

Guide d'installation de l'application utilisateur

Novell® Module de provisioning basé sur les rôles Identity Manager

3.7

18 septembre 2009

www.novell.com



Mentions légales

Novell, Inc. n'accorde aucune garantie, explicite ou implicite, quant au contenu 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.

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

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

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

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

Marques de Novell

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

Éléments tiers

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

Table des matières

À propos de ce guide	7
1 Présentation de l'installation du module de provisioning basé sur les rôles	9
1.1 Liste de contrôle de l'installation	9
1.2 À propos du programme d'installation	10
1.3 Configuration système requise	11
2 Conditions préalables	17
2.1 Installation du méta-annuaire Identity Manager	17
2.2 Téléchargement du module de provisioning basé sur les rôles	17
2.3 Installation d'un serveur d'applications	19
2.3.1 Installation du serveur d'applications JBoss	19
2.3.2 Installation du serveur d'applications WebLogic	23
2.3.3 Installation du serveur d'applications WebSphere	23
2.4 Installation d'une base de données	23
2.4.1 Remarques sur la configuration d'une base de données MySQL	24
2.4.2 Remarques sur la configuration d'une base de données Oracle	26
2.4.3 Remarques sur la configuration d'une base de données MS SQL Server	27
2.4.4 Remarques sur la configuration d'une base de données DB2	27
2.5 Installation du kit de développement Java	29
3 Installation du module de provisioning basé sur les rôles dans le méta-annuaire	31
3.1 À propos de l'installation du module de provisioning basé sur les rôles	31
3.2 Exécution de l'utilitaire NrfCaseUpdate	32
3.2.1 Présentation de NrfCaseUpdate	32
3.2.2 Présentation de l'installation	32
3.2.3 Conséquences de l'utilitaire NrfCaseUpdate sur le schéma	33
3.2.4 Création d'une sauvegarde des pilotes d'application utilisateur	33
3.2.5 Utilisation de NrfCaseUpdate	33
3.2.6 Vérification du processus NrfCaseUpdate	35
3.2.7 Activation du JRE pour les connexions SSL	36
3.2.8 Restauration des pilotes d'application utilisateur invalidés	36
3.3 Exécution du programme d'installation du RBPM	38
4 Création des pilotes	45
4.1 Création du pilote d'application utilisateur dans iManager	45
4.2 Création du pilote du service de rôles et de ressources dans iManager	47
5 Installation de l'application utilisateur sur JBoss	51
5.1 Installation et configuration du fichier WAR de l'application utilisateur	51
5.1.1 Affichage des fichiers journaux et d'installation	65
5.2 Tester l'installation	65

6	Installation de l'application utilisateur sur WebSphere	67
6.1	Installation et configuration du fichier WAR de l'application utilisateur	67
6.1.1	Affichage des fichiers journaux d'installation	81
6.2	Configuration de l'environnement WebSphere	81
6.2.1	Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM	82
6.2.2	Importation de la racine approuvée d'eDirectory dans la zone de stockage des clés WebSphere	83
6.3	Déploiement du fichier WAR	83
6.3.1	Configuration supplémentaire pour WebSphere 6.1	84
6.4	Démarrage et accès à l'application utilisateur	84
7	Installation de l'application utilisateur sur WebLogic	85
7.1	Liste de contrôle pour l'installation de WebLogic	85
7.2	Installation et configuration du fichier WAR de l'application utilisateur	86
7.2.1	Affichage des fichiers journaux et d'installation	99
7.3	Préparation de l'environnement WebLogic	99
7.3.1	Configurez la réserve de connexions	100
7.3.2	Définition de l'emplacement des fichiers de configuration du RBPM	100
7.3.3	Plug-in de workflow et configuration de WebLogic	101
7.4	Déploiement du fichier WAR de l'application utilisateur	102
7.5	Accès à l'application utilisateur	102
8	Installation depuis la console ou à l'aide d'une commande unique	103
8.1	Installation de l'application utilisateur à partir de la console	103
8.2	Installation de l'application utilisateur avec une seule commande	104
9	Tâches post-installation	115
9.1	Enregistrement de la clé maîtresse	115
9.2	Configuration de l'application utilisateur	115
9.2.1	Configuration de la consignation	116
9.3	Configuration d'eDirectory	116
9.3.1	Création d'index dans eDirectory	116
9.3.2	Installation et configuration de la méthode d'authentification SAML	116
9.4	Reconfiguration du fichier WAR de l'application utilisateur après l'installation	118
9.5	Configuration de la gestion externe des mots de passe oubliés	118
9.5.1	Spécification d'un fichier WAR externe de gestion des mots de passe oubliés	118
9.5.2	Spécification d'un WAR de mot de passe interne	119
9.5.3	Test de la configuration du fichier WAR externe pour les mots de passe oubliés	119
9.5.4	Configuration de la communication SSL entre serveurs JBoss	119
9.6	Mise à jour des paramètres de mot de passe oublié	119
9.7	Considérations relatives à la sécurité	120
9.8	Dépannage	120
A	Référence de configuration de l'application utilisateur IDM	123
A.1	Configuration de l'application utilisateur : paramètres de base	123
A.2	Configuration de l'application utilisateur : tous les paramètres	125

À propos de ce guide

Ce guide explique la procédure d'installation du module de provisioning basé sur les rôles Novell® Identity Manager 3.7.0. Il aborde les points suivants :

- ♦ Chapitre 1, « Présentation de l'installation du module de provisioning basé sur les rôles », page 9
- ♦ Chapitre 2, « Conditions préalables », page 17
- ♦ Chapitre 3, « Installation du module de provisioning basé sur les rôles dans le méta-annuaire », page 31
- ♦ Chapitre 4, « Création des pilotes », page 45
- ♦ Chapitre 5, « Installation de l'application utilisateur sur JBoss », page 51
- ♦ Chapitre 6, « Installation de l'application utilisateur sur WebSphere », page 67
- ♦ Chapitre 7, « Installation de l'application utilisateur sur WebLogic », page 85
- ♦ Chapitre 8, « Installation depuis la console ou à l'aide d'une commande unique », page 103
- ♦ Chapitre 9, « Tâches post-installation », page 115
- ♦ Annexe A, « Référence de configuration de l'application utilisateur IDM », page 123

Public

Ce guide s'adresse aux administrateurs et aux consultants qui planifient et mettent en oeuvre le module de provisioning basé sur les rôles 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 proposée au bas de chaque page de la documentation en ligne ou accédez à la page Web www.novell.com/documentation/feedback.html (en anglais).

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 de l'installation du module de provisioning basé sur les rôles

1

Cette section présente les étapes de l'installation du module de provisioning basé sur les rôles. Les rubriques sont les suivantes :

- ♦ [Section 1.1, « Liste de contrôle de l'installation », page 9](#)
- ♦ [Section 1.2, « À propos du programme d'installation », page 10](#)
- ♦ [Section 1.3, « Configuration système requise », page 11](#)

Si vous effectuez une migration depuis une version antérieure de l'application utilisateur ou du module de provisioning basé sur les rôles, reportez-vous au manuel *User Application: Migration Guide* (<http://www.novell.com/documentation/idmrbpm37/index.html>) (Guide de migration de l'application utilisateur).

1.1 Liste de contrôle de l'installation

Pour installer le module de provisioning basé sur les rôles Novell® Identity Manager, procédez comme suit :

- Vérifiez que votre logiciel dispose de la configuration système requise. Reportez-vous à la [Section 1.3, « Configuration système requise », page 11](#).
- Téléchargez le module de provisioning basé sur les rôles Identity Manager. Reportez-vous à la [Section 2.2, « Téléchargement du module de provisioning basé sur les rôles », page 17](#).
- Configurez les composants de prise en charge suivants :
 - Veillez à ce qu'un méta-annuaire Identity Manager pris en charge soit installé. Reportez-vous à la [Section 2.1, « Installation du méta-annuaire Identity Manager », page 17](#).
 - Installez et configurez un serveur d'applications. Reportez-vous à la [Section 2.3, « Installation d'un serveur d'applications », page 19](#).
 - Installez une base de données et configurez-la. Reportez-vous à la [Section 2.4, « Installation d'une base de données », page 23](#).
- Installez les composants du méta-annuaire du module de provisioning basé sur les rôles. Reportez-vous au [Chapitre 3, « Installation du module de provisioning basé sur les rôles dans le méta-annuaire », page 31](#).
- Créez le pilote de l'application utilisateur dans iManager ou Designer 3.5 pour Identity Manager.
 - ♦ Pour iManager : [Section 4.1, « Création du pilote d'application utilisateur dans iManager », page 45](#).
 - ♦ Pour Designer : [Guide de conception de l'application utilisateur \(http://www.novell.com/documentation/idmrbpm37/index.html\)](http://www.novell.com/documentation/idmrbpm37/index.html) .

- ❑ Créez le pilote du service de rôles et de ressources dans iManager ou Designer 3.5 pour Identity Manager.
 - ♦ Pour iManager : [Section 4.2, « Création du pilote du service de rôles et de ressources dans iManager », page 47.](#)
 - ♦ Pour Designer : [User Application: Design Guide \(http://www.novell.com/documentation/idmrbpm37\)](http://www.novell.com/documentation/idmrbpm37) (Guide de conception de l'application utilisateur).
- ❑ Installez et configurez l'application utilisateur Novell Identity Manager. (Vous devez avoir installé le JDK* correct avant de démarrer le programme d'installation. Reportez-vous à la [Section 2.5, « Installation du kit de développement Java », page 29.](#))

Le programme d'installation peut être exécuté dans l'un des trois modes proposés :

 - ♦ Interface Utilisateur Graphique. Consultez l'une des sections suivantes :
 - ♦ [Chapitre 5, « Installation de l'application utilisateur sur JBoss », page 51.](#)
 - ♦ [Chapitre 6, « Installation de l'application utilisateur sur WebSphere », page 67.](#)
 - ♦ [Chapitre 7, « Installation de l'application utilisateur sur WebLogic », page 85.](#)
 - ♦ Interface de console (ligne de commande). Reportez-vous à la [Section 8.1, « Installation de l'application utilisateur à partir de la console », page 103.](#)
 - ♦ Installation en mode silencieux. Reportez-vous à la [Section 8.2, « Installation de l'application utilisateur avec une seule commande », page 104.](#)
- ❑ Procédez aux tâches de post-installation décrites au [Chapitre 9, « Tâches post-installation », page 115.](#)

Important : le présent guide ne fournit pas d'instructions sur la configuration de l'environnement de sécurité. Pour plus d'informations concernant la sécurité, reportez-vous au manuel [User Application: Administration Guide \(http://www.novell.com/documentation/idmrbpm37/index.html\)](http://www.novell.com/documentation/idmrbpm37/index.html) (Guide d'administration de l'application utilisateur).

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*, Microsoft* SQL Server* ou PostgreSQL*. 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. Sous WebSphere* et WebLogic*, vous devez déployer le fichier WAR manuellement.
- ♦ Permet d'activer la consignation via les clients d'audit Novell ou OpenXDAS (selon vos besoins).
- ♦ Permet d'importer une clé principale existante pour restaurer une installation particulière du module de provisioning basé sur les rôles et pour prendre en charge les grappes.

1.3 Configuration système requise

Pour utiliser la version 3.7.0 du module de provisioning basé sur les rôles Identity Manager, vous devez avoir installé chacun des composants requis répertoriés dans le [Tableau 1-1](#).

Tableau 1-1 Configuration système requise

Composant système requis	Configuration système requise
Identity Manager 3.6 et eDirectory	Pour connaître la liste des systèmes d'exploitation pris en charge, consultez la documentation relative à Identity Manager et eDirectory.
Identity Manager 3.6.1 et eDirectory	Pour connaître la liste des systèmes d'exploitation pris en charge, consultez la documentation relative à Identity Manager et eDirectory.
Serveur d'administration basé sur le Web	Pour connaître la liste des systèmes d'exploitation pris en charge, consultez la documentation relative à iManager. Les plug-ins suivants sont requis :
♦ iManager 2.7 SP2 et plug-ins	♦ Plug-in Identity Manager 3.6.1b pour iManager 2.7 ♦ Plug-in 3.6.1b de gestion des mots de passe pour iManager 2.7
Service d'audit	Pour connaître la liste des systèmes d'exploitation pris en charge, consultez la documentation relative à Sentinel ou à Novell Identity Audit.
♦ Sentinel™ 6.1	
♦ Novell Identity Audit 1.0	

Composant système requis	Configuration système requise
Serveur d'applications de l'application utilisateur	<p>L'application utilisateur s'exécute sur JBoss*, WebSphere* et WebLogic* (voir ci-dessous).</p> <p>L'application utilisateur avec JBoss 5.0.1 requiert le JRE* 1.6.0-14 de Sun et est prise en charge sous :</p> <ul style="list-style-type: none"> ♦ Windows 2003 Server (32 et 64 bits) ♦ Windows 2008 Server (32 et 64 bits) ♦ Novell Open Enterprise Server (OES) SP1 (32 et 64 bits) ♦ SUSE Linux Enterprise Server 10 (32 et 64 bits) ♦ SUSE Linux Enterprise Server 11 (32 et 64 bits) ♦ Red Hat Linux 5 (32 et 64 bits) ♦ Solaris 10 (32 et 64 bits) <p>L'application utilisateur avec WebSphere 6.1 requiert la machine virtuelle J9 d'IBM (version 2.3, J2RE 1.5.0). Elle est prise en charge sur les plates-formes suivantes :</p> <ul style="list-style-type: none"> ♦ Windows 2003 Server (32 et 64 bits) ♦ Windows 2008 Server (32 et 64 bits) ♦ SUSE Linux Enterprise Server 10 (32 et 64 bits) ♦ SUSE Linux Enterprise Server 11 (32 et 64 bits) ♦ Red Hat Linux 5 (32 et 64 bits) ♦ AIX 5.3 (64 bits) (uniquement avec une base de données Oracle 10g) ♦ Solaris 10 (32 et 64 bits) <p>L'application utilisateur avec WebSphere 7.0 requiert la machine virtuelle J9 d'IBM (version 2.4, J2RE 1.6.0). Elle est prise en charge sur les plates-formes suivantes :</p> <ul style="list-style-type: none"> ♦ Windows 2003 Server (32 et 64 bits) ♦ Windows 2008 Server (32 et 64 bits) ♦ SUSE Linux Enterprise Server 10 (32 et 64 bits) ♦ SUSE Linux Enterprise Server 11 (32 et 64 bits) ♦ Red Hat Linux 5 (32 et 64 bits) ♦ Solaris 10 (32 et 64 bits) <p>L'application utilisateur avec WebLogic 10.3 requiert la machine virtuelle Java 1.6.0_05 de JRockit* et est prise en charge sur les plates-formes suivantes :</p> <ul style="list-style-type: none"> ♦ Windows 2003 Server (32 et 64 bits) ♦ Windows 2008 Server (32 et 64 bits) ♦ SUSE Linux Enterprise Server 10 (32 et 64 bits) ♦ SUSE Linux Enterprise Server 11 (32 et 64 bits) ♦ Red Hat Linux 5 (32 et 64 bits) ♦ Solaris 10 (32 ou 64 bits)
	<p>Remarque : l'application utilisateur prend en charge la virtualisation Xen et VMWare à condition que le système d'exploitation invité soit également pris en charge par l'application utilisateur.</p>

Composant système requis	Configuration système requise
Navigateur de l'application utilisateur	<p>L'application utilisateur prend en charge Firefox* et Internet Explorer (voir ci-dessous).</p> <p>FireFox* 3 est pris en charge sur les systèmes suivants :</p> <ul style="list-style-type: none">◆ Windows XP avec SP3◆ Windows Vista◆ SUSE Linux Enterprise Desktop 11◆ Novell OpenSuSE 10◆ Novell OpenSuSE 11◆ Apple Mac <p>Firefox* 2 (version 2.0.0.20 uniquement) est pris en charge sur les systèmes suivants :</p> <ul style="list-style-type: none">◆ Novell SUSE Linux Enterprise Desktop 10◆ Novell SUSE Linux Enterprise Server 10◆ Novell OpenSuSE 10 <p>Internet Explorer 8 est pris en charge sur les systèmes suivants :</p> <ul style="list-style-type: none">◆ Windows XP avec SP3◆ Windows Vista <p>Internet Explorer 7 est pris en charge sur les systèmes suivants :</p> <ul style="list-style-type: none">◆ Windows XP SP3

Composant système requis	Configuration système requise
Serveur de base de données pour l'application utilisateur	<p>Les bases de données suivantes sont prises en charge avec JBoss :</p> <ul style="list-style-type: none"> ◆ MS SQL 2005 ◆ MySQL version 5.1 ◆ Oracle 10g ◆ Oracle 11g ◆ PostgreSQL 8.8.3 <p>Les bases de données suivantes sont prises en charge avec WebSphere 6.1 :</p> <ul style="list-style-type: none"> ◆ DB2 9.5 ◆ MS SQL 2005 ◆ Oracle 10g ◆ Oracle 11g <p>Les bases de données suivantes sont prises en charge avec WebSphere 7.0 :</p> <ul style="list-style-type: none"> ◆ DB2 9.5 ◆ MS SQL 2005 ◆ Oracle 10g ◆ Oracle 11g <p>Les bases de données suivantes sont prises en charge avec WebLogic 10.3 :</p> <ul style="list-style-type: none"> ◆ MS SQL 2005 ◆ Oracle 10g ◆ Oracle 11g <p>Les pilotes JDBC suivants sont pris en charge :</p> <p>MS SQL Server : sqljdbc_1.0 (sqljdbc.jar), sqljdbc_1.1 (sqljdbc.jar), sqljdbc_1.2 (sqljdbc.jar) et sqljdbc_2.0 (sqljdbc.jar et sqljdbc4.jar)</p> <p>Oracle10g ou Oracle11g avec WebLogic : ojdbc6.jar (intégré à WebLogic)</p> <p>Serveur léger Oracle : pilote JDBC Oracle, version 10.2.0.1.0.</p> <p>Pilote OCI Oracle : pilote JDBC Oracle, version 10.2.0.2.0.</p> <p>MySQL : mysql-connector-java.jar version 5.1.7</p> <p>IBM DB2 9.5 : DB2 JDBC Universal Driver Architecture 3.52.95</p> <p>PostgreSQL : PostgreSQL 8.1 JBDC 3</p>
Designer	Designer 3.5
OpenXDAS	<p>OpenXDAS version 0.8.345</p> <p>Les versions suivantes d'OpenXDAS sont requises pour SLES10 :</p> <ul style="list-style-type: none"> ◆ openxdas-0.8.351-1.1.i586.rpm ◆ openxdas-0.8.351-1.1.x86_64.rpm

Composant système requis	Configuration système requise
Intégration SSO de l'application utilisateur	Novell Access Manager 3.1.1 ou 3.1.1 IR1 Novell Secure Login 6.1
Domain Services	OES 2 SP1 Domain Services pour Windows
Réponse de vérification d'identité de mot de passe	Méthode de login NMAS avec réponse de vérification d'identité version 2770 build 20080603 ou supérieure requise pour la fonctionnalité de réponse de vérification d'identité au niveau des mots de passe.

Conditions préalables

2

Cette section décrit les logiciels et les composants que vous devez installer ou configurer pour pouvoir installer le module de provisioning basé sur les rôles (RBPM) Identity Manager. Les rubriques sont les suivantes :

- ♦ [Section 2.1, « Installation du méta-annuaire Identity Manager », page 17](#)
- ♦ [Section 2.2, « Téléchargement du module de provisioning basé sur les rôles », page 17](#)
- ♦ [Section 2.3, « Installation d'un serveur d'applications », page 19](#)
- ♦ [Section 2.4, « Installation d'une base de données », page 23](#)
- ♦ [Section 2.5, « Installation du kit de développement Java », page 29](#)

2.1 Installation du méta-annuaire Identity Manager

Le module de provisioning basé sur les rôles version 3.7 peut être utilisé avec le méta-annuaire Identity Manager 3.6 ou 3.6.1.

Pour consulter les instructions d'installation du méta-annuaire Identity Manager, reportez-vous au [Guide d'installation de Novell Identity Manager \(http://www.novell.com/documentation/idm36/\)](http://www.novell.com/documentation/idm36/).

2.2 Téléchargement du module de provisioning basé sur les rôles

Procurez-vous la version 3.7 du module de provisioning basé sur les rôles Identity Manager auprès du [site Web de téléchargement Novell \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp). Téléchargez les fichiers image `.iso` correspondant à votre produit (voir [Tableau 2-1](#)).

Tableau 2-1 Les fichiers de téléchargement `.iso`

Pour ce produit	Téléchargez ce fichier <code>.iso</code>
Application utilisateur	<code>Identity_Manager_RBPM_3_7_0_User_Application.iso</code>
Composants du module de provisioning basé sur les rôles pour le méta-annuaire	<code>Identity_Manager_RBPM_3_7_0_Driver_Install_Utility.iso</code>

Le [Tableau 2-2](#) décrit les fichiers d'installation fournis dans les fichiers `.iso` de l'application utilisateur et du module de provisioning basé sur les rôles.

Tableau 2-2 Fichiers et scripts inclus dans les fichiers ISO

Fichier	Description
IDMProv.war	Fichier WAR du module de provisioning basé sur les rôles. Il contient l'application utilisateur Identity Manager avec les fonctions Self-service d'identité et Module de provisioning basé sur les rôles.
IDMUserApp.jar	Programme d'installation de l'application utilisateur.
silent.properties	Fichier contenant les paramètres requis pour une installation silencieuse. 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. Vous devez copier ce fichier et en modifier le contenu pour l'adapter à votre environnement d'installation.
JBossMySQL.bin ou JBossMySQL.exe	Utilitaire pratique permettant d'installer le serveur d'applications JBoss et la base de données MySQL.
nmassaml.zip	Contient une méthode eDirectory de prise en charge de SAML. Nécessaire uniquement si vous n'utilisez pas Access Manager.
rbpm_driver_install.exe	Programme d'installation Windows pour les composants du méta-annuaire du module de provisioning basé sur les rôles (pilote du service de rôles et de ressources, pilote de l'application utilisateur et schéma eDirectory).
rbpm_driver_install_aix.bin	Programme d'installation AIX pour les composants du méta-annuaire du module de provisioning basé sur les rôles (pilote du service de rôles et de ressources, pilote de l'application utilisateur et schéma eDirectory).
rbpm_driver_install_linux.bin	Programme d'installation Linux pour les composants du méta-annuaire du module de provisioning basé sur les rôles (pilote du service de rôles et de ressources, pilote de l'application utilisateur et schéma eDirectory).
rbpm_driver_install_solaris.bin	Programme d'installation Solaris pour les composants du méta-annuaire du module de provisioning basé sur les rôles (pilote du service de rôles et de ressources, pilote de l'application utilisateur et schéma eDirectory).

Le système sur lequel vous installez le module de provisioning basé sur les rôles Identity Manager doit disposer d'au moins 320 Mo d'espace de stockage disponible, auxquels il convient d'ajouter l'espace requis pour les applications de prise en charge (base de données, serveur d'applications, etc.). Comptez également qu'avec le temps, le système nécessitera de l'espace supplémentaire pour prendre en charge le volume croissant des autres données (journaux de la base de données, du serveur d'applications, etc.).

Le répertoire d'installation par défaut est :

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

Vous pouvez sélectionner un répertoire d'installation par défaut 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 pouvoir y accéder en écriture.

2.3 Installation d'un serveur d'applications

- ♦ [Section 2.3.1, « Installation du serveur d'applications JBoss », page 19](#)
- ♦ [Section 2.3.2, « Installation du serveur d'applications WebLogic », page 23](#)
- ♦ [Section 2.3.3, « Installation du serveur d'applications WebSphere », page 23](#)

2.3.1 Installation du serveur d'applications JBoss

Si vous prévoyez d'utiliser le serveur d'applications JBoss, vous pouvez au choix :

- ♦ Télécharger et installer le serveur d'applications JBoss en vous conformant aux instructions du fabricant. Reportez-vous à la [Section 1.3, « Configuration système requise », page 11](#) pour connaître la version prise en charge.
- ♦ Utiliser l'utilitaire JbossMysql inclus dans le téléchargement du module de provisioning basé sur les rôles pour installer un serveur d'applications JBoss (et MySQL le cas échéant). Pour plus d'informations, reportez-vous à la [« Installation du serveur d'applications JBoss et de la base de données MySQL » page 20](#).

Ne démarrez pas le serveur JBoss avant d'avoir installé le module de provisioning basé sur les rôles Identity Manager. Le démarrage du serveur JBoss constitue en effet une tâche post-installation.

Tableau 2-3 Configuration système minimale recommandée du serveur d'applications JBoss

Composant	Recommandation
RAM	La mémoire vive recommandée pour le serveur d'applications JBoss lors de l'exécution du module de provisioning basé sur les rôles Identity Manager est de 512 Mo.
Port	La valeur par défaut pour le serveur d'applications est 8080. Notez le port que votre serveur d'applications utilise.
SSL	Activez SSL si vous prévoyez utiliser la gestion de mots de passe externe. <ul style="list-style-type: none">♦ Activez SSL sur les serveurs JBoss sur lesquels vous déployez le module de provisioning basé sur les rôles Identity Manager et le fichier <code>IDMPwdMgt.war</code>.♦ Veillez à ce que le port SSL soit ouvert dans votre pare-feu.

Pour en savoir plus sur l'activation de SSL, reportez-vous à la documentation de JBoss.

Pour plus d'informations sur le fichier `IDMPwdMgt.war`, reportez-vous à la [Section 9.5, « Configuration de la gestion externe des mots de passe oubliés », page 118](#) et au manuel [User Application: Administration Guide \(Guide d'administration de l'application utilisateur\)](#) (<http://www.novell.com/documentation/idmrbpm37/index.html>).

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

L'utilitaire JBossMysql installe le serveur d'applications JBoss et MySQL sur votre système. Il ne prend pas en charge le mode console et requiert une interface graphique. Il est recommandé aux utilisateurs Linux/Unix de procéder à l'installation en tant qu'utilisateur non root.

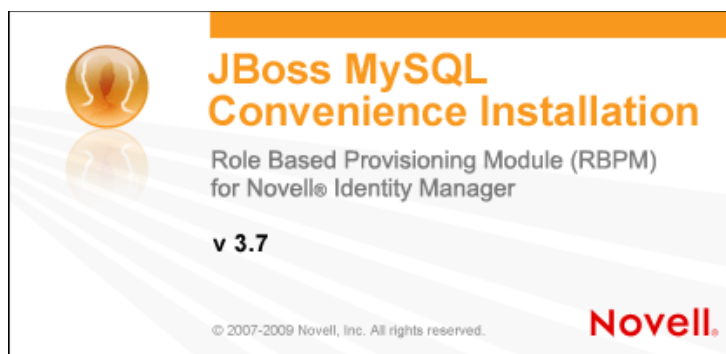
- 1 Recherchez et exécutez JBossMySQL.bin ou JBossMySQL.exe à partir du fichier .iso.

/linux/jboss/JBossMySQL.bin (Linux)

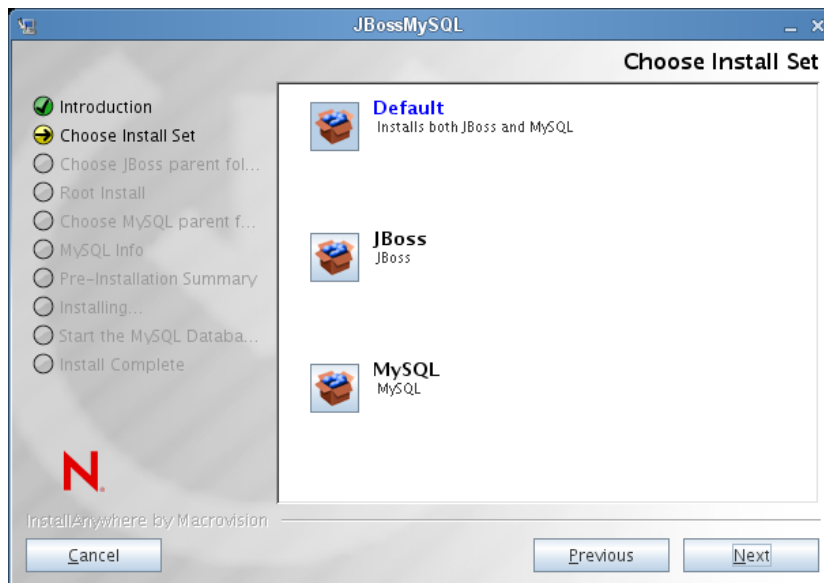
/nt/jboss/JBossMySQL.exe (Windows)

Cet utilitaire n'est pas disponible avec Solaris.

L'écran de démarrage de l'utilitaire JBossMySQL s'affiche :



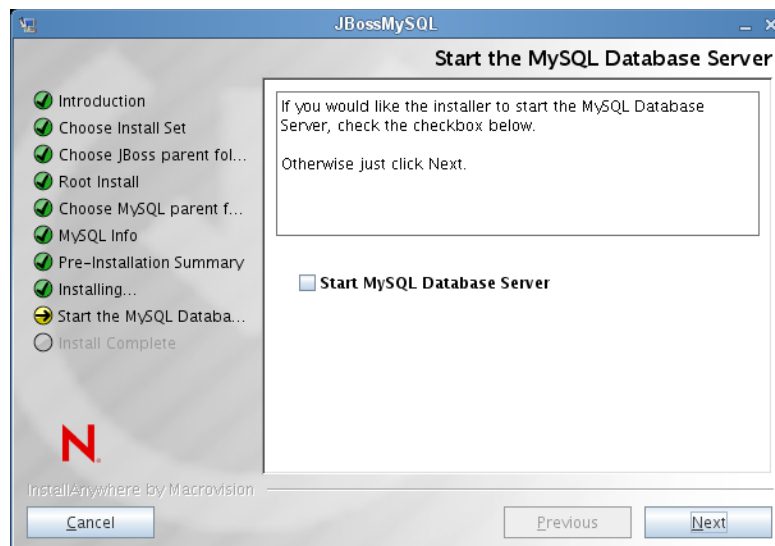
L'utilitaire affiche ensuite l'écran *Choisir l'ensemble d'installation* :



- 2 Suivez les instructions affichées à l'écran pour naviguer dans l'utilitaire. Reportez-vous au tableau suivant pour en savoir plus.

Écran d'installation	Description
Choisir l'ensemble d'installation	<p>Choisissez les produits à installer.</p> <ul style="list-style-type: none">♦ <i>Par défaut</i> : installe, dans le répertoire que vous indiquez, JBoss et MySQL, ainsi que les scripts permettant de les démarrer et de les arrêter.♦ <i>JBoss</i> : installe le serveur d'applications JBoss dans le répertoire que vous indiquez, ainsi que les scripts permettant de le démarrer et de l'arrêter. <hr/> <p>Remarque : cet utilitaire n'installe pas le serveur d'applications JBoss en tant que service Windows. Pour plus d'informations, reportez-vous à la section « Installation du serveur d'applications JBoss en tant que service ou daemon » page 22.</p> <hr/> <ul style="list-style-type: none">♦ <i>MySQL</i> : installe MySQL et crée une base de données MySQL dans le répertoire que vous indiquez, ainsi que les scripts permettant de le démarrer et de l'arrêter.
Sélectionnez le dossier parent JBoss.	Cliquez sur <i>Sélectionner</i> pour choisir un dossier d'installation autre que le dossier par défaut.
Sélectionnez le dossier parent MySQL.	Cliquez sur <i>Sélectionner</i> pour choisir un dossier d'installation autre que le dossier par défaut.
Infos sur MySQL	<p>Saisissez les informations suivantes :</p> <ul style="list-style-type: none">♦ <i>Nom de base de données</i> : indiquez le nom de la base de données que le programme d'installation doit créer. L'utilitaire d'installation de l'application utilisateur vous invite à saisir ce nom : notez-le, ainsi que l'emplacement.♦ <i>Mot de passe utilisateur 'root'</i> (et confirmation du mot de passe) : indiquez le mot de passe root (et confirmez-le) pour cette base de données.
Résumé de la pré-installation	Consultez la page Résumé. Si les indications sont correctes, cliquez sur <i>Installer</i> .

Écran d'installation	Description
Démarrer MySQL Database Server	Si vous avez installé la base de données MySQL, l'utilitaire vous invite à démarrer le serveur de base de données :



Vous devez lancer le serveur de base de données avant de poursuivre l'installation de l'application utilisateur. Sélectionnez *Démarrer MySQL Database Server*, puis cliquez sur *Suivant* si vous souhaitez installer l'application immédiatement.

Si vous avez installé la base de données MySQL, vous devez également la configurer, tel que décrit dans la [Section 2.4.1, « Remarques sur la configuration d'une base de données MySQL »](#), page 24.

Installation terminée	<p>L'utilitaire affiche un message dès qu'il a fini d'installer les produits que vous avez sélectionnés :</p> <pre>The Installer has completed successfully. Thank you for choosing Novell</pre>
-----------------------	--

Important : sachez que l'utilitaire JBossMySQL ne sécurise pas la console JMX ni la console Web JBoss. L'environnement JBoss reste ouvert. Pour éliminer tout risque lié à la sécurité, verrouillez l'environnement dès que vous avez terminé l'installation.

Installation du serveur d'applications JBoss en tant que service ou daemon

Pour démarrer l'application JBoss en tant que daemon, reportez-vous aux instructions de [JBoss](http://www.jboss.org/community/wiki/StartJBossOnBootWithLinux) (<http://www.jboss.org/community/wiki/StartJBossOnBootWithLinux>).

Utilisation de JavaServiceWrapper Vous pouvez utiliser JavaServiceWrapper (wrapper de service Java) pour installer, démarrer et arrêter le serveur d'applications JBoss comme service Windows ou comme processus daemon Linux ou UNIX. Reportez-vous aux recommandations de JBoss à l'adresse <http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows> (<http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows>). L'un de ces wrappers se trouve à l'adresse <http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html> ([http://](http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html)

wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html) : vous pouvez le gérer par JMX (reportez-vous à l'adresse <http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss> (<http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss>)).

Important : pour les versions précédentes, vous pouvez exécuter un utilitaire tiers tel que JavaService pour installer, démarrer et arrêter le serveur d'applications JBoss en tant que service Windows. JBoss recommande toutefois de ne plus utiliser JavaService. Pour plus de détails, reportez-vous au site <http://www.jboss.org/wiki/JavaService> (<http://www.jboss.org/community/wiki/JavaService>).

2.3.2 Installation du serveur d'applications WebLogic

Si vous envisagez d'utiliser le serveur d'applications WebLogic, téléchargez-le et installez-le. Reportez-vous à la [Section 1.3, « Configuration système requise », page 11](#) pour en savoir plus sur les versions prises en charge.

2.3.3 Installation du serveur d'applications WebSphere

Si vous envisagez d'utiliser le serveur d'applications WebSphere, téléchargez-le et installez-le. Reportez-vous à la [Section 1.3, « Configuration système requise », page 11](#) pour en savoir plus sur les versions prises en charge.

Pour consulter des remarques relatives à la configuration de DB2, reportez-vous aux [« Remarques sur la configuration d'une base de données DB2 » page 27](#).

2.4 Installation d'une base de données

L'application utilisateur utilise une base de données pour diverses tâches (stockage des données de configuration, stockage des données relatives aux activités de workflow, etc.). Pour pouvoir installer le module de provisioning basé sur les rôles et l'application utilisateur, vous devez avoir installé et configuré l'une des bases de données prises en charge pour votre plate-forme. Cela implique les opérations suivantes :

- Installation de la base de données et de son pilote.
- Création d'une base de données ou d'une instance de base de données.
- Enregistrement des paramètres de base de données suivants en vue de les utiliser dans la procédure d'installation de l'application utilisateur :
 - ♦ hôte et port
 - ♦ nom de la base de données, nom et mot de passe de l'utilisateur
- Création d'un fichier de source de données pointant vers la base de données.

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

- ❑ Les bases de données doivent prendre en charge le codage Unicode.

L'application utilisateur nécessite que le jeu de caractères de la base de données utilise le codage Unicode. Ainsi, UTF-8 est un exemple de jeu de caractères employant ce codage, alors que Latin1 ne l'utilise pas. Avant d'installer l'application utilisateur, vérifiez que votre base de données est configurée avec un jeu de caractères utilisant le codage Unicode.

Remarque : si vous effectuez une migration vers une nouvelle version du module de provisioning basé sur les rôles, vous devez utiliser la même base de données d'application utilisateur que pour l'installation précédente, c'est-à-dire celle depuis laquelle vous effectuez la migration.

2.4.1 Remarques sur la configuration d'une base de données MySQL

L'application utilisateur nécessite certaines options de configuration pour MySQL. Si vous installez vous-même MySQL, c'est à vous de configurer ces paramètres. 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 24](#)
- ♦ [« Ensemble de caractères » page 24](#)
- ♦ [« Distinction de la casse » page 25](#)
- ♦ [« Paramètre Ansi » page 25](#)
- ♦ [« Conditions relatives au compte utilisateur » 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`.

Au lieu de configurer l'option `default-table-type=innodb`, vous pouvez ajouter l'option `ENGINE=InnoDB` aux instructions de création de table dans le script SQL de votre base de données.

Ensemble de caractères

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

```
character_set_server=utf8
```

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 l'exemple suivant :

```
<connection-url>jdbc:mysql://localhost:3306/  
databasename?useUnicode=true&characterEncoding=utf8&connectionCollati  
on=utf8_bin</connection-url>
```

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.

Paramètre Ansi

Si vous choisissez d'utiliser votre propre programme d'installation pour MySQL 5.1, vous devez ajouter l'entrée `ansi` au fichier `my.cnf` (Linux) ou `my.ini` (Windows). Si vous ne le faites pas, les tables RBPM sont créées mais les données initiales des tables ne sont pas chargées et vous risquez de recevoir un message d'erreur de type « Définition de page du conteneur de l'invité introuvable ».

Une fois que vous avez ajouté l'entrée `ansi`, le fichier `my.cnf` (ou `my.ini`) doit se présenter comme suit :

```
# These variables are required for IDM User Application  
character_set_server=utf8  
default-table-type=innodb
```

```
# Put the server in ANSI SQL mode.  
#See http://www.mysql.com/doc/en/ANSI\_mode.html  
ansi
```

Pour vérifier que la modification permettant d'utiliser le mode Ansi a bien été prise en compte, vous pouvez exécuter l'instruction SQL suivante sur votre serveur MySQL :

```
mysql> select @@global.sql_mode;  
+-----+  
| @@global.sql_mode |  
+-----+  
| REAL_AS_FLOAT,PIPES_AS_CONCAT,ANSI_QUOTES,IGNORE_SPACE,ANSI |  
+-----+  
1 row in set (0.00 sec)
```

Conditions relatives au compte utilisateur

Le compte utilisateur employé au cours du processus d'installation doit bénéficier d'un accès total à la base de données qui sera utilisée par l'application utilisateur (c'est-à-dire en être propriétaire). En outre, ce compte doit pouvoir accéder aux tables du système. Celles-ci peuvent varier en fonction de votre environnement.

Créez un utilisateur devant se loguer au serveur MySQL et accordez-lui des privilèges, par exemple :

```
GRANT ALL PRIVILEGES ON <nom_base_de_données.>* TO <nom_utilisateur>@<hôte>
IDENTIFIED BY 'mot_de_passe'
```

L'ensemble minimum de privilèges est CREATE, INDEX, INSERT, UPDATE, DELETE et LOCK TABLES. Pour obtenir des informations sur la commande GRANT, reportez-vous à <http://www.mysql.org/doc/refman/5.0/en/grant.html> (<http://www.mysql.org/doc/refman/5.0/en/grant.html>).

Important : le compte utilisateur doit également posséder des droits de sélection au niveau de la table mysql.user. Pour configurer les droits appropriés, la syntaxe SQL doit être la suivante :

```
USE mysql;
GRANT SELECT ON mysql.user TO <username>@<host>;
```

2.4.2 Remarques sur la configuration d'une base de données Oracle

Lorsque vous créez votre base de données Oracle, veillez à bien utiliser AL32UTF8 afin de définir un ensemble de caractères codés en Unicode. (Voir [AL32UTF8](http://download-east.oracle.com/docs/cd/B19306_01/server.102/b14225/glossary.htm#sthref2039) (http://download-east.oracle.com/docs/cd/B19306_01/server.102/b14225/glossary.htm#sthref2039).

Lorsque vous créez un utilisateur pour votre base de données Oracle, vous devez générer les instructions suivantes à l'aide de l'utilitaire SQL Plus. Ces instructions créent l'utilisateur et définissent ses privilèges. Accordez les privilèges CONNECT et RESOURCE, par exemple :

```
CREATE USER utilisateur_IDM IDENTIFIED BY mot_de_passe

GRANT CONNECT, RESOURCE to utilisateur_IDM
```

UTF-8 sur Oracle 11g Sur Oracle 11g, vous pouvez entrer la commande suivante afin de confirmer que la base prend en charge le codage UTF-8 :

```
select * from nls_database_parameters;
```

Si vous n'avez pas configuré la base pour UTF-8, les données renvoyées sont les suivantes :

```
NLS_CHARACTERSET
WE8MSWIN1252
```

Si vous avez configuré la base pour UTF-8, les données renvoyées sont les suivantes :

```
NLS_CHARACTERSET
AL32UTF8
```

2.4.3 Remarques sur la configuration d'une base de données MS SQL Server

Configurez votre base de données MS SQL Server comme suit :

- 1 Installez MS SQL Server.
- 2 Connectez-vous au serveur et ouvrez une application pour créer la base de données et l'utilisateur de la base de données (généralement l'application SQL Server Management Studio).
- 3 Créez une base de données. SQL Server ne permet pas aux utilisateurs de sélectionner le jeu de caractères des bases de données. L'application utilisateur IDM stocke les données caractères SQL Server dans un type de colonne NCHAR qui prend en charge le codage UTF-8.
- 4 Créez un login.
- 5 Ajoutez le login en tant qu'utilisateur de la base de données.
- 6 Accordez ces privilèges au login : CREATE TABLE, CREATE INDEX, SELECT, INSERT, UPDATE et DELETE.

L'application utilisateur requiert la version 1.0.809.102 du pilote JDBC pour Microsoft SQL Server 2005. Notez que seuls les systèmes d'exploitation Sun Solaris, Red Hat Linux et Windows 2000 ou version ultérieure sont officiellement pris en charge avec ce pilote JDBC.

2.4.4 Remarques sur la configuration d'une base de données DB2

Cette section contient des remarques sur la configuration de DB2.

Sélection des fichiers JAR du pilote de base de données

Les fichiers JAR du pilote de base de données doivent être sélectionnés au cours de l'installation, dans l'écran *Nom d'utilisateur et mot de passe de la base de données*. Toutefois, le bouton *Parcourir* en regard du champ *Fichier JAR du pilote de base de données* ne vous permet de sélectionner qu'un seul fichier JAR. Or, pour DB2, vous devez fournir 2 fichiers JAR :

- ♦ db2jcc.jar
- ♦ db2jcc_license_cu.jar

Par conséquent, si vous exécutez le programme d'installation sous WebSphere (le seul serveur d'applications pris en charge avec DB2), vous pouvez sélectionner un fichier JAR mais vous devrez saisir manuellement le second fichier. Pour ce faire, utilisez le séparateur de fichiers approprié pour le système d'exploitation sous lequel s'exécute le programme. Vous pouvez aussi spécifier manuellement les deux fichiers.

Par exemple, sous Windows :

```
c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar
```

Par exemple, sous Solaris et Linux :

```
/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar
```

Optimisation des bases de données DB2 pour éviter les blocages et les timeouts

Si vous utilisez DB2, vous pouvez rencontrer une erreur indiquant que la transaction en cours a été annulée du fait d'un blocage ou d'un timeout. Cela peut résulter de la présence simultanée d'un grand nombre d'utilisateurs et de bases de données.

DB2 propose plusieurs moyens de résoudre les conflits de verrous, notamment le réglage de l'optimiseur basé sur les coûts. Excellente source de la documentation d'administration de DB2, le *guide des performances* contient de nombreuses informations sur le réglage.

Aucune valeur de réglage n'est définie pour toutes les installations car le niveau de simultanéité et la taille des données varient. Toutefois, les conseils suivants sur le réglage de DB2 peuvent servir à votre installation :

- ♦ La commande `reorgchk update statistics` actualisera les statistiques utilisées par l'optimiseur. Les mises à jour périodiques de ces statistiques peuvent suffire à minimiser le problème.
- ♦ L'utilisation du paramètre de registre DB2 `DB2 DB2_RR_TO_RS` peut améliorer la simultanéité du fait du non-verrouillage de la clé de ligne suivante insérée ou mise à jour.
- ♦ Augmentez la valeur des paramètres `MAXLOCKS` et `LOCKLIST` (base de données).
- ♦ Augmentez la valeur de la propriété `currentLockTimeout` (pool de connexion de la base de données).
- ♦ Utilisez l'assistant de configuration de base de données et optimisez-le pour accélérer les transactions.
- ♦ Rendez `VOLATILES` toutes les tables de l'application utilisateur pour indiquer à l'optimiseur que la cardinalité variera considérablement. Pour rendre `VOLATILE` la table `AFACTIVITY` par exemple, vous pouvez émettre la commande : `ALTER TABLE AFACTIVITY VOLATILE`

La commande `ALTER TABLE` doit être exécutée après le démarrage de l'application utilisateur et une fois les tables de la base de données créées. Pour plus d'informations, reportez-vous à la documentation sur cette instruction. Voici les instructions SQL pour toutes les tables de l'application utilisateur :

```
ALTER TABLE AFACTIVITY VOLATILE
ALTER TABLE AFACTIVITYTIMERTASKS VOLATILE
ALTER TABLE AFBRANCH VOLATILE
ALTER TABLE AFCOMMENT VOLATILE
ALTER TABLE AFDOCUMENT VOLATILE
ALTER TABLE AFENGINE VOLATILE
ALTER TABLE AFENGINESTATE VOLATILE
ALTER TABLE AFMODEL VOLATILE
ALTER TABLE AFPROCESS VOLATILE
ALTER TABLE AFPROVISIONINGSTATUS VOLATILE
ALTER TABLE AFQUORUM VOLATILE
ALTER TABLE AFRESOURCEREQUESTINFO VOLATILE
ALTER TABLE AFWORKTASK VOLATILE
ALTER TABLE AF_ROLE_REQUEST_STATUS VOLATILE
ALTER TABLE ATTESTATION_ATTESTER VOLATILE
ALTER TABLE ATTESTATION_ATTRIBUTE VOLATILE
ALTER TABLE ATTESTATION_QUESTION VOLATILE
ALTER TABLE ATTESTATION_REPORT VOLATILE
ALTER TABLE ATTESTATION_REQUEST VOLATILE
ALTER TABLE ATTESTATION_RESPONSE VOLATILE
ALTER TABLE ATTESTATION_SURVEY_QUESTION VOLATILE
ALTER TABLE ATTESTATION_TARGET VOLATILE
```

```

ALTER TABLE AUTHPROPS VOLATILE
ALTER TABLE DATABASECHANGELOG VOLATILE
ALTER TABLE DATABASECHANGELOGLOCK VOLATILE
ALTER TABLE DSS_APPLET_BROWSER_TYPES VOLATILE
ALTER TABLE DSS_APPLET_CFG VOLATILE
ALTER TABLE DSS_APPLET_CFG_MAP VOLATILE
ALTER TABLE DSS_BROWSER_TYPE VOLATILE
ALTER TABLE DSS_CONFIG VOLATILE
ALTER TABLE DSS_EXT_KEY_USAGE_RESTRICTION VOLATILE
ALTER TABLE DSS_USR_POLICY_SET VOLATILE
ALTER TABLE JBM_COUNTER VOLATILE
ALTER TABLE JBM_DUAL VOLATILE
ALTER TABLE JBM_ID_CACHE VOLATILE
ALTER TABLE JBM_MSG VOLATILE
ALTER TABLE JBM_MSG_REF VOLATILE
ALTER TABLE JBM_POSTOFFICE VOLATILE
ALTER TABLE JBM_ROLE VOLATILE
ALTER TABLE JBM_TX VOLATILE
ALTER TABLE JBM_USER VOLATILE
ALTER TABLE PORTALCATEGORY VOLATILE
ALTER TABLE PORTALPORTLETHANDLES VOLATILE
ALTER TABLE PORTALPORTLETSETTINGS VOLATILE
ALTER TABLE PORTALPRODUCERREGISTRY VOLATILE
ALTER TABLE PORTALPRODUCERS VOLATILE
ALTER TABLE PORTALREGISTRY VOLATILE
ALTER TABLE PROFILEGROUPPREFERENCES VOLATILE
ALTER TABLE PROFILEUSERPREFERENCES VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP_LABEL VOLATILE
ALTER TABLE PROVISIONING_VIEW_VALUE VOLATILE
ALTER TABLE PROVISIONING_VIEW_VALUE_LABEL VOLATILE
ALTER TABLE SECURITYACCESSRIGHTS VOLATILE
ALTER TABLE SECURITYPERMISSIONMETA VOLATILE
ALTER TABLE SECURITYPERMISSIONS VOLATILE
ALTER TABLE SEC_DELPROXY_CFG VOLATILE
ALTER TABLE SEC_DELPROXY_SRV_CFG VOLATILE
ALTER TABLE SEC_SYNC_CLEANUP_QUEUE VOLATILE

```

2.5 Installation du kit de développement Java

Pour exécuter le programme d'installation de l'application utilisateur, vous devez utiliser la version appropriée de l'environnement Java correspondant à votre serveur d'applications, comme décrit ci-après :

- ♦ Pour JBoss 5.01, vous devez utiliser la plate-forme Java 2 Standard Edition Development version 1.6 (JDK ou JRE) de Sun.

Remarque : pour plus de simplicité, l'utilitaire JBossMySQL installe la version appropriée du JRE pour JBoss.

- ♦ Pour WebSphere 6.1, vous devez utiliser le JDK 1.5 d'IBM.
- ♦ Pour WebSphere 7.0, vous devez utiliser le JDK 1.6 d'IBM.
- ♦ Pour WebLogic 10.3, vous devez utiliser le JDK 1.6 de JRockit.

Définissez la variable d'environnement `JAVA_HOME` de façon à ce qu'elle pointe vers le JDK* à utiliser avec l'application utilisateur. Vous pouvez également indiquer manuellement le chemin d'accès lors de l'installation de l'application utilisateur pour remplacer `JAVA_HOME`.

Remarque : pour les utilisateurs de SUSE Linux Enterprise Server (SLES) : ne pas utiliser le JDK IBM* fourni avec SLES. Cette version n'est en effet pas compatible avec certaines parties de l'installation.

Installation du module de provisioning basé sur les rôles dans le méta-annuaire

Cette section explique comment installer les composants du méta-annuaire du module RBPM dans Identity Manager. Les rubriques sont les suivantes :

- ♦ [Section 3.1, « À propos de l'installation du module de provisioning basé sur les rôles », page 31](#)
- ♦ [Section 3.2, « Exécution de l'utilitaire NrfCaseUpdate », page 32](#)
- ♦ [Section 3.3, « Exécution du programme d'installation du RBPM », page 38](#)

Important : les étapes décrites dans cette section sont obligatoires lorsque vous installez le module de provisioning basé sur les rôles sur une version antérieure d'Identity Manager (par exemple, Identity Manager 3.6 ou 3.6.1). Identity Manager 3.7 installe automatiquement les composants fondamentaux du module RBPM.

3.1 À propos de l'installation du module de provisioning basé sur les rôles

Le programme d'installation du module de provisioning basé sur les rôles (RBPM) pour Identity Manager installe plusieurs composants dans le méta-annuaire d'Identity Manager. Ces composants incluent les éléments suivants :

- ♦ Pilote de rôles et de ressources
- ♦ Pilote d'application utilisateur
- ♦ Schéma eDirectory

Le programme d'installation du RBPM doit être exécuté sur la machine sur laquelle votre environnement de méta-annuaire Identity Manager est installé.

Une fois que ces éléments sont installés dans Identity Manager, suivez la procédure décrite au [Chapitre 4, « Création des pilotes », page 45](#) afin de créer les pilotes requis pour l'application utilisateur.

Important : si votre arborescence eDirectory contient un pilote d'application utilisateur créé avec une version précédente du RBPM, vous devez exécuter l'utilitaire NrfCaseUpdate avant d'exécuter le programme d'installation du module de provisioning basé sur les rôles. Dans le cas contraire, l'installation échouera.

3.2 Exécution de l'utilitaire NrfCaseUpdate

Cette section fournit des informations concernant l'utilitaire NrfCaseUpdate. Les rubriques sont les suivantes :

- ♦ [Section 3.2.1, « Présentation de NrfCaseUpdate », page 32](#)
- ♦ [Section 3.2.2, « Présentation de l'installation », page 32](#)
- ♦ [Section 3.2.3, « Conséquences de l'utilitaire NrfCaseUpdate sur le schéma », page 33](#)
- ♦ [Section 3.2.4, « Création d'une sauvegarde des pilotes d'application utilisateur », page 33](#)
- ♦ [Section 3.2.5, « Utilisation de NrfCaseUpdate », page 33](#)
- ♦ [Section 3.2.6, « Vérification du processus NrfCaseUpdate », page 35](#)
- ♦ [Section 3.2.7, « Activation du JRE pour les connexions SSL », page 36](#)
- ♦ [Section 3.2.8, « Restauration des pilotes d'application utilisateur invalidés », page 36](#)

3.2.1 Présentation de NrfCaseUpdate

La procédure NrfCaseUpdate est nécessaire pour permettre la prise en charge des recherches de rôles et de ressources avec casse mixte. Cette procédure met à jour le schéma en modifiant les attributs nrfLocalizedDescs et nrfLocalizedNames, qui sont utilisés par les pilotes de l'application utilisateur. Elle doit être effectuée avant l'installation du RBPM 3.7 et avant la migration des pilotes existants dans Designer 3.5.

3.2.2 Présentation de l'installation

Cette section présente les étapes permettant de mettre à niveau et de migrer un environnement RBPM existant. Elle met l'accent sur l'utilisation de Designer 3.5 pour la création de sauvegardes des pilotes de l'application utilisateur avant de procéder à n'importe quelle mise à niveau. Cette présentation part également du principe que la version d'IDM utilisée est 3.6 ou ultérieure.

- 1 Installez Designer 3.5.
- 2 Vérifiez l'état de santé du coffre-fort d'identité afin de vous assurer que le schéma s'étend correctement. Pour la procédure de vérification de l'état de santé, reportez-vous au document TID 3564075.
- 3 Importez les pilotes d'application utilisateur existants dans Designer 3.5.
- 4 Archivez le projet Designer. Il correspond à l'état du pilote avant l'installation de RBPM 3.7.
- 5 Exécutez le processus NrfCaseUpdate.
- 6 Créez un projet Designer 3.5 et importez le pilote d'application utilisateur afin de préparer la migration.
- 7 Installez RBPM 3.7.
- 8 Migrez le pilote à l'aide de Designer 3.5.
- 9 Déployez le pilote migré.

3.2.3 Conséquences de l'utilitaire NrfCaseUpdate sur le schéma

Lorsque l'utilitaire NrfCaseUpdate met à jour des attributs existants dans le schéma eDirectory, toutes les instances existantes de ces attributs sont effectivement supprimées. Les pilotes d'application utilisateur se servent de ces attributs et seront donc affectés par cette mise à jour du schéma, en particulier les noms et la description des rôles et des séparations des tâches, les requêtes d'attestation personnalisées et les rapports.

La procédure NrfCaseUpdate met à jour les pilotes d'application utilisateur existants via un utilitaire permettant d'exporter ces pilotes vers un fichier LDIF avant d'exécuter la mise à jour du schéma. L'importation des fichiers LDIF après la mise à jour du schéma recrée tous les objets supprimés au cours de la mise à jour.

Comme toujours, il est important de sauvegarder tous les pilotes d'application utilisateur existants, par mesure de précaution. N'oubliez pas que les mises à jour de schéma affectent toutes les partitions IDM. Il est donc essentiel d'utiliser NrfCaseUpdate pour exporter les pilotes d'application utilisateur dans l'arborescence.

3.2.4 Création d'une sauvegarde des pilotes d'application utilisateur

Novell recommande l'utilisation de Designer pour créer une sauvegarde de vos pilotes d'application utilisateur. Avant de lancer la procédure NrfCaseUpdate, suivez les instructions ci-après pour sauvegarder vos pilotes d'application utilisateur existants :

- 1 Installez Designer 3.5 (fourni avec RBPM 3.7).
- 2 Créez un coffre-fort d'identité et assignez-le à votre serveur IDM contenant les pilotes d'application utilisateur.
- 3 Utilisez l'option *En direct* -> *Importer* pour importer votre ensemble de pilotes et vos pilotes d'application utilisateur.
- 4 Enregistrez et archivez ce projet Designer.

3.2.5 Utilisation de NrfCaseUpdate

L'utilitaire NrfCaseUpdate vous invite à exporter chaque pilote, puis procède à la mise à jour du schéma. Si vous n'êtes pas sûr de l'existence ou de l'emplacement de certains pilotes d'application utilisateur, il est conseillé de ne pas poursuivre, car la mise à jour du schéma risque d'invalider les pilotes d'application utilisateur existants.

Il est possible d'utiliser le JRE fourni dans le répertoire d'installation d'IDM, généralement `/root/idm/jre`, pour exécuter NrfCaseUpdate. Si vous avez besoin de connexions SSL à eDirectory, vous devez activer votre JRE pour les connexions SSL. Pour ce faire, suivez les instructions décrites à la [Section 3.2.7, « Activation du JRE pour les connexions SSL », page 36](#).

Vous pouvez également exécuter l'utilitaire NrfCaseUpdate à distance, à partir d'un hôte avec un JRE doté du certificat eDirectory, par exemple l'hôte du serveur de l'application utilisateur. Dans ce cas, vous devez quitter l'utilitaire NrfCaseUpdate à l'aide de la combinaison de touches CTRL+C, après avoir exporté tous les pilotes vers le fichier LDIF et avant de mettre à jour le schéma. Ensuite, vous pouvez mettre à jour le schéma manuellement sur l'hôte eDirectory à l'aide de la commande `ndssch`, comme illustré ci-après :

```
ndssch -h hostname adminDN update-nrf-case.sch
```

Remarque : NrfCaseUpdate accepte plusieurs arguments dans la ligne de commande. Utilisez la commande `-help` ou `-?` pour plus d'informations.

Pour exécuter l'utilitaire NrfCaseUpdate, procédez comme suit :

1 Assurez-vous d'avoir vérifié l'état de santé du coffre-fort d'identité avant d'exécuter l'utilitaire NrfCaseUpdate. Pour la procédure de vérification de l'état de santé, reportez-vous au document TID 3564075.

2 Avant de lancer l'utilitaire, identifiez tous les DN des pilotes d'application utilisateur existants. Pour exporter ces pilotes vers LDIF, vous devrez indiquer les références d'authentification.

3 Exécutez l'utilitaire NrfCaseUpdate. Éventuellement, vous pouvez utiliser la commande `-v` pour obtenir une sortie plus verbeuse :

```
/root/idm/jre/bin/java -jar NrfCaseUpdate.jar -v
```

4 Vous êtes invité à indiquer si vous possédez un pilote d'application utilisateur. Répondez par l'affirmative si tel est le cas. Sinon, répondez par la négative et passez à l'[Étape 6 page 34](#).

```
Do you currently have a User Application Driver configured [DEFAULT true]
:
```

5 Ensuite, l'utilitaire vous demande si vous possédez plusieurs pilotes d'application utilisateur. Répondez par l'affirmative si tel est le cas :

```
Do you currently have more than one (1) User Application Driver configured
[DEFAULT false] :
```

6 Indiquez le DN de l'administrateur ainsi que les références appropriées pour l'exportation du pilote d'application utilisateur :

```
Specify the DN of the Identity Vault administrator user.
This user must have inherited supervisor rights to the user application
driver specified above.
(e.g. cn=admin,o=acme):
```

7 Saisissez le mot de passe de cet administrateur :

```
Specify the Identity Vault administrator password:
```

8 Indiquez le nom d'hôte ou l'adresse IP du serveur IDM hébergeant le pilote d'application utilisateur :

```
Specify the DNS address of the Identity Vault (e.g acme.com):
```

9 Spécifiez le port à utiliser pour la connexion :

```
Specify the Identity Vault port [DEFAULT 389]:
```

10 Ensuite, vous êtes invité à préciser si vous voulez utiliser SSL pour la connexion. Dans l'affirmative, le JRE nécessite que le certificat eDirectory soit présent dans la zone de stockage approuvée. Pour conserver le certificat, suivez les instructions décrites à la [Section 3.2.7, « Activation du JRE pour les connexions SSL », page 36](#).

```
Use SSL to connect to Identity Vault: [DEFAULT false] :
```

11 Indiquez le nom distinctif complet du pilote d'application utilisateur à exporter :

```
Specify the fully qualified LDAP DN of the User Application driver located
in the Identity Vault
(e.g. cn=UserApplication,cn=driverset,o=acme):
```

12 Indiquez le nom du fichier LDIF dans lequel l'application utilisateur va être exportée :

Specify the LDIF file name where the restore data will be written (enter defaults to nrf-case-restore-data.ldif) :

13 L'utilitaire publie les informations relatives aux objets enregistrés dans le fichier LDIF.

14 Si vous avez indiqué que vous possédez plusieurs pilotes, vous recevez l'invite suivante :

```
You indicated you have more than one (1) User Application Driver to
configure.
```

```
Do you have another driver to export? [DEFAULT false] :
```

```
If you have another driver to export then specify true. The utility will
repeat Steps 5 through 12 for each driver.
```

```
If you do not have another driver to export then specify false. Ensure that
you have exported all existing drivers before proceeding as the utility
will proceed with the schema update.
```

15 Vous êtes invité à indiquer l'emplacement de votre utilitaire `ndssch` ainsi que les emplacements génériques. L'utilitaire `ndssch` permet de mettre à jour le schéma.

```
Please enter the path to the schema utility:
```

```
For Unix/Linux typically /opt/novell/eDirectory/bin/ndssch
```

```
For Windows C:\Novell\NDS\schemaStart.bat:
```

16 L'utilitaire publie le message d'état pour la mise à jour du schéma :

```
Schema has successfully been updated for mixed case compliance!
```

Remarque : veillez à accorder suffisamment de temps à eDirectory pour la synchronisation des modifications du schéma, faute de quoi l'importation du fichier LDIF échoue.

17 Vérifiez de nouveau l'état de santé du coffre-fort d'identité afin de vous assurer, avant l'importation du fichier LDIF, que le schéma s'est étendu correctement. Pour la procédure de vérification de l'état de santé, reportez-vous au document TID 3564075.

18 Une fois que tous les pilotes sont exportés et que la mise à jour du schéma est correctement appliquée, vous devez importer chaque fichier LDIF. Indiquez que vous souhaitez autoriser les références en aval dans votre commande `ice`. La ligne de commande ci-dessous est fournie à titre d'exemple :

```
ice -l[mylogfile.log] -v -SLDIF -f[your_created_ldif] -c -DLDA -
s[hostname] -p[389/636] -d[cn=myadmin,o=mycompany] -w[MYPASSWORD] -F -B
```

19 Lorsque tous les pilotes sont réimportés, vérifiez que le processus `NrfCaseUpdate` a abouti. Pour plus d'informations, reportez-vous à la [Section 3.2.6, « Vérification du processus NrfCaseUpdate », page 35](#).

20 Une fois que vous avez vérifié que le processus `NrfCaseUpdate` a abouti, vous pouvez poursuivre l'installation du RBPM 3.7.

3.2.6 Vérification du processus NrfCaseUpdate

Une fois tous les pilotes réimportés, assurez-vous que la restauration a abouti. Pour ce faire, vérifiez les éléments suivants dans l'application utilisateur :

- ◆ Nom et description des rôles
- ◆ Nom et description des séparations des tâches
- ◆ Requêtes d'attestation, y compris les requêtes personnalisées
- ◆ Rapports

Une fois cette vérification terminée, vous pouvez poursuivre l'installation et effectuer la mise à niveau vers RBPM 3.7.

3.2.7 Activation du JRE pour les connexions SSL

Cette section explique comment configurer le JRE pour qu'il utilise une connexion SSL.

En premier lieu, exportez un certificat auto-signé à partir de l'autorité de certification dans le coffre-fort d'identité :

- 1 Dans la vue *Rôles et tâches* d'iManager, cliquez sur *Administration de l'annuaire > Modifier un objet*.
- 2 Sélectionnez l'objet Autorité de certification pour le coffre-fort d'identité, puis cliquez sur *OK*. Il se trouve généralement dans le conteneur Sécurité et est nommé *NOM_ARBORESCENCE CA.Security*.
- 3 Cliquez sur *Certificat > Certificat auto-signé*.
- 4 Cliquez sur *Exporter*.
- 5 Lorsque vous êtes invité à indiquer si vous souhaitez exporter la clé privée avec le certificat, cliquez sur *Non*, puis sur *Suivant*.
- 6 Sélectionnez le format DER binaire.
- 7 Cliquez sur le lien *Enregistrer le certificat exporté*.
- 8 Accédez à l'emplacement dans lequel vous souhaitez enregistrer le fichier, puis cliquez sur *Enregistrer*.
- 9 Cliquez sur *Fermer*.

Ensuite, importez le certificat auto-signé dans la zone de stockage approuvée du JRE.

- 1 Exécutez l'utilitaire keytool inclus dans le JRE.
- 2 Importez le certificat dans la zone de stockage approuvée de l'administrateur d'assignation des rôles. Pour ce faire, saisissez la commande suivante en réponse à l'invite :

```
keytool -import -file name_of_cert_file -trustcacerts -noprompt -keystore filename -storepass password
```

Par exemple :

```
keytool -import -file tree_ca_root.b64 -trustcacerts -noprompt -keystore cacerts -storepass changeit
```

3.2.8 Restauration des pilotes d'application utilisateur invalidés

Si la mise à jour du schéma est appliquée à un pilote d'application utilisateur avant que l'utilitaire NrfCaseUpdate traite ce pilote, ce dernier est invalidé et vous devez le restaurer à l'aide d'une sauvegarde.

Important : ne supprimez et ne renommez *pas* le pilote d'application utilisateur invalidé, car cela invaliderait toutes les associations du pilote. En outre, si le pilote du service de rôles et de ressources est en cours d'exécution et que vous supprimez le pilote d'application utilisateur, le pilote du service de rôles et de ressources détecte les suppressions de rôles et supprime les rôles des utilisateurs concernés.

Par ailleurs, il ne suffit pas de redéployer le pilote sauvegardé dans IDM, car le changement de schéma ne peut pas être actualisé de cette façon. La procédure suivante effectue la restauration en déployant une copie renommée du pilote afin de générer les données à restaurer.

Cette procédure décrit le processus de restauration d'une sauvegarde de pilote d'application utilisateur à l'aide de Designer 3.5 :

- 1 Redémarrez le serveur eDirectory afin de vérifier que la modification du schéma a été prise en compte.
- 2 Ouvrez une copie du projet Designer 3.5 contenant la sauvegarde du pilote d'application utilisateur UserAppDriver. Cette procédure modifie le nom du pilote ; il est donc important d'utiliser une copie du projet.
- 3 Sélectionnez le connecteur entre le pilote d'application utilisateur et le coffre-fort d'identité, cliquez avec le bouton droit de la souris, puis choisissez *Propriétés*.
- 4 Indiquez un nouveau nom, par exemple UserAppDriver_restore. Cliquez sur *Appliquer*, puis sur *OK*.
- 5 Cliquez sur *Enregistrer* pour enregistrer le projet.
- 6 Synchronisez le schéma du coffre-fort d'identité : sélectionnez le coffre-fort d'identité, puis accédez au menu *En direct -> Schéma -> Comparer* et choisissez *Mettre à jour Designer pour l'opération de rapprochement*.
- 7 Enregistrez le projet.
- 8 Déployez le pilote renommé : sélectionnez le pilote puis choisissez *Pilote -> Déployer*.
- 9 Exécutez l'utilitaire NrfCaseUpdate et exportez le pilote renommé vers un fichier LDIF.
- 10 Créez une copie du fichier LDIF afin de pouvoir le modifier.
- 11 Modifiez le fichier LDIF et renommez toutes les références du pilote en fonction du pilote d'application utilisateur que vous restaurez. Par exemple, si votre pilote d'application utilisateur initial est cn=UserAppDriver, renommez cn=UserAppDriver_restore en cn=UserAppDriver. Cette étape crée un fichier LDIF reflétant le pilote d'application utilisateur réel.
- 12 Importez le fichier LDIF modifié à l'aide de la commande ice :

```
ice -l[mylogfile.log] -v -SLDIF -f[your_created_ldif] -c -DLdap -s[hostname] -p[389/636] -d[cn=myadmin,o=mycompany] -w[MYPASSWORD] -F -B
```
- 13 Vérifiez l'état de l'importation à l'aide de la commande ice afin de vous assurer qu'elle a abouti.
- 14 Suivez les instructions de la [Section 3.2.6, « Vérification du processus NrfCaseUpdate », page 35](#) pour vérifier la restauration du pilote.
- 15 Supprimez le pilote renommé de l'ensemble de pilotes.

3.3 Exécution du programme d'installation du RBPM

- 1 Lancez le programme d'installation approprié pour votre plate-forme :

Linux

`rbpm_driver_install_linux.bin`

Solaris

`rbpm_driver_install_solaris.bin`

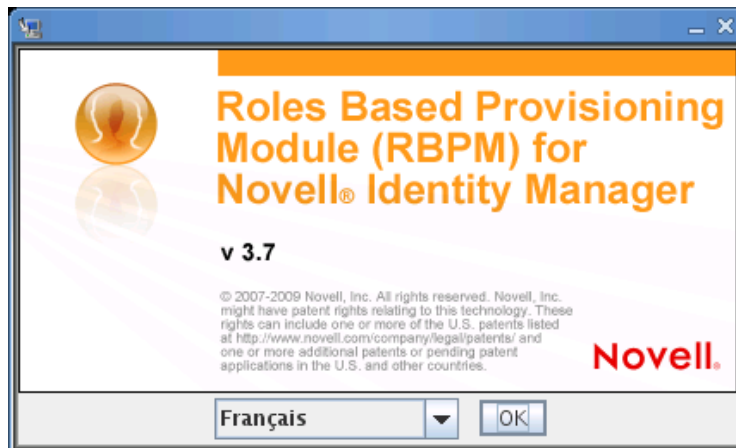
AIX

`rbpm_driver_install_aix.bin`

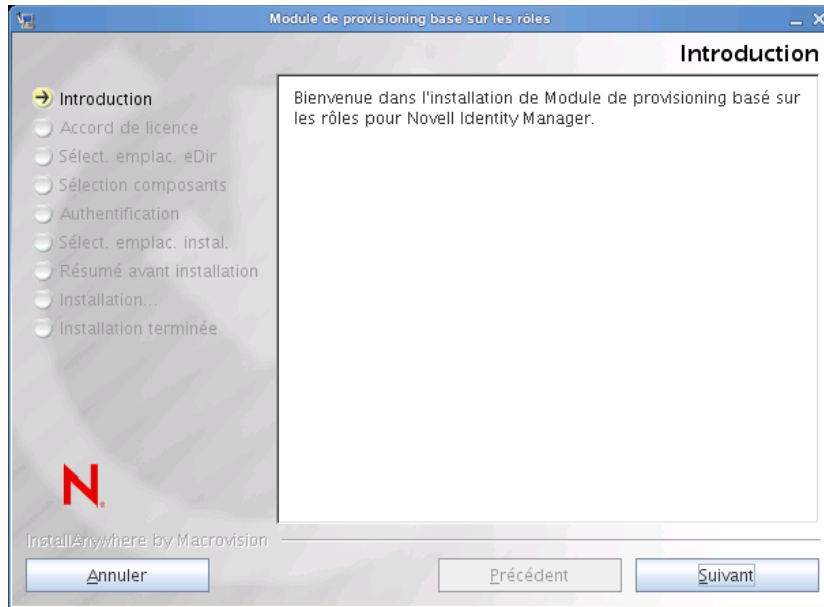
Windows

`rbpm_driver_install.exe`

Lors du lancement du programme d'installation, vous êtes invité à choisir une langue :

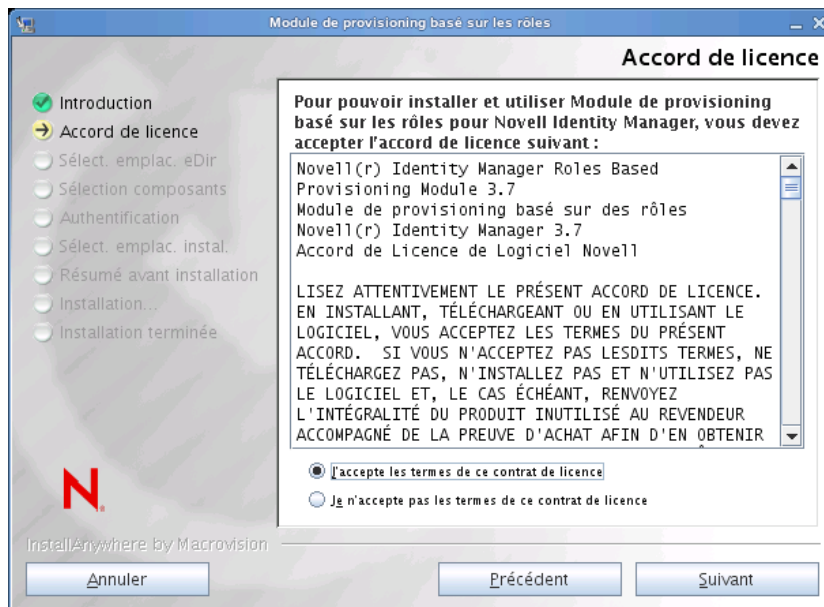


- 2 Sélectionnez la langue d'installation, puis cliquez sur OK.
Le programme d'installation affiche l'écran Introduction.



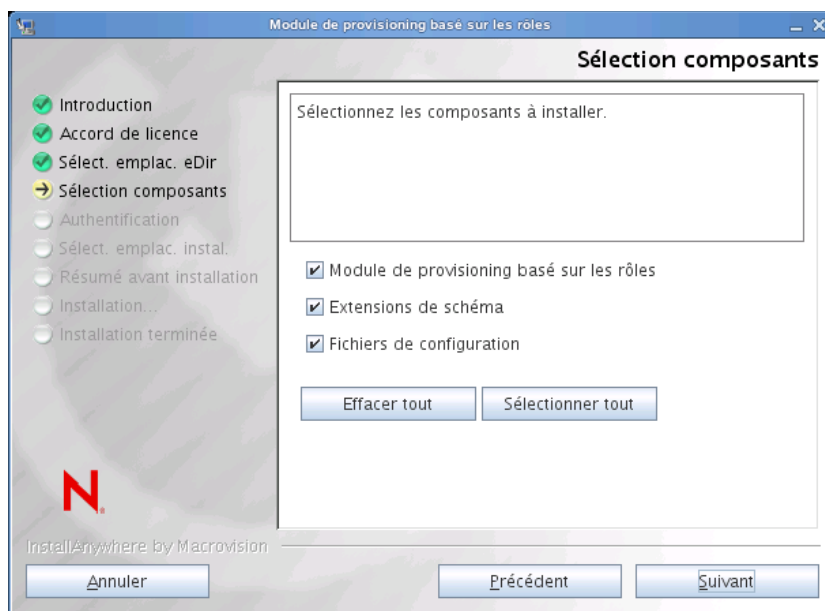
3 Cliquez sur *Suivant*.

L'écran Accord de licence s'affiche.



4 Acceptez l'accord de licence, puis cliquez sur *Suivant*.

L'écran Sélection composants s'affiche et répertorie les composants du méta-annuaire requis pour l'exécution de l'application utilisateur RBPM :

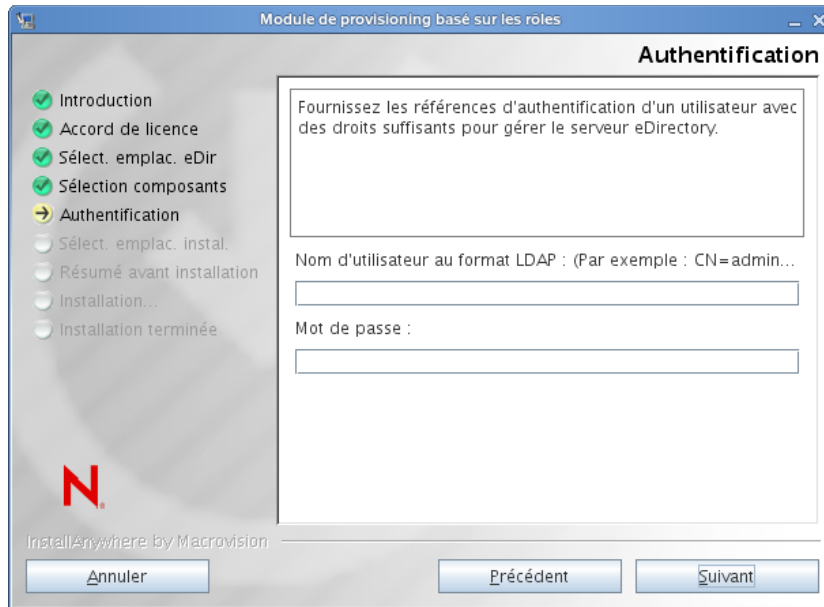


Ces composants sont décrits ci-après :

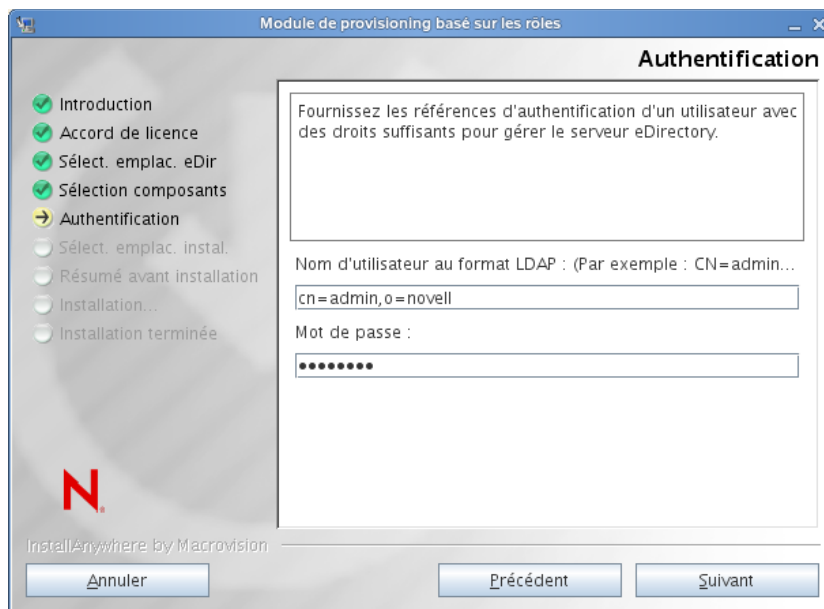
Composant	Description
Module de provisioning basé sur les rôles	Installe le pilote d'application utilisateur et le pilote de rôles et de ressources.
Extensions de schéma	Installe les extensions de schéma eDirectory.
Fichiers de configuration	Installe les fichiers de configuration des pilotes.

- 5 Sélectionnez les composants à installer, puis cliquez sur *Suivant*. En règle générale, tous les composants doivent être installés.

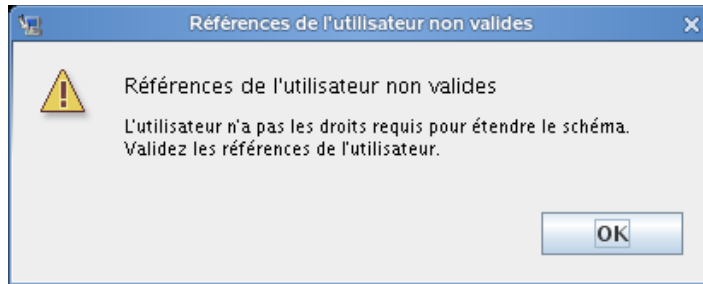
Le programme d'installation affiche l'écran Authentification :



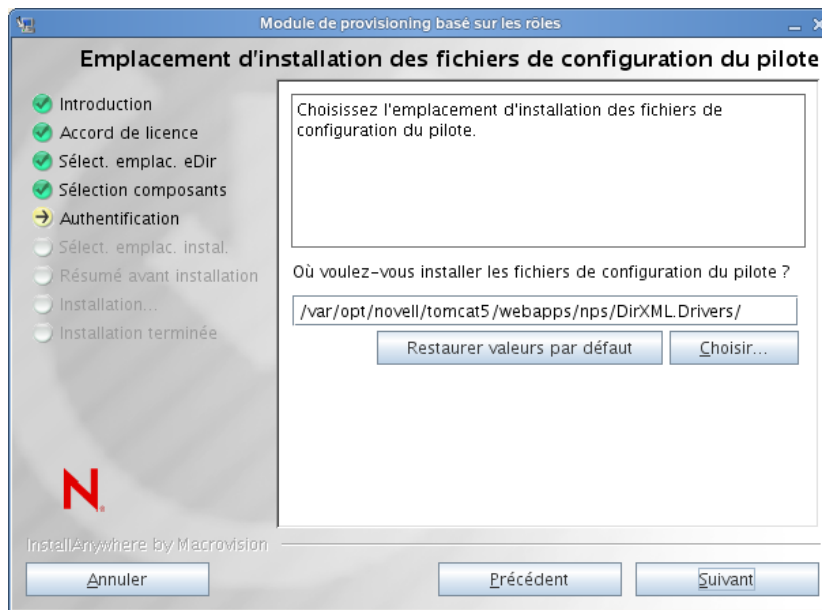
6 Indiquez le nom d'utilisateur au format LDAP et saisissez le mot de passe :



Si les références de l'utilisateur ne sont pas valides ou si l'utilisateur ne possède pas les droits suffisants, le programme d'installation affiche un message d'erreur :

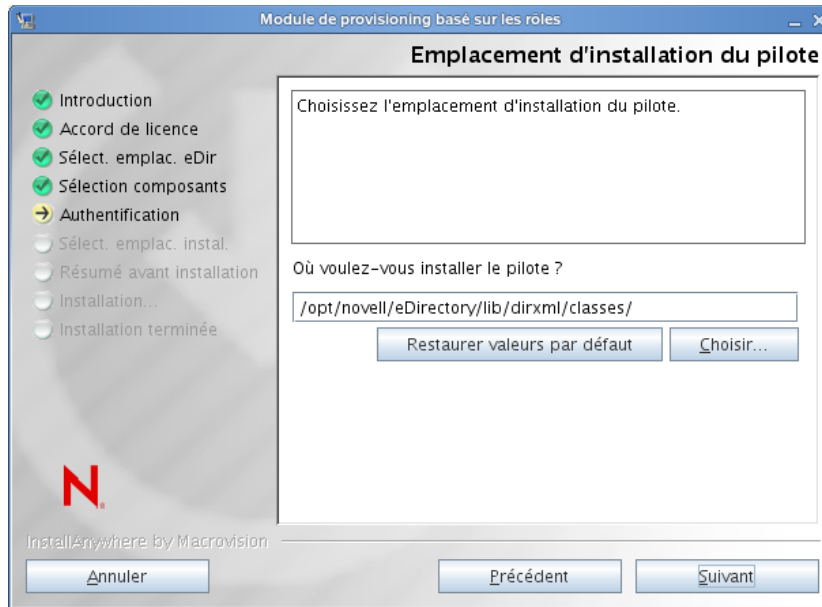


Si les références de l'utilisateur sont valides et que l'utilisateur possède les droits appropriés, le programme d'installation affiche l'écran Emplacement d'installation des fichiers de configuration du pilote :



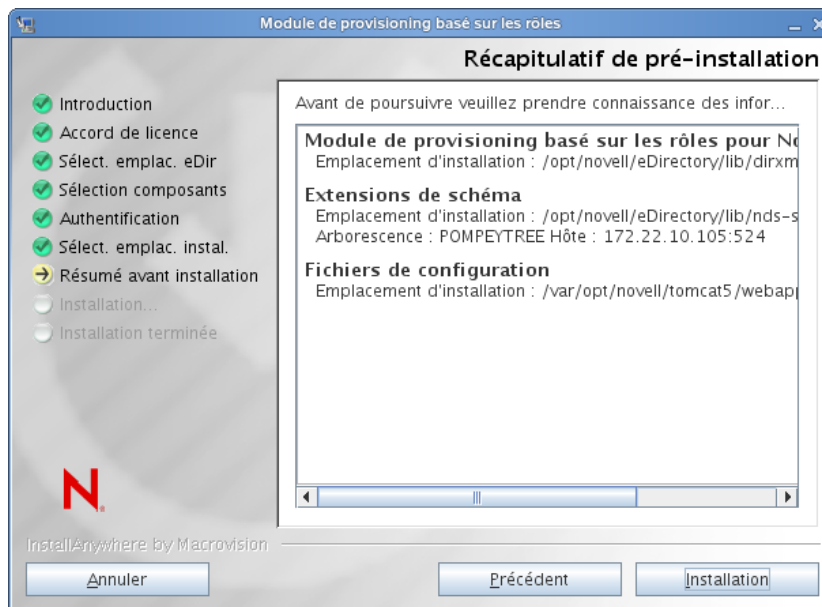
7 Définissez l'emplacement cible sur le disque pour le stockage des fichiers de configuration du pilote, puis cliquez sur *Suivant*.

Le programme d'installation affiche l'écran Emplacement d'installation du pilote :



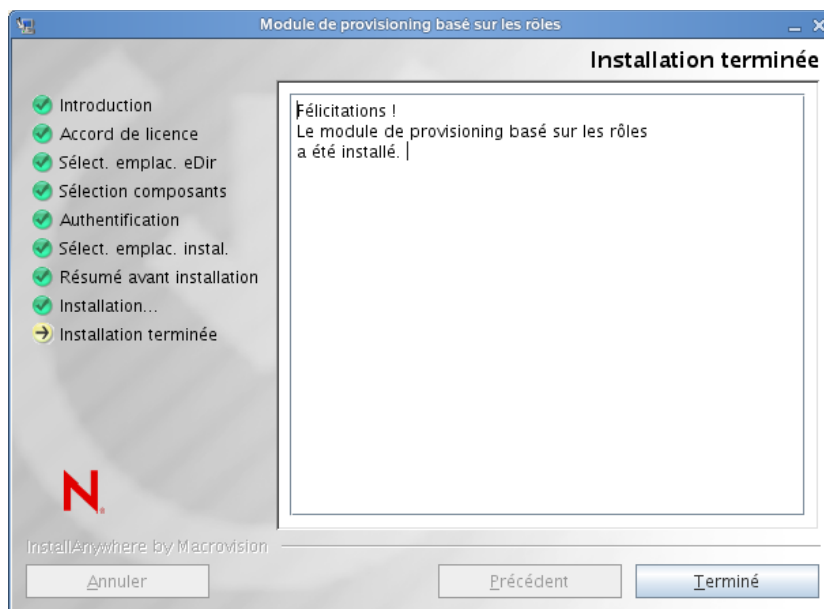
8 Indiquez l'emplacement cible du pilote, puis cliquez sur *Suivant*.

Le programme d'installation affiche l'écran Récapitulatif de pré-installation :



9 Si le résumé de l'installation vous semble correct, cliquez sur *Installer* pour lancer l'installation.

Une fois l'installation terminée, le programme d'installation affiche l'écran correspondant :



Création des pilotes

4

Cette section décrit comment créer les pilotes en vue d'utiliser le module de provisioning basé sur les rôles (RBPM). Les rubriques sont les suivantes :

- ♦ [Section 4.1, « Création du pilote d'application utilisateur dans iManager », page 45](#)
- ♦ [Section 4.2, « Création du pilote du service de rôles et de ressources dans iManager », page 47](#)

Important : vous devez créer le pilote d'application utilisateur avant celui du service de rôles et de ressources. En effet, ce dernier référence le conteneur du coffre-fort de rôle (RoleConfig.AppConfig) dans le pilote d'application utilisateur.

La prise en charge de la configuration du pilote vous permet d'effectuer les tâches suivantes :

- ♦ Associer un pilote d'application utilisateur unique à un pilote de service de rôles et de ressources.
- ♦ Associer une application utilisateur unique à un pilote d'application utilisateur.

4.1 Création du pilote d'application utilisateur dans iManager

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.

Vous devez créer un pilote d'application utilisateur distinct pour chaque application utilisateur RBPM, sauf pour celles membres d'une grappe. Les applications utilisateur faisant partie d'une même grappe doivent partager le même pilote d'application utilisateur. Pour plus d'informations sur l'exécution de l'application utilisateur dans une grappe, reportez-vous au manuel *User Application: Administration Guide* (<http://www.novell.com/documentation/idmrpbpm37/index.html>) (Guide d'administration de l'application utilisateur).

Important : la configuration d'un ensemble d'applications utilisateur RBPM non mises en grappe pour partager un seul pilote crée une ambiguïté pour 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 dans un navigateur Web.
- 2 Accédez au menu *Rôles et tâches > Utilitaires Identity Manager* et sélectionnez *Importer la configuration*.
- 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.

3b Cliquez sur *Suivant*.

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

5 Sélectionnez le fichier de configuration du pilote de l'application utilisateur dans la liste déroulante. Le nom du fichier est :

UserApplication_3_7_0-IDM3_6_0-V1.xml

Si ce fichier ne figure pas dans la liste, le pilote du module de provisioning basé sur les rôles n'est peut-être pas être installé correctement.

6 Cliquez sur *Suivant*.

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

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 <i>IDM</i> .
<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>	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 opérations de pilote (par exemple, les rôles administratifs), puis cliquez sur *OK*.
- 12 Cliquez sur *OK* pour fermer la fenêtre Équivalents de sécurité, puis cliquez sur *Suivant* pour afficher la page de résumé.
- 13 Si les informations sont correctes, cliquez sur *Terminer*.

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

4.2 Création du pilote du service de rôles et de ressources dans iManager

Pour créer et configurer le pilote du service de rôles et de ressources dans iManager, procédez comme suit :

- 1 Ouvrez iManager dans un navigateur Web.
- 2 Accédez au menu *Rôles et tâches > Utilitaires Identity Manager* et sélectionnez *Importer la configuration*.

Installez le pilote d'application utilisateur avant le pilote du service de rôles et de ressources. Utilisez la version 3.7.0 du pilote d'application utilisateur (`UserApplication_3_7_0-IDM3_6_0-V1.xml`) avec le pilote du service de rôles et de ressources. Si vous utilisez une version différente du pilote d'application utilisateur, le catalogue de rôles et de ressources ne sera peut-être pas disponible.

- 3 Dans l'Assistant, conservez la valeur par défaut *Dans un ensemble de pilotes existant*. Recherchez l'ensemble de pilotes que vous avez créé à la [Section 4.1, « Création du pilote d'application utilisateur dans iManager »](#), page 45. Cliquez sur *Suivant*.

Remarque : le pilote d'application utilisateur et le pilote des rôles et des ressources doivent se trouver dans le même ensemble de pilotes.

- 4 Dans la liste déroulante, sélectionnez `RoleResourceService_3_7_0-IDM3_6_0-V1.xml`. Il s'agit du fichier de configuration du pilote du service de rôles et de ressources prenant en charge le module de provisioning basé sur les rôles.

Si ce fichier ne figure pas dans la liste, le programme d'installation du module de provisioning basé sur les rôles n'est peut-être pas installé correctement.

Cliquez sur *Suivant*.

- 5 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 rôles et de ressources). 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 conteneur de base du groupe d'utilisateurs</i>	Le pilote agit uniquement sur les utilisateurs, les conteneurs et les groupes de ce conteneur de base. S'il existe des assignations de rôles ou de ressources de groupe, le pilote du service de rôles et de ressources n'accorde ou ne révoque les rôles et les ressources que pour les membres appartenant au domaine du conteneur.
<i>DN du pilote d'application utilisateur</i>	Nom distinctif de l'objet Pilote d'application utilisateur qui héberge le système de rôles ou de ressources. 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.

- 6** Une fois les informations renseignées, cliquez sur *Suivant*.
- 7** 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.

- 8** (Facultatif, mais recommandé) Cliquez sur *Exclure les rôles administratifs*.
- 9** Cliquez sur *Ajouter*, sélectionnez les utilisateurs que vous souhaitez exclure des opérations de pilote (par exemple, les rôles administratifs), puis cliquez sur *OK*.
- 10** Cliquez sur *OK* pour fermer la fenêtre Équivalents de sécurité, puis cliquez sur *Suivant* pour afficher la page de résumé.
- 11** Si les informations sont correctes, cliquez sur *Terminer*.

Installation de l'application utilisateur sur JBoss

5

Cette section décrit l'installation de l'application utilisateur pour le module de provisioning basé sur les rôles sur un serveur d'applications JBoss à l'aide de l'interface graphique du programme d'installation. Elle comprend les rubriques suivantes :

- ♦ [Section 5.1, « Installation et configuration du fichier WAR de l'application utilisateur », page 51](#)
- ♦ [Section 5.2, « Tester l'installation », page 65](#)

Si vous préférez utiliser la ligne de commande, reportez-vous au [Chapitre 8, « Installation depuis la console ou à l'aide d'une commande unique », page 103](#).

Exécutez le programme d'installation en tant qu'utilisateur non-root.

Migration de données Pour en savoir plus sur la migration, reportez-vous au manuel *User Application: Migration Guide* (<http://www.novell.com/documentation/idmr bpm37/index.html>) (Guide de migration de l'application utilisateur).

5.1 Installation et configuration du fichier WAR de l'application utilisateur

Remarque : pour JBoss 5.0.1, le programme d'installation requiert la version 1.6 du kit de développement de la plate-forme Java 2, Standard Edition (JRE ou JDK) de Sun. Si vous utilisez une autre version, la procédure d'installation ne configure pas correctement le fichier WAR de l'application utilisateur. L'installation semblera réussir, mais vous rencontrerez des erreurs lorsque vous tenterez de démarrer l'application utilisateur.

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

Veillez à utiliser la version appropriée du JDK de Sun pour lancer le programme d'installation de l'application utilisateur, comme suit :

Linux/Solaris

```
$ /opt/jdk1.6.0_14/bin/java -jar IdmUserApp.jar
```

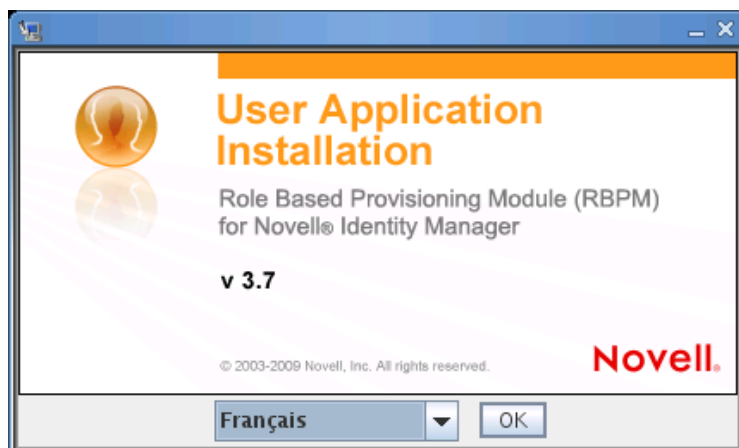
Windows

```
C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.6.0_14\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/jkd1.6.0_14.

Remarque : utilisateurs SLES : n'utilisez pas le JDK IBM* fourni avec SLES. Cette version est incompatible avec certaines parties de l'installation et peut provoquer des erreurs de corruption de la clé principale.


Lors du lancement du programme d'installation, vous êtes invité à choisir une langue :



- 2 Utilisez les informations suivantes pour choisir la langue, confirmer l'accord de licence et sélectionner la plate-forme du serveur d'applications :

Écran d'installation	Description
Installation de l'application utilisateur	Sélectionnez la langue du programme d'installation. La valeur par défaut est Français.
Accord de licence	Lisez l'accord de licence, puis sélectionnez <i>J'accepte les termes de l'accord de licence</i> .
Plate-forme du serveur d'applications	Sélectionnez <i>JBoss</i> . Lorsque vous installez l'application sur JBoss, vous devez lancer le programme d'installation à partir de l'environnement Java de Sun. Si vous sélectionnez JBoss comme serveur d'applications alors que vous n'utilisez pas l'environnement Java de Sun pour lancer l'installation, vous recevez un message d'erreur et l'installation s'interrompt :

*** Probleme Java

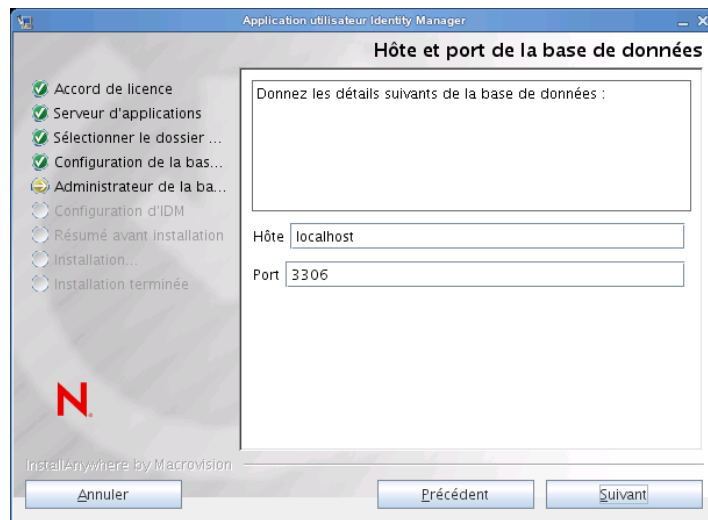
 Version non valide

Java Vendor is IBM Corporation
La version de Java exécutée ne convient pas au serveur d'applications choisi. Vous devez utiliser la machine virtuelle Java Sun Microsystems afin de pouvoir continuer. Version de Java non valide

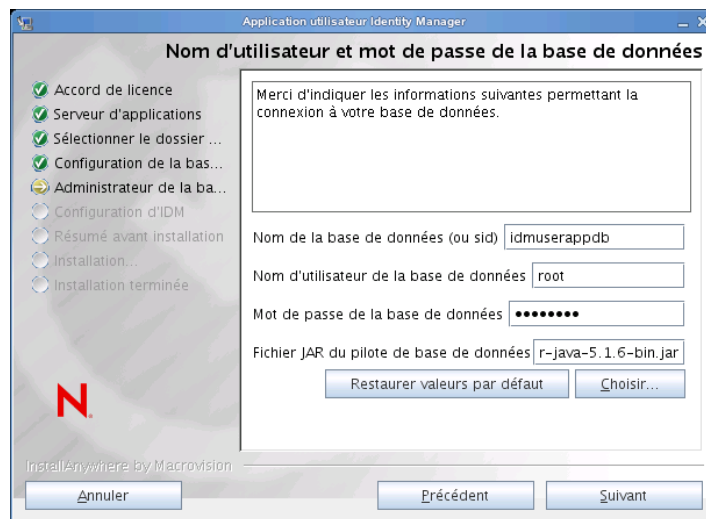
Pour le serveur d'applications JBoss, seule la version 1.6 de Java de Sun est prise en charge.
Veuillez quitter l'installation et utiliser cette version pour lancer l'installation.

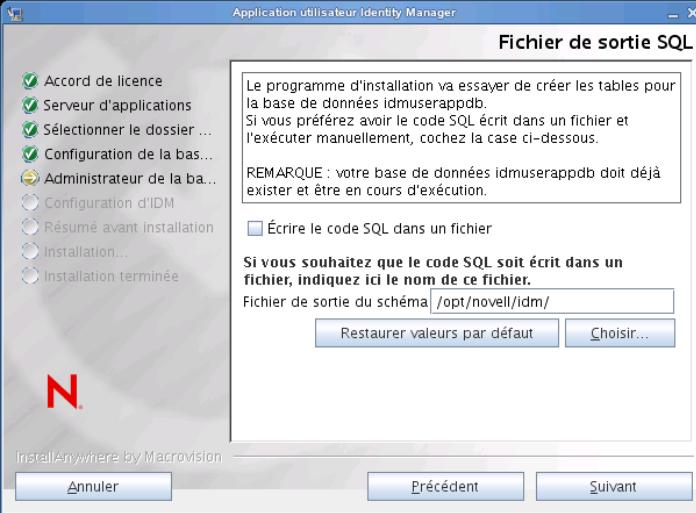
- 3 Aidez-vous des informations suivantes pour sélectionner le type d'installation, choisir un dossier d'installation et configurer la base de données :

Écran d'installation	Description
Type d'installation	<i>Provisioning basé sur les rôles</i> : sélectionnez cette option pour installer le module de provisioning basé sur les rôles. Il s'agit du seul type d'installation pris en charge avec cette version.
Sélectionnez le dossier d'installation	Indiquez l'emplacement auquel le programme d'installation doit mettre les fichiers.
Plate-forme de la base de données	Sélectionnez la plate-forme de la base de données. Vous devez avoir installé la base de données et le pilote JDBC. Pour JBoss, les options sont les suivantes : <ul style="list-style-type: none"> ◆ MySQL ◆ Oracle (prend en charge Oracle 10g et 11g uniquement. Oracle 9i n'est plus pris en charge.) ◆ PostgreSQL (disponible uniquement pour l'installation sur JBoss) ◆ Microsoft SQL Server ◆ IBM DB2 (prend en charge la version 9.5 uniquement. La version 9.1 n'est plus prise en charge.)
Hôte et port de la base de données	<p><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.</p> <p><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.</p>



Écran d'installation	Description
Nom d'utilisateur et mot de passe de la base de données	<p><i>Nom de la base de données (ou SID)</i> : pour MySQL, MS SQL Server ou PostgreSQL, indiquez le nom de votre base de données préconfigurée. Pour Oracle, donnez l'identificateur système Oracle (SID) que vous avez créé précédemment. Pour une grappe, indiquez le même nom ou SID de base de données pour chaque membre de la grappe.</p> <p><i>Nom d'utilisateur de la base de données</i> : indiquez le nom d'utilisateur de la base de données. Pour une grappe, indiquez le même utilisateur de base de données pour chaque membre de la grappe.</p> <p><i>Mot de passe de la base de données</i> : indiquez le mot de passe de la base de données. Pour une grappe, indiquez le même mot de passe de base de données pour chaque membre de la grappe.</p> <p><i>Fichier JAR du pilote de base de données</i> : indiquez le fichier JAR du client léger pour le serveur de base de données. Ce paramètre est obligatoire.</p>

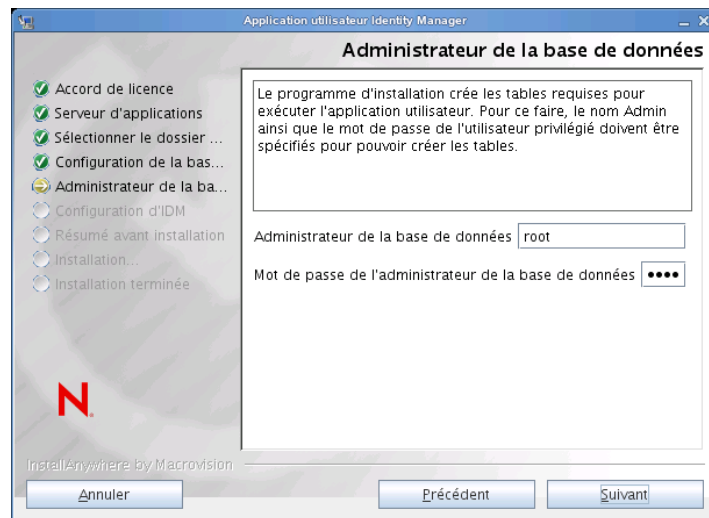


Écran d'installation	Description
Fichier de sortie SQL	<p>Dans cette version, les tables de base de données peuvent être créées au cours de l'installation de l'application utilisateur, plutôt qu'au lancement du serveur d'applications (comme c'était le cas dans les versions précédentes).</p> <p>L'écran Fichier de sortie SQL vous permet de créer un fichier de schéma que l'administrateur de base de données peut utiliser pour créer des tables (plutôt que de laisser le programme d'installation les créer).</p> <p>Si vous souhaitez générer un fichier de schéma, cochez la case <i>Écrire le code SQL dans un fichier</i> et indiquez un nom pour le fichier dans le champ <i>Fichier de sortie du schéma</i>.</p> 

Écran d'installation**Description**

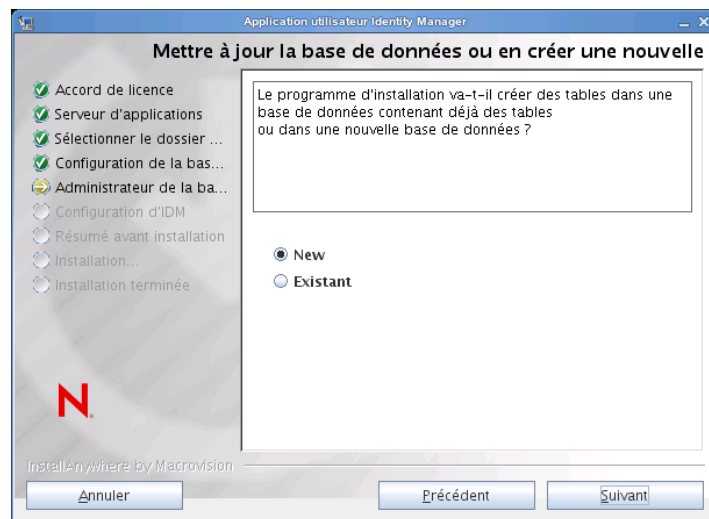
Administrateur de la base de données

Cette page est préremplie avec les mêmes nom d'utilisateur et mot de passe que sur la page Nom d'utilisateur et mot de passe de la base de données. Si l'utilisateur de base de données spécifié précédemment ne possède pas les autorisations suffisantes pour créer des tables sur le serveur de base de données, alors vous devez indiquer l'ID d'un utilisateur possédant les droits requis.

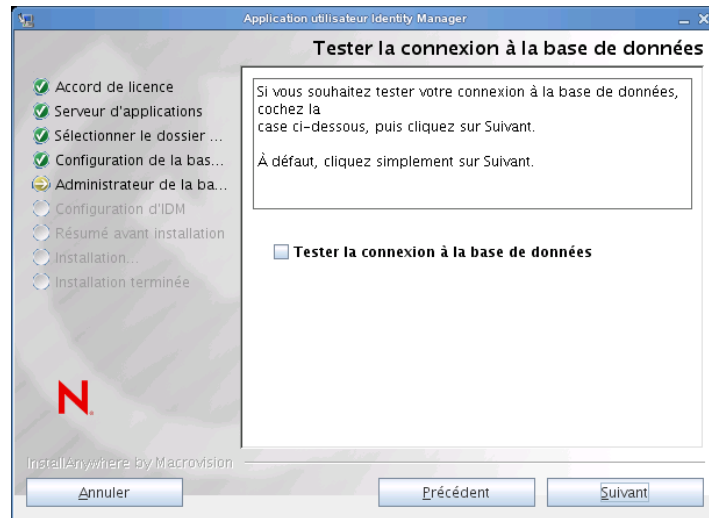


Mettre à jour la base de données ou en créer une nouvelle

Si la base de données à utiliser est nouvelle ou vide, sélectionnez *Nouveau*. Si la base de données provient d'une installation précédente, sélectionnez *Existant*.



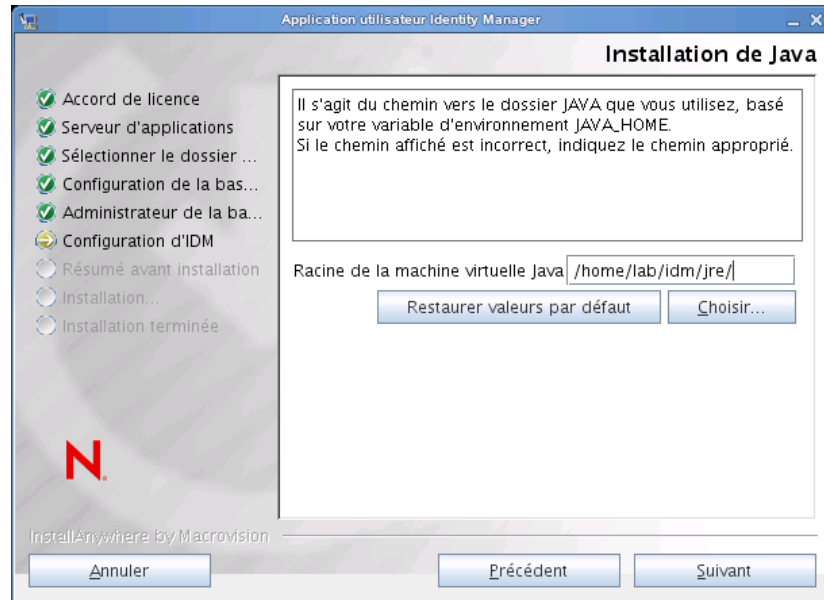
Écran d'installation	Description
Tester la connexion à la base de données	Pour vérifier que les informations fournies dans les écrans précédents sont correctes, vous pouvez tester la connexion à la base de données en cochant la case <i>Tester la connexion à la base de données</i> :



- 4 Aidez-vous des informations suivantes pour configurer Java, l'installation sur JBoss et IDM ainsi que les paramètres d'audit et la sécurité.

Écran d'installation Description

Installation de Java Indiquez le dossier d'installation racine de Java. L'écran Installation de Java fournit le chemin d'accès à Java à partir de votre variable d'environnement JAVA_HOME et vous permet de le rectifier :



À ce stade, le programme d'installation vérifie également que la plate-forme Java sélectionnée est appropriée pour le serveur d'applications spécifié. En outre, il vérifie qu'il peut éditer le fichier cacerts du JRE indiqué.

Vous êtes ensuite invité à indiquer des informations sur l'emplacement d'installation du serveur d'applications JBoss :

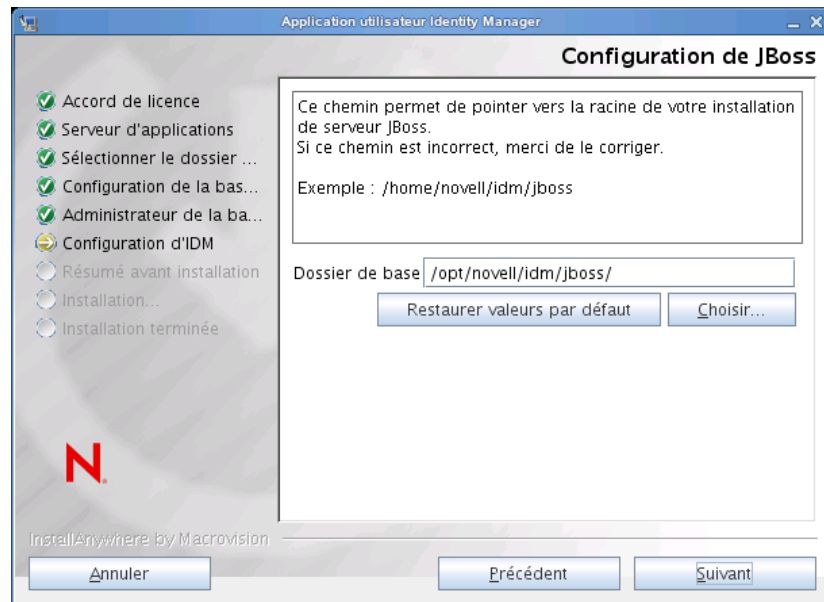
Écran d'installation Description

Configuration de JBoss

Indique à l'application utilisateur où le serveur d'applications JBoss se trouve.

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 « [Installation du serveur d'applications JBoss et de la base de données MySQL](#) » page 20.

Dossier de base : indiquez l'emplacement du serveur d'applications.



Écran d'installation Description

Configuration d'IDM

Sélectionnez le type de configuration du serveur d'applications :

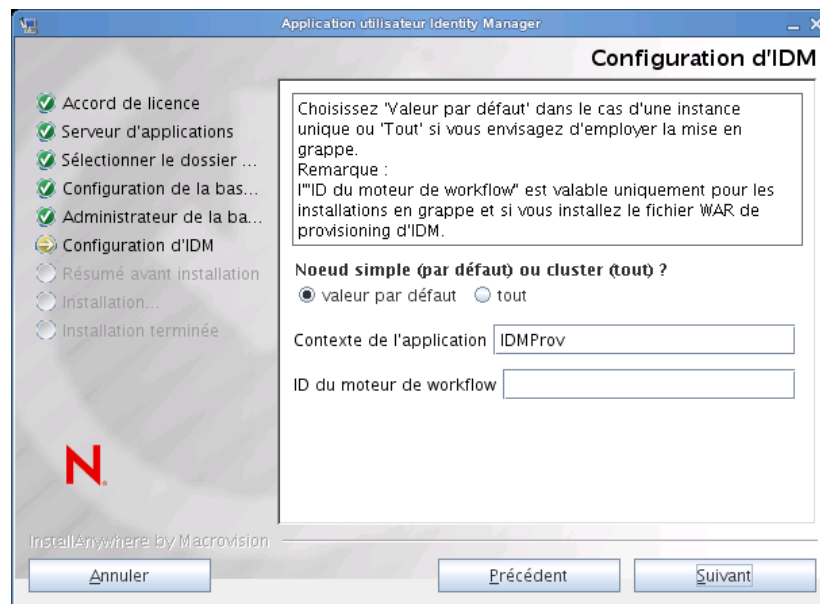
- ◆ Sélectionnez *par défaut* si cette installation est sur un noeud simple qui ne fait pas partie d'une grappe.

Si vous sélectionnez *par défaut* et décidez que vous aurez besoin d'une grappe ultérieurement, vous devrez réinstaller l'application utilisateur.

- ◆ Sélectionnez *tout* si cette installation fait partie d'une grappe.

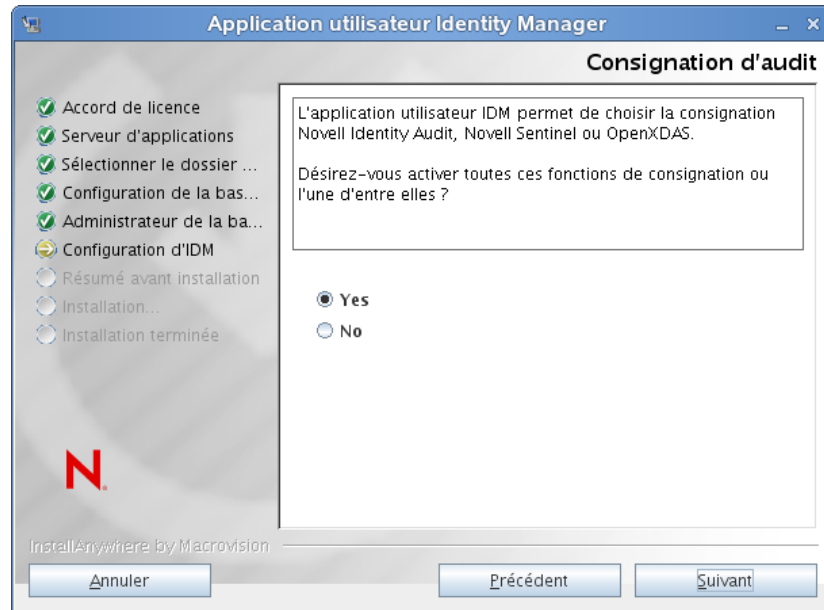
Contexte de l'application : noms de la configuration du serveur d'applications, du fichier WAR de l'application et du contexte de l'URL. Le script d'installation crée une configuration serveur et par défaut nomme la configuration en fonction du *Nom de l'application*. Notez le nom de l'application et ajoutez-le dans l'URL lorsque vous démarrez l'application utilisateur dans un navigateur.

ID du moteur de workflow : chaque serveur d'une grappe doit avoir un ID de moteur de workflow unique. L'ID du moteur de workflow n'est valide que pour les installations de grappe et si vous installez le fichier WAR de provisioning d'IDM. Il est limité à 32 caractères. Les ID de moteur de workflow sont décrits dans le manuel *User Application: Administration Guide* (Guide d'administration de l'application utilisateur) à la section relative à la configuration de workflows pour la mise en grappe.



Écran d'installation Description

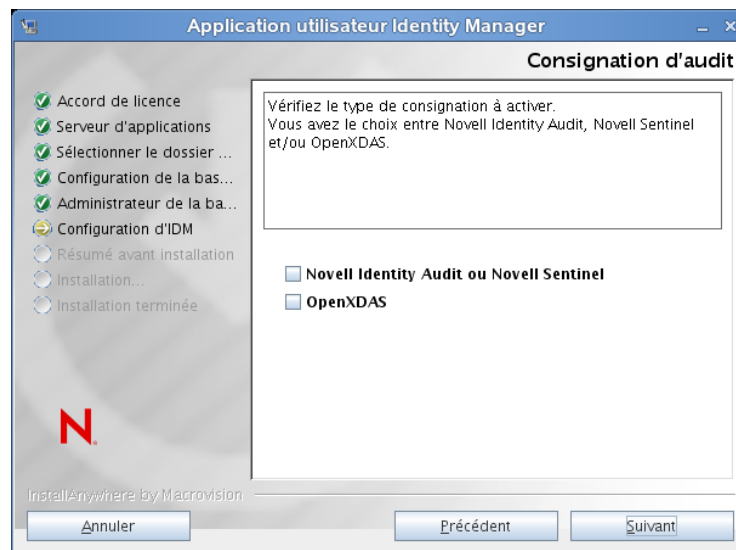
Consignation Audit Pour activer la consignation, cliquez sur *Oui*. Pour désactiver la consignation, cliquez sur *Non*.



Le tableau de bord suivant vous invite à indiquer le type de consignation. Choisissez parmi les options suivantes :

- ♦ *Novell Identity Audit ou Novell Sentinel* : permet d'activer la consignation via un client Novell pour l'application utilisateur.
- ♦ *OpenXDAS* : les événements sont consignés sur votre serveur de consignation OpenXDAS.

Pour plus d'informations sur la configuration de la consignation , reportez-vous au manuel *User Application: Administration Guide* (Guide d'administration de l'application utilisateur).



Écran d'installation	Description
Novell Audit	<p><i>Serveur</i> : si vous activez la consignation, indiquez le nom d'hôte ou l'adresse IP du serveur. Si vous désactivez la consignation, cette valeur est ignorée.</p> <p><i>Dossier de cache des journaux</i> : indiquez le répertoire du cache de consignation.</p>
Sécurité : clé principale	<p><i>Oui</i> : vous permet d'importer une clé principale existante. Si vous choisissez d'importer une clé maîtresse codée existante, coupez et collez la clé dans la fenêtre de procédure d'installation.</p> <p><i>Non</i> : crée une clé principale. Une fois l'installation terminée, vous devez enregistrer manuellement la clé maîtresse comme décrit dans la Section 9.1, « Enregistrement de la clé maîtresse », page 115.</p> <p>La procédure d'installation inscrit la clé maîtresse codée dans le fichier <code>master-key.txt</code> dans le répertoire d'installation.</p> <p>Voici des raisons d'importer une clé principale existante :</p> <ul style="list-style-type: none"> ♦ 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.

- 5** Cliquez sur *Suivant* pour afficher le volet de configuration du module de provisioning basé sur les rôles. (Si le programme ne vous invite pas à saisir ces informations, vous n'avez peut-être pas suivi toutes les étapes définies à la [Section 2.5, « Installation du kit de développement Java », page 29.](#))

La vue par défaut du volet de configuration du module de provisioning basé sur les rôles contient les six champs suivants :

Le programme d'installation utilisera la valeur du champ DN du conteneur racine et l'appliquera aux valeurs suivantes :

- ♦ DN du conteneur de l'utilisateur
- ♦ DN du conteneur du groupe

Le programme d'installation utilisera la valeur du champ Administrateur de l'application utilisateur et l'appliquera aux valeurs suivantes :

- ♦ Administrateur du provisioning
- ♦ Administrateur de conformité
- ♦ Administrateur de rôles
- ♦ Administrateur de la sécurité
- ♦ Administrateur de ressources
- ♦ Administrateur de la configuration RBPM

Pour définir ces valeurs explicitement, vous pouvez cliquer sur le bouton *Aff. options avancées* et les modifier :

Configuration du module de provisioning basé sur les rôles (RBPM)

Paramètres du coffre-fort d'identité

Serveur du coffre-fort d'identité :
 Port LDAP :
 Port LDAP sécurisé :
 Administrateur du coffre-fort d'identité :
 Mot de passe de l'administrateur du coffre-for... :
 Utiliser un compte anonyme public :
 Invité LDAP :
 Mot de passe de l'invité LDAP :
 Connexion Admin sécurisée :
 Connexion utilisateur sécurisée :

DN du coffre-fort d'identité

DN du conteneur racine :
 Pilote de l'application utilisateur :
 Administrateur de l'application utilisateur :
 Administrateur du provisioning :
 Administrateur de conformité :
 Administrateur de rôles :
 Administrateur de la sécurité :
 Administrateur de ressources :
 Administrateur de la configuration RBPM :

Identité de l'utilisateur du coffre-fort d'identité

DN du conteneur de l'utilisateur :
 Ét. cont. Util. (sous-arb., 1 niv.) :
 Classe de l'objet utilisateur :
 Attribut de login :
 Attribut de nom :
 Attribut d'appartenance de l'utilisateur :

Groupes d'utilisateurs du coffre-fort d'identité

DN du conteneur du groupe :
 Ét. cont. Gpe (sous-arb., 1 niv.) :
 Classe de l'objet Groupe :
 Attribut d'appartenance au groupe :
 Utiliser des groupes dynamiques :
 Classe d'objets Groupe dynamique :

Certificats du coffre-fort d'identité

Chemin du fichier Keystore : ...
 Mot de passe Keystore :

6 Les informations suivantes permettent de terminer l'installation.

Écran d'installation	Description
Configuration de l'application utilisateur	<p>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 <code>configupdate.sh</code> ou <code>configupdate.bat</code> après l'installation ; les exceptions sont notées dans les descriptions des paramètres.</p> <p>Pour une grappe, indiquez les paramètres de configuration identiques de l'application utilisateur pour chaque membre de la grappe.</p> <p>Reportez-vous à l'Annexe A, « Référence de configuration de l'application utilisateur IDM », page 123 pour obtenir une description des options.</p>
Résumé pré-installation	<p>Lisez la page de résumé de la pré-installation pour vérifier vos paramètres d'installation.</p> <p>Si nécessaire, utilisez <i>Retour</i> pour retourner aux pages d'installation précédentes et modifier les paramètres d'installation.</p> <p>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. Lorsque vous êtes satisfait de vos paramètres d'installation et de configuration, retournez à la page Récapitulatif de pré-installation, puis cliquez sur <i>Installer</i>.</p>
Installation terminée	Indique que l'installation est terminée.

5.1.1 Affichage des fichiers journaux et d'installation

Si votre installation s'est terminée sans erreur, passez à la section [Tester l'installation](#). Si l'installation a émis des messages d'erreur ou d'avertissement, examinez les fichiers journaux pour déterminer les problèmes :

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

5.2 Tester l'installation

- 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)

Pour arrêter 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 X11 Window System, 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://nom_hôte:port/nom_application`

Dans cette URL, `nom_hôte: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). La valeur par défaut de `Nom_application` est `IDM`. 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 s'affiche.

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 la [Section 9.8, « Dépannage », page 120](#).

Installation de l'application utilisateur sur WebSphere

Cette section décrit l'installation de l'application utilisateur pour le module de provisioning basé sur les rôles sur un serveur d'applications WebSphere à l'aide de l'interface graphique du programme d'installation.

- ♦ [Section 6.1, « Installation et configuration du fichier WAR de l'application utilisateur », page 67](#)
- ♦ [Section 6.2, « Configuration de l'environnement WebSphere », page 81](#)
- ♦ [Section 6.3, « Déploiement du fichier WAR », page 83](#)
- ♦ [Section 6.4, « Démarrage et accès à l'application utilisateur », page 84](#)

Exécutez le programme d'installation en tant qu'utilisateur non-root.

Migration de données Pour en savoir plus sur la migration, reportez-vous au manuel *User Application: Migration Guide* (<http://www.novell.com/documentation/idmrpbpm37/index.html>) (Guide de migration de l'application utilisateur).

6.1 Installation et configuration du fichier WAR de l'application utilisateur

Remarque : pour WebSphere 6.1, le programme d'installation requiert le JDK IBM version 1.5 de la plate-forme Java 2 Standard Edition. Pour WebSphere 7.0, le programme d'installation requiert le JDK 1.6 d'IBM. Si vous utilisez une version différente, la procédure d'installation ne configurera pas correctement le fichier WAR de l'application utilisateur. L'installation semblera réussir, mais vous rencontrerez des erreurs lorsque vous tenterez de démarrer l'application utilisateur.

- 1 Accédez au répertoire contenant vos fichiers d'installation.
- 2 Lancez le programme d'installation à partir de l'environnement Java d'IBM, comme décrit ci-après :

Solaris

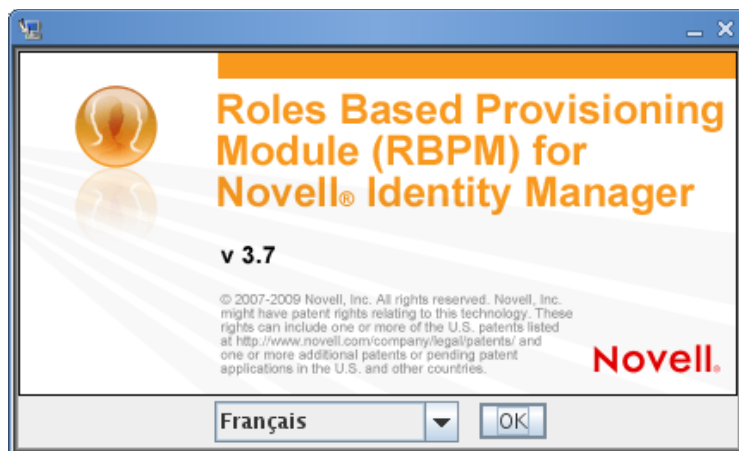
```
$ /opt/WS/IBM/WebSphere/AppServer/java/bin/java -jar IdmUserApp.jar
```

Windows

```
C:\WS\IBM\WebSphere\AppServer\java\bin\java -jar IdmUserApp.jar
```


Important : avec WebSphere, utilisez le JDK d'IBM sur lequel les fichiers de stratégie non restreints sont appliqués. Sans ces fichiers, l'erreur « Taille de clé incorrecte » sera générée. La première cause de ce problème est le manque de fichiers de stratégie non restreints. Veillez donc à utiliser le JDK d'IBM correct.

Lors du lancement du programme d'installation, vous êtes invité à choisir une langue.



- 3 Utilisez les informations suivantes pour sélectionner la langue, confirmer l'accord de licence et choisir la plate-forme du serveur d'applications :

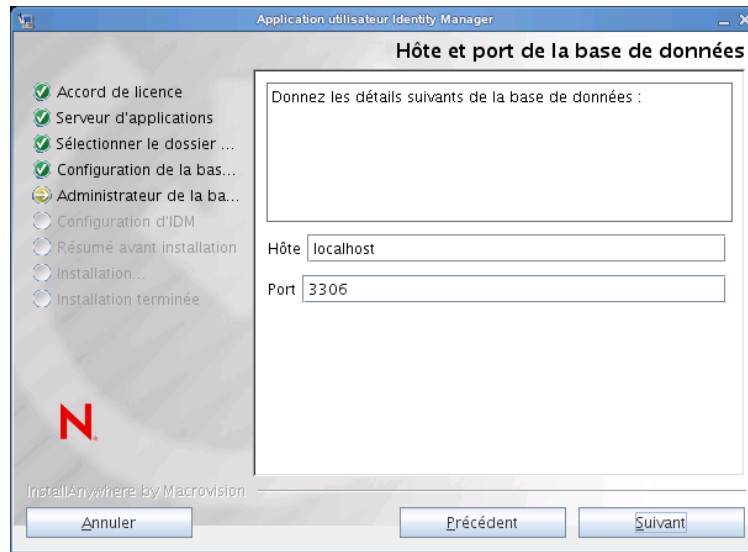
Écran d'installation	Description
Module de provisioning basé sur les rôles (RBPM) pour Novell Identity Manager	Sélectionnez la langue du programme d'installation. La valeur par défaut est Français.
Accord de licence	Lisez l'accord de licence, puis sélectionnez <i>J'accepte les termes de l'accord de licence</i> .

Écran d'installation	Description
Plate-forme du serveur d'applications	<p>Sélectionnez <i>WebSphere</i>.</p> <p>Si le fichier WAR de l'application utilisateur est dans un répertoire différent du programme d'installation, ce dernier vous invite à saisir le chemin d'accès au WAR.</p> <p>Si le fichier WAR se trouve à l'emplacement par défaut, vous pouvez cliquer sur <i>Restaurer le fichier par défaut</i>. Ou, pour spécifier l'emplacement du fichier WAR, cliquez sur <i>Choisir</i> et sélectionnez un emplacement.</p> <p>Lorsque vous installez l'application sur WebSphere, vous devez lancer le programme d'installation à partir de l'environnement Java d'IBM. Si vous sélectionnez WebSphere comme serveur d'applications alors que vous n'utilisez pas l'environnement Java d'IBM pour lancer l'installation, vous recevez un message d'erreur et l'installation s'interrompt :</p> 

- 4 Aidez-vous des informations suivantes pour sélectionner le type d'installation, choisir un dossier d'installation et configurer la base de données :

Écran d'installation	Description
Type d'installation	<i>Provisioning basé sur les rôles</i> : sélectionnez cette option pour installer le module de provisioning basé sur les rôles. Il s'agit du seul type d'installation pris en charge avec cette version.
Sélectionnez le dossier d'installation	Indiquez l'emplacement auquel le programme d'installation doit mettre les fichiers.
Plate-forme de la base de données	<p>Sélectionnez la plate-forme de la base de données. Vous devez avoir installé la base de données et le pilote JDBC. Pour WebSphere, les options sont les suivantes :</p> <ul style="list-style-type: none"> ◆ MySQL ◆ Oracle (prend en charge Oracle 10g et 11g uniquement. Oracle 9i n'est plus pris en charge.) ◆ Microsoft SQL Server ◆ IBM DB2 (prend en charge la version 9.5 uniquement. La version 9.1 n'est plus prise en charge.)

Écran d'installation	Description
Hôte et port de la base de données	<p><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.</p> <p><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.</p>



Écran d'installation	Description
----------------------	-------------

Nom d'utilisateur et mot de passe de la base de données

Nom de la base de données (ou SID) : pour MySQL, MS SQL Server ou PostgreSQL, indiquez le nom de votre base de données préconfigurée. Pour Oracle, donnez l'identificateur système Oracle (SID) que vous avez créé précédemment. Pour une grappe, indiquez le même nom ou SID de base de données pour chaque membre de la grappe.

Nom d'utilisateur de la base de données : indiquez le nom d'utilisateur de la base de données. Pour une grappe, indiquez le même utilisateur de base de données pour chaque membre de la grappe.

Mot de passe de la base de données : indiquez le mot de passe de la base de données. Pour une grappe, indiquez le même mot de passe de base de données pour chaque membre de la grappe.

Fichier JAR du pilote de base de données : indiquez le fichier JAR du client léger pour le serveur de base de données. Ce paramètre est obligatoire.

Important : le bouton Parcourir en regard du champ *Fichier JAR du pilote de base de données* ne vous permet de sélectionner qu'un seul fichier JAR. Or, pour DB2, vous devez fournir 2 fichiers JAR :

- ♦ db2jcc.jar
- ♦ db2jcc_license_cu.jar

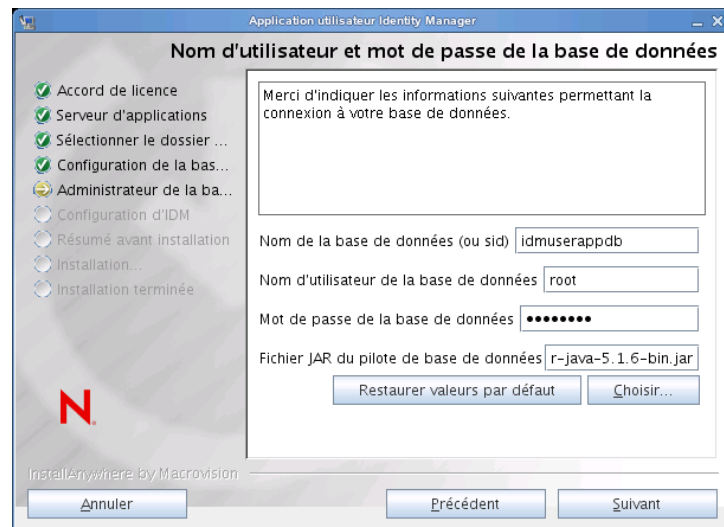
Par conséquent, vous pouvez ne sélectionner qu'un seul fichier JAR mais vous devrez saisir le deuxième fichier manuellement. Pour cela, utilisez le séparateur de fichiers approprié pour le système d'exploitation sous lequel s'exécute le programme d'installation. Vous pouvez aussi spécifier manuellement les deux fichiers.

Par exemple, sous Windows :

```
c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar
```

Par exemple, sous Solaris et Linux :

```
/home/lab/db2jars/db2jcc.jar:/home/lab/  
db2jcc_license_cu.jar
```

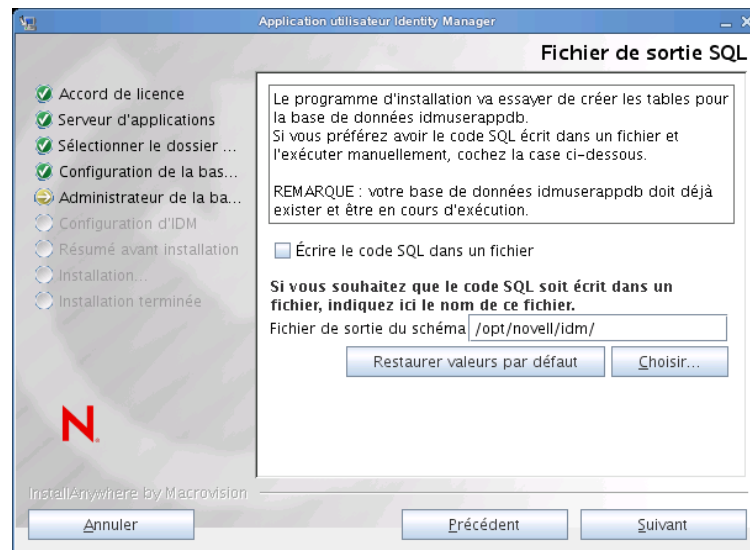


Écran d'installation	Description
----------------------	-------------

Fichier de sortie SQL	Dans cette version, les tables de base de données peuvent être créées au cours de l'installation de l'application utilisateur, plutôt qu'au lancement du serveur d'applications (comme c'était le cas dans les versions précédentes).
-----------------------	---

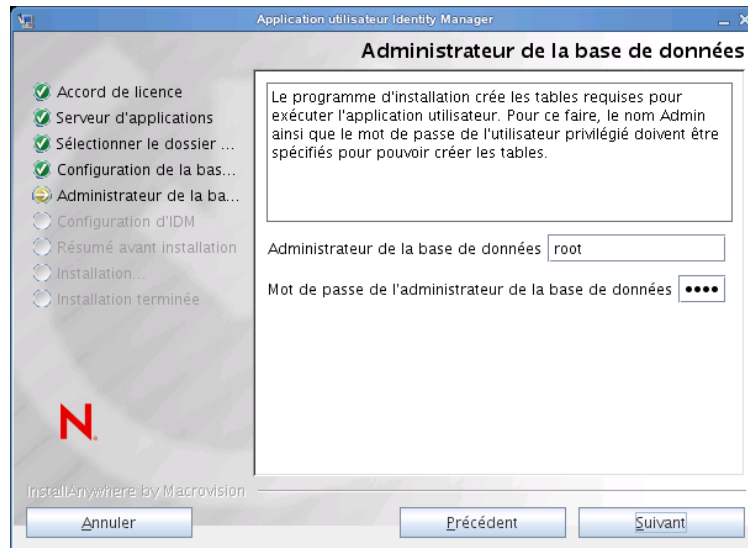
L'écran Fichier de sortie SQL vous permet de créer un fichier de schéma que l'administrateur de base de données peut utiliser pour créer des tables (plutôt que de laisser le programme d'installation les créer).

Si vous souhaitez générer un fichier de schéma, cochez la case *Écrire le code SQL dans un fichier* et indiquez un nom pour le fichier dans le champ *Fichier de sortie du schéma*.



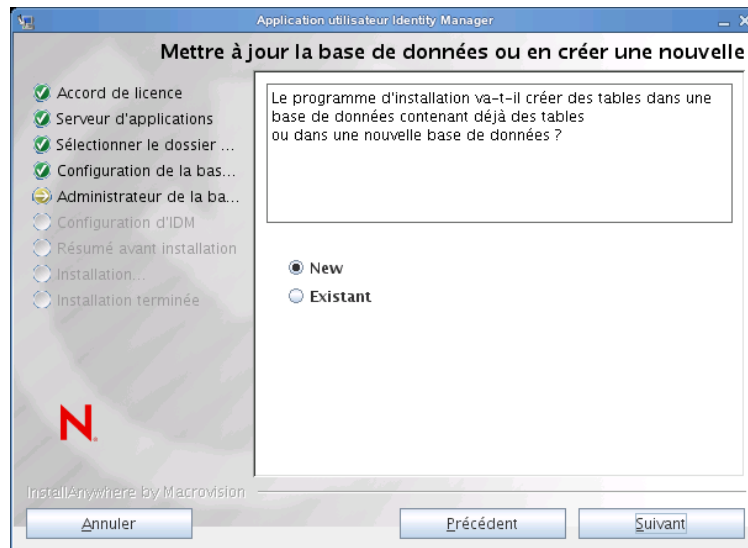
Écran d'installation	Description
----------------------	-------------

Administrateur de la base de données	Cette page est préremplie avec les mêmes nom d'utilisateur et mot de passe que sur la page Nom d'utilisateur et mot de passe de la base de données. Si l'utilisateur de base de données spécifié précédemment ne possède pas les autorisations suffisantes pour créer des tables sur le serveur de base de données, alors vous devez indiquer l'ID d'un utilisateur possédant les droits requis.
--------------------------------------	--

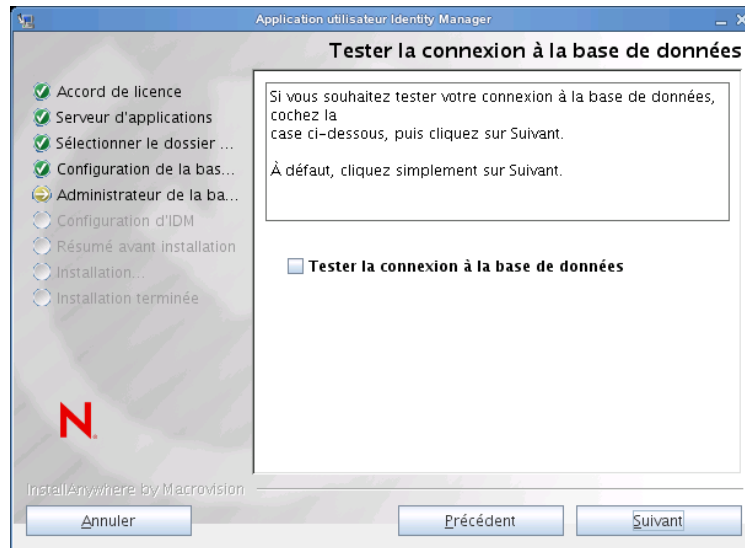


Mettre à jour la base de données ou en créer une nouvelle

Si la base de données à utiliser est nouvelle ou vide, sélectionnez *Nouveau*.
Si la base de données provient d'une installation précédente, sélectionnez *Existant*.



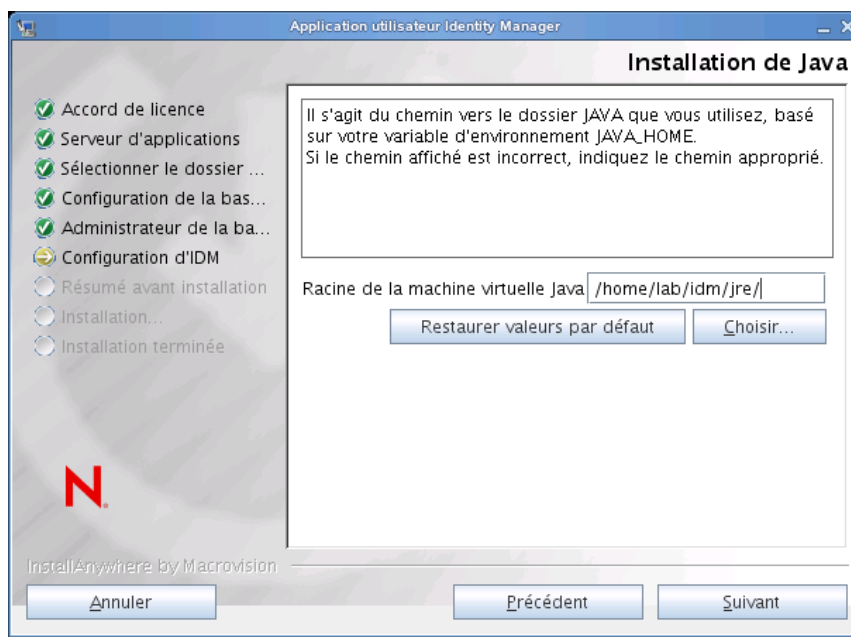
Écran d'installation	Description
Tester la connexion à la base de données	Pour vérifier que les informations fournies dans les écrans précédents sont correctes, vous pouvez tester la connexion à la base de données en cochant la case <i>Tester la connexion à la base de données</i> :



- 5 Aidez-vous des informations suivantes pour configurer Java et IDM ainsi que les paramètres d'audit et la sécurité.

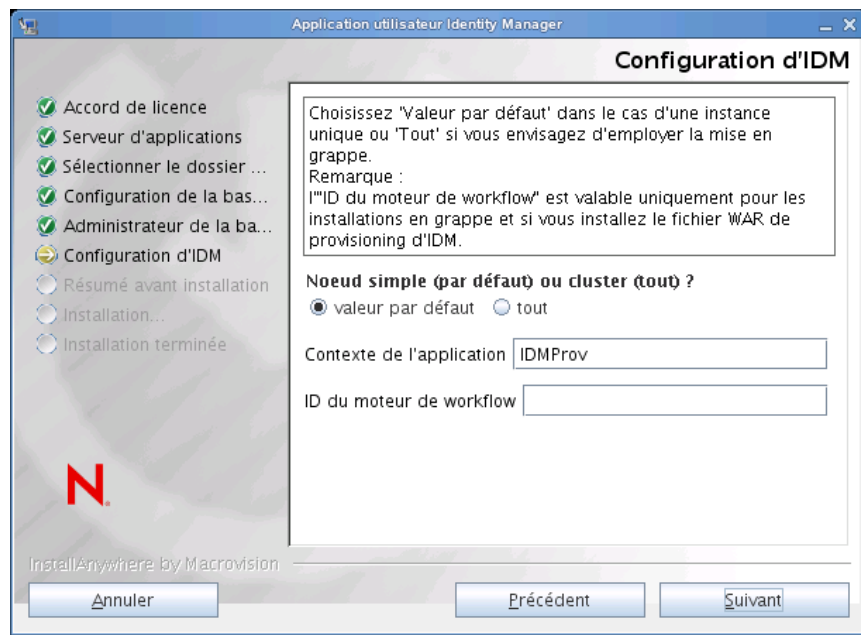
Écran d'installation**Description**

Installation de Java Indiquez le dossier d'installation racine de Java. L'écran Installation de Java fournit le chemin d'accès à Java à partir de votre variable d'environnement JAVA_HOME et vous permet de le rectifier :



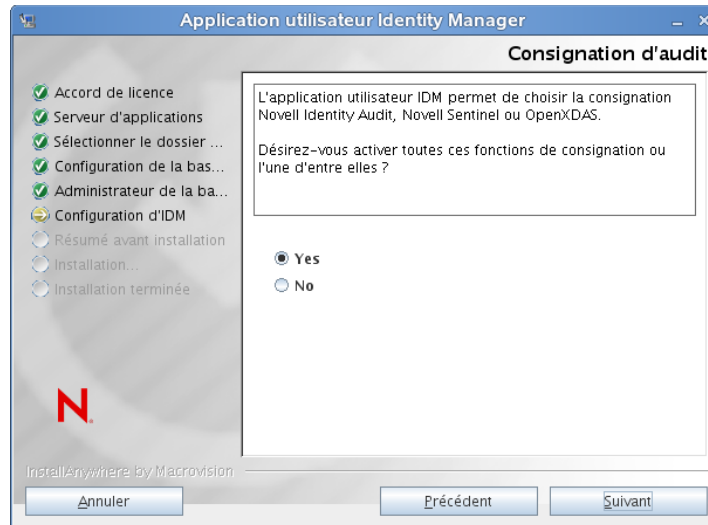
À ce stade, le programme d'installation vérifie également que la plate-forme Java sélectionnée est appropriée pour le serveur d'applications spécifié. En outre, il vérifie qu'il peut éditer le fichier cacerts du JRE indiqué.

Écran d'installation	Description
Configuration d'IDM	<p>Sélectionnez le type de configuration du serveur d'applications :</p> <ul style="list-style-type: none"> ◆ Sélectionnez <i>par défaut</i> si cette installation est sur un noeud simple qui ne fait pas partie d'une grappe. <p>Si vous sélectionnez <i>par défaut</i> et décidez que vous aurez besoin d'une grappe ultérieurement, vous devrez réinstaller l'application utilisateur.</p> <ul style="list-style-type: none"> ◆ Sélectionnez <i>tout</i> si cette installation fait partie d'une grappe. <p><i>Contexte de l'application</i> : noms de la configuration du serveur d'applications, du fichier WAR de l'application et 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>. Notez le nom de l'application et ajoutez-le dans l'URL lorsque vous démarrez l'application utilisateur dans un navigateur.</p>



Écran d'installation**Description**

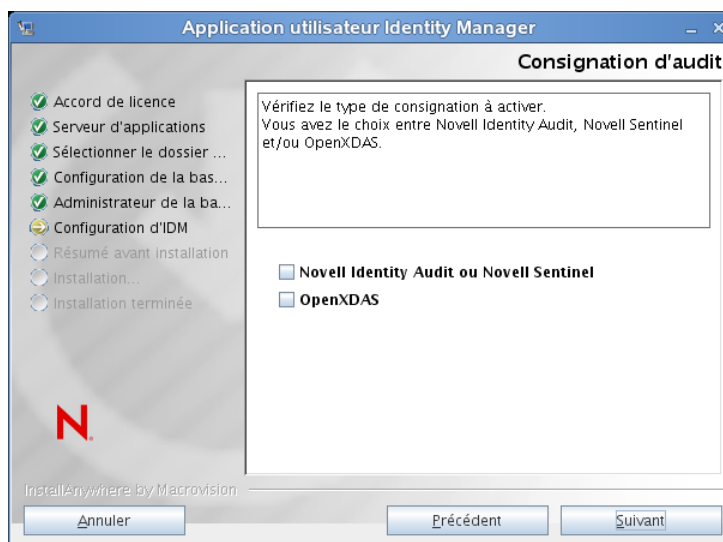
Consignation Audit Pour activer la consignation, cliquez sur *Oui*. Pour désactiver la consignation, cliquez sur *Non*.



Le tableau de bord suivant vous invite à indiquer le type de consignation. Choisissez parmi les options suivantes :

- ◆ *Novell Identity Audit ou Novell Sentinel* : permet d'activer la consignation Novell® pour l'application utilisateur.
- ◆ *OpenXDAS* : les événements sont consignés sur votre serveur de consignation OpenXDAS.

Pour plus d'informations sur la configuration de la consignation , reportez-vous au manuel *User Application: Administration Guide* (Guide d'administration de l'application utilisateur).



Écran d'installation	Description
Novell Audit	<p><i>Serveur</i> : si vous activez la consignation, indiquez le nom d'hôte ou l'adresse IP du serveur. Si vous désactivez la consignation, cette valeur est ignorée.</p> <p><i>Dossier de cache des journaux</i> : indiquez le répertoire du cache de consignation.</p>
Sécurité : clé principale	<p><i>Oui</i> : vous permet d'importer une clé principale existante. Si vous choisissez d'importer une clé maîtresse codée existante, coupez et collez la clé dans la fenêtre de procédure d'installation.</p> <p><i>Non</i> : crée une clé principale. Une fois l'installation terminée, vous devez enregistrer manuellement la clé maîtresse comme décrit dans la Section 9.1, « Enregistrement de la clé maîtresse », page 115.</p> <p>La procédure d'installation inscrit la clé maîtresse codée dans le fichier <code>master-key.txt</code> dans le répertoire d'installation.</p> <p>Voici des raisons d'importer une clé principale existante :</p> <ul style="list-style-type: none"> ♦ 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.

- 6** Cliquez sur *Suivant* pour afficher le volet de configuration du module de provisioning basé sur les rôles. (Si le programme ne vous invite pas à saisir ces informations, vous n'avez peut-être pas suivi toutes les étapes définies à la [Section 2.5, « Installation du kit de développement Java », page 29](#).)

La vue par défaut du volet de configuration du module de provisioning basé sur les rôles contient les six champs suivants :

Le programme d'installation utilisera la valeur du champ DN du conteneur racine et l'appliquera aux valeurs suivantes :

- ♦ DN du conteneur de l'utilisateur
- ♦ DN du conteneur du groupe

Le programme d'installation utilisera la valeur du champ Administrateur de l'application utilisateur et l'appliquera aux valeurs suivantes :

- ♦ Administrateur du provisioning
- ♦ Administrateur de conformité
- ♦ Administrateur de rôles
- ♦ Administrateur de la sécurité
- ♦ Administrateur de ressources
- ♦ Administrateur de la configuration RBPM

Pour définir ces valeurs explicitement, vous pouvez cliquer sur le bouton *Aff. options avancées* et les modifier :

Configuration du module de provisioning basé sur les rôles (RBPM)

Paramètres du coffre-fort d'identité

Serveur du coffre-fort d'identité : your_LDAP_host
 Port LDAP : 389
 Port LDAP sécurisé : 636
 Administrateur du coffre-fort d'identité :
 Mot de passe de l'administrateur du coffre-for...
 Utiliser un compte anonyme public :
 Invité LDAP :
 Mot de passe de l'invité LDAP :
 Connexion Admin sécurisée :
 Connexion utilisateur sécurisée :

DN du coffre-fort d'identité

DN du conteneur racine :
 Pilote de l'application utilisateur :
 Administrateur de l'application utilisateur :
 Administrateur du provisioning :
 Administrateur de conformité :
 Administrateur de rôles :
 Administrateur de la sécurité :
 Administrateur de ressources :
 Administrateur de la configuration RBPM :

Identité de l'utilisateur du coffre-fort d'identité

DN du conteneur de l'utilisateur :
 Ét. cont. Util. (sous-arb., 1 niv.) : subtree
 Classe de l'objet utilisateur : inetOrgPerson
 Attribut de login : cn
 Attribut de nom : cn
 Attribut d'appartenance de l'utilisateur : groupMembership

Groupes d'utilisateurs du coffre-fort d'identité

DN du conteneur du groupe :
 Ét. cont. Gpe (sous-arb., 1 niv.) : subtree
 Classe de l'objet Groupe : groupOfNames
 Attribut d'appartenance au groupe : member
 Utiliser des groupes dynamiques :
 Classe d'objets Groupe dynamique : dynamicGroup

Certificats du coffre-fort d'identité

Chemin du fichier Keystore : C:\Program Files\Java\jre6\lib\security\cacerts ...
 Mot de passe Keystore : *****

7 Les informations suivantes permettent de terminer l'installation.

Écran d'installation	Description
Configuration de l'application utilisateur	<p>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 <code>configupdate.sh</code> ou <code>configupdate.bat</code> après l'installation ; les exceptions sont notées dans les descriptions des paramètres.</p> <p>Pour une grappe, indiquez les paramètres de configuration identiques de l'application utilisateur pour chaque membre de la grappe.</p> <p>Reportez-vous à l'Annexe A, « Référence de configuration de l'application utilisateur IDM », page 123 pour obtenir une description des options.</p>
Résumé pré-installation	<p>Lisez la page de résumé de la pré-installation pour vérifier vos paramètres d'installation.</p> <p>Si nécessaire, utilisez <i>Retour</i> pour retourner aux pages d'installation précédentes et modifier les paramètres d'installation.</p> <p>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. Lorsque vous êtes satisfait de vos paramètres d'installation et de configuration, retournez à la page Récapitulatif de pré-installation, puis cliquez sur <i>Installer</i>.</p>
Installation terminée	Indique que l'installation est terminée.

6.1.1 Affichage des fichiers journaux d'installation

Si votre installation s'est terminée sans erreur, passez à la section [Section 6.2.1, « Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM », page 82](#).

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.

6.2 Configuration de l'environnement WebSphere

- ♦ [Section 6.2.1, « Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM », page 82](#)
- ♦ [Section 6.2.2, « Importation de la racine approuvée d'eDirectory dans la zone de stockage des clés WebSphere », page 83](#)

6.2.1 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.

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*.

6.2.2 Importation de la racine approuvée d'eDirectory dans la zone de stockage des clés WebSphere

- 1 Copiez les certificats racine approuvés eDirectory™ sur la machine qui héberge le serveur WebSphere.
La procédure d'installation de l'application utilisateur exporte les certificats vers le répertoire dans lequel vous installez l'application utilisateur.
- 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 83) ou la ligne de commande (« [Importation de certificats avec la ligne de commande](#) » page 83).
- 3 Après avoir importé les certificats, passez à la [Section 6.3, « Déploiement du fichier WAR »](#), page 83.

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.

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.

6.3 Déploiement du fichier WAR

Déployez le fichier WAR via les outils de déploiement WebSphere.

6.3.1 Configuration supplémentaire pour WebSphere 6.1

Si vous utilisez WebSphere 6.1, vous devez mettre à jour le fichier `ibm-web-ext.xmi` après avoir déployé le WAR. En effet, une fois ce déploiement effectué, vous devez ajouter dans le fichier `ibm-web-ext.xmi` une entrée similaire à la suivante :

```
<jspAttributes xmi:id="JSPAttribute_3" name="jdkSourceLevel" value="15"/>
```

Le nom doit être `jdkSourceLevel` et la valeur, 15. L'ID `JSPAttribute` doit être égal ou supérieur à `_3`. Pour plus d'informations, consultez les liens suivants :

- ♦ http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/tweb_jspengine.html (http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/tweb_jspengine.html)
- ♦ http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/rweb_jspengine.html (http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/rweb_jspengine.html)

Une fois le fichier WAR déployé, procédez comme suit :

- 1 Arrêtez le serveur d'applications WebSphere.
- 2 Modifiez le fichier `ibm-web-ext.xmi`, comme décrit ci-dessus. L'emplacement du fichier doit être spécifié dans votre documentation IBM. Par exemple, le fichier peut se situer à l'emplacement suivant :

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedApps/  
MyNode01Cell/IDMProv_war.ear/IDMProv.war/WEB-INF
```

- 3 Redémarrez le serveur d'applications WebSphere.

6.4 Démarrage et accès à l'application utilisateur

Pour démarrer l'application utilisateur :

- 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.

Accès à 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`

Installation de l'application utilisateur sur WebLogic

7

Le programme d'installation de l'interface graphique configure le fichier WAR de l'application utilisateur en fonction des informations que vous fournissez. Cette section contient des informations sur :

- ♦ [Section 7.1, « Liste de contrôle pour l'installation de WebLogic », page 85](#)
- ♦ [Section 7.2, « Installation et configuration du fichier WAR de l'application utilisateur », page 86](#)
- ♦ [Section 7.3, « Préparation de l'environnement WebLogic », page 99](#)
- ♦ [Section 7.4, « Déploiement du fichier WAR de l'application utilisateur », page 102](#)
- ♦ [Section 7.5, « Accès à l'application utilisateur », page 102](#)

Pour en savoir plus sur l'installation avec une interface utilisateur non graphique, reportez-vous au [Chapitre 8, « Installation depuis la console ou à l'aide d'une commande unique », page 103](#).

Exécutez le programme d'installation en tant qu'utilisateur non-root.

Migration de données Pour en savoir plus sur la migration, reportez-vous au manuel *User Application: Migration Guide* (<http://www.novell.com/documentation/idmrbpm37/index.html>) (Guide de migration de l'application utilisateur).

7.1 Liste de contrôle pour l'installation de WebLogic

- Installez WebLogic.
Suivez les instructions données dans la documentation de WebLogic.
- Créez un fichier WAR compatible avec WebLogic.
Utilisez le programme d'installation de l'application utilisateur Identity Manager pour réaliser cette tâche. Reportez-vous à la [Section 7.2, « Installation et configuration du fichier WAR de l'application utilisateur », page 86](#).
- Préparez l'environnement WebLogic afin de déployer le fichier WAR en copiant les fichiers de configuration aux emplacements WebLogic appropriés.
Reportez-vous à la [Section 7.3, « Préparation de l'environnement WebLogic », page 99](#).
- Déployez le fichier WAR.
Reportez-vous à la [Section 7.4, « Déploiement du fichier WAR de l'application utilisateur », page 102](#).

7.2 Installation et configuration du fichier WAR de l'application utilisateur

Remarque : pour WebLogic 10.3, le programme d'installation requiert la version 1.6 du JDK de JRockit pour la plate-forme Java 2 Standard Edition. Si vous utilisez une version différente, la procédure d'installation ne configurera pas correctement le fichier WAR de l'application utilisateur. L'installation semblera réussir, mais vous rencontrerez des erreurs lorsque vous tenterez de démarrer l'application utilisateur.

- 1 Accédez au répertoire contenant vos fichiers d'installation.
- 2 Lancez le programme d'installation pour votre plate-forme à partir de la ligne de commande, à l'aide de l'environnement Java de JRockit :

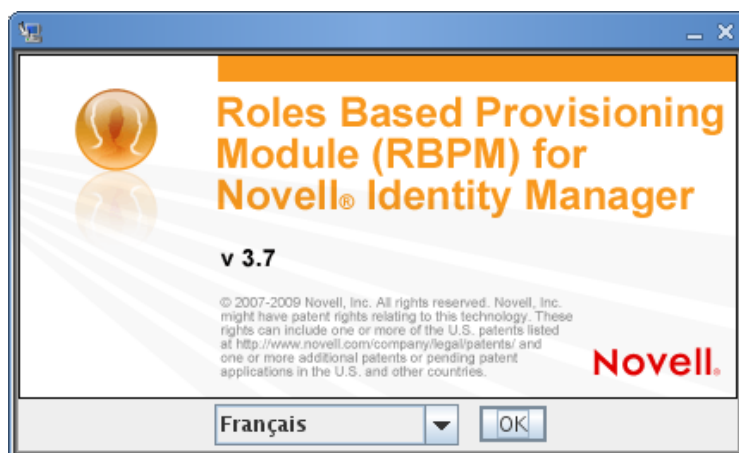
Solaris

```
$ /opt/WL/bea/jrockit_160_05/bin/java -jar IdmUserApp.jar
```

Windows

```
C:\WL\bea\jrockit_160_05\bin\java -jar IdmUserApp.jar
```

Lors du lancement du programme d'installation, vous êtes invité à choisir une langue.



- 3 Utilisez les informations suivantes pour sélectionner la langue, confirmer l'accord de licence et choisir la plate-forme du serveur d'applications :

Écran d'installation	Description
Module de provisioning basé sur les rôles (RBPM) pour Novell Identity Manager	Sélectionnez la langue du programme d'installation. La valeur par défaut est Français.
Accord de licence	Lisez l'accord de licence, puis sélectionnez <i>J'accepte les termes de l'accord de licence</i> .

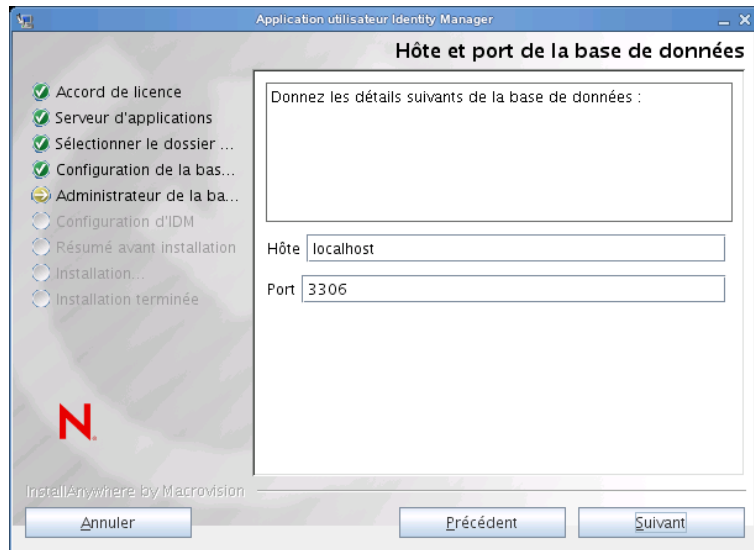
Écran d'installation	Description
Plate-forme du serveur d'applications	<p>Sélectionnez <i>WebLogic</i>.</p> <p>Si le fichier WAR de l'application utilisateur est dans un répertoire différent du programme d'installation, ce dernier vous invite à saisir le chemin d'accès au WAR.</p> <p>Si le fichier WAR se trouve à l'emplacement par défaut, vous pouvez cliquer sur <i>Restaurer le fichier par défaut</i>. Ou, pour spécifier l'emplacement du fichier WAR, cliquez sur <i>Choisir</i> et sélectionnez un emplacement.</p> <p>Lorsque vous installez l'application sur WebLogic, vous devez lancer le programme d'installation à partir de l'environnement Java de BEA (JRockit). Si vous sélectionnez WebLogic comme serveur d'applications alors que vous n'utilisez pas l'environnement JRockit pour lancer l'installation, vous recevez un message d'erreur et l'installation s'interrompt :</p>



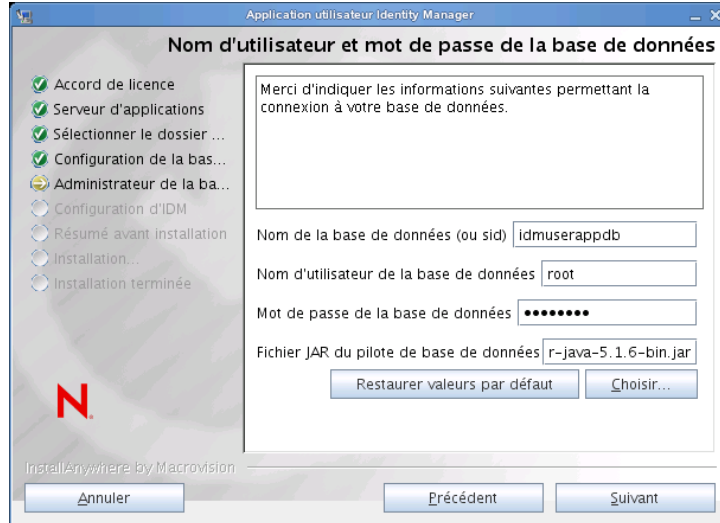
4 Aidez-vous des informations suivantes pour sélectionner le type d'installation, choisir un dossier d'installation et configurer la base de données :

Écran d'installation	Description
Type d'installation	<i>Provisioning basé sur les rôles</i> : sélectionnez cette option pour installer le module de provisioning basé sur les rôles. Il s'agit du seul type d'installation pris en charge avec cette version.
Sélectionnez le dossier d'installation	Indiquez l'emplacement auquel le programme d'installation doit mettre les fichiers.
Plate-forme de la base de données	<p>Sélectionnez la plate-forme de la base de données. Vous devez avoir installé la base de données et le pilote JDBC. Pour WebLogic, les options sont les suivantes :</p> <ul style="list-style-type: none"> ◆ Oracle (prend en charge Oracle 10g et 11g uniquement. Oracle 9i n'est plus pris en charge.) ◆ Microsoft SQL Server

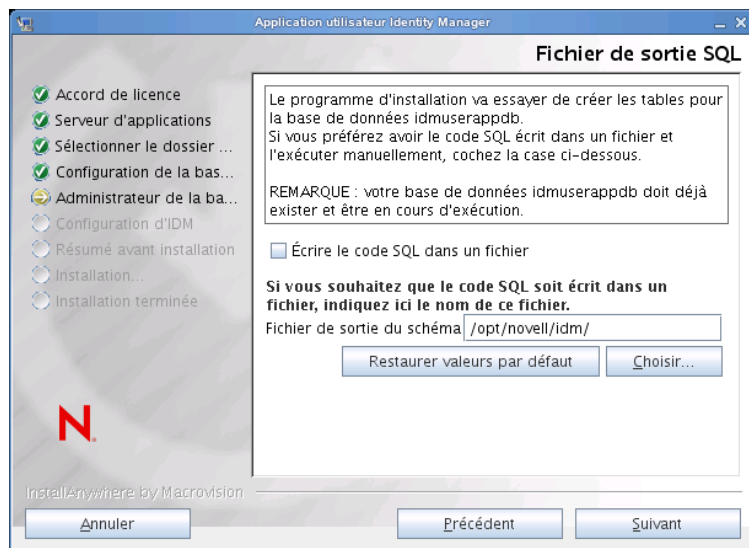
Écran d'installation	Description
Hôte et port de la base de données	<p><i>Hôte</i> : indiquez le nom d'hôte ou l'adresse IP du serveur de bases de données. Pour une grappe, indiquez le même nom d'hôte ou la même adresse IP pour chaque membre de la grappe.</p> <p><i>Port</i> : indiquez le numéro du port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



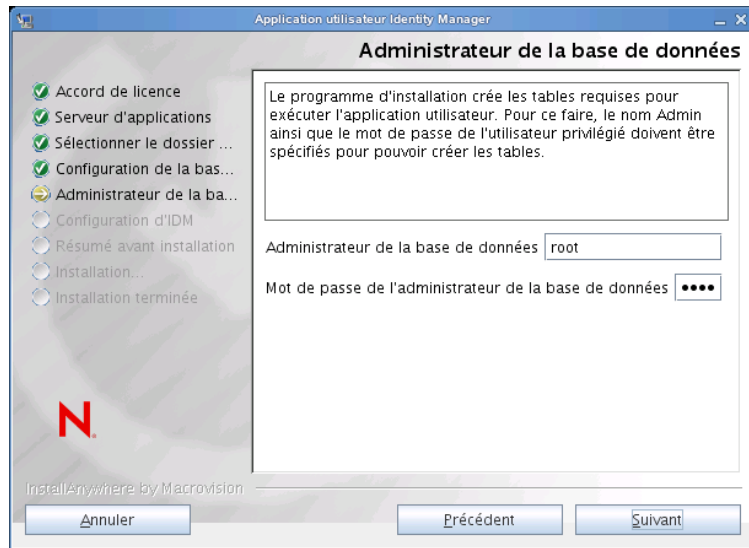
Écran d'installation	Description
Nom d'utilisateur et mot de passe de la base de données	<p><i>Nom de la base de données (ou SID)</i> : pour MySQL, MS SQL Server ou PostgreSQL, indiquez le nom de votre base de données préconfigurée. Pour Oracle, donnez l'identificateur système Oracle (SID) que vous avez créé précédemment. Pour une grappe, indiquez le même nom ou SID de base de données pour chaque membre de la grappe.</p> <p><i>Nom d'utilisateur de la base de données</i> : indiquez le nom d'utilisateur de la base de données. Pour une grappe, indiquez le même utilisateur de base de données pour chaque membre de la grappe.</p> <p><i>Mot de passe de la base de données</i> : indiquez le mot de passe de la base de données. Pour une grappe, indiquez le même mot de passe de base de données pour chaque membre de la grappe.</p> <p><i>Fichier JAR du pilote de base de données</i> : indiquez le fichier JAR du client léger pour le serveur de base de données. Ce paramètre est obligatoire.</p>



Écran d'installation	Description
Fichier de sortie SQL	<p>Dans cette version, les tables de base de données peuvent être créées au cours de l'installation de l'application utilisateur, plutôt qu'au lancement du serveur d'applications (comme c'était le cas dans les versions précédentes).</p> <p>L'écran Fichier de sortie SQL vous permet de créer un fichier de schéma que l'administrateur de base de données peut utiliser pour créer des tables (plutôt que de laisser le programme d'installation les créer).</p> <p>Si vous souhaitez générer un fichier de schéma, cochez la case <i>Écrire le code SQL dans un fichier</i> et indiquez un nom pour le fichier dans le champ <i>Fichier de sortie du schéma</i>.</p>

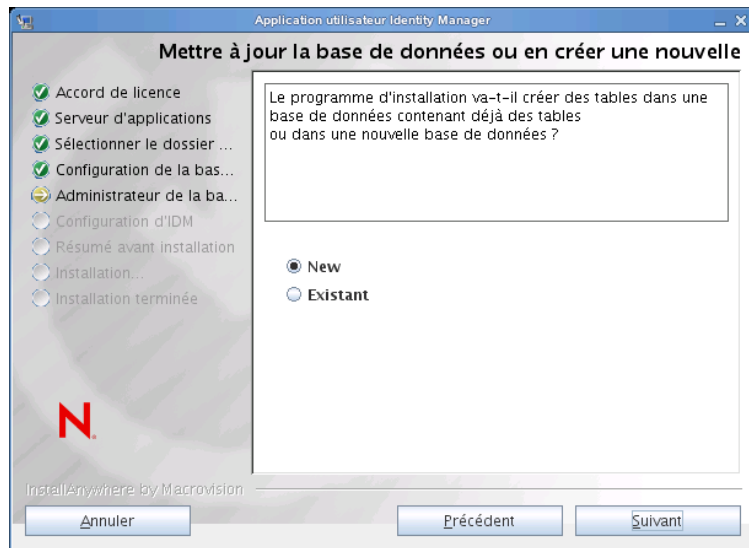


Écran d'installation	Description
Administrateur de la base de données	Cette page est préremplie avec les mêmes nom d'utilisateur et mot de passe que sur la page Nom d'utilisateur et mot de passe de la base de données. Si l'utilisateur de base de données spécifié précédemment ne possède pas les autorisations suffisantes pour créer des tables sur le serveur de base de données, alors vous devez indiquer l'ID d'un utilisateur possédant les droits requis.

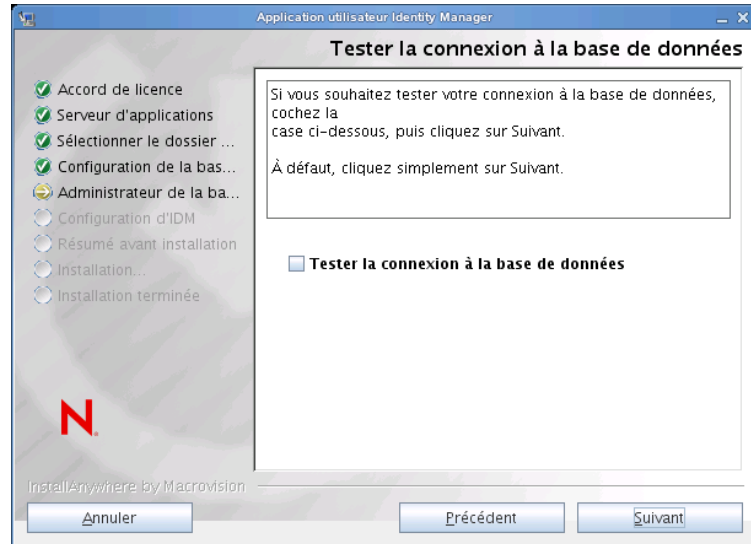


Mettre à jour la base de données ou en créer une nouvelle

Si la base de données à utiliser est nouvelle ou vide, sélectionnez *Nouveau*. Si la base de données provient d'une installation précédente, sélectionnez *Existant*.



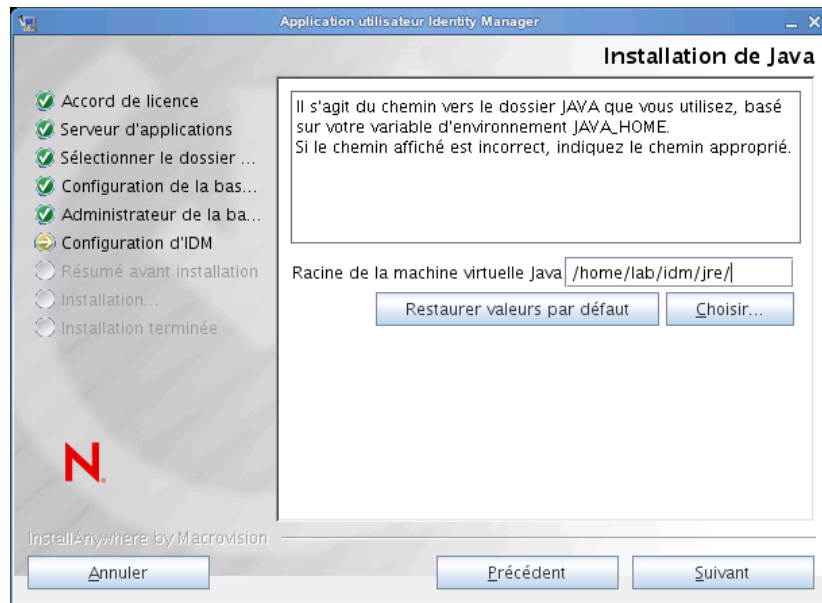
Écran d'installation	Description
Tester la connexion à la base de données	Pour vérifier que les informations fournies dans les écrans précédents sont correctes, vous pouvez tester la connexion à la base de données en cochant la case <i>Tester la connexion à la base de données</i> :



- 5 Aidez-vous des informations suivantes pour configurer Java et IDM ainsi que les paramètres d'audit et la sécurité.

Écran d'installation	Description
----------------------	-------------

Installation de Java	Indiquez le dossier d'installation racine de Java. L'écran Installation de Java fournit le chemin d'accès à Java à partir de votre variable d'environnement JAVA_HOME et vous permet de le rectifier :
----------------------	--



À ce stade, le programme d'installation vérifie également que la plate-forme Java sélectionnée est appropriée pour le serveur d'applications spécifié. En outre, il vérifie qu'il peut éditer le fichier cacerts du JRE indiqué.

Écran d'installation	Description
----------------------	-------------

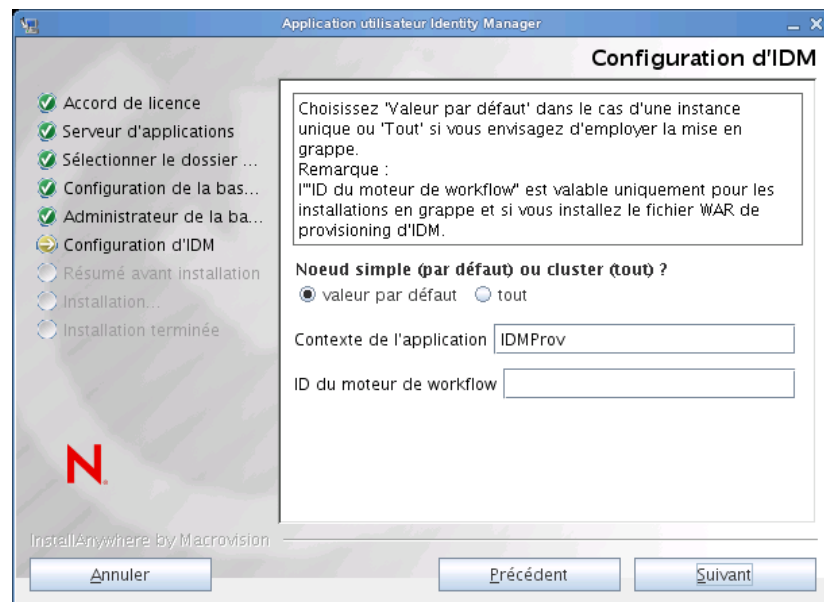
Configuration d'IDM Sélectionnez le type de configuration du serveur d'applications :

- ◆ Sélectionnez *par défaut* si cette installation est sur un noeud simple qui ne fait pas partie d'une grappe.

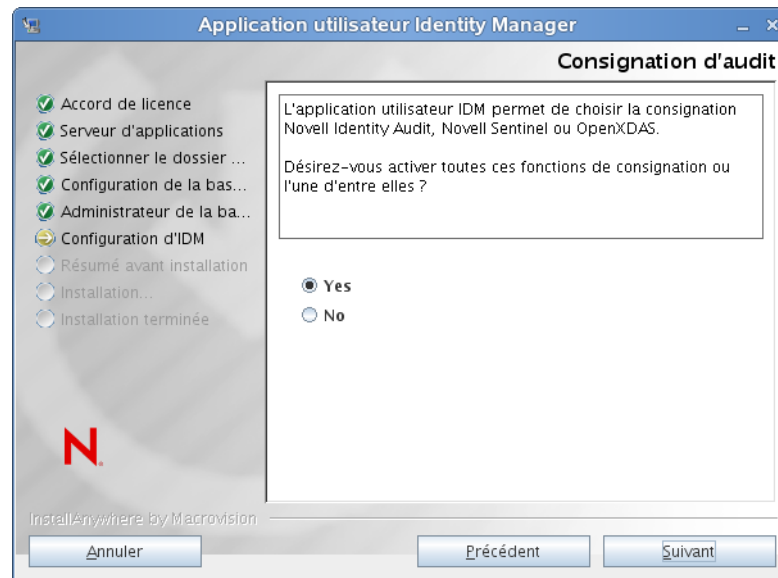
Si vous sélectionnez *par défaut* et décidez que vous aurez besoin d'une grappe ultérieurement, vous devrez réinstaller l'application utilisateur.

- ◆ Sélectionnez *tout* si cette installation fait partie d'une grappe.

Contexte de l'application : noms de la configuration du serveur d'applications, du fichier WAR de l'application et du contexte de l'URL. Le script d'installation crée une configuration serveur et par défaut nomme la configuration en fonction du *Nom de l'application*. Notez le nom de l'application et ajoutez-le dans l'URL lorsque vous démarrez l'application utilisateur dans un navigateur.



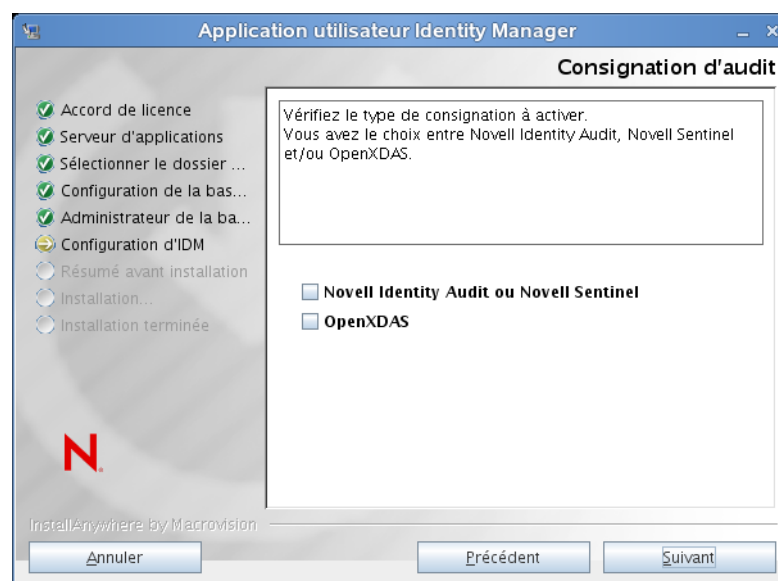
Écran d'installation	Description
Consignation Audit	Pour activer la consignation, cliquez sur <i>Oui</i> . Pour désactiver la consignation, cliquez sur <i>Non</i> .



Le tableau de bord suivant vous invite à indiquer le type de consignation. Choisissez parmi les options suivantes :

- ◆ *Novell Identity Audit* ou *Novell Sentinel* : permet d'activer la consignation via un client d'audit Novell pour l'application utilisateur.
- ◆ *OpenXDAS* : les événements sont consignés sur votre serveur de consignation OpenXDAS.

Pour plus d'informations sur la configuration de la consignation , reportez-vous au manuel *User Application: Administration Guide* (Guide d'administration de l'application utilisateur).



Écran d'installation	Description
Novell Audit	<p><i>Serveur</i> : si vous activez la consignation, indiquez le nom d'hôte ou l'adresse IP du serveur. Si vous désactivez la consignation, cette valeur est ignorée.</p> <p><i>Dossier de cache des journaux</i> : indiquez le répertoire du cache de consignation.</p>
Sécurité : clé principale	<p><i>Oui</i> : vous permet d'importer une clé principale existante. Si vous choisissez d'importer une clé maîtresse codée existante, coupez et collez la clé dans la fenêtre de procédure d'installation.</p> <p><i>Non</i> : crée une clé principale. Une fois l'installation terminée, vous devez enregistrer manuellement la clé maîtresse comme décrit dans la Section 9.1, « Enregistrement de la clé maîtresse », page 115.</p> <p>La procédure d'installation inscrit la clé maîtresse codée dans le fichier <code>master-key.txt</code> dans le répertoire d'installation.</p> <p>Voici des raisons d'importer une clé principale existante :</p> <ul style="list-style-type: none"> ◆ 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.

- 6 Cliquez sur *Suivant* pour afficher le volet de configuration du module de provisioning basé sur les rôles. (Si le programme ne vous invite pas à saisir ces informations, vous n'avez peut-être pas suivi toutes les étapes définies à la [Section 2.5, « Installation du kit de développement Java », page 29.](#))

La vue par défaut du volet de configuration du module de provisioning basé sur les rôles contient les six champs suivants :

Le programme d'installation utilisera la valeur du champ DN du conteneur racine et l'appliquera aux valeurs suivantes :

- ◆ DN du conteneur de l'utilisateur
- ◆ DN du conteneur du groupe

Le programme d'installation utilisera la valeur du champ Administrateur de l'application utilisateur et l'appliquera aux valeurs suivantes :

- ◆ Administrateur du provisioning
- ◆ Administrateur de conformité
- ◆ Administrateur de rôles
- ◆ Administrateur de la sécurité
- ◆ Administrateur de ressources
- ◆ Administrateur de la configuration RBPM

Pour définir ces valeurs explicitement, vous pouvez cliquer sur le bouton *Aff. options avancées* et les modifier :

Configuration du module de provisioning basé sur les rôles (RBPM)

Paramètres du coffre-fort d'identité

Serveur du coffre-fort d'identité :
 Port LDAP :
 Port LDAP sécurisé :
 Administrateur du coffre-fort d'identité :
 Mot de passe de l'administrateur du coffre-for... :
 Utiliser un compte anonyme public :
 Invité LDAP :
 Mot de passe de l'invité LDAP :
 Connexion Admin sécurisée :
 Connexion utilisateur sécurisée :

DN du coffre-fort d'identité

DN du conteneur racine :
 Pilote de l'application utilisateur :
 Administrateur de l'application utilisateur :
 Administrateur du provisioning :
 Administrateur de conformité :
 Administrateur de rôles :
 Administrateur de la sécurité :
 Administrateur de ressources :
 Administrateur de la configuration RBPM :

Identité de l'utilisateur du coffre-fort d'identité

DN du conteneur de l'utilisateur :
 Ét. cont. Util. (sous-arb., 1 niv.) :
 Classe de l'objet utilisateur :
 Attribut de login :
 Attribut de nom :
 Attribut d'appartenance de l'utilisateur :

Groupes d'utilisateurs du coffre-fort d'identité

DN du conteneur du groupe :
 Ét. cont. Gpe (sous-arb., 1 niv.) :
 Classe de l'objet Groupe :
 Attribut d'appartenance au groupe :
 Utiliser des groupes dynamiques :
 Classe d'objets Groupe dynamique :

Certificats du coffre-fort d'identité

Chemin du fichier Keystore : ...
 Mot de passe Keystore :

7 Les informations suivantes permettent de terminer l'installation.

Écran d'installation	Description
Configuration de l'application utilisateur	<p>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 <code>configupdate.sh</code> ou <code>configupdate.bat</code> après l'installation ; les exceptions sont notées dans les descriptions des paramètres.</p> <p>Pour une grappe, indiquez les paramètres de configuration identiques de l'application utilisateur pour chaque membre de la grappe.</p> <p>Reportez-vous à l'Annexe A, « Référence de configuration de l'application utilisateur IDM », page 123 pour obtenir une description des options.</p>
Résumé pré-installation	<p>Lisez la page de résumé de la pré-installation pour vérifier vos paramètres d'installation.</p> <p>Si nécessaire, utilisez <i>Retour</i> pour retourner aux pages d'installation précédentes et modifier les paramètres d'installation.</p> <p>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. Lorsque vous êtes satisfait de vos paramètres d'installation et de configuration, retournez à la page Récapitulatif de pré-installation, puis cliquez sur <i>Installer</i>.</p>
Installation terminée	Indique que l'installation est terminée.

7.2.1 Affichage des fichiers journaux et d'installation

Si votre installation s'est terminée sans erreur, passez à la section [Préparation de l'environnement WebLogic](#). 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.

7.3 Préparation de l'environnement WebLogic

- ♦ [Section 7.3.1, « Configurez la réserve de connexions », page 100](#)
- ♦ [Section 7.3.2, « Définition de l'emplacement des fichiers de configuration du RBPM », page 100](#)
- ♦ [Section 7.3.3, « Plug-in de workflow et configuration de WebLogic », page 101](#)

7.3.1 Configurez la réserve de connexions

- ❑ Copiez les fichiers JAR du pilote de votre base de données vers le domaine où vous déploierez l'application utilisateur.
- ❑ Copiez les fichiers `antlr-2.7.6.jar` et `log4j.jar` du répertoire d'installation de l'application utilisateur vers le dossier de la bibliothèque de domaine (par exemple, `c:\bea\user_projects\domains\idm\lib\`). Copiez également le fichier `commons-logging.jar` du dossier `c:\bea\tools\eclipse` vers le dossier de la bibliothèque de domaine.
- ❑ Créez votre source de données.

Suivez les instructions permettant de créer une source de données dans la documentation WebLogic.

Notez que le nom JNDI de la source de données doit être `jdbc/IDMUADataSource`, quel que soit le nom spécifié pour la source de données ou la base de données lors de la création du fichier WAR de l'application utilisateur.

7.3.2 Définition de l'emplacement des fichiers de configuration du RBPM

L'application utilisateur WebLogic doit pouvoir localiser le fichier `sys-configuration-xmldata.xml` et le fichier `idmuserapp_logging.xml`. Pour ce faire, ajoutez l'emplacement des fichiers dans le fichier `setDomainEnv.cmd`.

Pour les rendre disponibles pour le serveur d'applications, indiquez l'emplacement dans le fichier `setDomainEnv.cmd` ou `setDomainEnv.sh` :

1 Ouvrez le fichier `setDomainEnv.cmd` ou `setDomainEnv.sh`.

2 Localisez la ligne qui ressemble à ce qui suit :

```
set JAVA_PROPERTIES
export JAVA_PROPERTIES
```

3 Sous l'entrée `JAVA_PROPERTIES`, ajoutez des entrées des éléments suivants :

- ♦ `-Dextend.local.config.dir==<chemin_répertoire>` : indiquez le dossier (et non le fichier) qui contient le fichier `sys-configuration.xml`.
- ♦ `-Didmuserapp.logging.config.dir==<chemin_répertoire>` : indiquez le dossier (et non le fichier) qui contient le fichier `idmuserapp_logging.xml`.

Par exemple, sous Windows :

```
set JAVA_OPTIONS=-Dextend.local.config.dir=c:\novell\idm
set JAVA_OPTIONS=%JAVA_OPTIONS% -
Didmuserapp.logging.config.dir=c:\novell\idm
```

4 Définissez la variable d'environnement `EXT_PRE_CLASSPATH` pour qu'elle pointe vers les fichiers `antlr.jar`, `log4j.jar` et `commons-logging.jar`.

4a Recherchez cette ligne :

```
ADD EXTENSIONS TO CLASSPATH
```

4b Ajoutez `EXT_PRE_CLASSPATH` en dessous. Par exemple, sous Windows :

```
set
EXT_PRE_CLASSPATH=C:\bea\user_projects\domains\base_domain\lib\antlr-
2.7.6.jar;C:\bea\user_projects\domain\base_domain\lib\log4j.jar;C:\be
a\user_projects\domains\base_domain\lib\commons-logging.jar
```

Par exemple, sous Linux :

```
export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/
lib/antlr-
2.7.6.jar;C:\bea\user_projects\domain\base_domain\lib\log4j.jar;C:\be
a\user_projects\domains\base_domain\lib\commons-logging.jar
```

5 Enregistrez le fichier et quittez l'application.

Les fichiers XML sont également utilisés par l'utilitaire configuré ; par conséquent, vous devez modifier les fichiers `configupdate.bat` ou `configupdate.sh` comme suit :

1 Ouvrez `configupdate.bat` ou `configupdate.sh`.

2 Repérez la ligne suivante :

```
-Duser.language=en -Duser.region="
```

3 Mettez à jour la ligne existante pour inclure l'instruction suivante :

```
-Dextend.local.config.dir=<directory-path>\extend.local.config.dir
```

4 Enregistrez et fermez le fichier.

5 Exécutez l'utilitaire de mise à jour de la configuration pour installer le certificat dans le keystore du JDK sous `BEA_HOME`.

Lorsque vous exécutez une mise à jour de la configuration, le programme vous invite à indiquer le fichier `cacerts` sous le JDK que vous utilisez. Si vous n'utilisez pas le JDK spécifié pendant l'installation, vous devez exécuter la commande `configupdate` sur le fichier `WAR`. Soyez attentif au JDK indiqué, car cette entrée doit pointer vers le JDK utilisé par WebLogic. Ceci sert à importer un fichier de certificat pour la connexion au coffre-fort d'identité. L'objectif est d'importer un certificat pour la connexion à eDirectory.

Dans l'utilitaire `configupdate`, la valeur Certificats du coffre-fort d'identité doit pointer vers l'emplacement suivant :

```
c:\jrockit\jre\lib\security\cacerts
```

7.3.3 Plug-in de workflow et configuration de WebLogic

Le plug-in Administration du workflow d'iManager ne peut pas se connecter au pilote de l'application utilisateur en cours d'exécution sur WebLogic si `enforce-valid-basic-auth-credentials` est défini sur `vrai`. Pour que la connexion réussisse, vous devez désactiver le drapeau.

Pour désactiver `enforce-valid-basic-auth-credentials`, procédez comme suit :

1 Ouvrez le fichier `config.xml` dans le dossier

```
<WLHome>\user_projects\domains\idm\config\.
```

2 Ajoutez la ligne suivante à la section `<security-configuration>` :

```
<enforce-valid-basic-auth-credentials>>false</enforce-valid-basic-auth-
credentials>
```

3 Enregistrez le fichier et redémarrez le serveur.

Une fois cette modification effectuée, vous devriez être en mesure de vous loguer au plug-in Administration du workflow.

7.4 Déploiement du fichier WAR de l'application utilisateur

- ❑ Copiez le fichier WAR mis à jour de l'application utilisateur depuis le répertoire d'installation (en général `Novell\IDM` vers le domaine d'application. Par exemple :

```
bea\user_projects\domains\base_domain\servers\AdminServer\upload
```

- ❑ Déployez le fichier WAR de l'application utilisateur à l'aide de la procédure de déploiement WebLogic standard.

7.5 Accès à l'application utilisateur

- ❑ Naviguez vers l'URL de l'application utilisateur :

```
http://application-server-host:port/application-context
```

Par exemple :

```
http://localhost:8080/IDMProv
```

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

8

Cette section décrit les méthodes d'installation dont vous disposez si vous ne souhaitez pas utiliser l'interface graphique décrite au [Chapitre 5, « Installation de l'application utilisateur sur JBoss », page 51](#). Les rubriques sont les suivantes :

- [Section 8.1, « Installation de l'application utilisateur à partir de la console », page 103](#)
- [Section 8.2, « Installation de l'application utilisateur avec une seule commande », page 104](#)

8.1 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.

Remarque : le programme d'installation requiert au moins la version 1.5 du kit de développement de la plate-forme Java 2, Standard Edition. Si vous utilisez une version antérieure, la procédure d'installation ne configurera pas correctement le fichier WAR de l'application utilisateur. L'installation semblera réussir, mais vous rencontrerez des erreurs lorsque vous tenterez de démarrer l'application utilisateur.

- 1 Une fois que vous êtes en possession des fichiers d'installation décrits dans le [Tableau 2-2 page 18](#), connectez-vous et ouvrez une session de terminal.
- 2 Lancez le programme d'installation correspondant à votre plate-forme avec Java en utilisant la commande suivante :

```
java -jar IdmUserApp.jar -i console
```
- 3 Suivez les mêmes étapes que pour l'interface utilisateur graphique au [Chapitre 5, « Installation de l'application utilisateur sur JBoss », page 51](#) : 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.
- 4 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 la [Section A.1, « Configuration de l'application utilisateur : paramètres de base », page 123](#).
- 5 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.
- 6 Passez au [Chapitre 9, « Tâches post-installation », page 115](#).

8.2 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 2-2 page 18](#).
- 2 Loguez-vous et ouvrez une session de terminal.
- 3 Recherchez le fichier de propriétés Identity Manager, `silent.properties`, qui se trouve avec le s 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 8-1](#) 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 /chemin_de_votre_répertoire/  
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 8-1 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 à eDirectory™ : hôte LDAP. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP.

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_LDAPADMIN=	<p>Paramètres de login eDirectory : administrateur LDAP.</p> <p>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.</p>
NOVL_CONFIG_LDAPADMINPASS=	<p>Paramètres de login eDirectory : mot de passe administrateur LDAP.</p> <p>Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.</p>
NOVL_CONFIG_ROOTCONTAINERNAME=	<p>DN eDirectory : DN du conteneur racine.</p> <p>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>Indiquez le nom distinctif du pilote de l'application utilisateur que vous avez créé auparavant dans la Section 4.1, « Création du pilote d'application utilisateur dans iManager », page 45. 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>

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_LOCKSMITH=	<p data-bbox="810 310 1330 336">DN eDirectory : admin. de l'application utilisateur.</p> <p data-bbox="810 363 1349 533">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 data-bbox="810 560 1349 846">Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, Novell Designer pour Identity Manager ou l'application utilisateur (onglet <i>Requêtes et approbations</i>), vous devez accorder à cet administrateur des autorisations 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</i> pour en savoir plus.</p> <p data-bbox="810 873 1349 982">Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration > Sécurité</i> de l'application utilisateur.</p>
NOVL_CONFIG_PROVLOCKSMITH=	<p data-bbox="810 1010 1330 1060">DN eDirectory : administrateur de l'application de provisioning.</p> <p data-bbox="810 1087 1349 1373">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 data-bbox="810 1400 1349 1514">Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration > 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_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 > Assignations de rôles</i> de l'application utilisateur.</p>
NOVL_CONFIG_COMPLIANCECONTAINERDN	<p>L'administrateur du module de conformité est un rôle système qui permet aux membres d'exécuter toutes les fonctions de l'onglet <i>Conformité</i>. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné comme administrateur du module de conformité.</p>
NOVL_CONFIG_USERCONTAINERDN=	<p>Identité utilisateur du méta-annuaire : DN du conteneur utilisateur.</p> <p>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>Important : vérifiez que l'administrateur de l'application utilisateur indiqué 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>
NOVL_CONFIG_GROUPCONTAINERDN=	<p>Groupes d'utilisateurs du méta-annuaire : DN du conteneur de groupes.</p> <p>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 keystore (<code>cacerts</code>) du JRE utilisé par le serveur d'applications. 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>

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_KEYSTOREPASSWORD=	<p>Certificats eDirectory : mot de passe du keystore.</p> <p>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>Requis. 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>Requis. 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>Requis. Indiquez un intervalle de timeout de session d'application.</p>
NOVL_CONFIG_LDAPPLAINPORT=	<p>Paramètres de connexion eDirectory : port non sécurisé LDAP.</p> <p>Requis. 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>Requis. 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>Requis. 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 <code>NOVL_CONFIG_GUEST</code>.</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_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="810 856 1182 882">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>
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	<p>Courrier électronique : jeton du port sécurisé du modèle de notification.</p> <p>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</p>
NOVL_CONFIG_NOTFSMTPEMAILFROM=	<p>Courrier électronique : notification SMTP - expéditeur du courrier électronique.</p> <p>Requis. 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>Requis. 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>

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_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_EXTPWDWARRTNPATH</code>.</p> <p>Indiquez <i>Faux</i> pour utiliser la fonction de gestion des mots de passe interne par défaut, <code>/jsps/pwdmgt/ForgotPassword.jsp</code> (sans le protocole <code>http(s)</code> 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.jsp</code>, dans un fichier WAR de gestion de mot de passe externe ou interne. Vous pouvez également accepter le fichier WAR de gestion de mot de passe interne par défaut. Pour plus de détails, reportez-vous à la section « Configuration de la gestion externe des mots de passe oubliés » page 118.</p>
NOVL_CONFIG_EXTPWDWARRTNPATH=	<p>Gestion des mots de passe : liaison de retour Mot de passe oublié.</p> <p>Définissez le paramètre Lien Retour mot de passe oublié afin que l'utilisateur puisse cliquer dessus après une opération de type Mot de passe oublié.</p>
NOVL_CONFIG_FORGOTWEBSERVICEURL=	<p>Gestion des mots de passe : URL du service Web de mot de passe oublié</p> <p>Il s'agit de l'URL que le fichier WAR externe de mot de passe oublié utilise pour revenir à l'application utilisateur en vue d'exécuter les fonctions de base de mot de passe oublié. Le format de cette URL est le suivant :</p> <pre data-bbox="812 1554 1300 1608">https://<idmhost>:<sslport>/<idm>/pwdmgt/service</pre>
NOVL_CONFIG_USEROBJECTATTRIBUTE=	<p>Identité utilisateur du méta-annuaire : classe d'objets utilisateur.</p> <p>Requis. La classe d'objets utilisateur LDAP (généralement <code>inetOrgPerson</code>).</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_LOGINATTRIBUTE=	<p>Identité utilisateur du méta-annuaire : attribut de login.</p> <p>Requis. L'attribut LDAP (par exemple, CN) 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>Requis. 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>Requis. 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>Requis. La classe d'objets Groupe LDAP (généralement <code>groupOfNames</code>).</p>
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	<p>Groupes d'utilisateurs du méta-annuaire : attribut d'adhésion à un groupe.</p> <p>Requis. 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>Requis. Indiquez <i>Vrai</i> si vous souhaitez utiliser les groupes dynamiques. Indiquez <i>Faux</i> dans le cas contraire.</p>
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	<p>Groupes d'utilisateurs du méta-annuaire : classe d'objets de groupe dynamique.</p> <p>Requis. Indiquez la classe d'objets de groupe dynamique LDAP (généralement <code>dynamicGroup</code>).</p>
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 <code>System</code> <code>javax.net.ssl.trustStore</code>. Si le chemin n'y est pas, il est supposé être <code>jre/lib/security/cacerts</code>.</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_TRUSTEDSTOREPASSWORD=	Keystore approuvé : mot de passe du keystore approuvé.
NOVL_CONFIG_AUDITCERT=	Certificat de signature numérique
NOVL_CONFIG_AUDITKEYFILEPATH=	Chemin d'accès au fichier de clé privée de signature numérique
NOVL_CONFIG_ICSSLOGOUTENABLED=	Paramètres Access Manager et IChain : logout simultané activé
NOVL_CONFIG_ICSSLOGOUTPAGE=	<p>Indiquez <i>Vrai</i> pour activer 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.</p> <p>Indiquez <i>Faux</i> pour désactiver le logout simultané.</p> <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 consignation ICS est activée et qu'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=	Courrier électronique : jeton du port sécurisé du modèle de notification.
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>

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_CREATEDIRECTORYINDEX	<p>Divers : créer un index eDirectory</p> <p>Indiquez Vrai si vous souhaitez que le programme d'installation silencieux crée des index sur les attributs <code>manager</code>, <code>ismanager</code> et <code>srvprvUUID</code> sur le serveur eDirectory indiqué dans <code>NOVL_CONFIG_SERVERDN</code>. Si ce paramètre est défini sur Vrai, <code>NOVL_CONFIG_REMOVEEDIRECTORYINDEX</code> ne peut pas être Vrai.</p> <p>Pour que les performances soient optimales, la création de l'index doit être terminée. Les index doivent être en mode En ligne pour que vous puissiez rendre l'Application utilisateur disponible.</p>
NOVL_CONFIG_REMOVEDIRECTORYINDEX	<p>Divers : supprimer un index eDirectory</p> <p>Indiquez Vrai si vous souhaitez que le programme d'installation silencieux supprime des index sur le serveur indiqué dans <code>NOVL_CONFIG_SERVERDN</code>. Si ce paramètre est défini sur Vrai, <code>NOVL_CONFIG_CREATEEDIRECTORYINDEX</code> ne peut pas être Vrai.</p>
NOVL_CONFIG_SERVERDN	<p>Divers : DN de serveur</p> <p>Indiquez le serveur eDirectory sur lequel les index doivent être créés ou duquel ils doivent être supprimés.</p>
NOVL_DATABASE_NEW	<p>Indique si la base de données est nouvelle ou existe déjà. Choisissez <i>Vrai</i> dans le cas d'une nouvelle base de données. Choisissez <i>Faux</i> dans le cas d'une base de données existante.</p>
NOVL_RBPM_SEC_ADMINDN	<p>Administrateur de la sécurité</p> <p>Ce rôle permet aux membres d'accéder à toutes les fonctionnalités du domaine Sécurité.</p> <p>L'administrateur de la sécurité peut effectuer toutes les opérations possibles sur tous les objets au sein du domaine Sécurité. Le domaine Sécurité permet également à l'administrateur de la sécurité de configurer des autorisations d'accès pour tous les objets dans tous les domaines du module de provisioning basé sur les rôles. L'administrateur de la sécurité peut configurer des équipes et assigner des administrateurs de domaine, des administrateurs délégués et d'autres administrateurs de la sécurité.</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_RBPM_RESOURCE_ADMINDN	<p>Administrateur de ressources</p> <p>Ce rôle permet aux membres d'accéder à toutes les fonctionnalités du domaine Ressource. L'administrateur de ressources peut effectuer toutes les opérations possibles sur tous les objets au sein du domaine Ressource.</p>
NOVL_RBPM_CONFIG_ADMINDN	<p>Ce rôle permet aux membres d'accéder à toutes les fonctionnalités du domaine Configuration. L'administrateur de la configuration RBPM peut effectuer toutes les opérations possibles pour tous les objets au sein du domaine Configuration. Il contrôle l'accès aux éléments de navigation dans le module de provisioning basé sur les rôles. En outre, l'administrateur de la configuration RBPM configure le service de délégation et proxy, le service de signature numérique, l'interface utilisateur de provisioning et le moteur de workflow.</p>

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

- ♦ [Section 9.1, « Enregistrement de la clé maîtresse », page 115](#)
- ♦ [Section 9.2, « Configuration de l'application utilisateur », page 115](#)
- ♦ [Section 9.3, « Configuration d'eDirectory », page 116](#)
- ♦ [Section 9.4, « Reconfiguration du fichier WAR de l'application utilisateur après l'installation », page 118](#)
- ♦ [Section 9.5, « Configuration de la gestion externe des mots de passe oubliés », page 118](#)
- ♦ [Section 9.6, « Mise à jour des paramètres de mot de passe oublié », page 119](#)
- ♦ [Section 9.7, « Considérations relatives à la sécurité », page 120](#)
- ♦ [Section 9.8, « Dépannage », page 120](#)

9.1 Enregistrement de la clé maîtresse

Immédiatement après l'installation, copiez la clé maîtresse codée et enregistrez-la en lieu sûr.

- 1 Ouvrez le fichier `master-key.txt` dans le répertoire d'installation.
- 2 Copiez la clé maîtresse codée dans un emplacement sûr accessible en cas de défaillance système.

Avertissement : conservez toujours une copie de la clé maîtresse codée. Vous avez besoin de la clé maîtresse codée pour accéder à nouveau aux données codées en cas de perte de la clé maîtresse, par exemple en raison d'une défaillance de l'équipement.

Si cette installation est sur le premier membre d'une grappe, utilisez cette clé maîtresse codée lors de l'installation de l'application utilisateur sur d'autres membres de la grappe.

9.2 Configuration de l'application utilisateur

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 Administration Guide* (Guide d'administration du module de provisioning basé sur les rôles Novell IDM).
- ♦ Le manuel *Novell IDM Roles Based Provisioning Module Design Guide* (Guide de conception du module de provisioning basé sur les rôles Novell IDM).

9.2.1 Configuration de la consignation

Pour configurer la consignation, suivez les instructions de la section « Setting Up Logging (Configuration de la consignation) » dans le manuel [User Application: Administration Guide \(http://www.novell.com/documentation/idmrbpm37/index.html\)](http://www.novell.com/documentation/idmrbpm37/index.html) (Guide d'administration de l'application utilisateur).

9.3 Configuration d'eDirectory

- ♦ [Section 9.3.1, « Création d'index dans eDirectory », page 116](#)
- ♦ [Section 9.3.2, « Installation et configuration de la méthode d'authentification SAML », page 116](#)

9.3.1 Création d'index dans eDirectory

Pour améliorer les performances de l'application utilisateur, l'administrateur d'eDirectory™ doit créer des index pour les attributs manager, ismanager et srvprvUUID. Sans index sur ces attributs, les performances de l'application utilisateur peuvent être réduites, en particulier dans les environnements en grappes.

Ces index peuvent être créés automatiquement pendant l'installation si vous sélectionnez *Créer des index eDirectory* sous l'onglet *Avancé* du volet Configuration de l'application utilisateur (décrit dans le [Tableau A-2 page 126](#)). Reportez-vous au *Guide d'administration de Novell eDirectory* (<http://www.novell.com/documentation>) pour obtenir des instructions sur l'utilisation du gestionnaire d'index en vue de créer des index.

9.3.2 Installation et configuration de la méthode d'authentification SAML

Cette configuration est nécessaire uniquement si vous souhaitez utiliser la méthode d'authentification SAML et que vous n'utilisez pas Access Manager. Si vous utilisez Access Manager, votre arborescence eDirectory comprend déjà la méthode. La procédure comprend :

- L'installation de la méthode SAML dans l'arborescence eDirectory.
- La modification des attributs eDirectory à l'aide d'iManager.

L'installation de la méthode SAML dans l'arborescence eDirectory.

- 1 Localisez le fichier `nmassaml.zip` du fichier `.iso` puis dézippez-le.
- 2 Installez la méthode SAML dans votre arborescence eDirectory.

2a Étendez le schéma stocké dans le fichier `authsaml.sch`

L'exemple suivant montre comment procéder sous Linux :

```
ndssch -h <edir_ip> <edir_admin> authsaml.sch
```

2b Installez la méthode SAML.

L'exemple suivant montre comment procéder sous Linux :

```
nmasinst -addmethod <edir_admin> <tree> ./config.txt
```

Modification des attributs eDirectory

- 1 Ouvrez iManager et allez à *Rôles et tâches > Administration de répertoire > Créer un objet*.
- 2 Sélectionnez *Afficher toutes les classes d'objets*.
- 3 Créez un objet de la classe `authsamlAffiliate`.
- 4 Sélectionnez `authsamlAffiliate`, puis cliquez sur *OK*. (Vous pouvez attribuer tout nom valide à cet objet.)
- 5 Pour préciser le contexte, sélectionnez l'objet du conteneur *SAML Assertion.Authorized Login Methods.Security* dans l'arborescence, puis cliquez sur *OK*.
- 6 Vous devez ajouter des attributs à l'objet de la classe `authsamlAffiliate`.
 - 6a Allez dans l'onglet iManager *Afficher les objets > Parcourir* et cherchez votre nouvel objet affilié dans le conteneur *SAML Assertion.Authorized Login Methods.Security*.
 - 6b Sélectionnez le nouvel objet affilié, puis sélectionnez *Modifier l'objet*.
 - 6c Ajoutez l'attribut `authsamlProviderID` au nouvel objet affilié. Cet attribut permet d'associer une assertion à son affilié. Le contenu de cet attribut doit correspondre exactement à l'attribut *Issuer* (émetteur) envoyé par l'assertion SAML.
 - 6d Cliquez sur *OK*.
 - 6e Ajoutez les attributs `authsamlValidBefore` et `authsamlValidAfter` à l'objet affilié. Ces attributs définissent la durée (en secondes) autour de *IssueInstant* (instant d'émission) dans une assertion considérée comme valide. Une valeur par défaut classique est 180 secondes.
 - 6f Cliquez sur *OK*.
- 7 Sélectionnez le conteneur *Sécurité*, puis sélectionnez *Créer un objet* pour créer un *Conteneur de racine approuvée* dans votre conteneur *Sécurité*.
- 8 Créez des objets de *racine approuvée* dans le conteneur *racine approuvée*.
 - 8a Revenez à *Rôles et tâches > Gestion d'annuaire*, puis sélectionnez *Créer un objet*.
 - 8b Sélectionnez de nouveau *Afficher toutes les classes d'objets*.
 - 8c Création d'un objet de *racine approuvée* pour le certificat que votre affilié utilisera pour signer des assertions. Pour ce faire, vous devez avoir une copie codée der du certificat.
 - 8d Créez de nouveaux objets de *racine approuvée* pour chaque certificat de la chaîne des certificats de signature jusqu'au certificat CA *racine*.
 - 8e Définissez le contexte sur le conteneur de *racine approuvée* créé ci-dessus, puis cliquez sur *OK*.
- 9 Retournez à la visionneuse d'objets.
- 10 Ajoutez un attribut `authsamlTrustedCertDN` à votre objet affilié, puis cliquez sur *OK*.

Cet attribut doit pointer vers « l'objet de *racine approuvée* » du certificat de signature que vous avez créé à l'étape précédente. (Toutes les assertions de l'affilié doivent être signées par des certificats pointés par cet attribut, sinon elles seront rejetées.)
- 11 Ajoutez un attribut `authsamlCertContainerDN` à votre objet affilié, puis cliquez sur *OK*.

Cet attribut doit pointer vers le « conteneur de *racine approuvée* » que vous avez créé auparavant. (Cet attribut permet de vérifier la chaîne du certificat de signature.)

9.4 Reconfiguration du fichier WAR de l'application utilisateur après l'installation

Pour mettre votre fichier WAR à jour, vous devez exécuter l'utilitaire de mise à jour de la configuration 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'information sur les paramètres de l'utilitaire ConfigUpdate, reportez-vous à la [Section A.1, « Configuration de l'application utilisateur : paramètres de base », page 123](#) et au [Tableau 8-1 page 104](#).

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

Dans le cas de WebLogic et WebSphere, redéployez le fichier WAR sur le serveur d'applications. Dans le cas d'un serveur JBoss unique, les modifications sont appliquées au fichier WAR déployé. Si vous l'exécutez dans une grappe JBoss, le fichier WAR doit être mis à jour sur chaque serveur JBoss de la grappe.

9.5 Configuration de la gestion externe des mots de passe oubliés

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 9.5.1, « Spécification d'un fichier WAR externe de gestion des mots de passe oubliés », page 118](#)
- ♦ [Section 9.5.2, « Spécification d'un WAR de mot de passe interne », page 119](#)
- ♦ [Section 9.5.3, « Test de la configuration du fichier WAR externe pour les mots de passe oubliés », page 119](#)
- ♦ [Section 9.5.4, « Configuration de la communication SSL entre serveurs JBoss », page 119](#)

9.5.1 Spécification d'un fichier WAR externe de gestion des mots de passe oubliés

- 1 Utilisez soit la procédure d'installation, soit l'utilitaire configupdate.
- 2 Dans les paramètres de configuration de l'application utilisateur, cochez la case du paramètre de configuration *Utiliser le WAR de mot de passe externe*.
- 3 Pour le paramètre de configuration *Liaison Mot de passe oublié*, indiquez l'emplacement du WAR de mots de passe externe.

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

- 4 Pour l'option *Lien Retour mot de passe oublié*, indiquez le lien qui s'affiche lorsque l'utilisateur a terminé la procédure de mot de passe oublié. Lorsque l'utilisateur clique sur ce lien, il est redirigé vers le lien spécifié.

- 5 Pour l'option *URL du service Web de mot de passe oublié*, indiquez l'URL du service Web que le fichier WAR externe de mot de passe oublié utilise pour revenir à l'application utilisateur. Le format de l'URL doit être le suivant : `https://<hôte_idm>:<port_ssl>/<idm>/pwdmgt/service`.

La liaison de retour doit utiliser SSL pour assurer une communication sécurisée des services Web vers l'application utilisateur. Reportez-vous également à la [Section 9.5.4, « Configuration de la communication SSL entre serveurs JBoss », page 119](#).

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

9.5.2 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*.

9.5.3 Test de la configuration du fichier WAR externe pour les mots de passe oubliés

Si vous disposez d'un fichier WAR de mots de passe externe et souhaitez y accéder pour tester la fonction Mot de passe oublié, vous le trouverez à l'emplacement suivant :

- ♦ Directement, dans un navigateur. Accédez à la page Mot de passe oublié dans le WAR de mot de passe externe, par exemple `http://localhost:8080/ExternalPwd/jsp/pwdmgt/ForgotPassword.jsp`.
- ♦ Dans la page de login de l'application utilisateur, cliquez sur le lien *Mot de passe oublié*.

9.5.4 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 fichier WAR de l'application utilisateur et le fichier WAR externe de gestion des mots de passe oubliés. Reportez-vous à votre documentation JBoss pour obtenir des directives.

9.6 Mise à jour des paramètres de mot de passe oublié

Vous pouvez modifier les valeurs des paramètres *Lien Mot de passe oublié*, *Lien Retour mot de passe oublié* et *URL du service Web de mot de passe oublié* après l'installation. Utilisez soit l'utilitaire `configupdate`, soit 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 :

- ♦ *Lien Mot de passe oublié* (par exemple : `http://localhost:8080/ExternalPwd/jsp/pwdmgt/ForgotPassword.jsp`)
- ♦ *Lien Retour mot de passe oublié* (par exemple : `http://localhost/IDMProv`)
- ♦ *URL du service Web de mot de passe oublié* (par exemple : `https://<hôte_idm>:<port_ssl>/<idm>/pwdmgt/service`)

9.7 Considérations relatives à la sécurité

Au cours de l'installation, le programme d'installation écrit des fichiers journaux dans le répertoire d'installation. Ces fichiers contiennent des informations relatives à votre configuration. Une fois votre environnement configuré, il est conseillé de supprimer ces fichiers journaux ou de les stocker dans un emplacement sécurisé.

Au cours de l'installation, vous avez la possibilité d'écrire le schéma de base de données dans un fichier. Étant donné que ce fichier contient des informations descriptives sur votre base de données, il est conseillé de le déplacer dans un emplacement sécurisé une fois le processus d'installation terminé.

9.8 Dépannage

Votre représentant Novell® passera en revue tout problème d'installation et 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"> ♦ Connexions et certificats du coffre-fort d'identité ♦ Paramètres de messagerie électronique ♦ Identité utilisateur du méta-annuaire, groupes d'utilisateurs ♦ Paramètres Access Manager et iChain® 	<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>

Point	Actions suggérées
Des exceptions apparaissent lorsque le serveur d'application démarre, avec un message de journal port 8080 déjà en cours d'utilisation.	Arrêter toute instance de Tomcat (ou autre logiciel de serveur) qui pourrait déjà être en cours d'exécution. Si vous décidez de reconfigurer le serveur d'applications de façon à ce qu'il utilise un port autre que 8080, n'oubliez pas de modifier les paramètres <code>config</code> pour le pilote de l'application utilisateur dans iManager.
Au démarrage du serveur d'applications, un message s'affiche indiquant qu'aucun certificat approuvé n'a été trouvé.	Veillez à démarrer le serveur d'applications en utilisant le JDK indiqué pendant l'installation de l'application utilisateur.
Vous ne pouvez pas vous connecter à la page d'administration du portail.	Assurez-vous que le compte administrateur de l'application utilisateur existe. Ne le confondez pas avec votre compte administrateur iManager. Il s'agit de deux objets admin. différents (normalement).
Vous pouvez vous connecter en tant qu'administrateur, mais vous ne pouvez pas créer de nouveaux utilisateurs.	L'administrateur de l'application utilisateur doit être un ayant droit du conteneur maître et doit avoir des droits de superviseur. En attendant, vous pouvez essayer de configurer les droits administrateur de l'application utilisateur équivalents aux droits administrateur LDAP (via iManager).
Au démarrage du serveur d'applications, il y a des erreurs de connexion à MySQL.	<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>
Vous rencontrez des erreurs de keystore lors du démarrage du serveur d'applications.	<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 aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit</pre> <ul style="list-style-type: none"> ◆ Remplacez <code>aliasName</code> par un nom unique de votre choix pour ce certificat. ◆ Remplacez <code>certFile</code> par le chemin complet et le nom de votre fichier de certificat. ◆ Le mot de passe du keystore par défaut est <code>changeit</code> (si vous avez un mot de passe différent, indiquez-le).

Point	Actions suggérées
Aucune notification n'a été envoyée par courrier électronique.	Exécutez l'utilitaire configupdate pour vérifier que vous avez fourni les valeurs des paramètres de configuration de l'application utilisateur suivants : Message électronique de et Message électronique à. Sous Linux ou Solaris, exécutez cette commande depuis le répertoire d'installation (par défaut, /opt/novell/idm): <code>configupdate.sh</code> Sous Windows, exécutez la commande suivante depuis le répertoire d'installation (par défaut, c:\opt\novell\idm): <code>configupdate.bat</code>

Référence de configuration de l'application utilisateur IDM

A

Cette section décrit les options destinées à fournir des valeurs lors des mises à jour de la configuration ou de l'installation de l'application utilisateur.

- [Section A.1, « Configuration de l'application utilisateur : paramètres de base », page 123](#)
- [Section A.2, « Configuration de l'application utilisateur : tous les paramètres », page 125](#)

A.1 Configuration de l'application utilisateur : paramètres de base

Figure A-1 Options de base de configuration de l'application utilisateur

Configuration du module de provisioning basé sur les rôles (RBPM)

Paramètres du coffre-fort d'identité

Serveur du coffre-fort d'identité :

Administrateur du coffre-fort d'identité :

Mot de passe de l'administrateur du coffr...

DN du coffre-fort d'identité

DN du conteneur racine : 🔍

Pilote de l'application utilisateur : 🔍

Administrateur de l'application utilisateur : 🔍

OK Annul... Aff. options avancées

Tableau A-1 Options de base de configuration de l'application utilisateur

Type de paramètre	Option	Description
Paramètres du coffre-fort d'identité	<i>Serveur du coffre-fort d'identité</i>	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP et son port sécurisé. Par exemple : myLDAPhost
	<i>Administrateur du coffre-fort d'identité</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. Utilisez l'utilitaire ConfigUpdate pour modifier ce paramètre, à condition de ne pas l'avoir modifié à l'aide de l'onglet Administration de l'application utilisateur.
	<i>Mot de passe de l'administrateur du coffre-fort d'identité</i>	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse. Utilisez l'utilitaire ConfigUpdate pour modifier ce paramètre, à condition de ne pas l'avoir modifié à l'aide de l'onglet Administration de l'application utilisateur.

Type de paramètre	Option	Description
DN du coffre-fort d'identité	<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 l'application utilisateur</i>	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur (décrit dans la Section 4.1, « Création du pilote d'application utilisateur dans iManager », page 45). Par exemple, si votre pilote est <code>UserApplicationDriver</code> , que votre ensemble de pilotes est appelé <code>myDriverSet</code> et que l'ensemble de pilotes est dans un contexte <code>o=myCompany</code> , vous saisissez la valeur suivante : <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
	<i>Administrateur de l'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, Novell Designer pour Identity Manager ou l'application utilisateur (onglet <i>Requêtes et approbations</i>), vous devez accorder à cet administrateur des autorisations 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</i> pour en savoir plus. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration > Sécurité</i> de l'application utilisateur. Vous ne pouvez pas modifier ce paramètre via <code>ConfigUpdate</code> si vous avez démarré le serveur d'applications qui héberge l'application utilisateur.

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.

A.2 Configuration de l'application utilisateur : tous les paramètres

Ce tableau indique les paramètres de configuration disponibles lorsque vous cliquez sur *Afficher les options avancées*.

Tableau A-2 Configuration de l'application utilisateur : toutes les options

Type de paramètre	Option	Description
Paramètres du coffre-fort d'identité	<i>Serveur du coffre-fort d'identité</i>	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP. Par exemple : myLDAPhost
	<i>Port LDAP</i>	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	<i>Port LDAP sécurisé</i>	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	<i>Administrateur du coffre-fort d'identité</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 de l'administrateur du coffre-fort d'identité</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	Option	Description
DN du coffre-fort d'identité	<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 d'application utilisateur</i>	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur (décrit dans la Section 4.1, « Création du pilote d'application utilisateur dans iManager » , page 45). Par exemple, si votre pilote est <code>UserApplicationDriver</code> , que votre ensemble de pilotes est appelé <code>myDriverSet</code> et que l'ensemble de pilotes est dans un contexte <code>o=myCompany</code> , vous saisissez la valeur suivante : <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
	<i>Administrateur de l'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, Novell Designer pour Identity Manager ou l'application utilisateur (onglet <i>Requêtes et approbations</i>), vous devez accorder à cet administrateur des autorisations d'ayant droit sur les instances d'objets contenues dans le pilote de l'application utilisateur. Pour plus d'informations, reportez-vous au manuel <i>User Application: Administration Guide</i> (Guide d'administration de l'application utilisateur). Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages <i>Administration > Sécurité</i> de l'application utilisateur. Vous ne pouvez pas modifier ce paramètre via <code>ConfigUpdate</code> si vous avez démarré le serveur d'applications qui héberge l'application utilisateur.
	<i>Administrateur du provisioning</i>	L'administrateur du provisioning gère les fonctions de workflow de provisioning disponibles dans l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur du provisioning. Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page <i>Administration > Assignations de l'administrateur</i> de l'application utilisateur.

Type de paramètre	Option	Description
	<i>Administrateur de conformité</i>	<p>L'administrateur de conformité est un rôle système qui permet aux membres d'exécuter toutes les fonctions de l'onglet <i>Conformité</i>. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné comme administrateur du module de conformité.</p> <p>Lors des mises à jour de la configuration, les modifications apportées à cette valeur prennent effet uniquement si vous n'avez pas d'administrateur de conformité valide assigné. Si un administrateur de conformité valide existe, vos modifications ne sont pas enregistrées.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page <i>Administration > Assignations de l'administrateur</i> de l'application utilisateur.</p>
	<i>Administrateur de rôles</i>	<p>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>Administration > Assignations de l'administrateur</i> de l'application utilisateur.</p> <p>Lors des mises à jour de la configuration, les modifications apportées à cette valeur prennent effet uniquement si vous n'avez pas d'administrateur de module de conformité valide attribué. Si un administrateur de rôles valide existe, vos modifications ne sont pas enregistrées.</p>
	<i>Administrateur de la sécurité</i>	<p>Ce rôle permet aux membres d'accéder à toutes les fonctionnalités du domaine Sécurité.</p> <p>L'administrateur de la sécurité peut effectuer toutes les opérations possibles sur tous les objets au sein du domaine Sécurité. Le domaine Sécurité permet également à l'administrateur de la sécurité de configurer des autorisations d'accès pour tous les objets dans tous les domaines du module de provisioning basé sur les rôles. L'administrateur de la sécurité peut configurer des équipes et assigner des administrateurs de domaine, des administrateurs délégués et d'autres administrateurs de la sécurité.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page <i>Administration > Assignations de l'administrateur</i> de l'application utilisateur.</p>
	<i>Administrateur de ressources</i>	<p>Ce rôle permet aux membres d'accéder à toutes les fonctionnalités du domaine Ressource. L'administrateur de ressources peut effectuer toutes les opérations possibles pour tous les objets au sein du domaine Ressource.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page <i>Administration > Assignations de l'administrateur</i> de l'application utilisateur.</p>

Type de paramètre	Option	Description
	<i>Administrateur de la configuration RBPM</i>	<p>Ce rôle permet aux membres d'accéder à toutes les fonctionnalités du domaine Configuration. L'administrateur de la configuration RBPM peut effectuer toutes les opérations possibles pour tous les objets au sein du domaine Configuration. Il contrôle l'accès aux éléments de navigation dans le module de provisioning basé sur les rôles. En outre, l'administrateur de la configuration RBPM configure le service de délégation et proxy, le service de signature numérique, l'interface utilisateur de provisioning et le moteur de workflow.</p> <p>Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page <i>Administration > Assignations de l'administrateur</i> de l'application utilisateur.</p>
Identité de l'utilisateur du coffre-fort d'identité	<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>Les utilisateurs de ce conteneur (et en-dessous) sont autorisés à se loguer à l'application utilisateur.</p> <p>Vous ne pouvez pas modifier ce paramètre via ConfigUpdate si vous avez démarré le serveur d'applications qui héberge l'application utilisateur.</p> <hr/> <p>Important : Vérifiez que l'administrateur de l'application utilisateur indiqué 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>Étendue du conteneur d'utilisateurs</i>	Cela définit l'étendue de recherche d'utilisateurs.
	<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.

Type de paramètre	Option	Description
Groupes d'utilisateurs du coffre-fort d'identité	<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. Vous ne pouvez pas modifier ce paramètre via ConfigUpdate si vous avez démarré le serveur d'applications qui héberge l'application utilisateur.
	<i>Étendue du conteneur de groupes</i>	Cela définit l'étendue de recherche des groupes.
	<i>Classe d'objets Groupe</i>	La classe d'objets Groupe LDAP (généralement <code>groupofNames</code>).
	<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 <code>dynamicGroup</code>).
Certificats du coffre-fort d'identité	<i>Chemin d'accès au Keystore</i>	Requis. Indiquez le chemin d'accès complet au fichier keystore (<code>cacerts</code>) du JRE utilisé par le serveur d'applications pour s'exécuter, ou cliquez sur le petit bouton du navigateur pour accéder au fichier <code>cacerts</code> . 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>	Requis. Indiquez le mot de passe <code>cacerts</code> . L'unité par défaut est <code>changeit</code> .
	<i>Confirmer le mot de passe Keystore</i>	
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.
	<i>Keystore de type JKS</i>	Indique le type de signature numérique à utiliser. Si ce paramètre est sélectionné, cela signifie que le chemin de la zone de stockage approuvée est de type JKS.

Type de paramètre	Option	Description
Clé de certificat et signature numérique Novell Audit	<i>Keystore de type PKCS12</i>	Indique le type de signature numérique à utiliser. Si ce paramètre est sélectionné, cela signifie que le chemin de la zone de stockage approuvée est de type PKCS12.
	<i>Certificat de signature numérique Novell Audit</i>	Affiche le certificat de signature numérique pour le service d'audit.
	<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	<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 consignment ICS est activée et qu'un utilisateur se délogue de l'application utilisateur, il est réacheminé vers cette page.

Type de paramètre	Option	Description
Configuration du serveur de messagerie	<i>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>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>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>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>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>Nom du serveur SMTP</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	Option	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 indiquer des valeurs pour les paramètres <i>Lien Mot de passe oublié</i>, <i>Lien Retour mot de passe oublié</i> et <i>URL du service Web de 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.jsp</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.jsp</code> dans un fichier WAR de gestion des mots de passe externe ou interne.
	<i>Lien Retour mot de passe oublié</i>	Définissez le paramètre <i>Lien Retour mot de passe oublié</i> afin que l'utilisateur puisse cliquer dessus après une opération de type Mot de passe oublié.
	<i>URL du service Web de mot de passe oublié</i>	<p>Il s'agit de l'URL que le fichier WAR externe de mot de passe oublié utilise pour revenir à l'application utilisateur en vue d'exécuter les fonctions de base de mot de passe oublié. Le format de cette URL est le suivant :</p> <pre>https://<idmhost>:<sslport>/<idm>/pwdmgt/service</pre>
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	Option	Description
	<i>Créer un index de coffre-fort d'identité</i>	<p>Cochez cette case si vous souhaitez que l'utilitaire d'installation crée des index sur 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. Vous pouvez créer ces index manuellement en utilisant iManager après avoir installé l'application utilisateur. Reportez-vous à la Section 9.3.1, « Création d'index dans eDirectory », page 116.</p> <p>Pour que les performances soient optimales, la création de l'index doit être terminée. Les index doivent être en mode En ligne pour que vous puissiez rendre l'Application utilisateur disponible.</p>
	<i>Supprimer l'index de coffre-fort d'identité</i>	Supprime des index des attributs manager, ismanager et srvprvUUID.
	<i>DN du serveur</i>	Sélectionnez le serveur eDirectory sur lequel les index doivent être créés ou duquel ils doivent être supprimés.
		<hr/> <p>Remarque : pour configurer des index sur plusieurs serveurs eDirectory, vous devez exécuter l'utilitaire ConfigUpdate plusieurs fois. Vous ne pouvez indiquer qu'un seul serveur à la fois.</p> <hr/>
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 pouvant servir de conteneur.
	<i>Ajouter un nouvel objet Conteneur : nom d'attribut Conteneur</i>	Donnez le nom d'attribut de l'objet Conteneur.