP (par exemple, CN) qui représente le nom de login de l'utilisateur.
	<i>Attribut de nom</i>	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.
	<i>Attribut de l'adhésion utilisateur</i>	Facultatif. L'attribut LDAP qui représente l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.
	<i>Administrateur de rôles</i>	<p>Ce rôle est disponible dans le module de provisioning basé sur les rôles de Novell d'Identity Manager. Il permet aux membres de créer, de supprimer ou de modifier l'ensemble des rôles, ainsi que de révoquer les assignations de rôles des utilisateurs, des groupes ou des conteneurs. Il permet également à ses membres d'exécuter des rapports pour n'importe quel utilisateur. Par défaut, ce rôle est assigné à l'administrateur de l'application utilisateur.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page <i>Rôles &gt; Assignations de rôles</i> de l'application utilisateur.</p>

Type de paramètre	Champ	Description
Groupes d'utilisateurs du méta-annuaire	<i>DN de conteneur de groupes</i>	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.
	<i>Classe d'objets Groupe</i>	La classe d'objets Groupe LDAP (généralement groupofNames).
	<i>Attribut d'adhésion à un groupe</i>	L'attribut qui représente l'adhésion d'un utilisateur à un groupe. N'utilisez pas d'espaces pour le nom.
	<i>Utiliser des groupes dynamiques</i>	Sélectionnez cette option si vous souhaitez utiliser des groupes dynamiques.
	<i>Classe d'objets Groupe dynamique</i>	La classe d'objets Groupe dynamique LDAP (généralement dynamicGroup).
Certificats eDirectory	<i>Chemin d'accès au Keystore</i>	Requis. Indiquez le chemin d'accès complet au fichier ( <i>cacerts</i> ) 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 <i>cacerts</i> .  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.
	<i>Mot de passe Keystore</i> <i>Confirmer le mot de passe Keystore</i>	Requis. Indiquez le mot de passe <i>cacerts</i> . L'unité par défaut est <i>changeit</i> .
Keystore privé	<i>Chemin d'accès au keystore privé</i>	Le keystore privé contient la clé privée et les certificats de l'application utilisateur. Réservez. Si vous laissez ce champ vierge, ce chemin d'accès est <i>/jre/lib/security/cacerts</i> par défaut.
	<i>Mot de passe Keystore privé</i>	Ce mot de passe est <i>changeit</i> , à moins d'indication contraire. Ce mot de passe est codé, en fonction de la clé maîtresse.
	<i>Alias de clé privée</i>	Cet alias est <i>novellIDMUserApp</i> , à moins d'indication contraire.
	<i>Mot de passe de la clé privée</i>	Ce mot de passe est <i>novellIDM</i> , à moins d'indication contraire. Ce mot de passe est codé, en fonction de la clé maîtresse.

Type de paramètre	Champ	Description
Banque de clés approuvée	<i>Chemin d'accès à la banque approuvée</i>	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 <code>javax.net.ssl.trustStore</code> . Si le chemin n'y est pas, il est supposé être <code>jre/lib/security/cacerts</code> .
	<i>Mot de passe de la banque approuvée</i>	Si ce champ est vierge, l'application utilisateur obtient le mot de passe à partir de la propriété système <code>javax.net.ssl.trustStorePassword</code> . S'il n'y a aucune valeur, <code>changeit</code> 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.
	<i>Certificat de signature numérique Novell Audit</i>	Affiche le certificat de signature numérique.
	<i>Clé privée de signature numérique Novell Audit</i>	Affiche la clé privée de signature numérique. Cette clé est codée, en fonction de la clé maîtresse.
Paramètres Access Manager et iChain	<i>Logout simultané activé</i>	Si cette option est activée, l'application utilisateur prend en charge le logout simultané de l'application utilisateur et de Novell Access Manager ou d'iChain. L'application utilisateur vérifie la présence du cookie iChain ou Novell Access Manager durant le logout ; s'il est présent, elle redirige l'utilisateur vers la page de logout simultané.
	<i>Page de Logout simultané</i>	L'URL pointant vers la page de logout de Novell Access Manager ou iChain, lorsque l'URL est un nom d'hôte attendu par Novell Access Manager ou iChain. Si la fonction de logout simultané est activée et si un utilisateur se délogue de l'application utilisateur, l'utilisateur est redirigé vers cette page. L'une des URL ci-dessous doit diriger la fonction de logout simultané vers la page correcte en fonction de l'environnement.  Access Manager : <code>https://votreServeurDePasserelleAccess/AGLogout</code>  iChain : <code>https://votreServeurIChain/cmd/ICSLogout</code>



Type de paramètre	Champ	Description
Courrier électronique	<i>Jeton de l'hôte du modèle de notification</i>	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.
	<i>Jeton du port du modèle de notification</i>	Utilisé pour remplacer le jeton \$PORT\$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	<i>Jeton du port sécurisé du modèle de notification</i>	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.
	<i>Jeton du protocole du modèle de notification</i>	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.
	<i>Jeton du protocole sécurisé du modèle de notification</i>	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.
	<i>Notification SMTP - expéditeur du courrier électronique</i>	Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
	<i>Notification SMTP - destinataire du courrier électronique</i>	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	<i>Utiliser le WAR de mots de passe externe</i>	<p>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.</p> <p>Si vous sélectionnez <i>Utiliser le WAR de mot de passe externe</i>, vous devez fournir des valeurs pour <i>Lien Mot de passe oublié</i> et <i>Lien Retour mot de passe oublié</i>.</p> <p>Si vous ne sélectionnez pas <i>Utiliser le WAR de mot de passe externe</i>, IDM utilise la fonction de gestion des mots de passe interne par défaut. <code>/jsp/pwdmgt/ForgotPassword.jsf</code> (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.</p>
	<i>Liaison Mot de passe oublié</i>	<p>Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier <code>ForgotPassword.jsf</code> dans un WAR de gestion des mots de passe externe ou interne. Pour plus de détails, reportez-vous à <b>« Utilisation des WAR de mots de passe » page 67</b>.</p>
	<i>Liaison de retour Mot de passe oublié</i>	<p>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 <code>https://idmhost:sslport/idm</code>.</p>
Divers	<i>Timeout de session</i>	Le timeout de session de l'application.
	<i>OCSP URI</i>	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 <code>http://host:port/ocspLocal</code> . L'URI OCSP met à jour le statut des certificats approuvés en ligne.
	<i>Chemin de configuration d'autorisation</i>	Nom complet du fichier de configuration de l'autorisation.

Type de paramètre	Champ	Description
Objet Conteneur	<i>Sélectionné</i>	Sélectionnez chaque type d'objet Conteneur à utiliser.
	<i>Type d'objet Conteneur</i>	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 <i>Ajouter un nouvel objet Conteneur</i> .
	<i>Nom de l'attribut Conteneur</i>	Indique le nom de type d'attribut associé au type d'objet Conteneur.
	<i>Ajouter un nouvel objet Conteneur : type d'objet Conteneur</i>	Indiquez le nom LDAP d'une classe d'objets du coffre-fort d'identité qui peut servir de conteneur.
	<i>Ajouter un nouvel objet Conteneur : nom d'attribut Conteneur</i>	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 4.16, « Vérification des choix et installation », page 68](#)

## 4.15 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.

- ♦ [Section 4.15.1, « Spécification d'un WAR de gestion des mots de passe externe », page 67](#)
- ♦ [Section 4.15.2, « Spécification d'un WAR de mot de passe interne », page 68](#)

### 4.15.1 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/jsp/pwdmgt/ForgotPassword.jsf`. Un WAR de mots de passe externe peut être en-dehors du pare-feu qui protège l'application utilisateur.

- 4 Pour le *Lien 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 7.4, « Configuration de la communication SSL entre serveurs JBoss », page 112](#).

- 5 Effectuez l'une des opérations suivantes :

- ♦ Si vous utilisez le programme d'installation, lisez les informations de cette étape, puis passez à l'[Étape 6 page 68](#).
- ♦ 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 page 68](#).

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.idmpwdmghost.com/ExternalPwd/jsp/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.

## 4.15.2 Spécification d'un WAR de mot de passe interne

- 1 Dans les paramètres de configuration de l'application utilisateur, ne cochez pas la case *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*.

## 4.16 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*.

## 4.17 Affichage des fichiers journaux

- 1 Si votre installation s'est terminée sans erreur, passez à [Chapitre 7, « Tâches post-installation »](#), page 111.
- 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 7.12, « Dépannage »](#), page 115.



# Installation depuis la console ou à l'aide d'une commande unique

# 5

Cette section décrit les méthodes d'installation dont vous disposez si vous ne souhaitez pas utiliser l'interface graphique décrite au [Chapitre 4, « Installation de JBoss depuis une interface graphique », page 39](#). Les rubriques incluent :

- ♦ [Section 5.1, « Installation de l'application utilisateur à partir de la console », page 71](#)
- ♦ [Section 5.2, « Installation de l'application utilisateur avec une seule commande », page 71](#)

## 5.1 Installation de l'application utilisateur à partir de la console

Cette section décrit l'installation de l'application utilisateur Identity Manager à l'aide de la console (ligne de commande) du programme d'installation.

- 1 Obtenez les fichiers d'installation appropriés décrits dans le [Tableau 2-1 page 27](#).
- 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 [Chapitre 4, « Installation de JBoss depuis une interface graphique », page 39](#) : 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 définir les paramètres de configuration de l'application utilisateur, lancez 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 4.14, « Configuration de l'application utilisateur », page 53](#).
- 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 [Chapitre 7, « Tâches post-installation », page 111](#).

## 5.2 Installation de l'application utilisateur avec une seule commande

Cette section décrit l'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 le [Tableau 2-1 page 27](#).
- 2 Loguez-vous et ouvrez une session de terminal.

**3** Recherchez le fichier de propriétés Identity Manager, `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 au **Tableau 5-1** 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 5-1** Paramètres de configuration de l'application utilisateur pour l'installation en mode silencieux

Nom du paramètre de l'application utilisateur dans <code>silent.properties</code>	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_LDAPHOST=	Paramètres de connexion eDirectory : hôte LDAP.  Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP.
NOVL_CONFIG_LDAPADMIN=	Paramètres de login eDirectory : administrateur LDAP.  Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer une connexion administrative 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.



Nom du paramètre de l'application utilisateur dans <code>silent.properties</code>	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_ROOTCONTAINERNAME=	<p>DN eDirectory : DN du conteneur racine.</p> <p>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.</p>
NOVL_CONFIG_PROVISIONROOT=	<p>DN eDirectory : DN du pilote de provisioning.</p> <p>Requis. Indiquez le nom distinctif du pilote de l'application utilisateur que vous avez créé auparavant dans <a href="#">Section 3.1, « Création du pilote d'application utilisateur dans iManager », page 33</a>. Par exemple, si votre pilote est <code>UserApplicationDriver</code> et si votre ensemble de pilotes est appelé <code>myDriverSet</code>, et si l'ensemble de pilotes est dans un contexte de <code>o=myCompany</code>, vous saisissez une valeur de :</p> <pre>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</pre>
NOVL_CONFIG_LOCKSMITH=	<p>DN eDirectory : admin. de l'application utilisateur.</p> <p>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 <i>Administration</i> de l'application utilisateur pour administrer le portail.</p> <p>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 <i>Requêtes et approbations</i>), 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 <i>Guide d'administration de l'application utilisateur IDM</i> pour en savoir plus.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration &gt; Sécurité</i> de l'application utilisateur.</p>

Nom du paramètre de l'application utilisateur dans <code>silent.properties</code>	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_PROVLOCKSMITH=	<p>DN eDirectory : administrateur de l'application de provisioning.</p> <p>Ce rôle est disponible dans la version de provisioning d'Identity Manager . L'administrateur de l'application de provisioning utilise l'onglet <i>Provisioning</i> (sous l'onglet <i>Administration</i>) pour gérer les fonctions de workflow du provisioning. Ces fonctions sont accessibles aux utilisateurs en passant par l'onglet <i>Requêtes et approbations</i> de l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur de l'application Provisioning.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration &gt; Sécurité</i> de l'application utilisateur.</p>
NOVL_CONFIG_ROLECONTAINERDN=	<p>Ce rôle est disponible dans le module de provisioning basé sur les rôles de Novell d'Identity Manager. Il permet aux membres de créer, de supprimer ou de modifier l'ensemble des rôles, ainsi que de révoquer les assignations de rôles des utilisateurs, des groupes ou des conteneurs. Il permet également à ses membres d'exécuter des rapports pour n'importe quel utilisateur. Par défaut, ce rôle est assigné à l'administrateur de l'application utilisateur.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page <i>Rôles &gt; Assignations de rôles</i> de l'application utilisateur.</p>
NOVL_CONFIG_USERCONTAINERDN=	<p>Identité utilisateur du méta-annuaire : DN du conteneur utilisateur.</p> <p>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.</p> <hr/> <p><b>Important</b> : 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.</p>

Nom du paramètre de l'application utilisateur dans <code>silent.properties</code>	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_GROUPCONTAINERDN=	<p>Groupes d'utilisateurs du méta-annuaire : DN du conteneur de groupes.</p> <p>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.</p>
NOVL_CONFIG_KEYSTOREPATH=	<p>Certificats eDirectory : chemin d'accès au keystore. Requis.</p> <p>Indiquez le chemin d'accès complet au fichier (<code>cacerts</code>) 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.</p>
NOVL_CONFIG_KEYSTOREPASSWORD=	<p>Certificats eDirectory : mot de passe du keystore.</p> <p>Requis. Indiquez le mot de passe <code>cacerts</code>. L'unité par défaut est <code>changeit</code>.</p>
NOVL_CONFIG_SECUREADMINCONNECTION=	<p>Paramètres de connexion eDirectory : connexion d'admin. sécurisée.</p> <p>Indiquez <i>Vrai</i> pour que toutes les communications utilisant le compte administrateur soient effectuées à l'aide d'un socket sécurisé (cette option peut nuire aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.</p> <p>Indiquez <i>Faux</i> si le compte administrateur n'utilise pas de communication à socket sécurisé.</p>
NOVL_CONFIG_SECUREUSERCONNECTION=	<p>Paramètres de connexion eDirectory : connexion utilisateur sécurisée.</p> <p>Indiquez <i>Vrai</i> pour que toutes les communications sur le compte de l'utilisateur logué soient effectuées via un socket sécurisé (cette option peut nuire fortement aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.</p> <p>Indiquez <i>Faux</i> si le compte utilisateur n'utilise pas de communication par socket sécurisé.</p>
NOVL_CONFIG_SESSIONTIMEOUT=	<p>Divers : timeout de session.</p> <p>Indiquez un intervalle de timeout de session d'application.</p>

Nom du paramètre de l'application utilisateur dans <code>silent.properties</code>	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_LDAPPLAINPORT=	<p>Paramètres de connexion eDirectory : port non sécurisé LDAP.</p> <p>Indiquez le port non sécurisé de votre serveur LDAP, par exemple 389.</p>
NOVL_CONFIG_LDAPSECUREPORT=	<p>Paramètres de connexion eDirectory : port sécurisé LDAP.</p> <p>Indiquez le port sécurisé de votre serveur LDAP, par exemple 636.</p>
NOVL_CONFIG_ANONYMOUS=	<p>Paramètres de connexion eDirectory : utiliser un compte anonyme public.</p> <p>Indiquez <i>Vrai</i> pour permettre aux utilisateurs non logués d'accéder au compte anonyme public LDAP.</p> <p>Indiquez <i>Faux</i> si vous préférez activer NOVL_CONFIG_GUEST.</p>
NOVL_CONFIG_GUEST=	<p>Paramètres de login eDirectory : invité LDAP.</p> <p>Permet aux utilisateurs non logués d'accéder à des portlets autorisés. Vous devez également désélectionner <i>Utiliser un compte anonyme public</i>. Le compte utilisateur Guest doit déjà exister dans le coffre-fort d'identité. Pour désactiver l'utilisateur Guest, sélectionnez <i>Utiliser un compte anonyme public</i>.</p>
NOVL_CONFIG_GUESTPASS=	<p>Paramètres de connexion eDirectory : mot de passe Guest LDAP.</p>
NOVL_CONFIG_EMAILNOTIFYHOST=	<p>Courrier électronique : jeton HÔTE du modèle de notification.</p> <p>Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple :</p> <pre data-bbox="873 1398 1289 1423">myapplication serverServer</pre> <p>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.</p>
NOVL_CONFIG_EMAILNOTIFYPORT=	<p>Courrier électronique : jeton du port du modèle de notification.</p> <p>Utilisé pour remplacer le jeton \$PORT\$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.</p>

Nom du paramètre de l'application utilisateur dans <code>silent.properties</code>	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_EMAILNOTIFYSECUREREPORT=	<p>Courrier électronique : jeton du port sécurisé du modèle de notification.</p> <p>Utilisé pour remplacer le jeton <code>\$SECURE_PORT\$</code> des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation</p>
NOVL_CONFIG_NOTFSMTPEMAILFROM=	<p>Courrier électronique : notification SMTP - expéditeur du courrier électronique.</p> <p>Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.</p>
NOVL_CONFIG_NOTFSMTPEMAILHOST=	<p>Courrier électronique : notification SMTP - destinataire du courrier électronique.</p> <p>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.</p>
NOVL_CONFIG_USEEXTPWDWAR=	<p>Gestion des mots de passe : utiliser un WAR de mots de passe externe.</p> <p>Indiquez <i>Vrai</i> si vous utilisez un WAR de gestion de mots de passe externe. Si vous indiquez <i>Vrai</i>, vous devez également fournir des valeurs pour <code>NOVL_CONFIG_EXTPWDWARPTH</code> et <code>NOVL_CONFIG_EXTPWDWARRTPATH</code>.</p> <p>Indiquez <i>Faux</i> pour utiliser la fonction de gestion des mots de passe interne par défaut. <code>/jssps/pwdmgt/ForgotPassword.jsf</code> (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.</p>
NOVL_CONFIG_EXTPWDWARPATH=	<p>Gestion des mots de passe : liaison Mot de passe oublié.</p> <p>Indiquez l'URL de la page de la fonction Mot de passe oublié, <code>ForgotPassword.jsf</code>, 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 « <a href="#">Utilisation des WAR de mots de passe</a> » page 67</p>

Nom du paramètre de l'application utilisateur dans <code>silent.properties</code>	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_EXTPWDWARRTPATH=	<p>Gestion des mots de passe : liaison de retour Mot de passe oublié.</p> <p>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 <code>https://idmhost:sslport/idm</code> .</p>
NOVL_CONFIG_USEROBJECTATTRIBUTE=	<p>Identité utilisateur du méta-annuaire : classe d'objets utilisateur.</p> <p>La classe d'objets utilisateur LDAP (généralement <code>inetOrgPerson</code>).</p>
NOVL_CONFIG_LOGINATTRIBUTE=	<p>Identité utilisateur du méta-annuaire : attribut de login.</p> <p>L'attribut LDAP (par exemple, <code>CN</code>) qui représente le nom de login de l'utilisateur.</p>
NOVL_CONFIG_NAMINGATTRIBUTE=	<p>Identité utilisateur du méta-annuaire : attribut d'assignation de nom.</p> <p>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.</p>
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	<p>Identité utilisateur du méta-annuaire : attribut d'adhésion utilisateur. Facultatif.</p> <p>L'attribut LDAP qui représente l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.</p>
NOVL_CONFIG GROUPOBJECTATTRIBUTE=	<p>Groupes d'utilisateurs du méta-annuaire : classe d'objets Groupe.</p> <p>La classe d'objets Groupe LDAP (généralement <code>groupofNames</code>).</p>
NOVL_CONFIG GROUPEMEMBERSHIPATTRIBUTE=	<p>Groupes d'utilisateurs du méta-annuaire : attribut d'adhésion à un groupe.</p> <p>Indiquez l'attribut représentant l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.</p>
NOVL_CONFIG_USEDYNAMICGROUPS=	<p>Groupes d'utilisateurs du méta-annuaire : utiliser des groupes dynamiques.</p> <p>Indiquez <i>Vrai</i> si vous souhaitez utiliser les groupes dynamiques. Indiquez <i>Faux</i> dans le cas contraire.</p>

Nom du paramètre de l'application utilisateur dans <code>silent.properties</code>	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASSES=	<p>Groupes d'utilisateurs du méta-annuaire : classe d'objets de groupe dynamique.</p> <p>Indiquez la classe d'objets de groupe dynamique LDAP (généralement <code>dynamicGroup</code>).</p>
NOVL_CONFIG_PRIVATESTOREPATH=	<p>Keystore privé : chemin du keystore privé.</p> <p>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 <code>/jre/lib/security/cacerts</code> par défaut.</p>
NOVL_CONFIG_PRIVATESTOREPASSWORD=	Keystore privé : mot de passe du keystore privé.
NOVL_CONFIG_PRIVATEKEYALIAS=	<p>Keystore privé : alias de clé privée.</p> <p>Cet alias est <code>novellIDMUserApp</code> à moins d'indication contraire.</p>
NOVL_CONFIG_PRIVATEKEYPASSWORD=	Keystore privé : mot de passe de clé privée.
NOVL_CONFIG_TRUSTEDSTOREPATH=	<p>Keystore approuvé : chemin de keystore approuvé.</p> <p>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 <code>javax.net.ssl.trustStore</code>. Si le chemin n'y est pas, il est supposé être <code>jre/lib/security/cacerts</code>.</p>
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.
NOVL_CONFIG_ICSLGOUTENABLED=	<p>Paramètres Access Manager et IChain : logout simultané activé</p> <p>Indiquez <i>Vrai</i> pour activer le logout simultané de l'application utilisateur et de Novell Access Manager® ou de iChain®. L'application utilisateur vérifie la présence du cookie Novell Access Manager ou iChain durant le logout ; s'il est présent, l'utilisateur est renvoyé à la page de logout simultané.</p> <p>Indiquez <i>Faux</i> pour désactiver le logout simultané.</p>

Nom du paramètre de l'application utilisateur dans <code>silent.properties</code>	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_ICSSLOGOUTPAGE=	<p>Paramètres Access Manager et IChain : page de logout simultané</p> <p>Indiquez l'URL pointant vers la page de logout de Novell Access Manager ou iChain (il doit s'agir d'un nom d'hôte attendu par Novell Access Manager ou iChain). Si la connexion à ICS est activée et si un utilisateur se délogue de l'application utilisateur, il est réacheminé vers cette page.</p>
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	<p>Courrier électronique : jeton PROTOCOLE du modèle de notification.</p> <p>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.</p>
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	<p>Courrier électronique : jeton du port sécurisé du modèle de notification.</p>
NOVL_CONFIG_OCSPURI=	<p>Divers : OCSP URI.</p> <p>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 <code>http://hstport/ocspLocal</code>. L'URI OCSP met à jour le statut des certificats approuvés en ligne.</p>
NOVL_CONFIG_AUTHCONFIGPATH=	<p>Divers : chemin de configuration d'autorisation.</p> <p>Le nom complet du fichier de configuration de l'autorisation.</p>



# Installation sur un serveur d'applications WebSphere

# 6

Cette section décrit l'installation de l'application utilisateur Identity Manager sur un serveur d'applications WebSphere à l'aide de l'interface graphique du programme d'installation.

- ♦ Section 6.1, « Lancement de l'interface utilisateur graphique du programme d'installation », page 81
- ♦ Section 6.2, « Choix d'une plate-forme de serveur d'applications », page 82
- ♦ Section 6.3, « Emplacement du WAR », page 83
- ♦ Section 6.4, « Choix d'un dossier d'installation », page 84
- ♦ Section 6.5, « Choix d'une plate-forme de base de données », page 85
- ♦ Section 6.6, « Spécification du répertoire racine Java », page 86
- ♦ Section 6.7, « Activation de la consignation Novell Audit », page 87
- ♦ Section 6.8, « Spécification d'une clé maîtresse », page 89
- ♦ Section 6.9, « Configuration de l'application utilisateur », page 90
- ♦ Section 6.10, « Vérification des choix et installation », page 105
- ♦ Section 6.11, « Affichage des fichiers journaux », page 106
- ♦ Section 6.12, « Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM », page 106
- ♦ Section 6.13, « Importation de la racine approuvée d'eDirectory dans la zone de stockage des clés WebSphere », page 107
- ♦ Section 6.14, « Déploiement du fichier WAR IDM », page 108
- ♦ Section 6.15, « Démarrage de l'application », page 109
- ♦ Section 6.16, « Accès au portail de l'application utilisateur », page 109

## 6.1 Lancement de 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
```

---

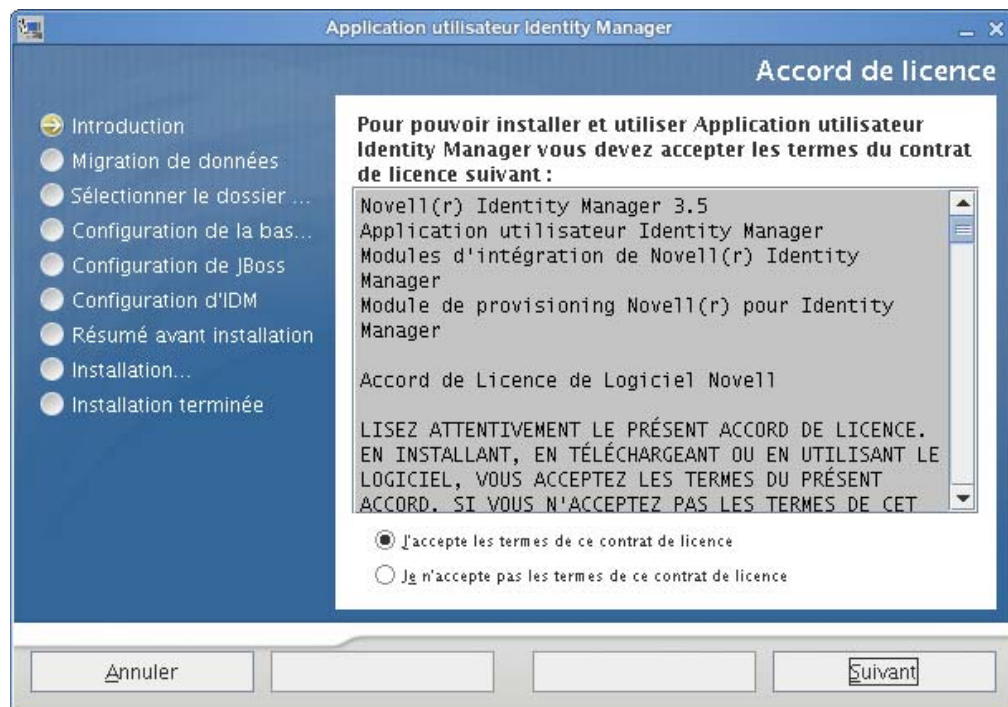
**Remarque :** avec WebSphere, utilisez le JDK d'IBM et appliquez les fichiers de stratégies accessibles.

---

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



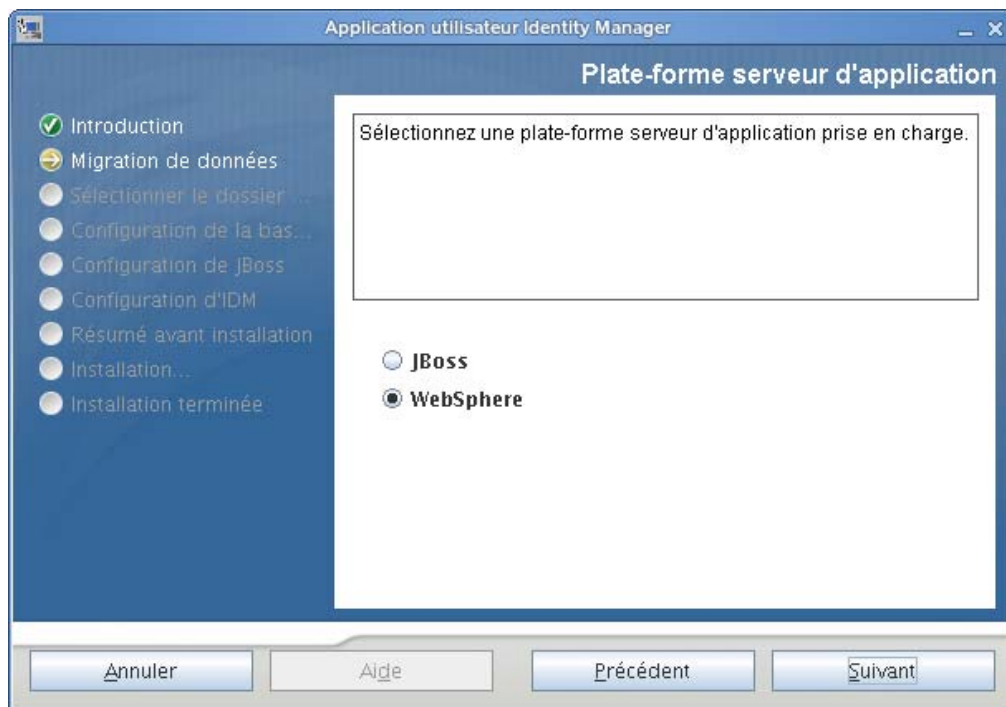
- 4 Lisez l'accord de licence, cliquez sur *J'accepte les termes ce contrat de licence*, puis cliquez sur *Suivant*.



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

## 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 6.3, « Emplacement du WAR »](#), page 83.

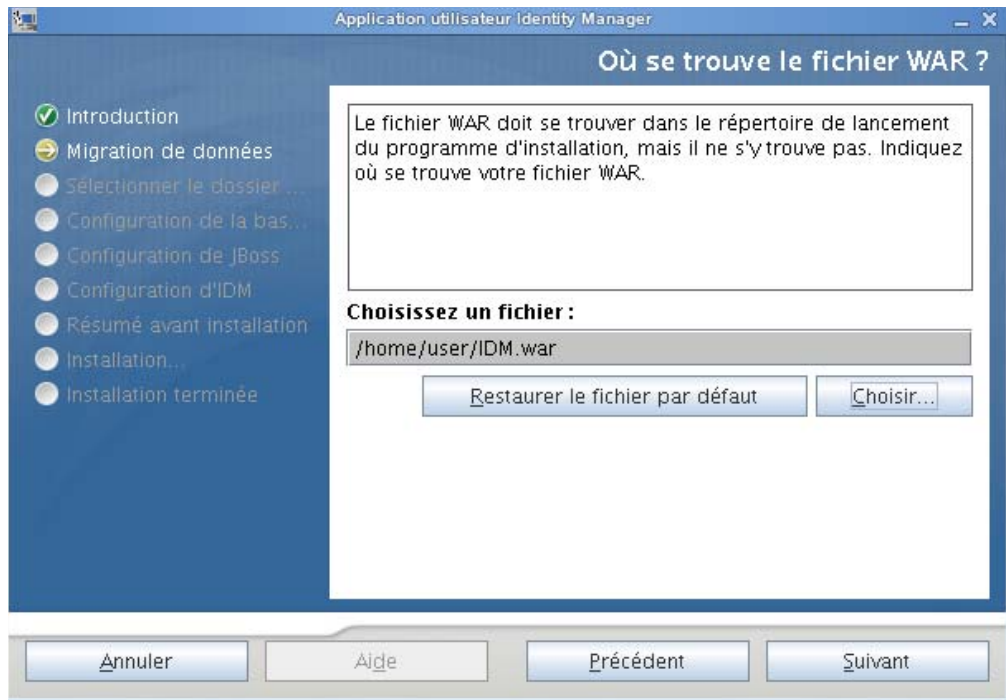


## 6.3 Emplacement du WAR

Effectuez la procédure décrite dans la [Section 6.1, « Lancement de l'interface utilisateur graphique du programme d'installation »](#), page 81, puis passez aux étapes ci-dessous.

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.

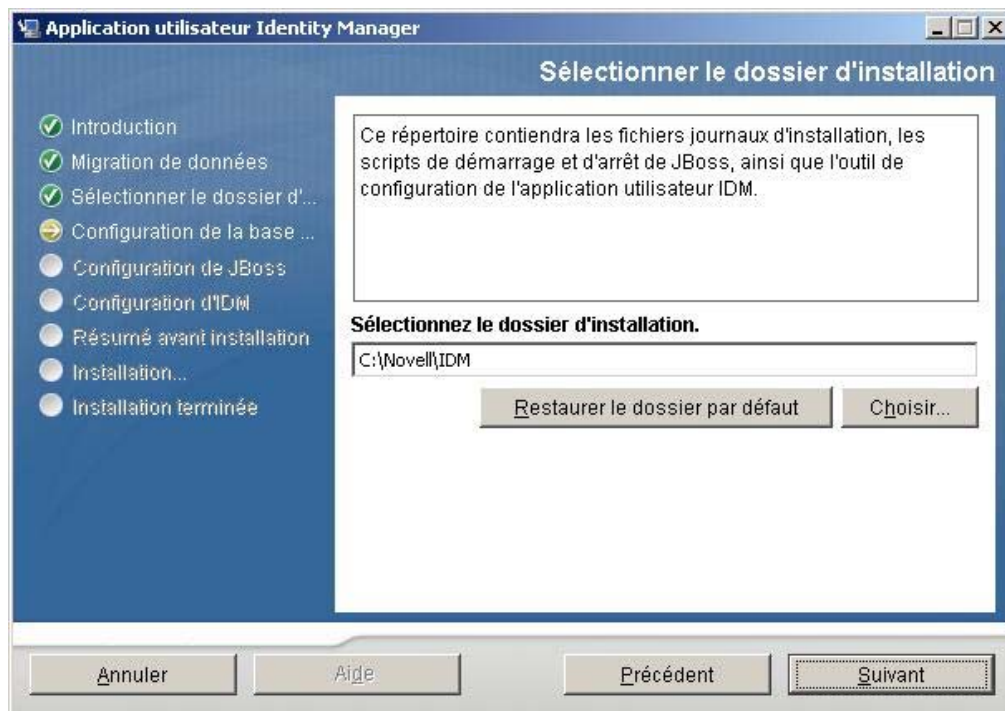
- 1 Si le fichier WAR se trouve à l'emplacement par défaut, vous pouvez cliquer sur *Restaurer le fichier par défaut*. Ou, pour spécifier l'emplacement du fichier WAR, cliquez sur *Choisir* et sélectionnez un emplacement.



- 2 Cliquez sur *Suivant*, puis passez à [Section 6.4, « Choix d'un dossier d'installation », page 84](#).

## 6.4 Choix d'un dossier d'installation

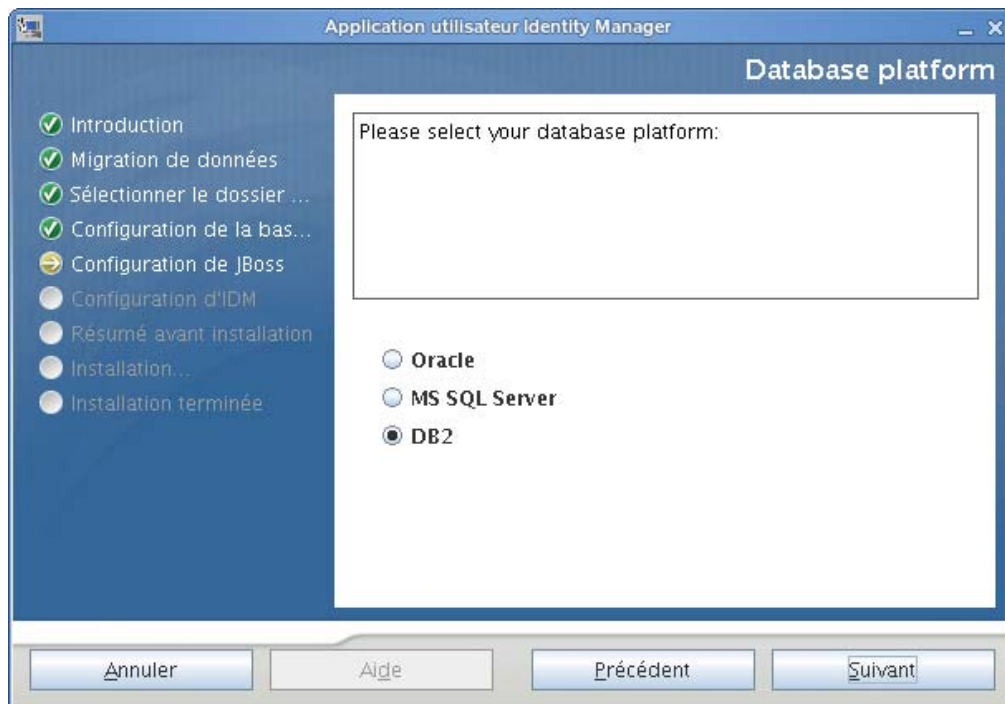
- 1 Sur la page Choisir un dossier d'installation, sélectionnez l'emplacement où installer l'application utilisateur. Si vous voulez souhaiter utiliser l'emplacement par défaut, cliquez sur *Restaurer le dossier par défaut* ; dans le cas contraire, cliquez sur *Choisir* et recherchez un emplacement.



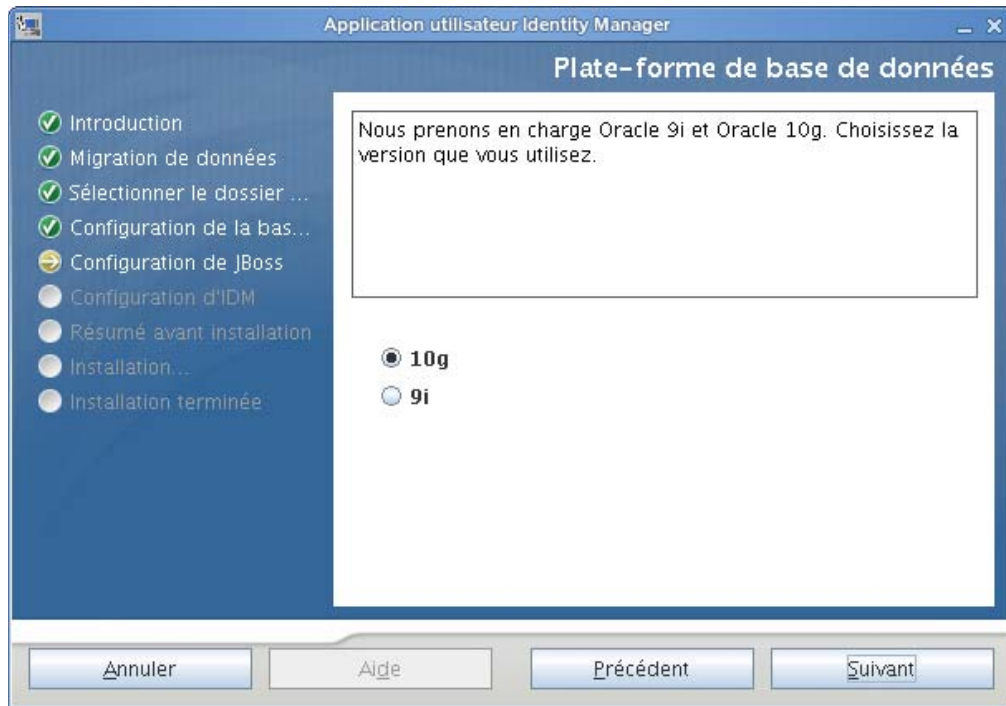
- 2 Cliquez sur *Suivant*, puis passez à [Section 6.5, « Choix d'une plate-forme de base de données »](#), page 85.

## 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 l'**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 6.6, « Spécification du répertoire racine Java », page 86**.

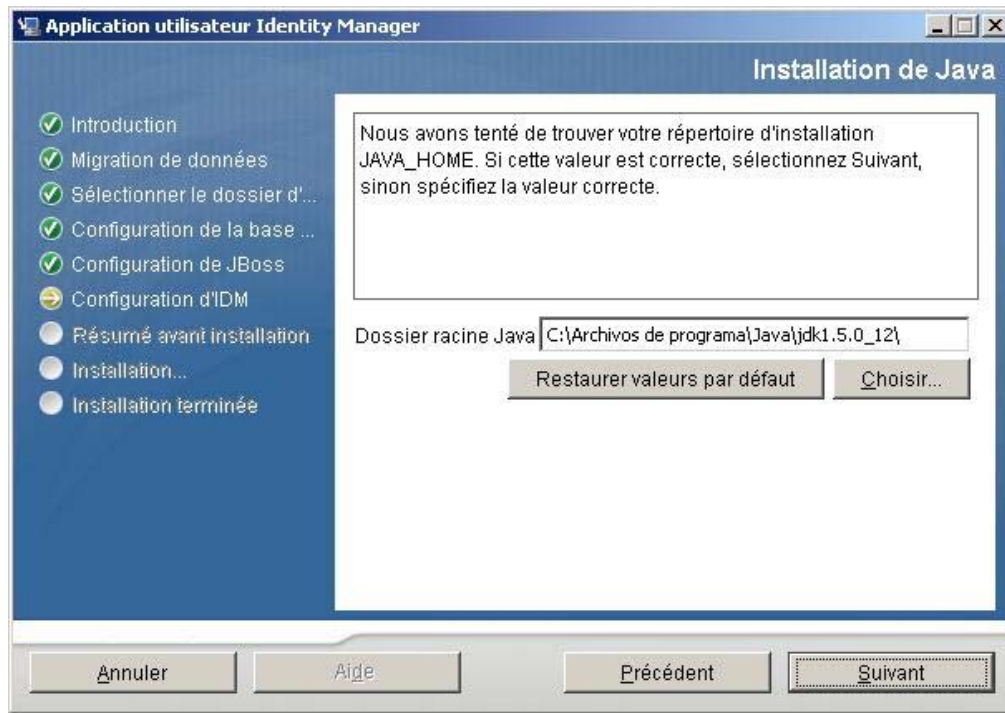
## 6.6 Spécification du répertoire racine Java

---

**Remarque :** avec WebSphere, utilisez le JDK d'IBM et appliquez les fichiers de stratégies accessibles.

---

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

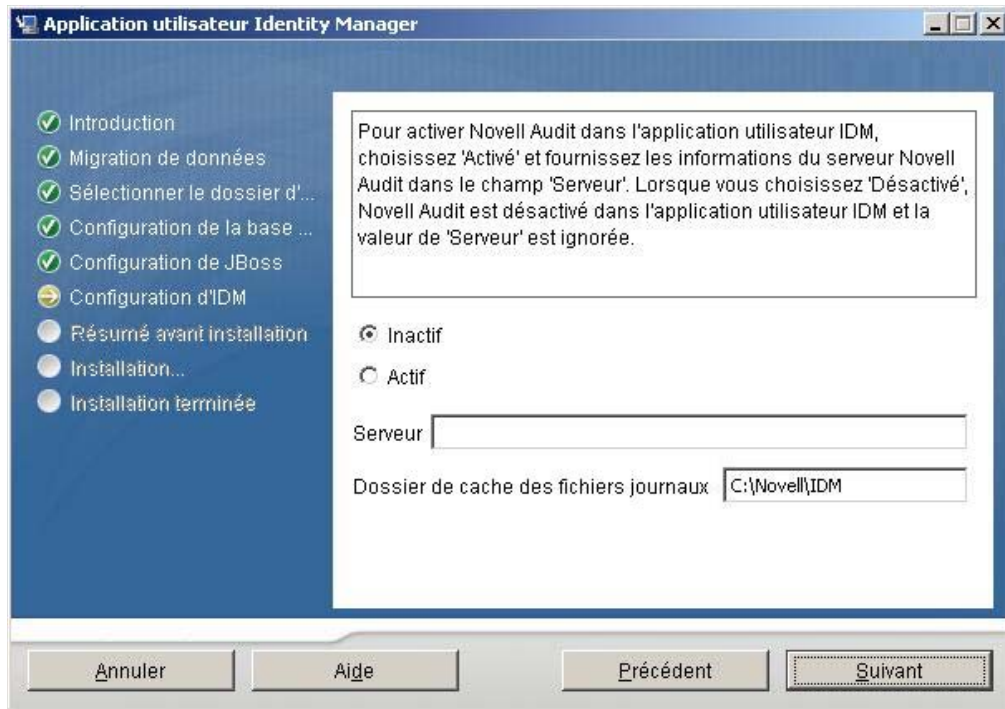


- 2 Cliquez sur *Suivant*, puis passez à [Section 6.7, « Activation de la consignation Novell Audit », page 87](#).

## 6.7 Activation de la consignation Novell Audit

Pour activer la consignation Novell<sup>®</sup> Audit (facultatif) de l'application utilisateur, procédez comme suit :

- 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 <i>Administration</i> de l'application utilisateur.  Pour plus d'informations sur l'activation de la consignation Novell Audit, reportez-vous au <i>Guide d'administration de l'application utilisateur Identity Manager</i> .
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 <i>Guide d'administration de l'application utilisateur Identity Manager</i> .
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 6.8, « Spécification d'une clé maîtresse », page 89](#).

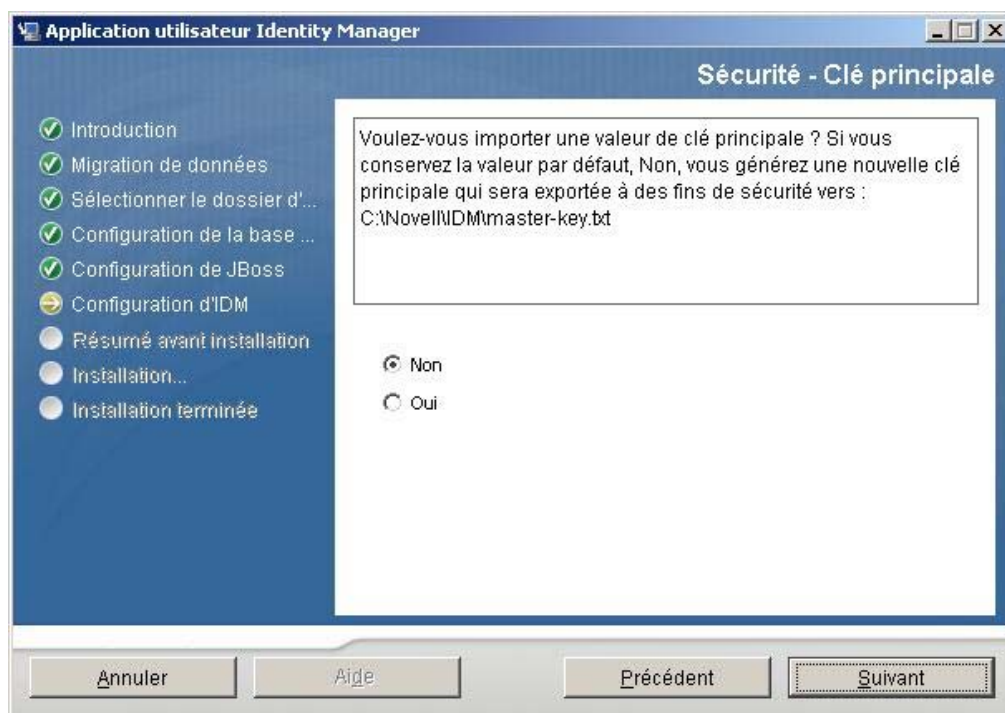


## 6.8 Spécification d'une clé maîtresse

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.

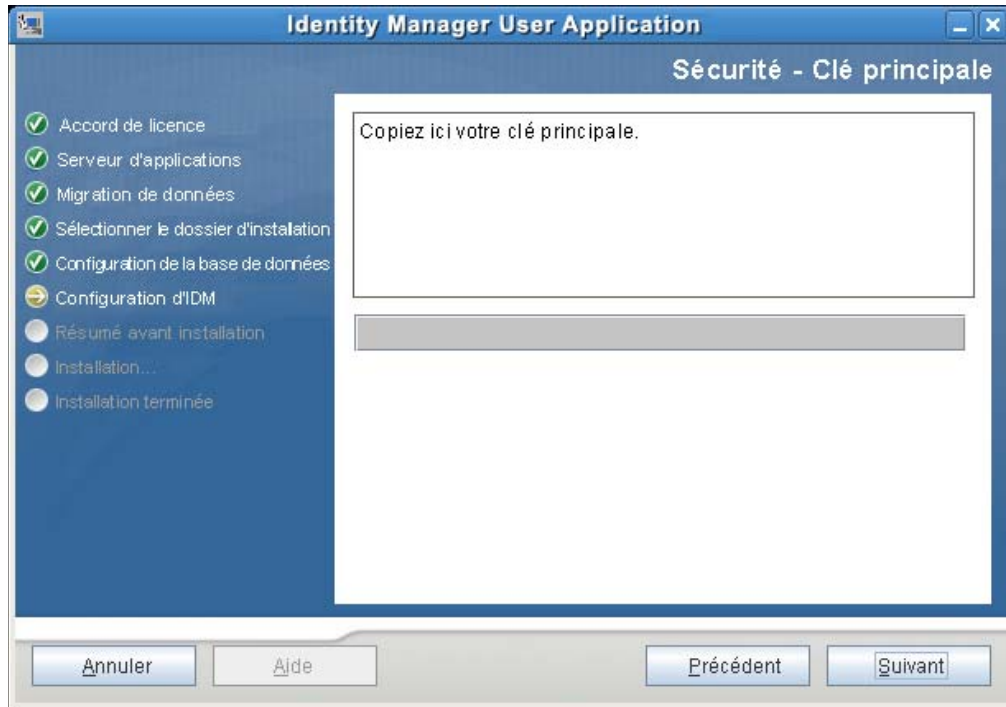


- 2 Cliquez sur *Suivant*.

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 l'[Section 6.9, « Configuration de l'application utilisateur », page 90](#). Une fois l'installation terminée, vous devez enregistrer manuellement la clé maîtresse. Si vous choisissez *Oui*, continuez avec [Étape 3 page 89](#).

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

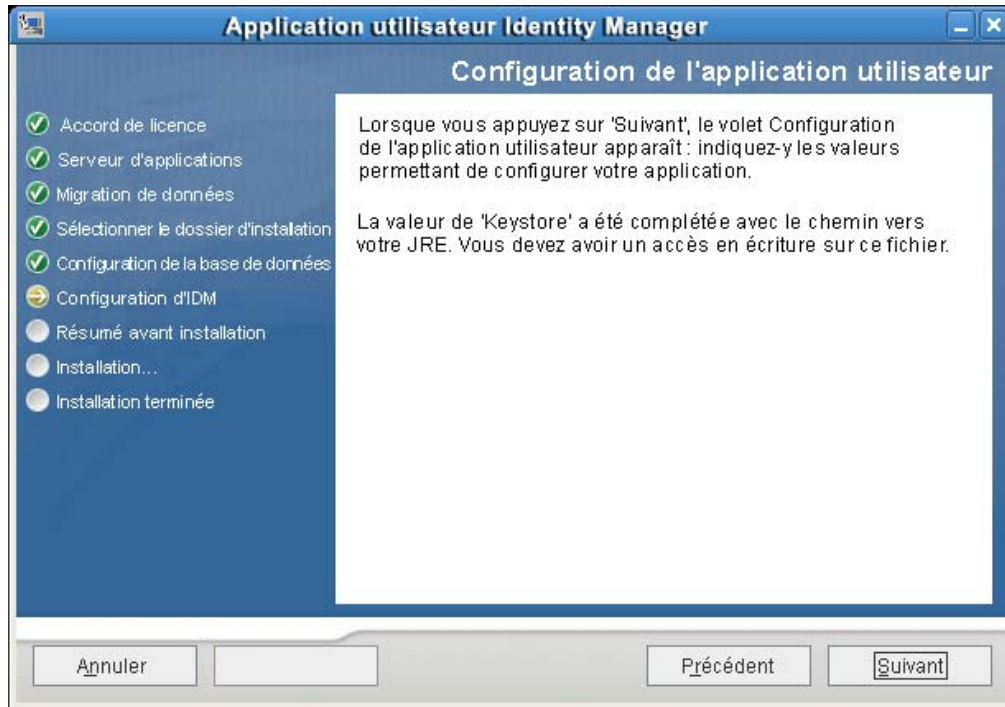


- 4 Cliquez sur *Suivant*, puis passez à [Section 6.9, « Configuration de l'application utilisateur », page 90.](#)

## 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 peuvent aussi être modifiés 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 le [Tableau 6-1 page 93](#), puis passez à l'[Étape 3](#).

Configuration de l'application utilisateur

**Paramètres de connexion eDirectory**

Hôte LDAP : mysystem.mycompany.com

Port LDAP non sécurisé : 389

Port LDAP sécurisé : 636

Administrateur LDAP : cn=admin,o=novell

Mot de passe de l'administrateur LDAP : \*\*\*\*\*

Utiliser un compte anonyme public :

Invité LDAP : cn=guest,ou=idmsample-test,o=novell

Mot de passe de l'invité LDAP : \*\*\*\*\*

Connexion admin sécurisée :

Connexion utilisateur sécurisée :

**DN eDirectory**

DN du conteneur racine : ou=idmsample-test,o=novell

DN du pilote de provisioning : cn=myDriver,cn=TestDrivers,o=novell

Admin d'application utilisateur : cn=admin,ou=ou=idmsample-test,o=novell

Admin d'application de provisioning : cn=adminprov,ou=ou=idmsample-test,o=novell

DN du conteneur de l'utilisateur :: ou=idmsample-test,o=novell

DN du conteneur du groupe :: ou=groups,ou=idmsample-test,o=novell

**Certificats eDirectory**

Chemin du fichier keystore : C:\Program Files\Java\jdk1.5.0\_06\lib\security' ...

Mot de passe Keystore : \*\*\*\*\*

Confirmer le mot de passe Keystore : \*\*\*\*\*

**Courrier électronique**

Adresse e-mail de l'administrateur :

OK    Annuler    Afficher les options avancées

**Tableau 6-1** Configuration de l'application utilisateur : paramètres de base

Type de paramètre	Champ	Description
Paramètres de connexion eDirectory	<i>Hôte LDAP</i>	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP et son port sécurisé. Par exemple : myLDAPhost
	<i>Port non sécurisé LDAP</i>	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	<i>Port sécurisé LDAP</i>	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	<i>Administrateur LDAP</i>	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer une connexion administrative au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
	<i>Mot de passe administrateur LDAP</i>	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
	<i>Utiliser le compte anonyme public</i>	Permet aux utilisateurs non logués d'accéder au compte anonyme public LDAP.
	<i>Guest LDAP</i>	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 l'invité LDAP, vous devez désactiver <i>Utiliser un compte anonyme public</i> . Pour désactiver l'utilisateur invité, sélectionnez <i>Utiliser un compte anonyme public</i> .
	<i>Mot de passe Guest LDAP</i>	Indiquez le mot de passe Guest LDAP.
	<i>Connexion admin. sécurisée</i>	Sélectionnez cette option pour que toutes les communications utilisant le compte administrateur soient effectuées à l'aide d'un socket sécurisé (cette option peut nuire aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.
	<i>Login utilisateur sécurisé</i>	Sélectionnez cette option pour que toutes les communications utilisant le compte de l'utilisateur logué soient effectuées à l'aide d'un socket sécurisé (cette option peut nuire aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.

Type de paramètre	Champ	Description
DN eDirectory	<i>DN du conteneur racine</i>	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.
	<i>DN du pilote de provisioning</i>	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 :  <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
	<i>Admin. application utilisateur</i>	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 <i>Administration</i> 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 <i>Requêtes et approbations</i> ), 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 <i>Guide d'administration de l'application utilisateur IDM</i> pour en savoir plus.  Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration &gt; Sécurité</i> de l'application utilisateur.
	<i>Admin. application provisioning</i>	L'administrateur de l'application de provisioning utilise l'onglet <i>Provisioning</i> (sous l'onglet <i>Administration</i> ) pour gérer les fonctions de workflow du provisioning. Ces fonctions sont accessibles aux utilisateurs en passant par l'onglet <i>Requêtes et approbations</i> 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 <i>Administration &gt; Sécurité</i> de l'application utilisateur.

Type de paramètre	Champ	Description
DN eDirectory (suite)	<i>Administrateur de rôles</i>	<p>Ce rôle est disponible dans le module de provisioning basé sur les rôles de Novell d'Identity Manager. Il permet aux membres de créer, de supprimer ou de modifier l'ensemble des rôles, ainsi que de révoquer les assignations de rôles des utilisateurs, des groupes ou des conteneurs. Il permet également à ses membres d'exécuter des rapports pour n'importe quel utilisateur. Par défaut, ce rôle est assigné à l'administrateur de l'application utilisateur.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page <i>Rôles &gt; Assignations de rôles</i> de l'application utilisateur.</p>
	<i>DN du conteneur d'utilisateurs</i>	<p>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.</p> <hr/> <p><b>Important :</b> 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.</p>
	<i>DN de conteneur de groupes</i>	<p>Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur de groupes.</p> <p>Utilisé par les définitions d'entités au sein de la couche d'abstraction d'annuaire.</p>
Certificats eDirectory	<i>Chemin d'accès au Keystore</i>	<p>Requis. Indiquez le chemin d'accès complet au fichier (<i>cacerts</i>) 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 <i>cacerts</i> .</p> <p>Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier.</p>
	<i>Mot de passe Keystore/ Confirmer mot de passe Keystore</i>	<p>Requis. Indiquez le mot de passe <i>cacerts</i>. L'unité par défaut est <i>changeit</i>.</p>

Type de paramètre	Champ	Description
Courrier électronique	<i>Jeton de l'hôte du modèle de notification</i>	Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple : <code>myapplication serverServer</code>  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.
	<i>Jeton du port du modèle de notification</i>	Utilisé pour remplacer le jeton \$PORT\$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	<i>Jeton du port sécurisé du modèle de notification</i>	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.
	<i>Notification SMTP - expéditeur du courrier électronique</i>	Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
	<i>Notification SMTP - destinataire du courrier électronique</i>	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	<i>Utiliser le WAR de mots de passe externe</i>	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 <i>Utiliser le WAR de mot de passe externe</i> , vous devez fournir des valeurs pour <i>Lien Mot de passe oublié</i> et <i>Lien Retour mot de passe oublié</i> .  Si vous ne sélectionnez pas <i>Utiliser le WAR de mot de passe externe</i> , IDM utilise la fonction de gestion des mots de passe interne par défaut. <code>/jsps/pwdmgt/ForgotPassword.jsf</code> (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.
	<i>Liaison Mot de passe oublié</i>	Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier <code>ForgotPassword.jsf</code> dans un WAR de gestion des mots de passe externe ou interne.



Type de paramètre	Champ	Description
	<i>Liaison de retour Mot de passe oublié</i>	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 <code>https:// idmhost:sslport/idm .</code>

- 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 6-2 page 98](#) décrit les paramètres des options avancées. Si vous ne souhaitez pas définir d'autres paramètres décrits dans cette étape, passez à l'[Étape 4](#).

**Tableau 6-2** Configuration de l'application utilisateur : tous les paramètres

Type de paramètre	Champ	Description
Paramètres de connexion eDirectory	<i>Hôte LDAP</i>	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP. Par exemple :  myLDAPhost
	<i>Port non sécurisé LDAP</i>	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	<i>Port sécurisé LDAP</i>	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	<i>Administrateur LDAP</i>	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer une connexion administrative au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
	<i>Mot de passe administrateur LDAP</i>	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
	<i>Utiliser le compte anonyme public</i>	Permet aux utilisateurs non logués d'accéder au compte anonyme public LDAP.
	<i>Guest LDAP</i>	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 <i>Utiliser le compte anonyme public</i> . Pour désactiver l'utilisateur Guest, sélectionnez <i>Utiliser le compte anonyme public</i> .
	<i>Mot de passe Guest LDAP</i>	Indiquez le mot de passe Guest LDAP.
	<i>Connexion admin. sécurisée</i>	Sélectionnez cette option pour que toutes les communications utilisant le compte administrateur soient effectuées à l'aide d'un socket sécurisé (cette option peut nuire aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.
	<i>Login utilisateur sécurisé</i>	Sélectionnez cette option pour que toutes les communications sur le compte de l'utilisateur logué soient effectuées à l'aide d'un socket sécurisé (cette option peut nuire aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.

Type de paramètre	Champ	Description
DN eDirectory	<i>DN du conteneur racine</i>	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.
	<i>DN du pilote de provisioning</i>	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
	<i>Admin. application utilisateur</i>	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 <i>Administration</i> 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 <i>Requêtes et approbations</i> ), 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 <i>Guide d'administration de l'application utilisateur IDM</i> pour en savoir plus.  Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration &gt; Sécurité</i> de l'application utilisateur.
	<i>Admin. application provisioning</i>	L'administration de l'application de provisioning gère les fonctions de workflow du provisioning accessibles par l'onglet <i>Requêtes et approbations</i> 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 <i>Administration &gt; Sécurité</i> de l'application utilisateur.

Type de paramètre	Champ	Description
Identité utilisateur du méta-annuaire	<i>DN du conteneur d'utilisateurs</i>	<p>Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur d'utilisateurs.</p> <p>Cela définit l'étendue de recherche d'utilisateurs et de groupes.</p> <p>Les utilisateurs de ce conteneur (et en-dessous) sont autorisés à se loguer à l'application utilisateur.</p> <hr/> <p><b>Important :</b> 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.</p> <hr/>
	<i>Classe d'objets Utilisateur</i>	La classe d'objets utilisateur LDAP (généralement inetOrgPerson).
	<i>Attribut de login</i>	L'attribut LDAP (par exemple, CN) qui représente le nom de login de l'utilisateur.
	<i>Attribut de nom</i>	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.
	<i>Attribut de l'adhésion utilisateur</i>	Facultatif. L'attribut LDAP qui représente l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.
	<i>Administrateur de rôles</i>	<p>Ce rôle est disponible dans le module de provisioning basé sur les rôles de Novell d'Identity Manager. Il permet aux membres de créer, de supprimer ou de modifier l'ensemble des rôles, ainsi que de révoquer les assignations de rôles des utilisateurs, des groupes ou des conteneurs. Il permet également à ses membres d'exécuter des rapports pour n'importe quel utilisateur. Par défaut, ce rôle est assigné à l'administrateur de l'application utilisateur.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page <i>Rôles &gt; Assignations de rôles</i> de l'application utilisateur.</p>

Type de paramètre	Champ	Description
Groupes d'utilisateurs du méta-annuaire	<i>DN de conteneur de groupes</i>	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.
	<i>Classe d'objets Groupe</i>	La classe d'objets Groupe LDAP (généralement groupofNames).
	<i>Attribut d'adhésion à un groupe</i>	L'attribut qui représente l'adhésion d'un utilisateur à un groupe. N'utilisez pas d'espaces pour le nom.
	<i>Utiliser des groupes dynamiques</i>	Sélectionnez cette option si vous souhaitez utiliser des groupes dynamiques.
	<i>Classe d'objets Groupe dynamique</i>	La classe d'objets Groupe dynamique LDAP (généralement dynamicGroup).
Certificats eDirectory	<i>Chemin d'accès au Keystore</i>	Requis. Indiquez le chemin d'accès complet au fichier ( <i>cacerts</i> ) 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 <i>cacerts</i> .  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.
	<i>Mot de passe Keystore</i> <i>Confirmer le mot de passe Keystore</i>	Requis. Indiquez le mot de passe <i>cacerts</i> . L'unité par défaut est <i>changeit</i> .
Keystore privé	<i>Chemin d'accès au keystore privé</i>	Le keystore privé contient la clé privée et les certificats de l'application utilisateur. Réservez. Si vous laissez ce champ vierge, ce chemin d'accès est <i>/jre/lib/security/cacerts</i> par défaut.
	<i>Mot de passe Keystore privé</i>	Ce mot de passe est <i>changeit</i> , à moins d'indication contraire. Ce mot de passe est codé, en fonction de la clé maîtresse.
	<i>Alias de clé privée</i>	Cet alias est <i>novellIDMUserApp</i> , à moins d'indication contraire.
	<i>Mot de passe de la clé privée</i>	Ce mot de passe est <i>novellIDM</i> , à moins d'indication contraire. Ce mot de passe est codé, en fonction de la clé maîtresse.

Type de paramètre	Champ	Description
Banque de clés approuvée	<i>Chemin d'accès à la banque approuvée</i>	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 <code>javax.net.ssl.trustStore</code> . Si le chemin n'y est pas, il est supposé être <code>jre/lib/security/cacerts</code> .
	<i>Mot de passe de la banque approuvée</i>	Si ce champ est vierge, l'application utilisateur obtient le mot de passe à partir de la propriété système <code>javax.net.ssl.trustStorePassword</code> . S'il n'y a aucune valeur, <code>changeit</code> 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.
	<i>Certificat de signature numérique Novell Audit</i>	Affiche le certificat de signature numérique.
	<i>Clé privée de signature numérique Novell Audit</i>	Affiche la clé privée de signature numérique. Cette clé est codée, en fonction de la clé maîtresse.
Paramètres Access Manager et iChain	<i>Logout simultané activé</i>	Si cette option est activée, l'application utilisateur prend en charge le logout simultané de l'application utilisateur et de Novell Access Manager ou d'iChain. L'application utilisateur vérifie la présence du cookie Novell Access Manager ou iChain durant le logout ; s'il est présent, l'utilisateur est renvoyé à la page de logout simultané.
	<i>Page de Logout simultané</i>	L'URL pointant vers la page de logout de Novell Access Manager ou iChain, lorsque l'URL est un nom d'hôte attendu par Novell Access Manager ou iChain. Si la connexion 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	<i>Jeton de l'hôte du modèle de notification</i>	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.
	<i>Jeton du port du modèle de notification</i>	Utilisé pour remplacer le jeton \$PORT\$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	<i>Jeton du port sécurisé du modèle de notification</i>	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.
	<i>Jeton du protocole du modèle de notification</i>	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.
	<i>Jeton du protocole sécurisé du modèle de notification</i>	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.
	<i>Notification SMTP - expéditeur du courrier électronique</i>	Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
	<i>Notification SMTP - destinataire du courrier électronique</i>	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	<i>Utiliser le WAR de mots de passe externe</i>	<p>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.</p> <p>Si vous sélectionnez <i>Utiliser le WAR de mot de passe externe</i>, vous devez fournir des valeurs pour <i>Lien Mot de passe oublié</i> et <i>Lien Retour mot de passe oublié</i>.</p> <p>Si vous ne sélectionnez pas <i>Utiliser le WAR de mot de passe externe</i>, IDM utilise la fonction de gestion des mots de passe interne par défaut. <code>/jsps/pwdmgt/ForgotPassword.jsf</code> (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.</p>
	<i>Liaison Mot de passe oublié</i>	Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier <code>ForgotPassword.jsf</code> dans un WAR de gestion des mots de passe externe ou interne.
	<i>Liaison de retour Mot de passe oublié</i>	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 <code>https:// idmhost:sslport/idm .</code>
Divers	<i>Timeout de session</i>	Le timeout de session de l'application.
	<i>OCSP URI</i>	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 <code>http://host:port/ocspLocal</code> . L'URI OCSP met à jour le statut des certificats approuvés en ligne.
	<i>Chemin de configuration d'autorisation</i>	Nom complet du fichier de configuration de l'autorisation.
	<i>Créer un index eDirectory</i>	
	<i>DN du serveur</i>	



Type de paramètre	Champ	Description
Objet Conteneur	<i>Sélectionné</i>	Sélectionnez chaque type d'objet Conteneur à utiliser.
	<i>Type d'objet Conteneur</i>	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 <i>Ajouter un nouvel objet Conteneur</i> .
	<i>Nom de l'attribut Conteneur</i>	Indique le nom de type d'attribut associé au type d'objet Conteneur.
	<i>Ajouter un nouvel objet Conteneur : type d'objet Conteneur</i>	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 <a href="http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf">Guide d'administration de Novell iManager 2.6 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)</a> .
	<i>Ajouter un nouvel objet Conteneur : nom d'attribut Conteneur</i>	Donnez le nom d'attribut de l'objet Conteneur.

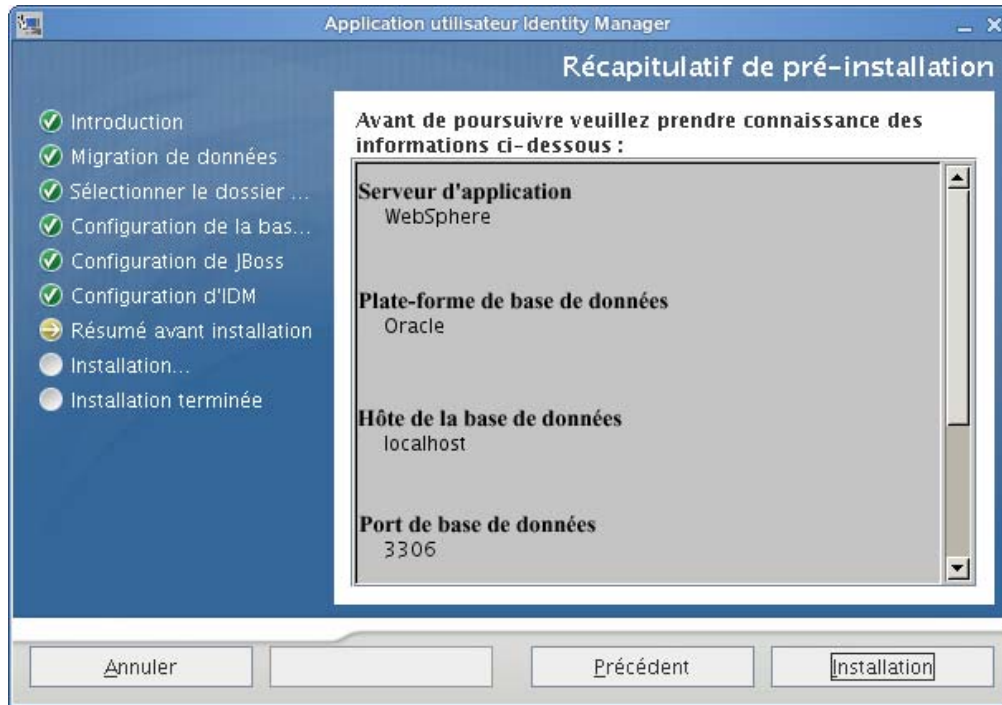
- 4 Une fois les paramètres configurés, cliquez sur *OK*, puis passez à **Section 6.10, « Vérification des choix et installation »**, page 105.

## 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*.



## 6.11 Affichage des fichiers journaux

Si votre installation s'est terminée sans erreur, passez à [Section 6.12, « Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM »](#), page 106.

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.

## 6.12 Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM

Les étapes suivantes permettent l'installation sous WebSphere.

- 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 panneau de gauche, accédez à *Serveurs > Serveur d'application*

- 4 Cliquez sur le nom du serveur dans la liste, par exemple serveur1.
- 5 Dans la liste des paramètres 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 nom du répertoire d'installation que vous avez spécifié lors de l'installation.  
Le programme d'installation y a écrit le fichier `sys-configuration-xmldata.xml`.
  - 9c *Description* permet de saisir la description de la propriété. (exemple : 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 nom du répertoire d'installation que vous avez spécifié lors de l'installation.
  - 10c *Description* permet de saisir la description de la propriété (exemple : chemin vers `idmuserapp_logging.xml`).
  - 10d Cliquez sur *OK* pour enregistrer la propriété.

---

**Remarque :** le fichier `idmuserapp-logging.xml` n'existe pas tant que vous n'avez pas appliqué les modifications dans *Application utilisateur > Administration > Configuration de l'application > Consignation*.

---

## 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. Pour cela, utilisez la console de l'administrateur WebSphere (« **Importation de certificats avec la console de l'administrateur WebSphere** » page 108) ou la ligne de commande (« **Importation de certificats avec la ligne de commande** » page 108).
- 3 Après avoir importé les certificats, passez à **Section 6.14, « Déploiement du fichier WAR IDM », page 108**.

## 6.13.1 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 paramètres de droite, accédez à *Zone de 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 Modifiez le type de donnée dans la liste déroulante en sélectionnant *Données DER binaires*.
- 9 Cliquez sur *OK*. À présent, le certificat doit apparaître dans la liste des certificats du signataire.

## 6.13.2 Importation de certificats avec la ligne de commande

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 pour que cela fonctionne. 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.

## 6.14 Déploiement du fichier WAR IDM

- 1 Loguez-vous à la console d'administration WebSphere en tant qu'utilisateur administrateur.
- 2 Dans le panneau de gauche, accédez à *Applications > Install New Application (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 indiqué au cours de l'installation de l'application utilisateur.
- 4 Saisissez la racine du contexte de l'application, par exemple `IDMPROV`. Elle correspond au chemin de l'URL.
- 5 Conservez la valeur du bouton d'option *Prompt me only when additional information is required (Ne me solliciter que lorsque des informations complémentaires sont nécessaires)*. Cliquez ensuite sur *Suivant* pour passer à la page *Select installation options (Sélectionner les options d'installation)*.

- 6 Acceptez les valeurs par défaut de cette page, puis cliquez sur *Next (Suivant)* pour passer à la page Map modules to servers (Assigner les modules aux serveurs).
- 7 Acceptez les valeurs par défaut de cette page, puis cliquez sur *Next (Suivant)* pour passer à la page Map resource references to resources page (Assigner les références de ressources à la page de ressources).
- 8 Pour sélectionner la méthode par authentification, cochez la case *Use default method (Utiliser la méthode par défaut)*. Puis, dans la liste déroulante *Authentication data entry (Saisie des données d'authentification)*, sélectionnez l'alias que vous avez créé précédemment, par exemple `Mon NoeudDeServeur01/MonAlias`.
- 9 Dans le tableau ci-dessous des paramètres d'authentification, recherchez le module que vous déployez. Sous la colonne intitulée *Target Resource JNDI Name (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, puis cliquez sur le bouton *Appliquer* pour revenir à la page Map resource references to resources (Assigner les références des ressources sur les ressources), par exemple `MyDataSource`.
- 10 Cliquez sur *Suivant* pour accéder à *Map virtual hosts for Web modules (Assigner les hôtes virtuels pour les modules Web)*.
- 11 Acceptez les valeurs par défaut de cette page, puis 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 6.15, « Démarrage de l'application », page 109](#).

## 6.15 Démarrage de l'application

- 1 Loguez-vous à la console d'administrateur WebSphere en tant qu'utilisateur administrateur.
- 2 Dans le panneau 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.

## 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
```



La présente section présente les tâches de post-installation. Les rubriques incluent :

- ♦ [Section 7.1, « Enregistrement de la clé maîtresse », page 111](#)
- ♦ [Section 7.2, « Configuration de post-installation », page 111](#)
- ♦ [Section 7.3, « Vérification de vos installations de grappes », page 112](#)
- ♦ [Section 7.4, « Configuration de la communication SSL entre serveurs JBoss », page 112](#)
- ♦ [Section 7.5, « Accès au WAR de mots de passe externe », page 112](#)
- ♦ [Section 7.6, « Mise à jour des paramètres Mot de passe oublié », page 112](#)
- ♦ [Section 7.7, « Configuration de la notification par message électronique », page 113](#)
- ♦ [Section 7.8, « Tester l'installation sur le serveur d'applications JBoss », page 113](#)
- ♦ [Section 7.9, « Configuration de votre équipe de provisioning et de ses requêtes », page 114](#)
- ♦ [Section 7.10, « Création d'index dans eDirectory », page 114](#)
- ♦ [Section 7.11, « Reconfiguration du fichier WAR IDM après l'installation », page 115](#)
- ♦ [Section 7.12, « Dépannage », page 115](#)

## 7.1 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.

## 7.2 Configuration de post-installation

Pour obtenir des informations sur la post-installation afin de configurer l'application utilisateur Identity Manager et le sous-système des rôles, reportez-vous aux documents suivants :

- ♦ La section “Configuring the User Application Environment” (Configuration de l'environnement de l'application utilisateur) du manuel *Novell IDM Roles Based Provisioning Module 3.6 Administration Guide (Guide d'administration de Novell IDM Roles Based Provisioning Module 3.6)*.
- ♦ Le manuel *Novell IDM Roles Based Provisioning Module 3.6 Design Guide (Guide de conception de Novell IDM Roles Based Provisioning Module 3.6)*

## 7.3 Vérification de vos installations de grappes

Vérifiez, dans les grappes JBoss, que chaque serveur d'applications de la grappe contient les éléments suivants :

- 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, dans les grappes WebSphere, que chaque serveur d'applications de la grappe possède 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/idmrbpm36/index.html>)

## 7.4 Configuration de la 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.

## 7.5 Accès au WAR de mots de passe externe

Si vous disposez d'un WAR de mots de passe externe et si vous souhaitez y accéder pour tester la fonction Mot de passe oublié, vous pouvez le faire :

- Directement, 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*.

## 7.6 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 saisissez `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/jsp/pwdmgt/ForgotPassword.jsf`)
- ♦ *Liaison retour Mot de passe oublié* (par exemple : `https://idmhost:sslport/idm`)

## 7.7 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*.

## 7.8 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.

Si vous n'utilisez pas le système X Window, vous devez inclure le drapeau `Djava.awt.headless=true` dans le script de démarrage du serveur. Cet élément est nécessaire à l'exécution des rapports. Vous pouvez, par exemple, ajouter la ligne suivante à votre script :

```
JAVA_OPTS="-Djava.awt.headless=true -server -Xms256M -Xmx256M-XX:MaxPermSize=256m"
```

- 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`
- nomhôte:port* représente le nom d'hôte du serveur d'applications (par exemple, `monserveur.domaine.com`) et le port de votre serveur d'applications (par exemple, 8080, valeur 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 7.12, « Dépannage », page 115](#).

## 7.9 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](http://www.novell.com/documentation/idmrbpm36/index.html) (<http://www.novell.com/documentation/idmrbpm36/index.html>).

## 7.10 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) (<http://www.novell.com/documentation>) pour plus d'informations sur l'utilisation du gestionnaire d'index et la création d'index.

## 7.11 Reconfiguration du fichier WAR IDM après l'installation

Pour mettre à jour le fichier WAR IDM, procédez comme suit :

- 1 Exécutez l'utilitaire ConfigUpdate dans le répertoire d'installation de l'application utilisateur via `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 au [Tableau 4-2 page 60](#), au [Tableau 5-1 page 72](#) ou au [Tableau 6-2 page 98](#).

- 2 Déployez le nouveau fichier WAR sur votre serveur d'applications.

## 7.12 Dépannage

Votre représentant Novell passera en revue tout problème de configuration avec vous. En attendant, voici quelques points à vérifier en cas de problème.

Point	Actions suggérées
<p>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 :</p> <ul style="list-style-type: none"><li>◆ Connexions et certificats du coffre-fort d'identité</li><li>◆ Paramètres de messagerie électronique</li><li>◆ Identité utilisateur du méta-annuaire, groupes d'utilisateurs</li><li>◆ Paramètres Access Manager et iChain®</li></ul>	<p>Exécutez l'utilitaire de configuration indépendamment du programme d'installation.</p> <p>Sous Linux et Solaris, exécutez la commande suivante depuis le répertoire d'installation (par défaut, <code>/opt/novell/idm</code>):</p> <pre>configupdate.sh</pre> <p>Sous Windows, exécutez la commande suivante depuis le répertoire d'installation (par défaut, <code>c:\opt\novell\idm</code>):</p> <pre>configupdate.bat</pre>
<p>Des exceptions apparaissent lorsque le serveur d'application démarre, avec un message de journal port 8080 déjà en cours d'utilisation.</p>	<p>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 <code>config</code> pour le pilote de l'application utilisateur dans iManager.</p>
<p>Au démarrage du serveur d'applications, un message s'affiche indiquant qu'aucun certificat approuvé n'a été trouvé.</p>	<p>Assurez-vous de démarrer le serveur d'applications via le JDK spécifié dans l'installation de l'application utilisateur.</p>
<p>Vous ne pouvez pas vous connecter à la page d'administration du portail.</p>	<p>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).</p>
<p>Vous pouvez vous connecter en tant qu'administrateur, mais vous ne pouvez pas créer de nouveaux utilisateurs.</p>	<p>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).</p>

Point	Actions suggérées
<p>Au démarrage du serveur d'applications, il y a des erreurs de connexion à MySQL.</p>	<p>N'exécutez rien en tant qu'utilisateur <code>root</code>. (La survenue de ce problème est cependant peu probable si vous exécutez la version de MySQL fournie avec Identity Manager.)</p> <p>Assurez-vous que MySQL fonctionne (et que la copie correcte est exécutée). Détruisez toute autre instance de MySQL. Exécutez <code>/idm/mysql/start-mysql.sh</code>, puis <code>/idm/start-jboss.sh</code>.</p> <p>Examinez <code>/idm/mysql/setup-mysql.sh</code> dans un éditeur de texte et corrigez toute valeur qui semble suspecte. Exécutez ensuite le script, puis <code>/idm/start-jboss.sh</code>.</p>
<p>Vous rencontrez des erreurs de keystore lors du démarrage du serveur d'applications.</p>	<p>Votre serveur d'applications n'exécute pas le JDK spécifié à l'installation de l'application utilisateur.</p> <p>Utilisez la commande <code>keytool</code> pour importer le fichier de certificat :</p> <pre>keytool -import -trustcacerts -alias <i>aliasName</i> -file <i>certFile</i> -keystore ..\lib\security\cacerts -storepass <i>changeit</i></pre> <ul style="list-style-type: none"> <li>◆ Remplacez <i>aliasName</i> par un nom unique de votre choix pour ce certificat.</li> <li>◆ Remplacez <i>certFile</i> par le chemin complet et le nom de votre fichier de certificat.</li> <li>◆ Le mot de passe du keystore par défaut est <code>changeit</code> (si vous avez un mot de passe différent, indiquez-le).</li> </ul>
<p>Aucune notification n'a été envoyée par courrier électronique.</p>	<p>Exécutez l'utilitaire <code>configupdate</code> pour vérifier que vous avez fourni les valeurs des paramètres de configuration de l'application utilisateur suivants : Message électronique de et Message électronique à.</p> <p>Sous Linux ou Solaris, exécutez cette commande depuis le répertoire d'installation (par défaut, <code>/opt/novell/idm</code>):</p> <pre>configupdate.sh</pre> <p>Sous Windows, exécutez la commande suivante depuis le répertoire d'installation (par défaut, <code>c:\opt\novell\idm</code>):</p> <pre>configupdate.bat</pre>