Guide d'installation de l'application utilisateur

Novell®
Module de provisioning basé sur les rôles Identity Manager

4.0

15 octobre 2010

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/) pour plus d'informations sur l'exportation des logiciels Novell. Novell décline toute responsabilité dans le cas où vous n'obtiendriez pas les autorisations d'exportation nécessaires.

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

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

Marques de Novell

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

Éléments tiers

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

Table des matières

À propos de ce guide 9

1 Présentation de l'installation du module de provisioning basé sur les rôles 11

1.1 Liste de contrôle de l'installation . . . 11
1.2 À propos du programme d'installation . . . 12
1.3 Configuration système requise . . . 12

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 . . . 25
2.3.3 Installation du serveur d'applications WebSphere . . . 25
2.4 Installation d'une base de données . . . 26
2.4.1 Remarques sur la configuration d'une base de données MySQL . . . 26
2.4.2 Remarques sur la configuration d'une base de données Oracle . . . 28
2.4.3 Remarques sur la configuration d'une base de données MS SQL Server . . . 29
2.4.4 Remarques sur la configuration d'une base de données DB2 . . . 29
2.5 Installation du kit de développement Java . . . 32

3 Installation du module de provisioning basé sur les rôles 33

3.1 À propos de l'installation du module de provisioning basé sur les rôles . . . 33
3.2 Exécution de l'utilitaire NrfCaseUpdate . . . 34
3.2.1 Présentation de NrfCaseUpdate . . . 34
3.2.2 Présentation de l'installation . . . 34
3.2.3 Conséquences de l'utilitaire NrfCaseUpdate sur le schéma . . . 35
3.2.4 Création d'une sauvegarde des pilotes d'application utilisateur . . . 35
3.2.5 Utilisation de NrfCaseUpdate . . . 35
3.2.6 Vérification du processus NrfCaseUpdate . . . 38
3.2.7 Activation du JRE pour les connexions SSL . . . 38
3.2.8 Restauration des pilotes d'application utilisateur invalidés . . . 39
3.3 Exécution du programme d'installation du module RBPM . . . 40
3.4 Extension manuelle du schéma . . . 46

4 Création des pilotes 49

4.1 Création des pilotes dans Designer . . . 49
4.1.1 Installation des paquetages . . . 49
4.1.2 Création du pilote d'application utilisateur dans Designer . . . 51
4.1.3 Création du pilote du service de rôles et de ressources dans Designer . . . 55
4.1.4 Déploiement des pilotes . . . 57

5 Installation de l'application utilisateur sur JBoss 59

5.1 Installation et configuration du fichier WAR de l'application utilisateur . . . 59
5.1.1 Affichage des fichiers journaux et d'installation . . . 79

5.2 Tester l’installation 79

6 Installation de l'application utilisateur sur WebSphere 81

6.1 Installation et configuration du fichier WAR de l'application utilisateur 81
6.1.1 Affichage des fichiers journaux d'installation 96
6.2 Configuration de l'environnement WebSphere. 96
6.2.1 Configuration d'une réserve de connexions. 96
6.2.2 Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM 104
6.2.3 Importation de la racine approuvée d'eDirectory dans le keystore WebSphere . . . 109
6.2.4 Transmission de la propriété preferIPv4Stack à la JVM 110
6.3 Déploiement du fichier WAR 110
6.3.1 Configuration supplémentaire pour WebSphere 7.0 111
6.4 Démarrage et accès à l'application utilisateur 111

7 Installation de l'application utilisateur sur WebLogic 113

7.1 Liste de contrôle pour l'installation de WebLogic 113
7.2 Installation et configuration du fichier WAR de l'application utilisateur 114
7.2.1 Affichage des fichiers journaux et d'installation 128
7.3 Préparation de l'environnement WebLogic 128
7.3.1 Configuration de la réserve de connexions 128
7.3.2 Définition de l'emplacement des fichiers de configuration du module RBPM 129
7.3.3 Suppression des fichiers JAR OpenSAML 131
7.3.4 Plug-in de workflow et configuration de WebLogic 131
7.4 Déploiement du fichier WAR de l'application utilisateur. 131
7.5 Accès à l'application utilisateur 131

8 Installation depuis la console ou à l'aide d'une commande unique 133

8.1 Installation de l'application utilisateur à partir de la console. 133
8.2 Installation de l'application utilisateur avec une seule commande 134
8.3 Exécution de l'utilitaire JBossPostgreSQL en mode console ou silencieux 145
8.4 Exécution du programme d'installation RIS en mode console ou silencieux 146

9 Tâches post-installation 149

9.1 Enregistrement de la clé maîtresse 149
9.2 Configuration de l'application utilisateur 149
9.2.1 Configuration de la consignation 150
9.3 Configuration d'eDirectory 150
9.3.1 Création d'index dans eDirectory. 150
9.3.2 Installation et configuration de la méthode d'authentification SAML 150
9.4 Reconfiguration du fichier WAR de l'application utilisateur après l'installation. 152
9.5 Configuration de la gestion externe des mots de passe oubliés 152
9.5.1 Spécification d'un fichier WAR externe de gestion des mots de passe oubliés. . . . 152
9.5.2 Spécification d'un WAR de mot de passe interne 153
9.5.3 Test de la configuration du fichier WAR externe pour les mots de passe oubliés 153
9.5.4 Configuration de la communication SSL entre serveurs JBoss 153
9.6 Mise à jour des paramètres de mot de passe oublié 153
9.7 Considérations relatives à la sécurité 154
9.8 Augmentation de la taille du tas Java d'IDM 154
9.9 Dépannage. 154

A Référence de configuration de l'application utilisateur IDM 157

A.1 Configuration de l'application utilisateur : paramètres de base 157
A.2 Configuration de l'application utilisateur : tous les paramètres 160

À propos de ce guide

Le présent guide décrit la procédure d'installation de la version 4.0 du module de provisioning basé sur les rôles Novell Identity Manager et comprend les sections suivantes :

- Chapitre 1, « Présentation de l'installation du module de provisioning basé sur les rôles », page 11
- Chapitre 2, « Conditions préalables », page 17
- Chapitre 3, « Installation du module de provisioning basé sur les rôles », page 33
- Chapitre 4, « Création des pilotes », page 49
- Chapitre 5, « Installation de l'application utilisateur sur JBoss », page 59
- Chapitre 6, « Installation de l'application utilisateur sur WebSphere », page 81
- Chapitre 7, « Installation de l'application utilisateur sur WebLogic », page 113
- Chapitre 8, « Installation depuis la console ou à l'aide d'une commande unique », page 133
- Chapitre 9, « Tâches post-installation », page 149
- Annexe A, « Référence de configuration de l'application utilisateur IDM », page 157

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 Identity Manager 4.0, reportez-vous au site Web de documentation d'Identity Manager (http://www.novell.com/documentation/idm40/index.html).

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 11
- Section 1.2, « À propos du programme d'installation », page 12
- Section 1.3, « Configuration système requise », page 12

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/idm40/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 12.
- ❑ 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 26.
- ❑ 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 », page 33.
- ❑ Créez le pilote de l'application utilisateur dans Designer 4.0 pour Identity Manager.
  - Reportez-vous à la Section 4.1, « Création des pilotes dans Designer », page 49.
- ❑ Créez le pilote du service de rôles et de ressources dans Designer 4.0 pour Identity Manager.
  - Reportez-vous à la Section 4.1, « Création des pilotes dans Designer », page 49.
- ❑ Installez et configurez l'application utilisateur Novell Identity Manager. (Vous devez avoir installé le bon JDK avant de démarrer le programme d'installation. Reportez-vous à la Section 2.5, « Installation du kit de développement Java », page 32.)

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 59.
  - Chapitre 6, « Installation de l'application utilisateur sur WebSphere », page 81.
  - Chapitre 7, « Installation de l'application utilisateur sur WebLogic », page 113.
- Interface de console (ligne de commande). Reportez-vous à la Section 8.1, « Installation de l'application utilisateur à partir de la console », page 133.
- Installation en mode silencieux. Reportez-vous à la Section 8.2, « Installation de l'application utilisateur avec une seule commande », page 134.

❑ Procédez aux tâches de post-installation décrites au Chapitre 9, « Tâches post-installation », page 149.

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/idm40/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 PostgreSQL, Oracle, DB2, Microsoft SQL Server ou MySQL. La base de données stocke les données de l'application utilisateur et les informations de configuration de l'application utilisateur.
- Configure le fichier des certificats de JDK pour que l'application utilisateur (exécutée sur le serveur d'applications) puisse communiquer avec le coffre-fort d'identité et le pilote de l'application utilisateur de façon sécurisée.
- Configure et déploie le fichier WAR (Web Application Archive) Java de l'application utilisateur Novell Identity Manager sur le serveur d'applications. Sur 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 pouvoir utiliser la version 4.0 du module de provisioning basé sur les rôles Novell Identity Manager, vous devez installer chacun des composants requis répertoriés dans le Tableau 1-1.

Tableau 1-1 *Configuration système requise*

Composant système requis	Configuration système requise
Méta-annuaire	eDirectory 8.8.6 avec Identity Manager 4.0 Pour connaître la liste des systèmes d'exploitation pris en charge, consultez la documentation relative à Identity Manager et eDirectory.
Serveur d'applications	L'application utilisateur s'exécute sur JBoss, WebSphere et WebLogic comme décrit ci-dessous. L'exécution de l'application utilisateur avec JBoss 5.1 requiert le JRE 1.6.0_20 de Sun et est prise en charge sur les plates-formes suivantes : ◆ Windows Server 2003 SP2 (32 bits uniquement) ◆ Windows Server 2008 R2 (64 bits uniquement) ◆ SUSE Linux Enterprise Server 10 SP3 (32 et 64 bits) ◆ SUSE Linux Enterprise Server 11 (32 et 64 bits) ◆ Red Hat Enterprise Linux 5.4 (32 et 64 bits) ◆ Solaris 10 (32 et 64 bits) L'exécution de l'application utilisateur sous WebSphere 7.0 requiert la machine virtuelle J9 (version 2.4, J2RE 1.6.0) et le Fix Pack 7 d'IBM. Elle est prise en charge sur les plates-formes suivantes : ◆ Windows Server 2003 SP2 (32 bits uniquement) ◆ Windows Server 2008 R2 (64 bits uniquement) ◆ SUSE Linux Enterprise Server 10 SP3 (32 et 64 bits) ◆ SUSE Linux Enterprise Server 11 (32 et 64 bits) ◆ Red Hat Enterprise Linux 5.4 (32 et 64 bits) ◆ AIX 5.3 (64 bits uniquement avec une base de données Oracle 11g) ◆ Solaris 10 (32 et 64 bits) L'exécution de l'application utilisateur sur WebLogic 10.3 requiert la machine virtuelle Java JRockit 1.6.0_17 et est prise en charge sur les plates-formes suivantes : ◆ Windows Server 2003 SP2 (32 bits uniquement) ◆ Windows Server 2008 R2 (64 bits uniquement) ◆ SUSE Linux Enterprise Server 10 SP3 (32 et 64 bits) ◆ SUSE Linux Enterprise Server 11 (32 et 64 bits) ◆ Red Hat Enterprise Linux 5.4 (32 et 64 bits) ◆ Solaris 10 (32 ou 64 bits) **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.

Composant système requis	Configuration système requise
Navigateur	L'application utilisateur prend en charge Firefox et Internet Explorer, comme indiqué ci-dessous. FireFox 3.6 est pris en charge sur les systèmes suivants : ◆ Windows XP avec SP3 ◆ Windows Vista ◆ Windows 7 ◆ SUSE Linux Enterprise Desktop 11 ◆ SUSE Linux Enterprise Server 11 ◆ Novell OpenSuSE 11.2 ◆ Apple Mac Internet Explorer 8 est pris en charge sur les systèmes suivants : ◆ Windows XP avec SP3 ◆ Windows Vista ◆ Windows 7 Internet Explorer 7 est pris en charge sur les systèmes suivants : ◆ Windows XP avec SP3
Serveur de base de données	Les bases de données suivantes sont prises en charge avec JBoss 5.1.0 : ◆ MS SQL 2008 ◆ MySQL version 5.1 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 Les bases de données suivantes sont prises en charge avec WebSphere 7.0 : ◆ DB2 9.5 ◆ MS SQL 2008 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 Les bases de données suivantes sont prises en charge avec WebLogic 10.3 : ◆ MS SQL 2008 ◆ Oracle 11g ◆ PostgreSQL 8.4.3
Designer	Designer 4.0
OpenXDAS	OpenXDAS version 0.8.345 Les versions suivantes d'OpenXDAS sont requises pour SLES10 : ◆ openxdas-0.8.351-1.1.i586.rpm ◆ openxdas-0.8.351-1.1.x86_64.rpm

Composant système requis	Configuration système requise
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 composants logiciels que vous devez installer ou configurer avant de 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 26
- Section 2.5, « Installation du kit de développement Java », page 32

2.1 Installation du méta-annuaire Identity Manager

La version 4.0 du module de provisioning basé sur les rôles doit être utilisée avec Identity Manager 4.0.

Pour obtenir les instructions relatives à l'installation d'Identity Manager 4.0, reportez-vous au site Web de documentation d'Identity Manager (http://www.novell.com/documentation/idm40/index.html).

2.2 Téléchargement du module de provisioning basé sur les rôles

Téléchargez la version 4.0 du module de provisioning basé sur les rôles Identity Manager à partir du site Web de téléchargement Novell (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 .iso
Application utilisateur	`Identity_Manager_RBPM_4_0_0_User_Application.iso`
Composants du module de provisioning basé sur les rôles pour le méta-annuaire	`Identity_Manager_RBPM_4_0_0_Driver_Install.iso`

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.
`JBossPostgreSQL.bin` ou `JBossPostgreSQL.exe`	Utilitaire pratique permettant d'installer le serveur d'applications JBoss et la base de données PostgreSQL.
`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_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 25
- Section 2.3.3, « Installation du serveur d'applications WebSphere », page 25

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 12 pour connaître la version prise en charge.
- Utiliser l'utilitaire JbossPostgreSQL inclus dans le téléchargement du module de provisioning basé sur les rôles pour installer un serveur d'applications JBoss (et PostgreSQL le cas échéant). Pour plus d'informations, reportez-vous à « Installation du serveur d'applications JBoss et de la base de données PostgreSQL » page 19.

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 8180. Notez le port que votre serveur d'applications utilise.
SSL	Activez SSL si vous prévoyez utiliser la gestion de mots de passe externe. ◆ Activez SSL sur les serveurs JBoss sur lesquels vous déployez le module de provisioning basé sur les rôles Identity Manager et le fichier `IDMPwdMgt.war`. ◆ 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 152 et au manuel *User Application: Administration Guide (Guide d'administration de l'application utilisateur)* (http://www.novell.com/documentation/idm40/index.html).

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

L'utilitaire JBossPostgreSQL installe le serveur d'applications JBoss et la base de données PostgreSQL sur votre système. Il ne prend pas en charge le mode console et requiert un environnement d'interface utilisateur graphique.

Remarque : avant d'exécuter le programme d'installation JBossPostgreSQL RBPM sous Windows 2008, vérifiez auprès de votre administrateur Windows la stratégie de mot de passe de votre système. La stratégie de mot de passe du serveur Windows 2008 exige d'un mot de passe qu'il

respecte un ensemble de règles. Par exemple, la stratégie peut imposer qu'un mot de passe contienne des caractères non alphabétiques, ainsi que des majuscules ou des minuscules, ou encore qu'il comporte au moins 8 caractères. La stratégie peut être modifiée ou désactivée par l'administrateur Windows.

Exécutez le programme d'installation en tant qu'utilisateur root. Vous devez exécuter le programme d'installation en tant qu'utilisateur root.

Pour exécuter l'utilitaire JBossPostgreSQL :

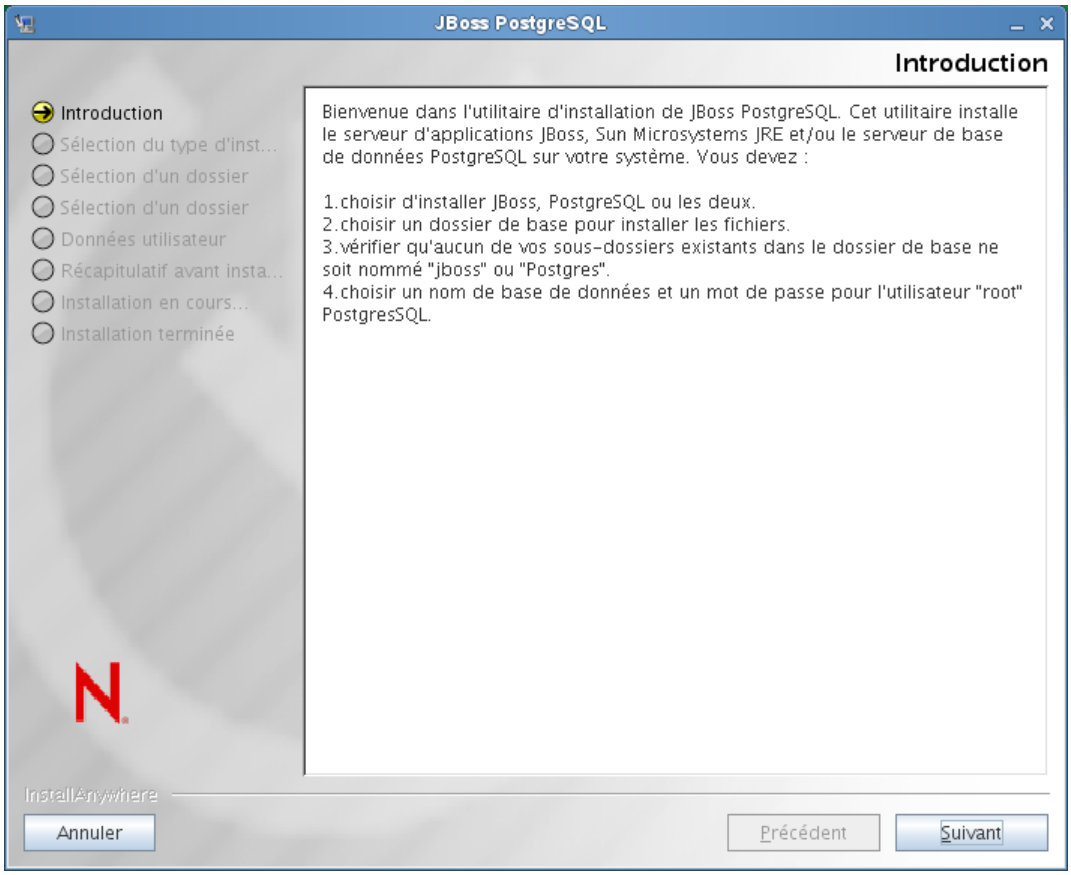
1 Recherchez et exécutez `JBossPostgreSQL.bin` ou `JBossPostgreSQL.exe` à partir du fichier .iso.

`/linux/jboss/JBossPostgreSQL.bin` (pour Linux)
`/nt/jboss/JBossPostgreSQL.exe` (pour Windows)

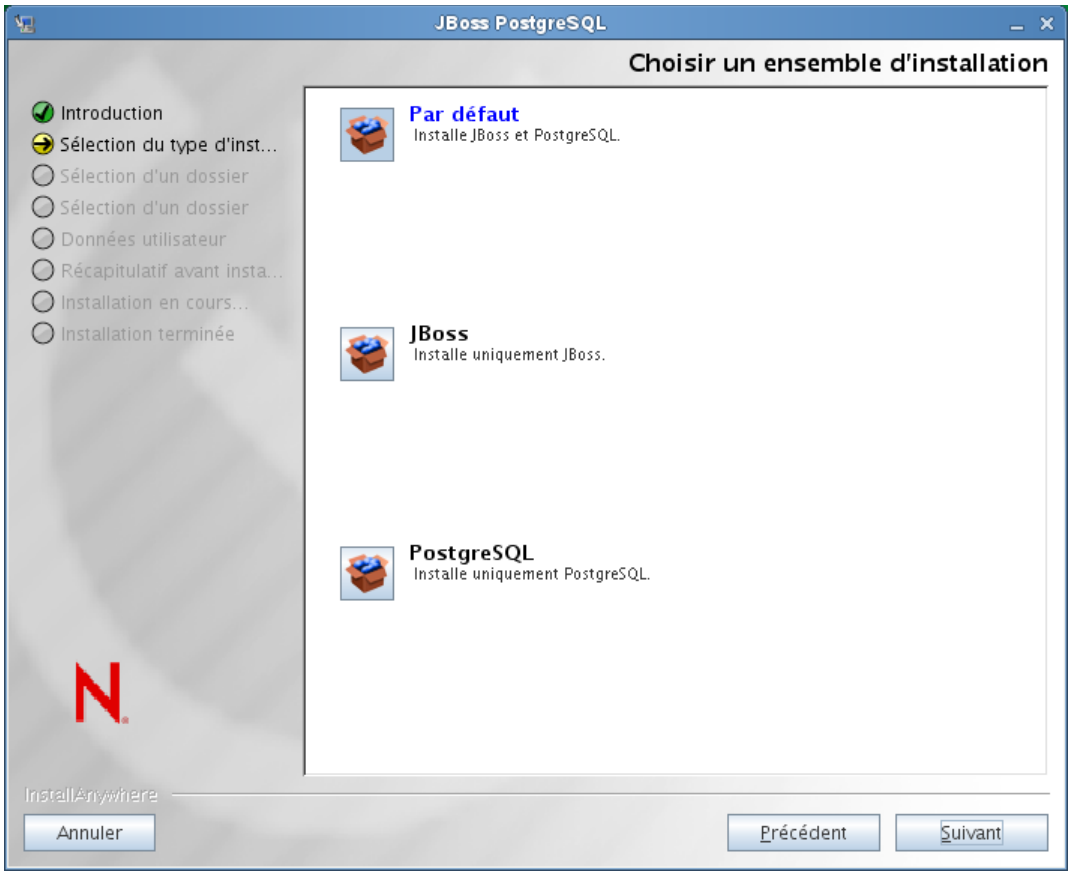
Cet utilitaire n'est pas disponible avec Solaris.

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

L'écran d'introduction s'affiche ensuite :

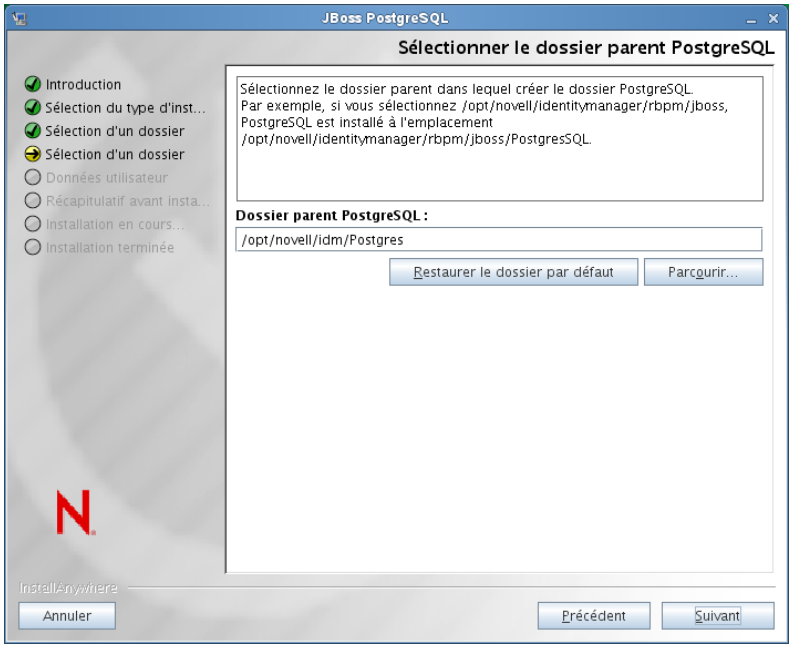


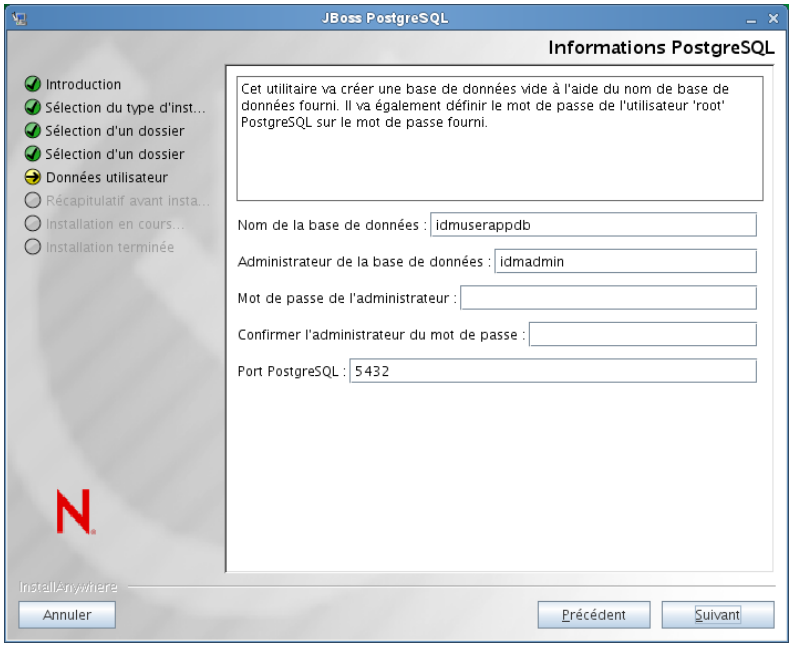
Si vous cliquez sur Suivant, l'écran *Choisir un ensemble d'installation* s'affiche :



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	Choisissez les produits à installer. ◆ *Par défaut :* installe JBoss et PostgreSQL dans le répertoire que vous indiquez, ainsi que les scripts permettant de les démarrer et de les arrêter. ◆ *JBoss* : installe le serveur d'applications JBoss dans le répertoire que vous indiquez, ainsi que les scripts permettant de le démarrer et de l'arrêter. **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 25. ◆ *PostgreSQL* : installe PostgreSQL et crée une base de données PostgreSQL dans le répertoire que vous indiquez, ainsi que les scripts de démarrage et d'arrêt.

Écran d'installation	Description
Sélectionnez le dossier parent JBoss	Cliquez sur *Sélectionner* pour choisir un dossier d'installation autre que le dossier par défaut. 
Sélectionnez le dossier parent PostgreSQL	Cliquez sur *Sélectionner* pour choisir un autre dossier d'installation que celui par défaut. 

Écran d'installation	Description
Informations PostgreSQL	Saisissez les informations suivantes : ◆ *Nom de base de données* : 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. Il est donc préférable de le noter, de même que l'emplacement. La base de données par défaut est `idmadmin`. ◆ *Administrateur de la base de données* : utilisateur chargé de l'administration de la base de données. L'administrateur par défaut est `idmuserappdb`. ◆ *Mot de passe de l'administrateur* : mot de passe de l'administrateur de la base de données. ◆ *Confirmer le mot de passe de l'administrateur* : confirmation du mot de passe. ◆ *Port PostgreSQL* : port d'écoute du serveur de la base de données PostgreSQL. 
Résumé de la pré-installation	Consultez la page Résumé. Si les indications sont correctes, cliquez sur *Installer.*

Écran d'installation	Description
Installation terminée	L'utilitaire affiche un message dès qu'il a fini d'installer les produits que vous avez sélectionnés : `The Installer has completed successfully.  Thank you for choosing Novell` **Le programme d'installation crée l'utilisateur novlua.** Le programme d'installation crée un nouvel utilisateur dont le nom est novlua. Le script jboss_init exécute JBoss sous l'identité de cet utilisateur et les autorisations définies dans les fichiers JBoss sont configurées pour ce dernier. **Important :** notez que l'utilitaire JBossPostgreSQL 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

Sous Linux, JBoss démarre en tant que service par défaut. Un script nommé /etc/init.d/jboss_init start/stop est installé pour lancer JBoss au redémarrage du système.

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://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 12 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 12 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 29.

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 requiert certaines options de configuration pour MySQL (voir ci-dessous).

- « Moteur de stockage et types de tables INNODB » page 27
- « Ensemble de caractères » page 27
- « Distinction de la casse » page 27
- « Paramètre Ansi » page 27
- « Conditions relatives au compte utilisateur » page 28

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. 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 celui de l'URL JDBC dans le fichier `IDM-ds.xml`, comme dans l'exemple suivant :

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

Vous devez ajouter l'entrée `ansi` à votre fichier my.cnf (sous Linux) ou my.ini (sous 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).)

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

Lorsque vous utilisez DB2, un message d'erreur indiquant que la transaction en cours a été annulée du fait d'un blocage ou d'un timeout peut apparaître. Il 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_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 JBossPostgreSQL installe la version appropriée du JRE pour JBoss.

- 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 lors de l'installation de l'application utilisateur pour remplacer JAVA_HOME.

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

Installation du module de provisioning basé sur les rôles

3

Cette section décrit la procédure d'installation des composants d'exécution du module de provisioning basé sur les rôles (RBPM) dans Identity Manager à l'aide du programme d'installation du module RBPM. Les rubriques sont les suivantes :

- Section 3.1, « À propos de l'installation du module de provisioning basé sur les rôles », page 33
- Section 3.2, « Exécution de l'utilitaire NrfCaseUpdate », page 34
- Section 3.3, « Exécution du programme d'installation du module RBPM », page 40
- Section 3.4, « Extension manuelle du schéma », page 46

Important : cette version ne permet plus de créer le pilote de l'application utilisateur ni le pilote du service de rôles et de ressources via iManager. Cette méthode de création des pilotes n'est plus prise en charge. Pour créer ces pilotes, vous devez désormais utiliser les nouvelles fonctions de gestion des paquetages fournies par Designer, comme décrit au Chapitre 4, « Création des pilotes », page 49.

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

Identity Manager 4.0 installe automatiquement les composants d'exécution fondamentaux du module RBPM. Toutefois, vous pouvez aussi lancer séparément le programme d'installation du module de provisioning basé sur les rôles.

Le programme d'installation du module RBPM doit être exécuté sur la machine sur laquelle votre environnement de méta-annuaire Identity Manager est installé. Si eDirectory n'est pas installé à l'emplacement par défaut ou à l'emplacement dib par défaut, l'installation échoue.

Remarque : si eDirectory ne s'exécute pas sur les ports LDAP par défaut, à savoir 389 et 636, le programme d'installation du module RBPM ne s'exécute pas correctement. Si vous n'utilisez pas les ports LDAP par défaut, des messages s'affichent pour vous indiquer que le schéma n'est pas valide et que vous devez exécuter l'utilitaire NrfCaseUpdate. Pour résoudre ce problème, vous devez étendre le schéma manuellement, comme décrit à la Section 3.4, « Extension manuelle du schéma », page 46.

Une fois que ces éléments sont installés dans Identity Manager, suivez la procédure décrite au Chapitre 4, « Création des pilotes », page 49 afin de créer les pilotes nécessaires à l'exécution de l'application utilisateur.

Important : si votre arborescence eDirectory contient un pilote d'application utilisateur créé sous RBPM 3.6.1 ou une version antérieure, vous devez exécuter l'utilitaire NrfCaseUpdate avant le programme d'installation du module de provisioning basé sur les rôles. Dans le cas contraire, l'installation échouera. Cette étape n'est pas nécessaire si vous procédez à une nouvelle installation de la version 4.0 ou à une mise à niveau depuis la version 3.7.

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 34
- Section 3.2.2, « Présentation de l'installation », page 34
- Section 3.2.3, « Conséquences de l'utilitaire NrfCaseUpdate sur le schéma », page 35
- Section 3.2.4, « Création d'une sauvegarde des pilotes d'application utilisateur », page 35
- Section 3.2.5, « Utilisation de NrfCaseUpdate », page 35
- Section 3.2.6, « Vérification du processus NrfCaseUpdate », page 38
- Section 3.2.7, « Activation du JRE pour les connexions SSL », page 38
- Section 3.2.8, « Restauration des pilotes d'application utilisateur invalidés », page 39

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 nrfLocalizedDescrs et nrfLocalizedNames, qui sont utilisés par les pilotes de l'application utilisateur. Si votre arborescence eDirectory a été créée sous RBPM 3.6.1 ou une version antérieure, cette procédure est nécessaire avant l'installation de RBPM 4.0 ou la migration de pilotes existants vers Designer 4.0. Cette étape n'est pas nécessaire si vous procédez à une nouvelle installation de la version 4.0 ou à une mise à niveau depuis la version 3.7.

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 4.0 pour la création de sauvegardes des pilotes de l'application utilisateur avant de procéder à n'importe quelle mise à niveau. Elle part également du principe que la version d'IDM utilisée est 3.6 ou une version ultérieure.

1. Installez Designer 4.0.
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 4.0.
4. Archivez le projet Designer. Il correspond à l'état du pilote avant l'installation de RBPM 4.0.
5. Exécutez le processus NrfCaseUpdate.
6. Créez un projet Designer 4.0 et importez le pilote d'application utilisateur à préparer pour la migration.
7. Installez RBPM 4.0.
8. Migrez le pilote à l'aide de Designer 4.0.
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 4.0 (fourni avec RBPM 4.0).
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 38.

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. Vous pouvez éventuellement utiliser la commande `-v` pour afficher des résultats plus détaillés :

   ```
   /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 36.

   ```
   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 38.

    ```
    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):
    ```

Si le DN contient un espace, il doit être délimité par des guillemets simples, comme dans l'exemple ci-dessous :

```
'cn=UserApplication driver,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 -DLDAP -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 38.

20 Une fois que vous avez vérifié que le processus NrfCaseUpdate a abouti, vous pouvez procéder à l'installation de RBPM 4.0.

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 4.0.

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 du pilote d'application utilisateur à l'aide de Designer 4.0 :

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 4.0 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 38 pour vérifier la restauration du pilote.

15 Supprimez le pilote renommé de l'ensemble de pilotes.

3.3 Exécution du programme d'installation du module RBPM

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

Linux

```
rbpm_driver_install_linux.bin
```

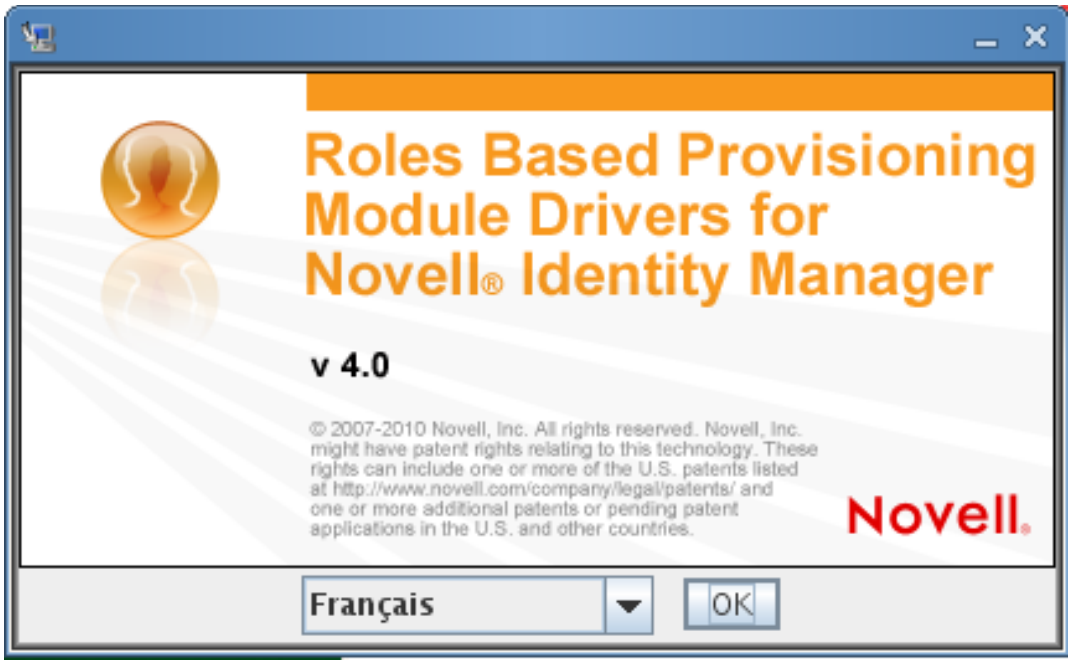
Solaris

```
rbpm_driver_install_solaris.bin
```

Windows

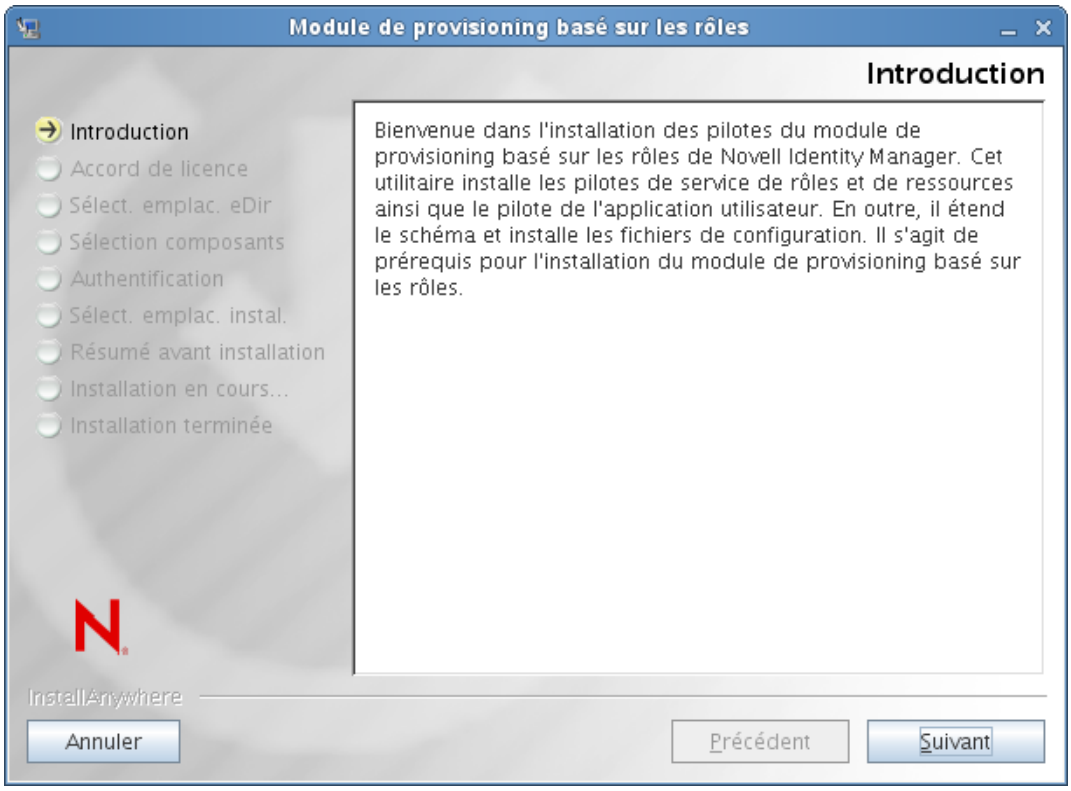
```
rbpm_driver_install.exe
```

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



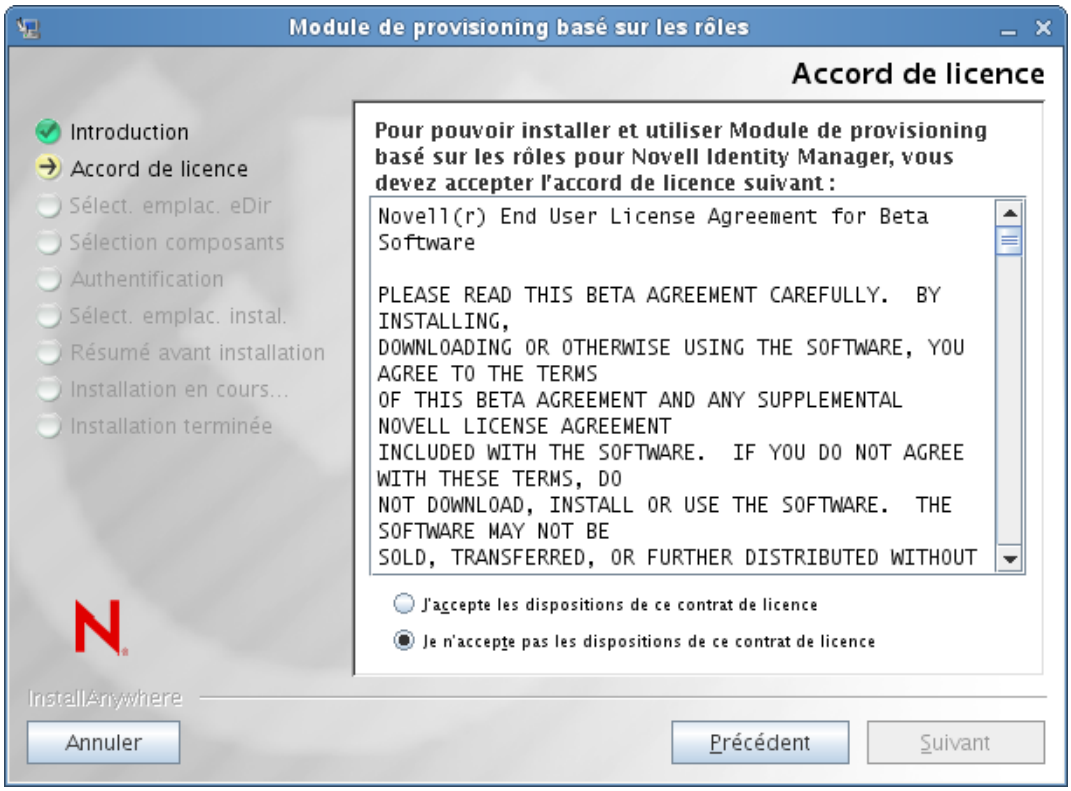
2 Sélectionnez la langue d'installation, puis cliquez sur OK.

Le programme d'installation affiche l'écran Introduction.



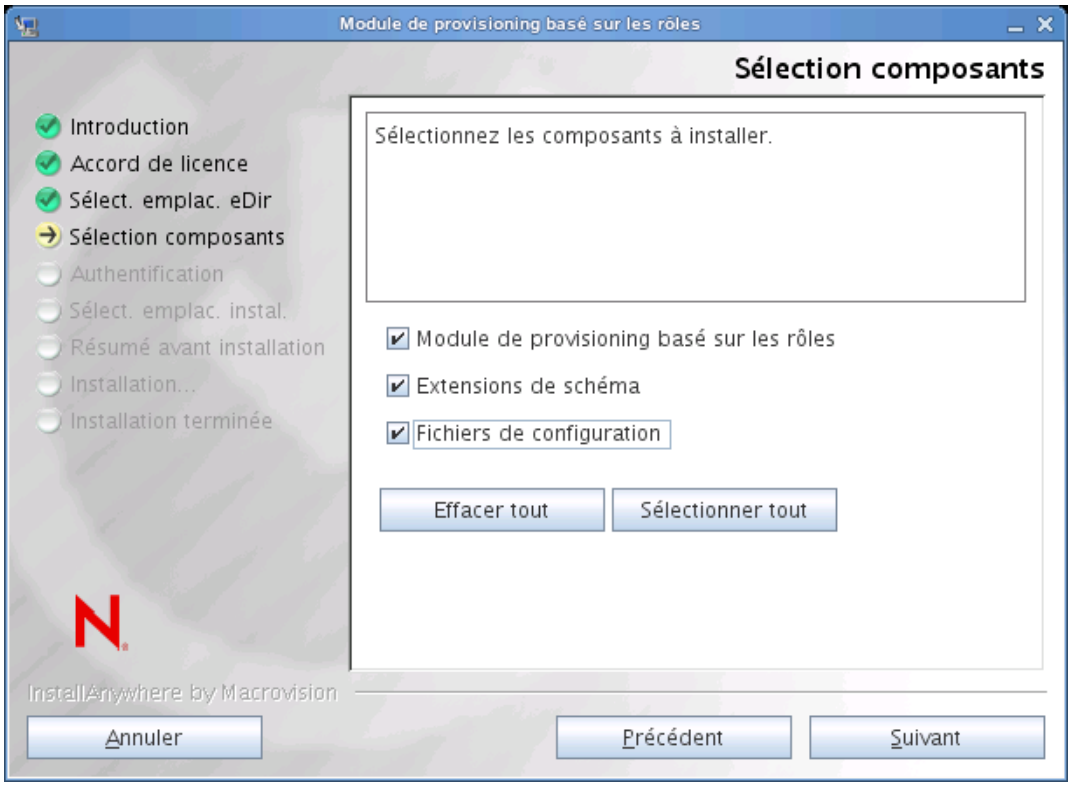
3 Cliquez sur *Suivant*.

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 :

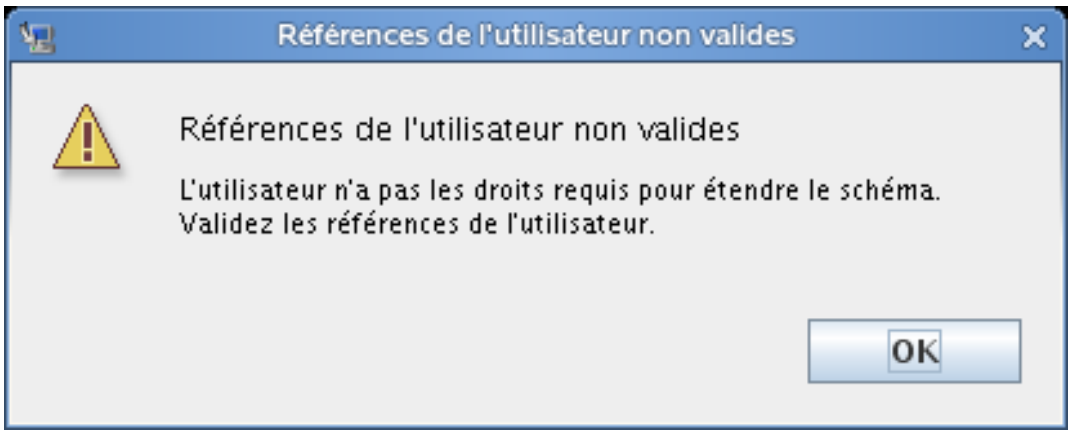
Composant	Description
Module de provisioning basé sur les rôles	Installe le pilote d'application utilisateur et le pilote de rôles et de ressources.
Extensions de schéma	Installe les extensions de schéma eDirectory.
Fichiers de configuration	Installe les fichiers de configuration des pilotes.

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

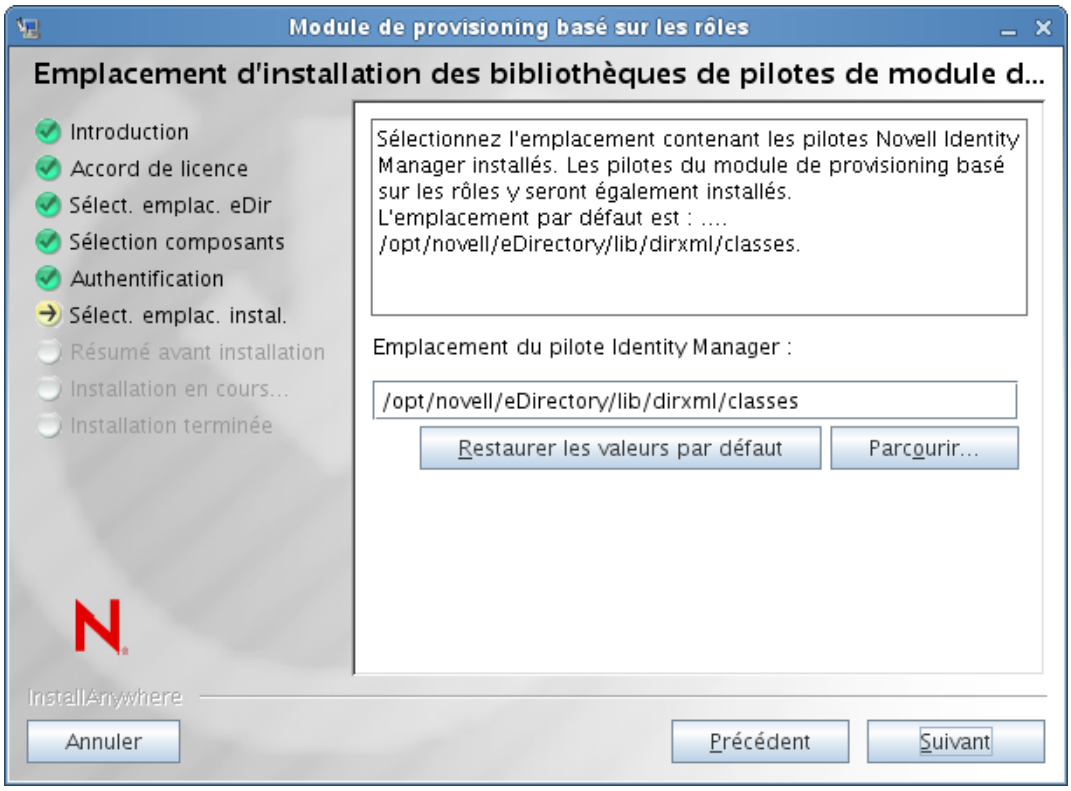
Le programme d'installation affiche l'écran Authentification :

6 Indiquez le nom de l'administrateur au format LDAP et saisissez son mot de passe. Spécifiez également le port du serveur LDAP.

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

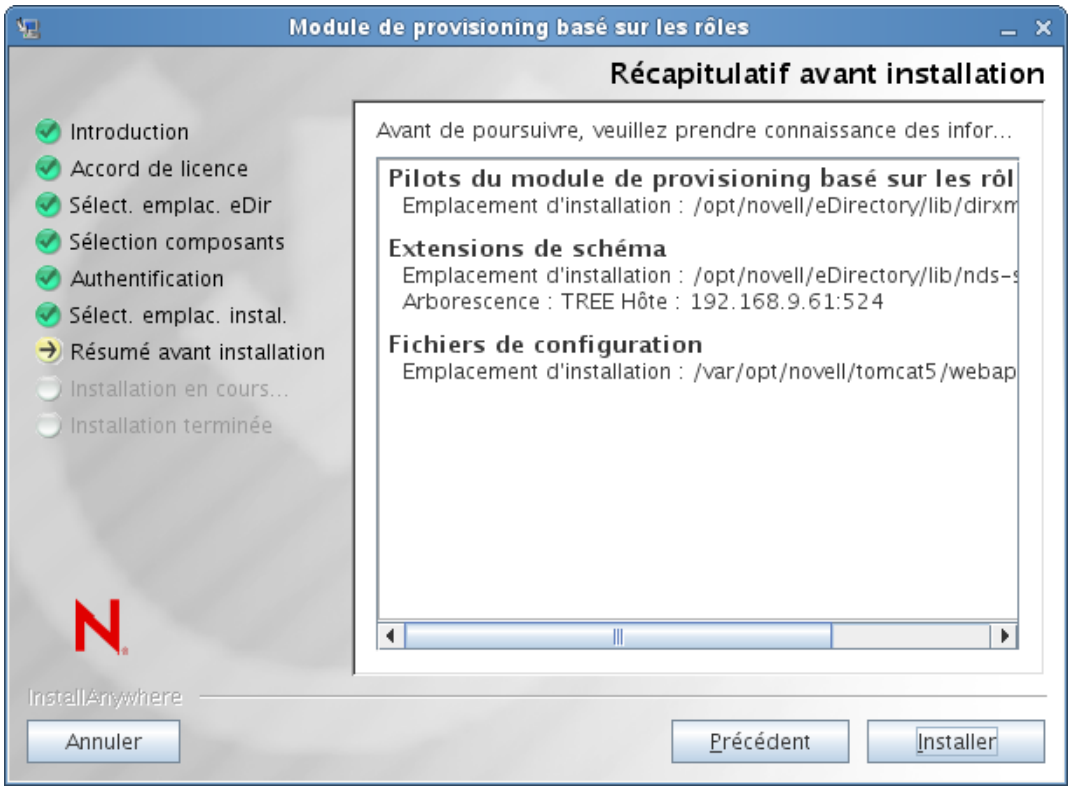


Si l'utilisateur dispose de références valides et de droits appropriés, le programme d'installation affiche l'écran Emplacement d'installation des bibliothèques de pilotes de module de provisioning basé sur les rôles :

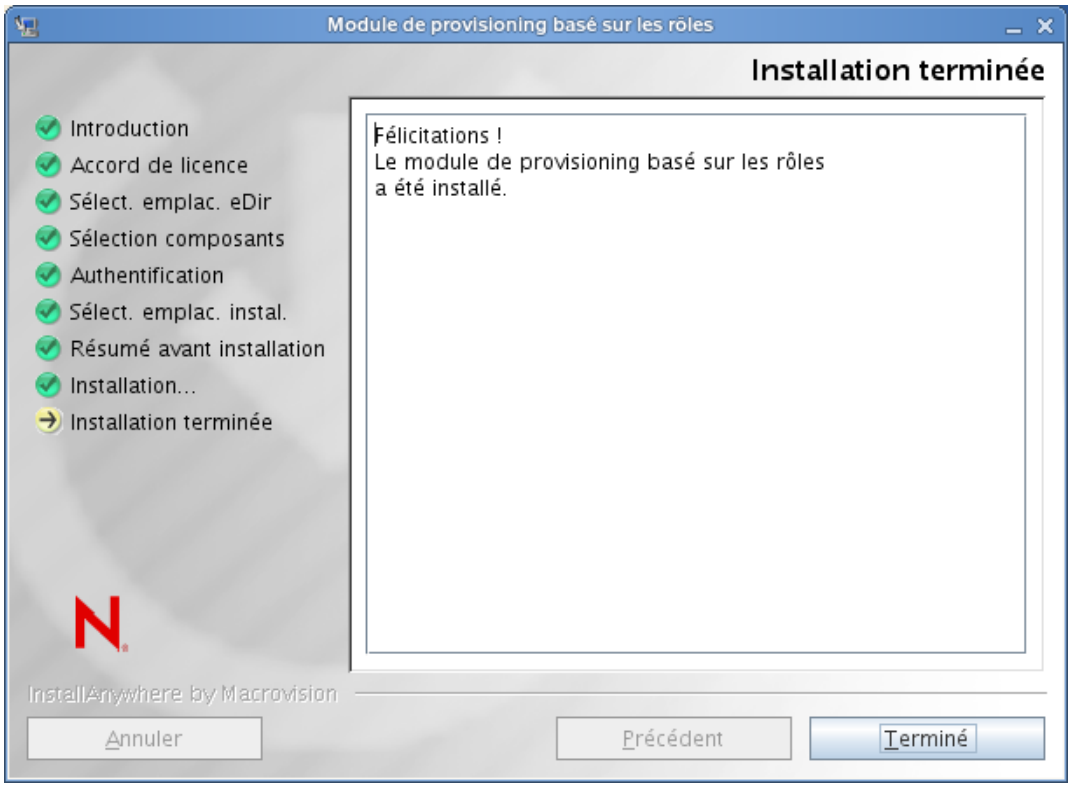


7 Indiquez l'emplacement cible sur le disque pour le stockage des bibliothèques de pilotes, puis cliquez sur *Suivant*.

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



8 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 :



Remarque : si vous devez désinstaller les composants d'exécution associés à RBPM, le programme de désinstallation redémarre automatiquement votre serveur, à moins que vous n'exécutiez le programme de désinstallation en mode silencieux sous Windows. Dans ce cas, vous devez redémarrer manuellement votre machine Windows. En outre, si vous souhaitez désinstaller Identity Manager en dehors du programme d'installation intégré, vous devez arrêter le service NDS avant de lancer le programme de désinstallation.

3.4 Extension manuelle du schéma

Cette section explique comment étendre le schéma manuellement. La procédure ci-dessous ne doit être utilisée que pour résoudre les problèmes qui surviennent lorsqu'eDirectory n'est pas installé à l'emplacement par défaut ou ne s'exécute pas sur les ports LDAP par défaut, à savoir les ports 389 et 636.

Pour étendre le schéma manuellement (Windows) :

1. Après l'installation d'Identity Manager, arrêtez eDirectory.
2. Exécutez la commande suivante pour étendre les schémas listés dans le fichier `sch_nt.cfg` situé dans le répertoire d'installation d'eDirectory.

   ```
   <eDirLocation>\schemaStart.bat <eDirLocation> yes <admin name with tree>
   <password> yes 6 " " " <schemafileName>"
   "<serverName>" <dibPathLocation>
   ```

   Remarque : <*chemin_emplacement_dib*> doit contenir le dossier DIBFiles.

   Voici un exemple de commande :

   ```
   C:\eDir\NDS\schemaStart.bat "C:\eDir\NDS" yes
   ".cn=admin.o=n.T=IDM-INSTALLISSUE." "n" yes 6 " "
   "C:\eDir\NDS\ vrschema.sch" ".CN=WIN2008-64-NDS.O=n.T=IDMINSTALLISSUE."
   "C:\DIB\NDS\DIBFiles"
   ```

   Remarque : la commande ci-dessus n'utilise pas le fichier sch_nt.cfg pour étendre tous les fichiers de schéma, mais étend manuellement chacun des fichiers de schéma listés dans le fichier sch_nt.cfg.

3. Installez le pilote de rôles et de ressources (comme décrit à la Section 3.3, « Exécution du programme d'installation du module RBPM », page 40), en désélectionnant la case *Extensions de schéma* dans la fenêtre *Sélection composants*. Terminez l'installation.
4. Après avoir installé le pilote de rôles et de ressources, étendez les fichiers de schéma basés sur les rôles `srvprv.sch` et `nrf-extensions.sch` en exécutant la commande mentionnée à l'Étape 2 page 46.

   Remarque : cette procédure étend les fichiers de schéma nécessaires à l'aide du fichier `schemaStart.bat`. Cette méthode est légèrement différente de celle décrite dans le *Fichier Lisez-moi du méta-annuaire IDM 3.6.1*.

5. Étendez le schéma NrfCaseupdate (`update-nrf-case.sch`) à l'aide de la commande mentionnée à l'Étape 2 page 46.
6. Démarrez eDirectory.

Pour étendre le schéma manuellement (SUSE) :

1. Installez le pilote de rôles et de ressources (comme décrit à la Section 3.3, « Exécution du programme d'installation du module RBPM », page 40), en décochant la case *Extensions de schéma* dans la fenêtre *Sélection composants*. Cliquez sur *Suivant*.
2. Choisissez un emplacement d'installation approprié pour le pilote, puis cliquez sur *Suivant*.
3. Choisissez un emplacement d'installation approprié pour les fichiers de configuration de pilote, puis cliquez sur *Suivant*. Terminez l'installation.

   Les étapes 1 à 3 permettent de copier le pilote et les fichiers de configuration de pilote à autre un emplacement dans eDirectory que celui par défaut.
4. Exécutez la commande `ndssch` pour étendre le schéma (à savoir `srvprv.sch` ou `nrf-extensions.sch`).

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

   Par exemple :

   ```
   ndssch -h 172.16.1.137:524 -t TESTTREE -p 'PASSWORD'
   .cn=admin.o=novell.T=TESTTREE.
   /opt/novell/eDirectory/lib/nds-schema/srvprv.sch'
   ```
5. Répétez l'étape 4 pour étendre le schéma `nrf-extensions.sch`.

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 des pilotes dans Designer », page 49

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.

Important : cette version ne permet plus de créer le pilote de l'application utilisateur ni le pilote du service de rôles et de ressources via iManager. Cette méthode de création des pilotes n'est plus prise en charge. Pour créer ces pilotes, vous devez désormais utiliser les nouvelles fonctions de gestion des paquetages fournies par Designer, comme décrit ci-dessous.

4.1 Création des pilotes dans Designer

Cette section explique comment créer les pilotes dans Designer. Les rubriques sont les suivantes :

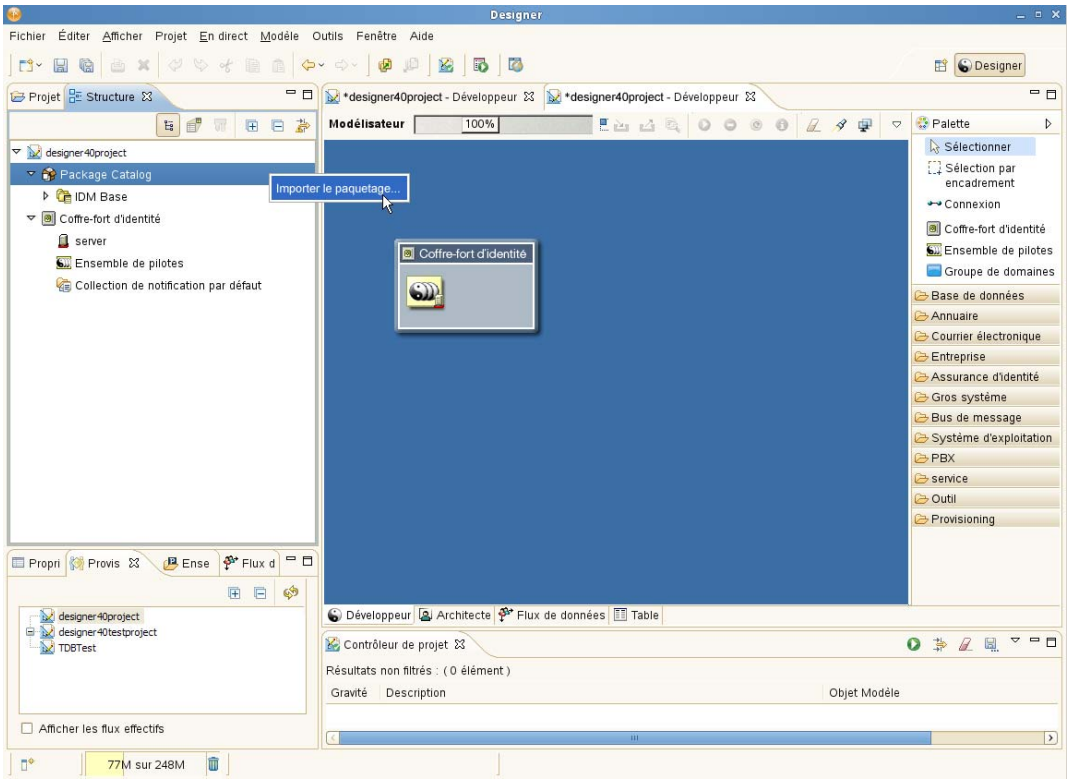
- Section 4.1.1, « Installation des paquetages », page 49
- Section 4.1.2, « Création du pilote d'application utilisateur dans Designer », page 51
- Section 4.1.3, « Création du pilote du service de rôles et de ressources dans Designer », page 55
- Section 4.1.4, « Déploiement des pilotes », page 57

4.1.1 Installation des paquetages

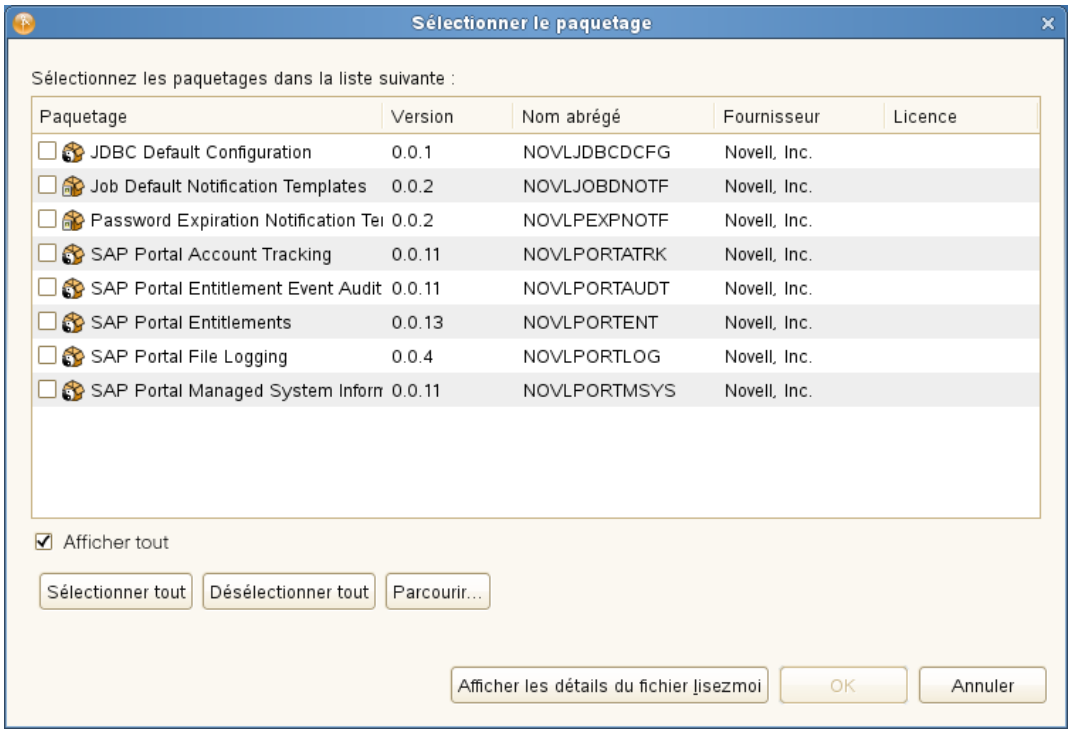
Avant toute tentative de configuration des pilotes, assurez-vous que vous disposez bien de tous les paquetages nécessaires dans le catalogue de paquetages. Lors de la création d'un nouveau projet Identity Manager, l'interface utilisateur vous invite automatiquement à importer plusieurs paquetages dans le nouveau projet. Si vous décidez de ne pas les importer à ce moment-là, vous devrez les installer par la suite, comme décrit ci-dessous.

Pour installer les paquetages après avoir créé un nouveau projet Identity Manager :

1. Après avoir créé un nouveau projet Identity Manager dans Designer, sélectionnez le *catalogue de paquetages*, puis cliquez sur *Importer le paquetage*.



Designer affiche la boîte de dialogue *Sélectionner le paquetage* :



2 Cliquez sur *Sélectionner tout*, puis sur *OK*.

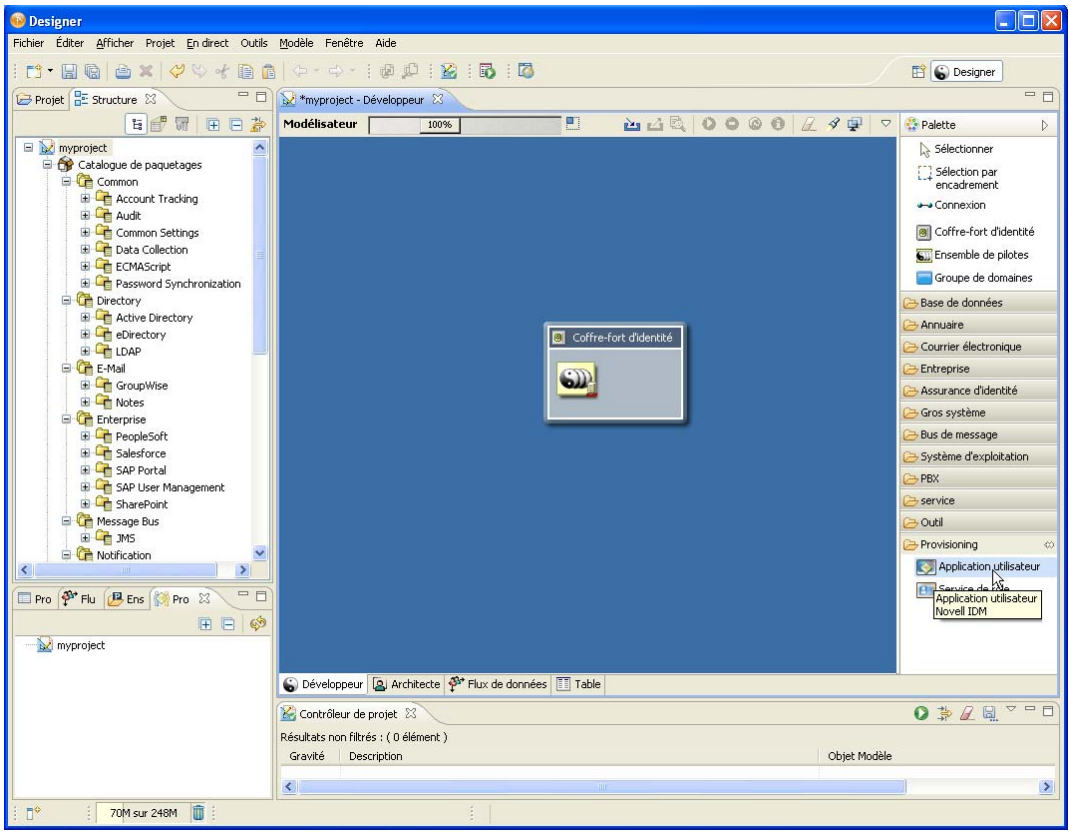
Designer ajoute plusieurs nouveaux dossiers de paquetage sous le *catalogue de paquetages*. Ces dossiers correspondent aux objets de la palette située à droite de la vue *Modélisateur* dans Designer.

3 Cliquez sur *Enregistrer* pour enregistrer votre projet.

4.1.2 Création du pilote d'application utilisateur dans Designer

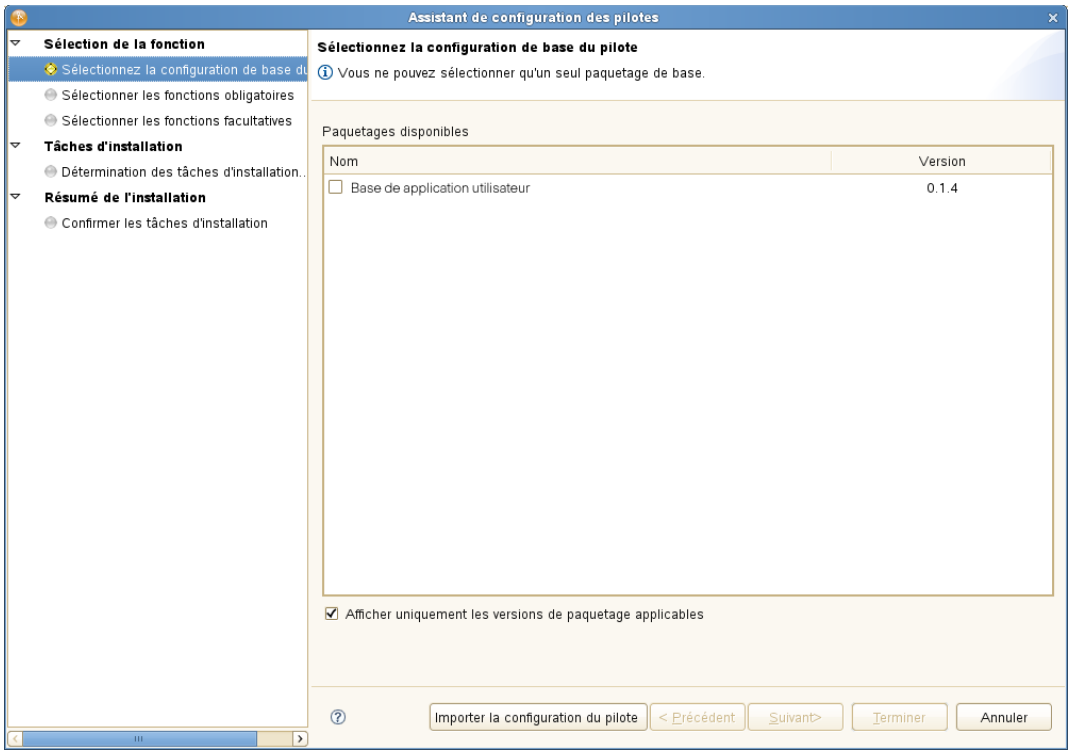
Pour créer le pilote d'application utilisateur dans Designer :

1 Sélectionnez *Application utilisateur* dans la palette de la vue *Modélisateur* :

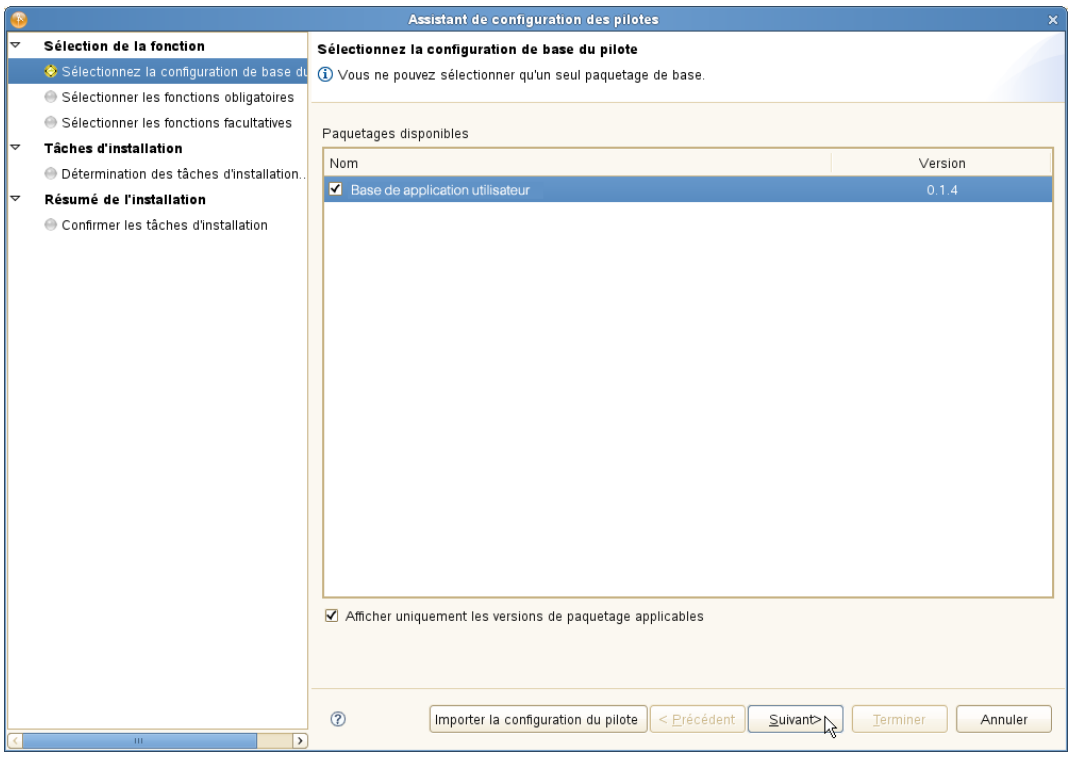


2 Faites glisser l'icône de l'*application utilisateur* dans la vue *Modélisateur*.

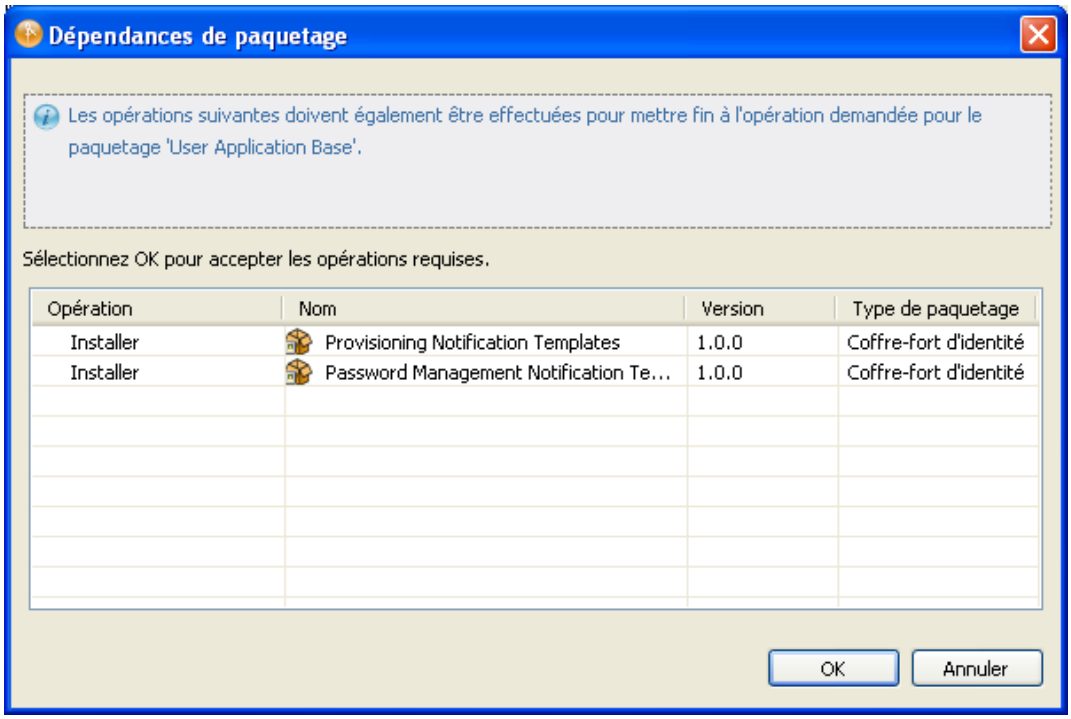
Designer affiche l'*assistant de configuration du pilote* :



3 Cochez la case *Base de l'application utilisateur*, puis cliquez sur *Suivant* :



L'interface affiche une boîte de dialogue pour vous indiquer que plusieurs paquetages supplémentaires sont requis :



4 Cliquez sur *OK* pour installer les paquetages requis.

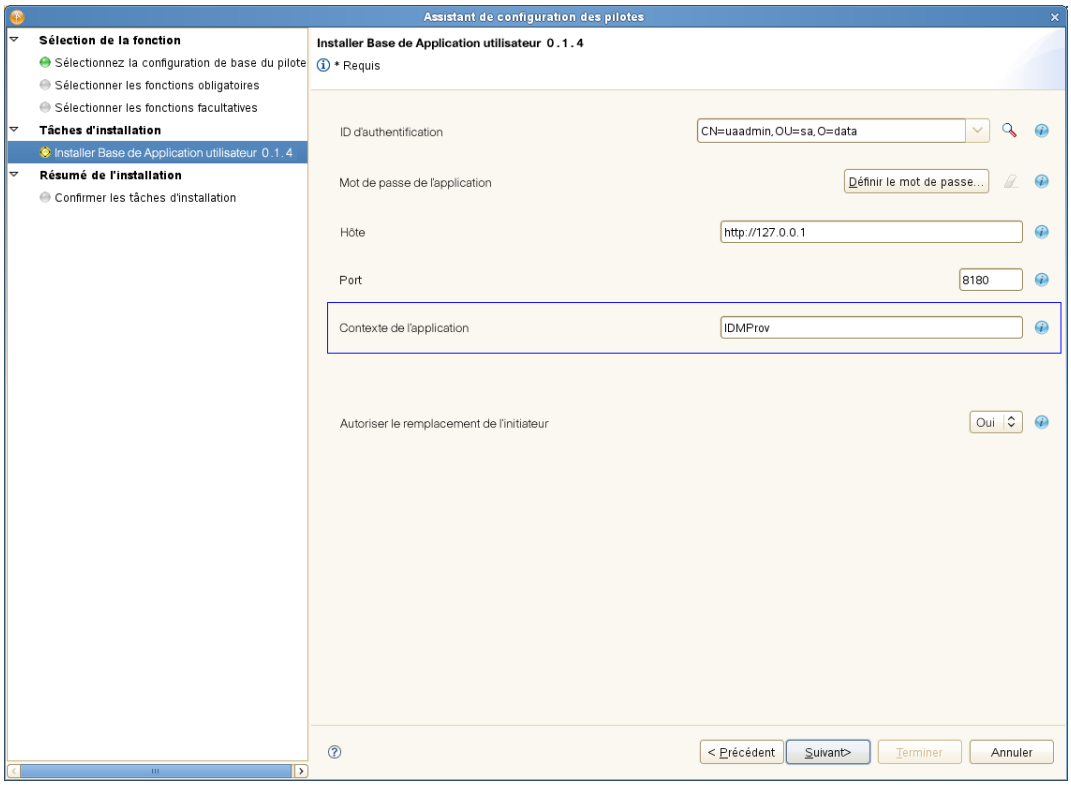
L'assistant affiche alors un écran dans lequel vous pouvez définir le nom du pilote.

5 Vous pouvez accepter le nom de pilote par défaut ou le modifier si vous le souhaitez.

Cliquez sur *Suivant*.

L'assistant affiche ensuite un écran dans lequel vous pouvez spécifier les paramètres de connexion du pilote.

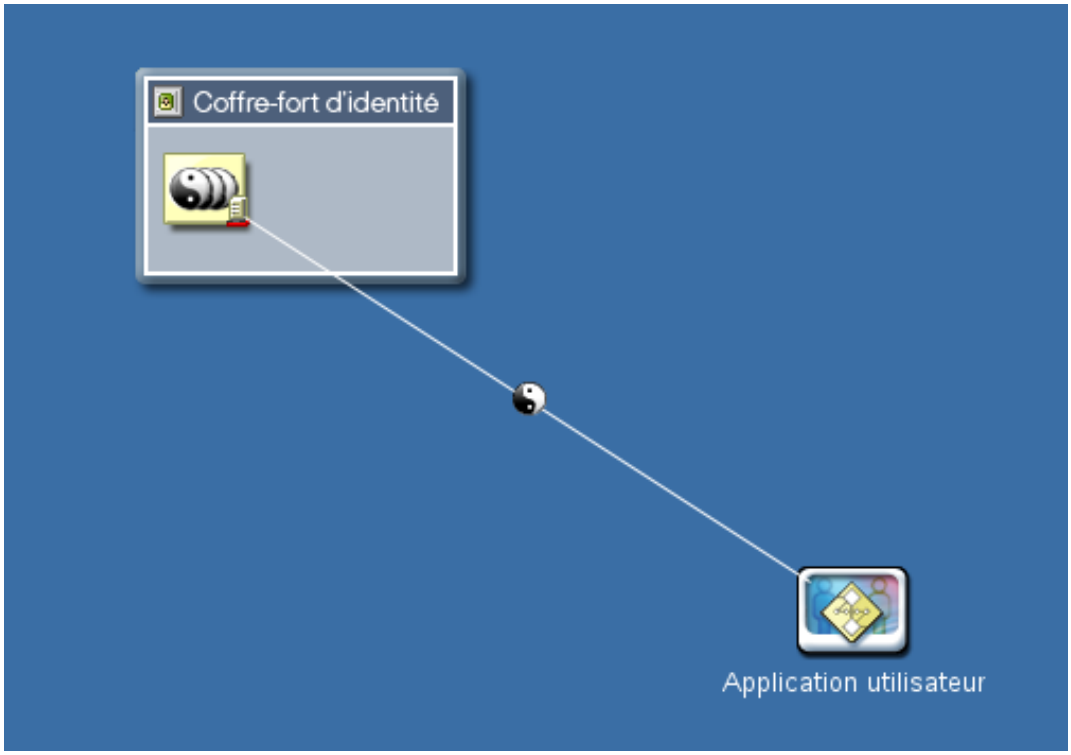
6 Indiquez l'ID et le mot de passe de l'administrateur de l'application utilisateur, ainsi que l'hôte, le port et le contexte d'application du serveur de l'application utilisateur. Si vous souhaitez autoriser l'administrateur du provisioning à démarrer des workflows au nom d'une personne pour qui il a été désigné proxy, définissez le paramètre *Autoriser le remplacement de l'initiateur* sur *Oui* :



L'assistant affiche alors l'écran *Confirmer les tâches d'installation*.

7 Si tout semble correct, cliquez sur *Terminer*.

Designer ajoute le pilote *Application utilisateur* à la vue *Modélisateur* :



4.1.3 Création du pilote du service de rôles et de ressources dans Designer

Pour créer le pilote du service de rôles et de ressources dans Designer :

1. Sélectionnez *Service de rôle* dans la palette de la vue *Modélisateur* :

2. Faites glisser l'icône du *service de rôle* dans la vue *Modélisateur*.

   Designer affiche l'*assistant de configuration du pilote*.

3. Cochez la case *Base de service de rôles et de ressources*, puis cliquez sur *Suivant*.

   L'assistant affiche un écran dans lequel vous pouvez définir le nom du pilote.

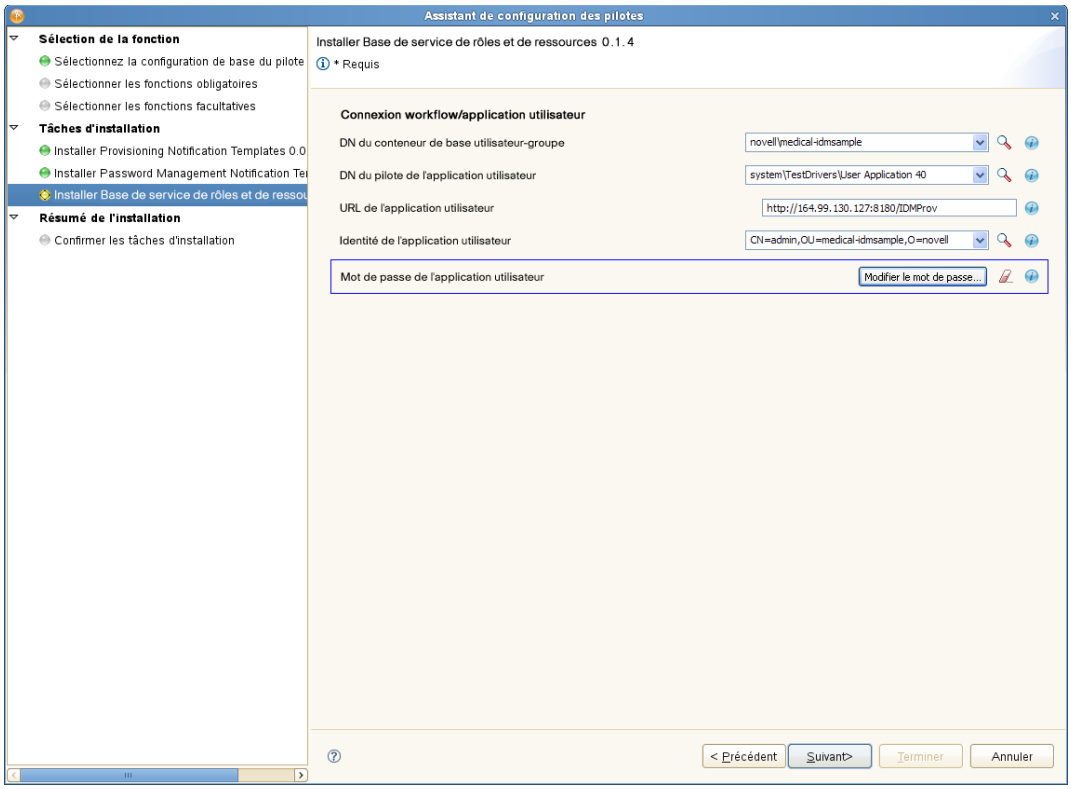
4. Vous pouvez accepter le nom de pilote par défaut ou le modifier si vous le souhaitez.

   Cliquez sur *Suivant*.

   L'assistant affiche ensuite un écran dans lequel vous pouvez spécifier les paramètres de connexion du pilote.

5. Spécifiez le DN du conteneur de base et du pilote d'application utilisateur que vous venez de créer. Étant donné que le pilote n'a pas encore été déployé, la fonction Parcourir n'affiche pas le pilote d'application utilisateur que vous venez de créer. Il se peut donc que vous deviez saisir le DN du pilote.

   Indiquez également l'URL de l'application utilisateur, ainsi que l'ID et le mot de passe de l'administrateur de l'application utilisateur :

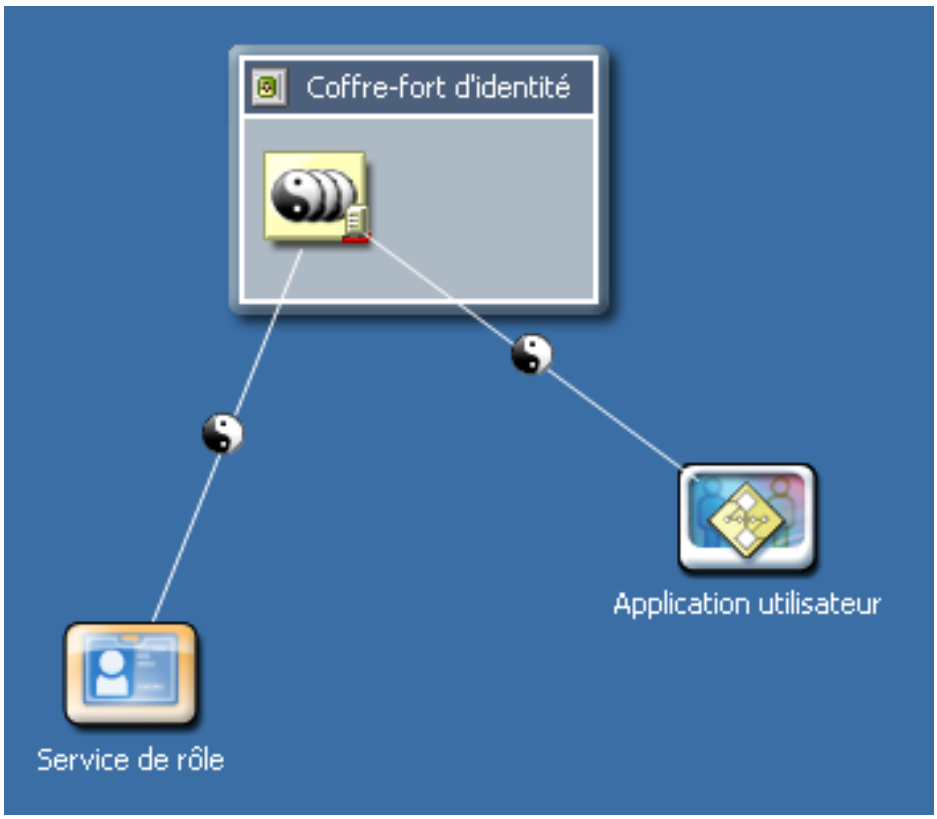


Cliquez sur *Suivant*.

L'assistant affiche alors l'écran *Confirmer les tâches d'installation*.

6 Si tout semble correct, cliquez sur *Terminer*.

Designer ajoute le pilote *Service de rôle* à la vue *Modélisateur* :

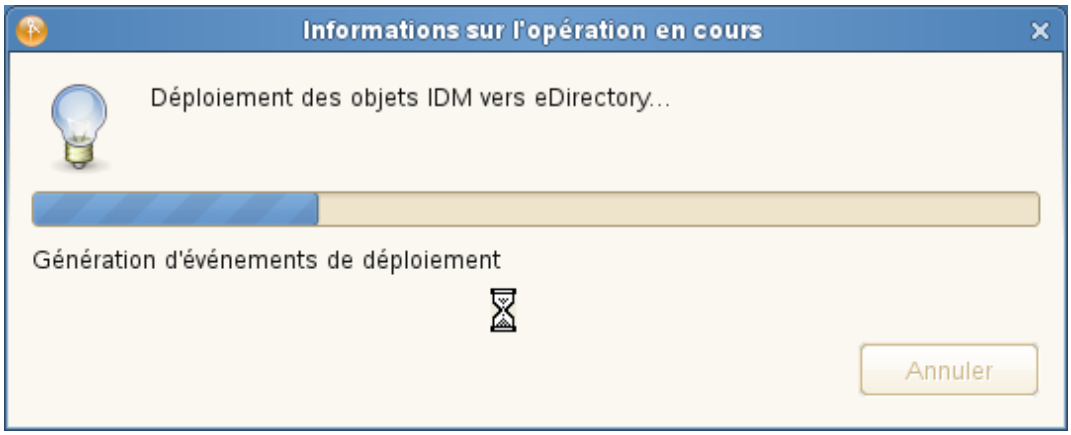


4.1.4 Déploiement des pilotes

Pour déployer les pilotes que vous venez de configurer :

1. Sélectionnez l'ensemble de pilotes (soit dans la vue *Modélisateur*, soit dans la vue *Aperçu*).
2. Sélectionnez *En direct* > *Déployer*.

   Designer affiche une fenêtre de progression montrant les objets en cours de déploiement :



Une fois le processus de déploiement terminé, vous pouvez démarrer les pilotes dans iManager.

Remarque : lorsque vous répliquez un environnement eDirectory, vous devez vous assurer que les répliques contiennent bien l'objet Serveur NCP pour Identity Manager. Identity Manager est limité aux répliques locales d'un serveur. Pour cette raison, le pilote de service de rôles et de ressources risque de ne pas démarrer correctement si l'objet Serveur est manquant sur un serveur secondaire.

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 59
- Section 5.2, « Tester l'installation », page 79

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 133.

Exécutez le programme d'installation en tant qu'utilisateur root. Vous devez exécuter le programme d'installation en tant qu'utilisateur root.

Migration de données. Pour en savoir plus sur la migration, reportez-vous au manuel *User Application: Migration Guide* (http://www.novell.com/documentation/idm40/index.html) (Guide de migration de l'application utilisateur).

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

---

Remarque : pour JBoss 5.1.0, 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 :

Assurez-vous d'utiliser la bonne version du JRE Sun (comme décrit à la Section 1.3, « Configuration système requise », page 12) avant de lancer le programme d'installation de l'application utilisateur. Si vous avez utilisé l'utilitaire JBossPostgreSQL fourni avec le module de provisioning basé sur les rôles pour installer le JRE, vous pouvez utiliser la commande suivante pour lancer le programme d'installation.

Linux/Solaris

```
$ /opt/novell/jre/bin/java -jar IdmUserApp.jar
```

Windows

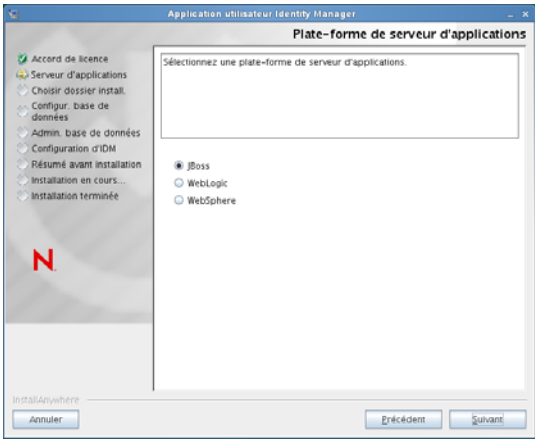
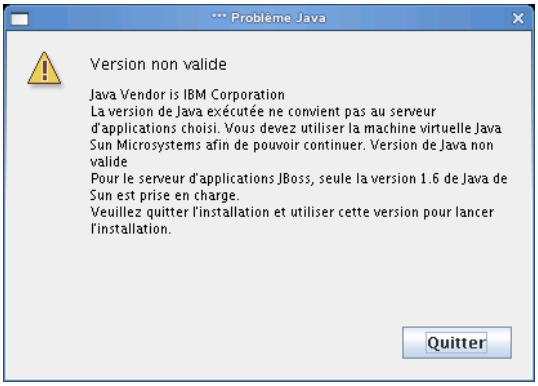
```
C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.6.0_14\bin\java.exe"
-jar IdmUserApp.jar
```

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.

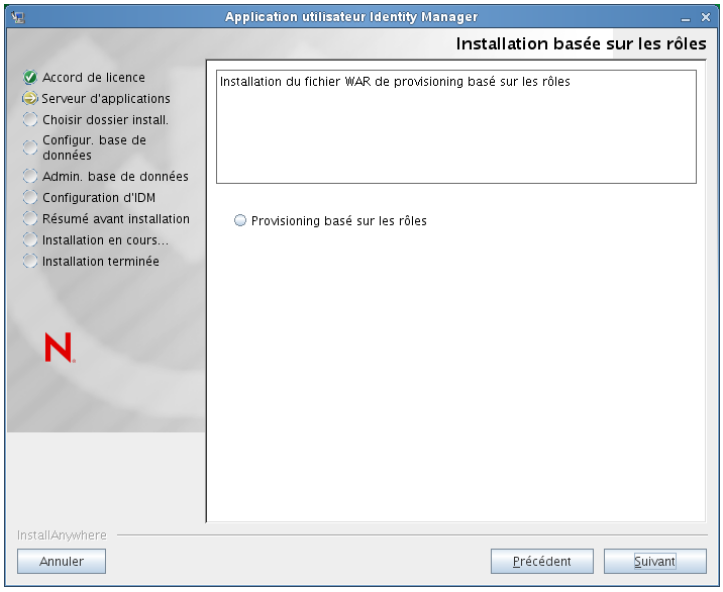
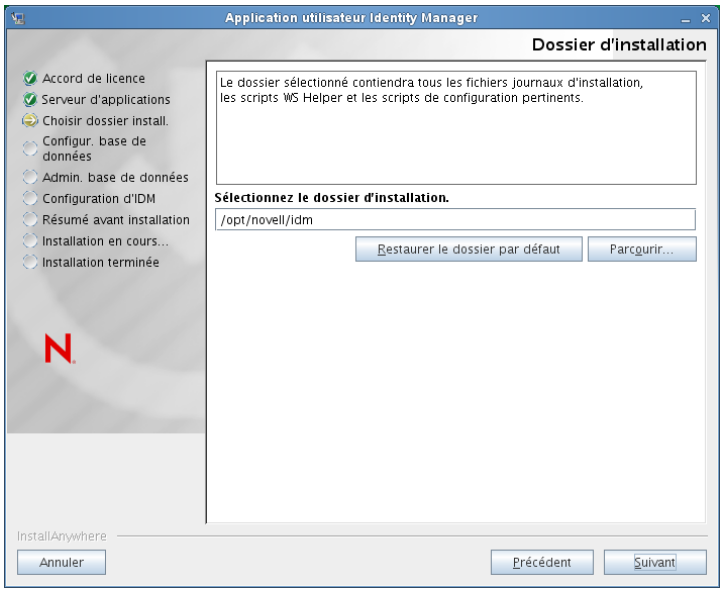
Lors du lancement du programme d'installation, vous êtes invité à choisir une langue :

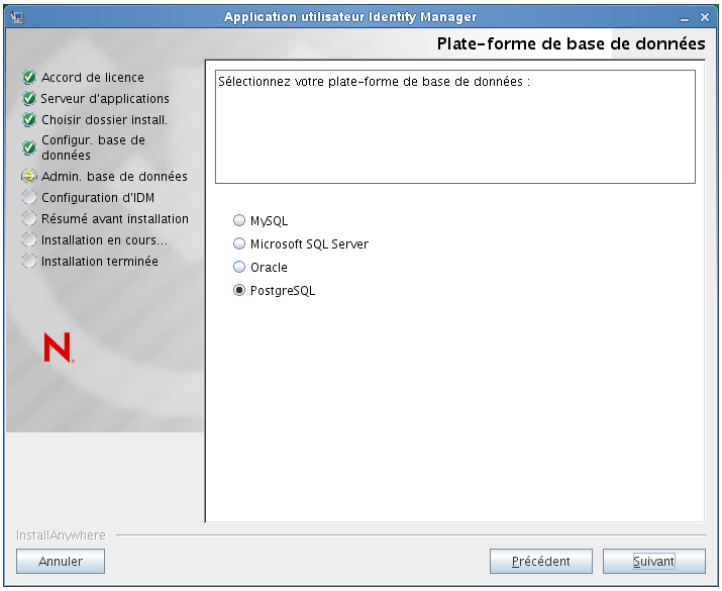
2 Utilisez les informations suivantes pour choisir la langue, confirmer l'accord de licence et sélectionner la plate-forme du serveur d'applications :

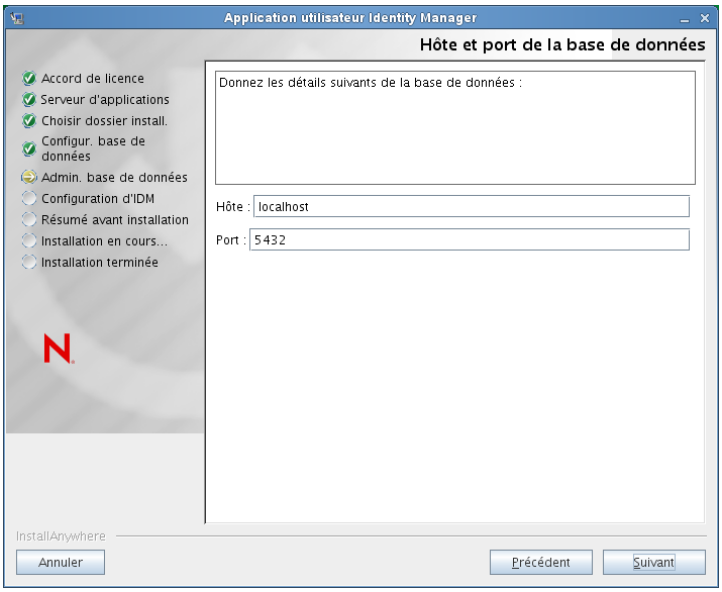
Écran d'installation	Description
Installation de l'application utilisateur	Sélectionnez la langue du programme d'installation. La valeur par défaut est Français.
Accord de licence	Lisez l'accord de licence, puis sélectionnez *J'accepte les termes de l'accord de licence*.

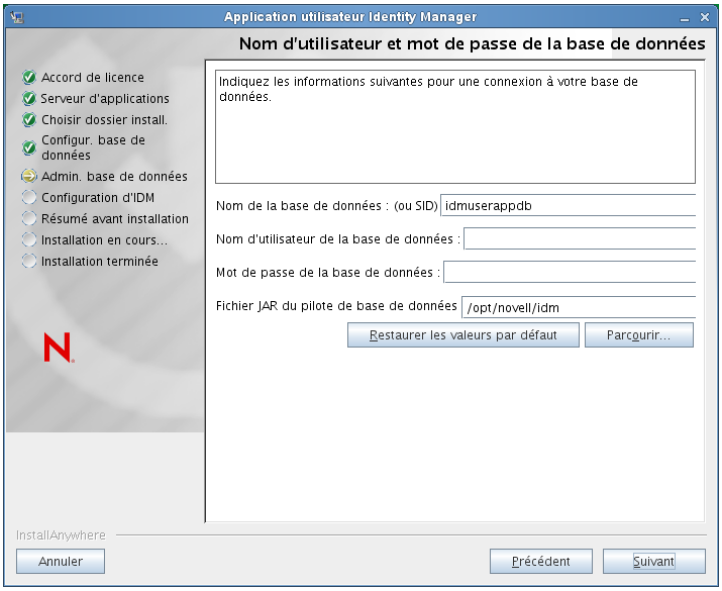
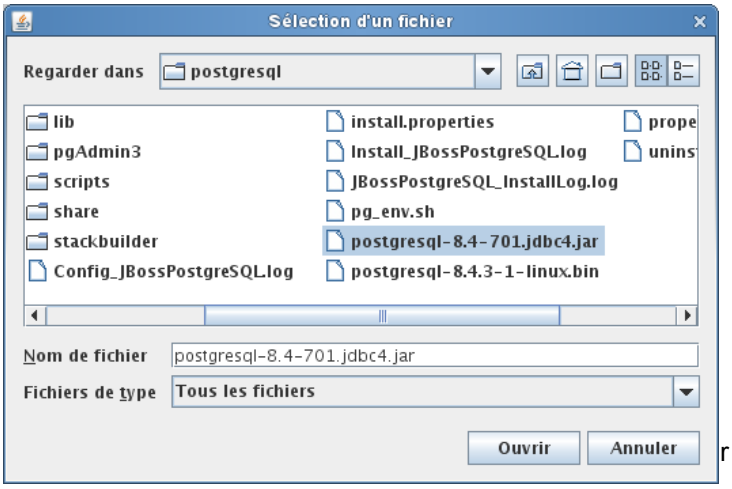
Écran d'installation	Description
Plate-forme du serveur d'applications	Sélectionnez *JBoss*.  Lorsque vous installez l'application sur JBoss, vous devez lancer le programme d'installation à partir de l'environnement Java de Sun. Si vous sélectionnez JBoss comme serveur d'applications alors que vous n'utilisez pas l'environnement Java de Sun pour lancer l'installation, vous recevez un message d'erreur et l'installation s'interrompt : 

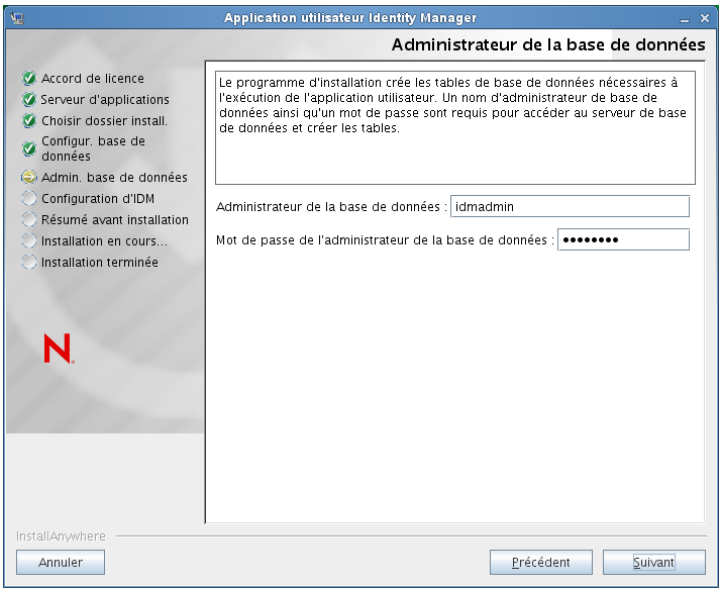
3 Aidez-vous des informations suivantes pour sélectionner le type d'installation, choisir un dossier d'installation et configurer la base de données :

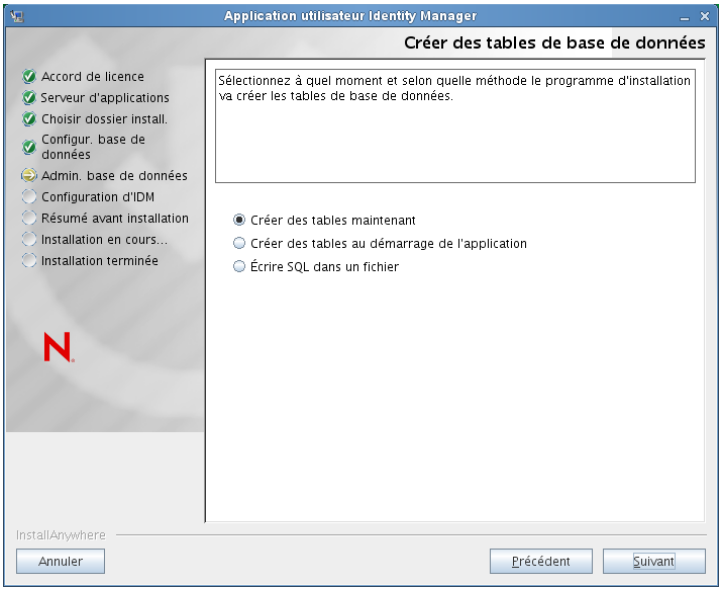
Écran d'installation	Description
Type d'installation	*Provisioning basé sur les rôles* : sélectionnez cette option pour installer le module de provisioning basé sur les rôles. Il s'agit du seul type d'installation pris en charge avec cette version. 
Sélectionnez le dossier d'installation	Indiquez l'emplacement auquel le programme d'installation doit mette les fichiers. 

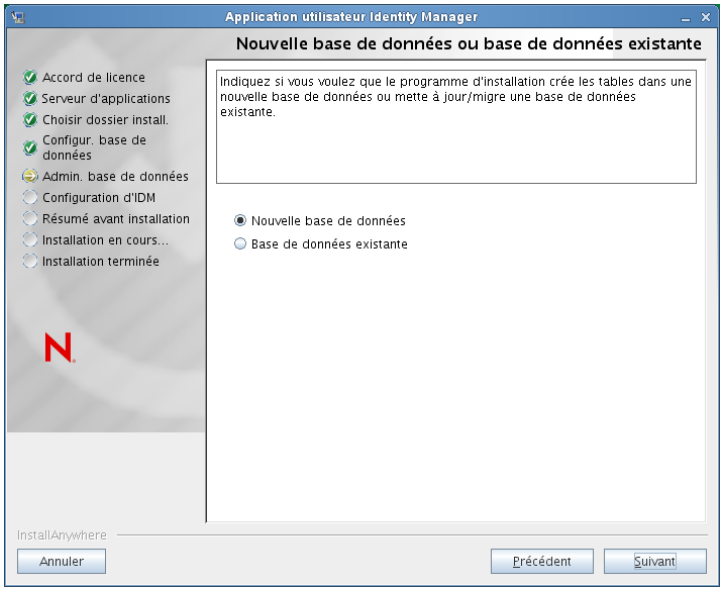
Écran d'installation	Description
Plate-forme de la base de données	Sélectionnez la plate-forme de la base de données :  Vous devez avoir installé la base de données et le pilote JDBC. Pour JBoss, les options sont les suivantes : ◆ MySQL ◆ Microsoft SQL Server ◆ Oracle ◆ PostgreSQL

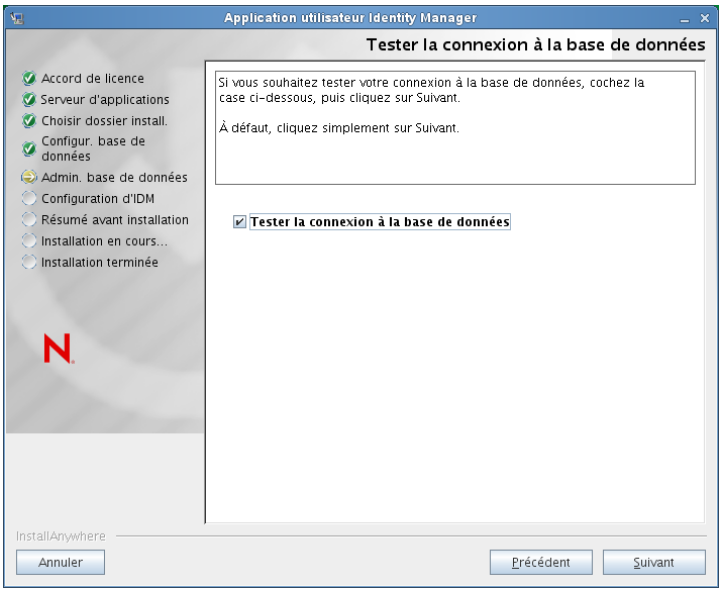
Écran d'installation	Description
Hôte et port de la base de données	*Hôte* : indiquez le nom d'hôte ou l'adresse IP du serveur de bases de données. Pour une grappe, indiquez le même nom d'hôte ou la même adresse IP pour chaque membre de la grappe. *Port* : indiquez le numéro du port d'écoute de la base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

Écran d'installation	Description
Nom d'utilisateur et mot de passe de la base de données	*Nom de la base de données* (ou identificateur système - SID) : pour PostgreSQL, MySQL ou MS SQL Server, indiquez le nom de votre base de données. Pour Oracle, indiquez l'identificateur système (SID) Oracle que vous avez créé précédemment. Pour une grappe, indiquez le même SID ou nom de base de données pour chaque membre de la grappe. Le nom de la base de données par défaut est `idmuserappdb`. *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.  Pour PostgreSQL, sélectionnez le fichier postgresql-8.4-701.jdbc4.jar : 

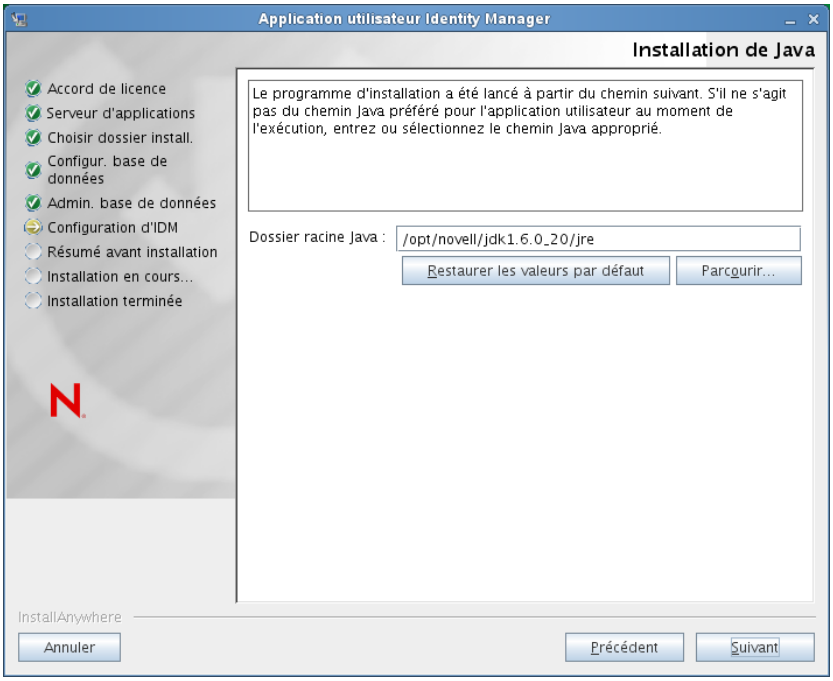
Écran d'installation	Description
Administrateur de la base de données	Cette page est préremplie avec les mêmes nom d'utilisateur et mot de passe que sur la page Nom d'utilisateur et mot de passe de la base de données. Si l'utilisateur de base de données spécifié précédemment ne possède pas les autorisations 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. 

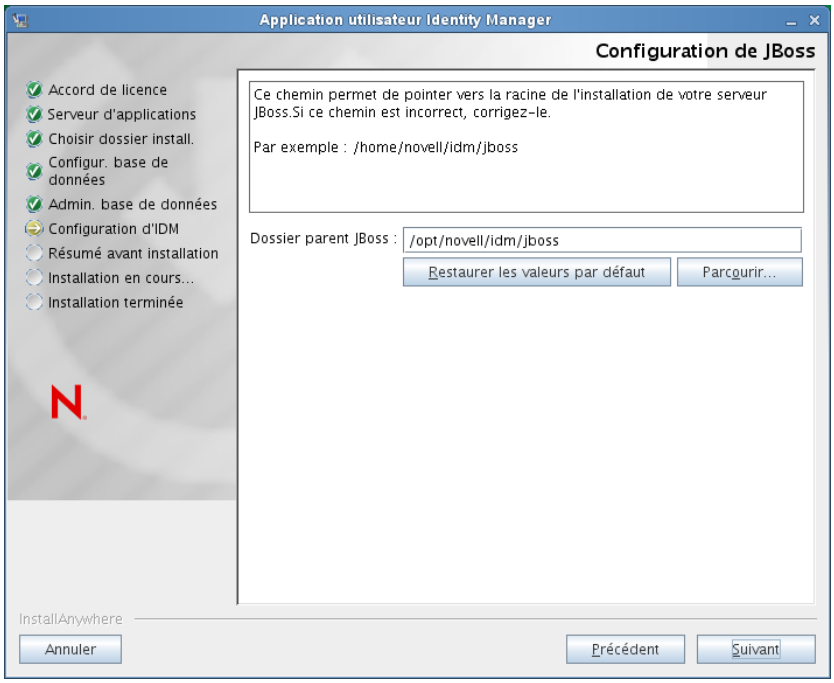
Écran d'installation	Description
Créer des tables de base de données	Indiquez le moment auquel les tables de base de données doivent être créées :  L'écran Créer des tables de base de données vous permet de créer les tables au moment de l'installation ou au démarrage de l'application. Vous pouvez également créer, lors de l'installation, un fichier de schéma que l'administrateur de la base de données utilisera ultérieurement pour créer les tables. Si vous souhaitez générer un fichier de schéma, cochez la case *Écrire SQL dans un fichier* et indiquez un nom pour le fichier dans le champ *Fichier de sortie du schéma*.

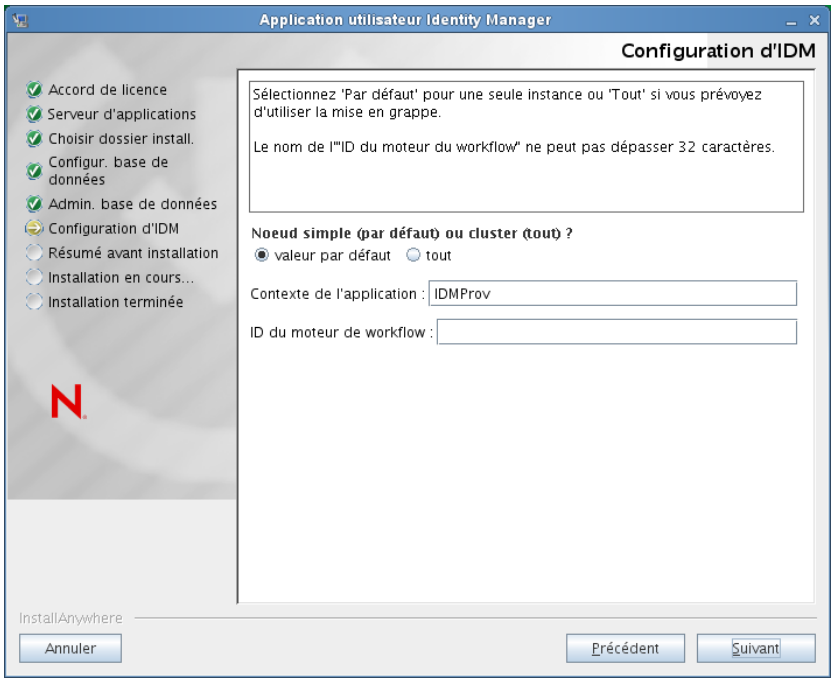
Écran d'installation	Description
Nouvelle base de données ou base de données existante	Si la base de données à utiliser est nouvelle ou vide, sélectionnez *Nouvelle base de données*. Si la base de données provient d'une installation précédente, sélectionnez *Base de données existante*. 

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 *Tester la connexion à la base de données* :  Le programme d'installation doit se connecter à la base de données pour créer les tables directement et créer le fichier .SQL. Un échec au test de connexion à la base de données permet néanmoins de poursuivre l'installation. Dans ce cas, vous devrez créer les tables après l'installation, comme décrit dans le *User Application: Administration Guide* (http://www.novell.com/documentation/idmrbpm40/agpro/?page=/documentation/idmrbpm40/agpro/data/bncf7rj.html) (Guide d'administration de l'application utilisateur).

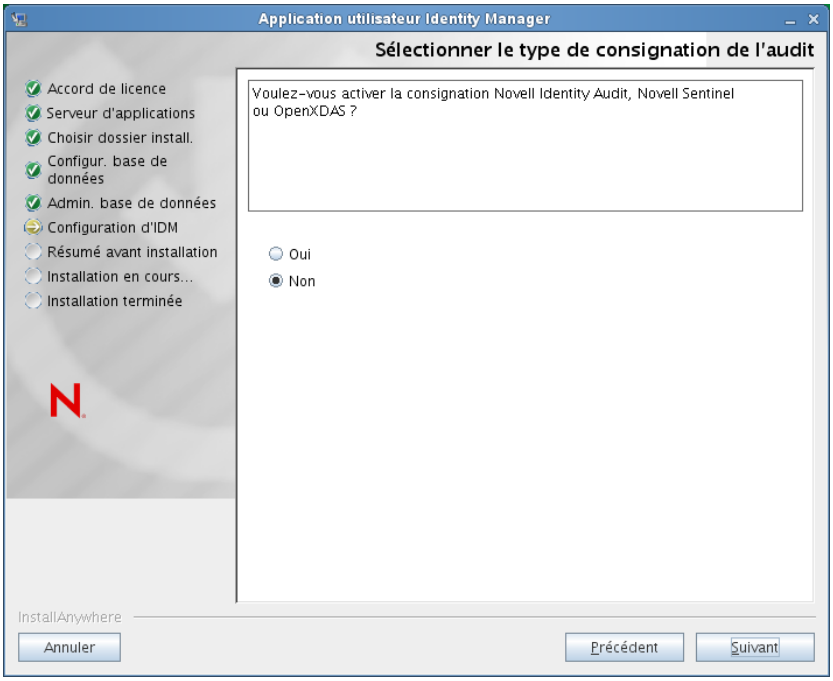
4 Aidez-vous des informations suivantes pour configurer Java, l'installation sur JBoss et IDM ainsi que les paramètres d'audit et la sécurité.

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 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 PostgreSQL » page 19. *Dossier parent JBoss* : indiquez l'emplacement du serveur d'applications JBoss. 

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. 

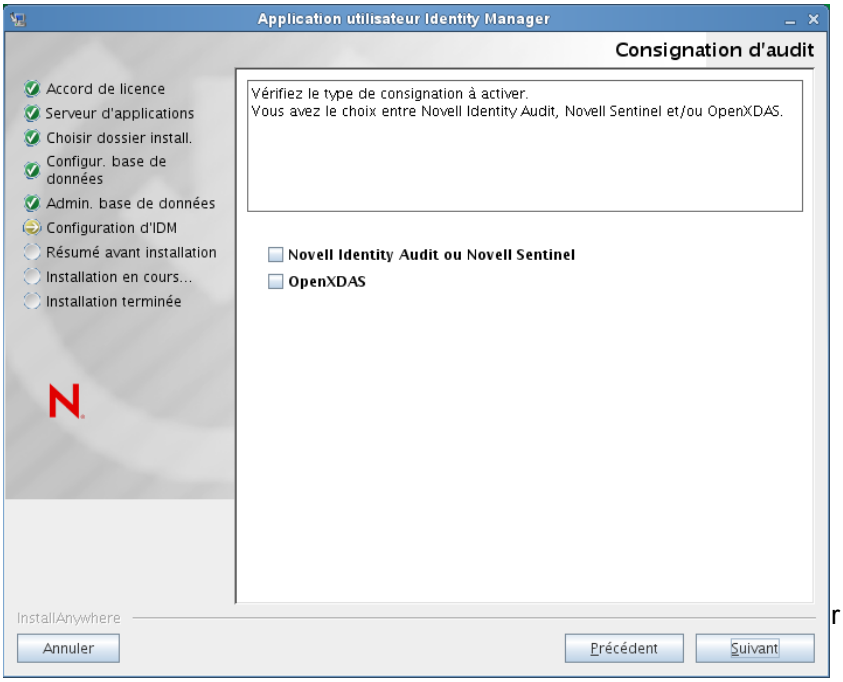
Écran d'installation	Description
Sélectionner le type de consignation de l'audit	Pour activer la consignation, cliquez sur *Oui*. Pour désactiver la consignation, cliquez sur *Non*.

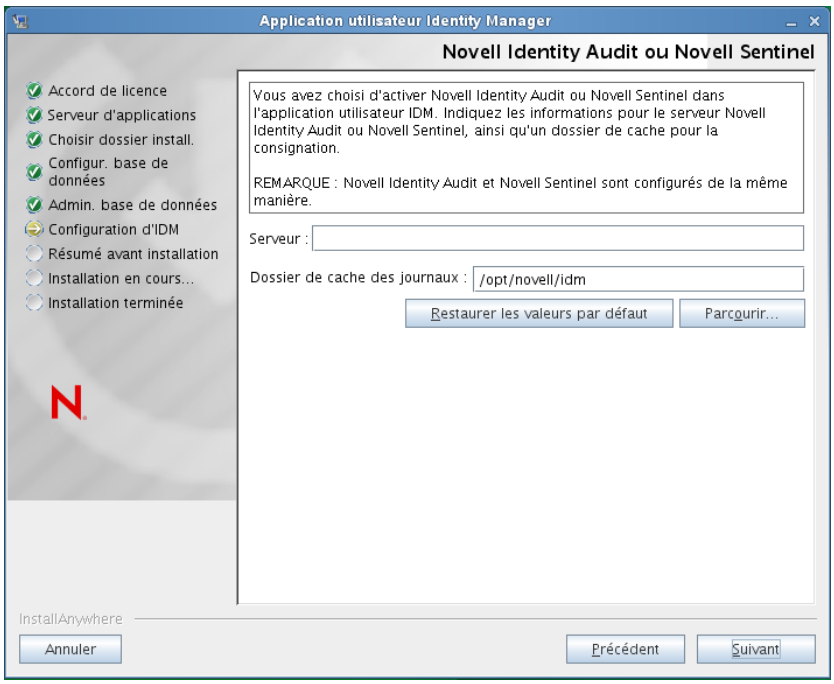


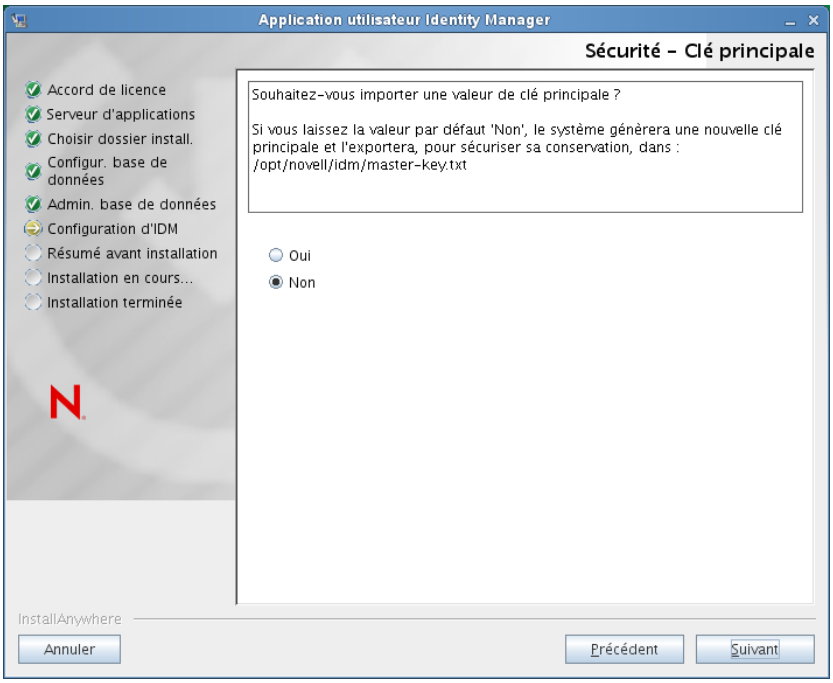
Le tableau de bord suivant vous invite à indiquer le type de consignation. Choisissez parmi les options suivantes :

- *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.

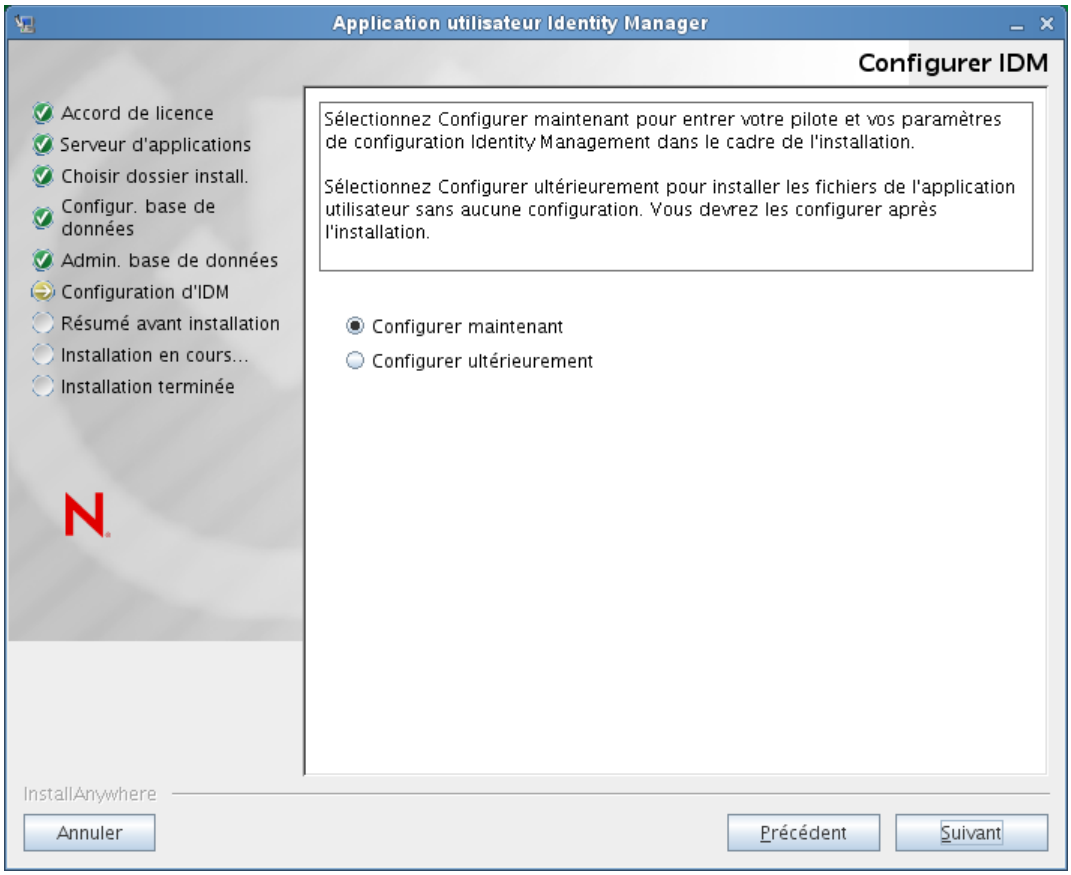
Pour plus d'informations sur la configuration de la consignation , reportez-vous au manuel *User Application: Administration Guide* (Guide d'administration de l'application utilisateur).



Écran d'installation	Description
Novell Identity Audit ou Novell Sentinel	*Serveur* : 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. *Dossier de cache des journaux* : indiquez le répertoire du cache de consignation. 

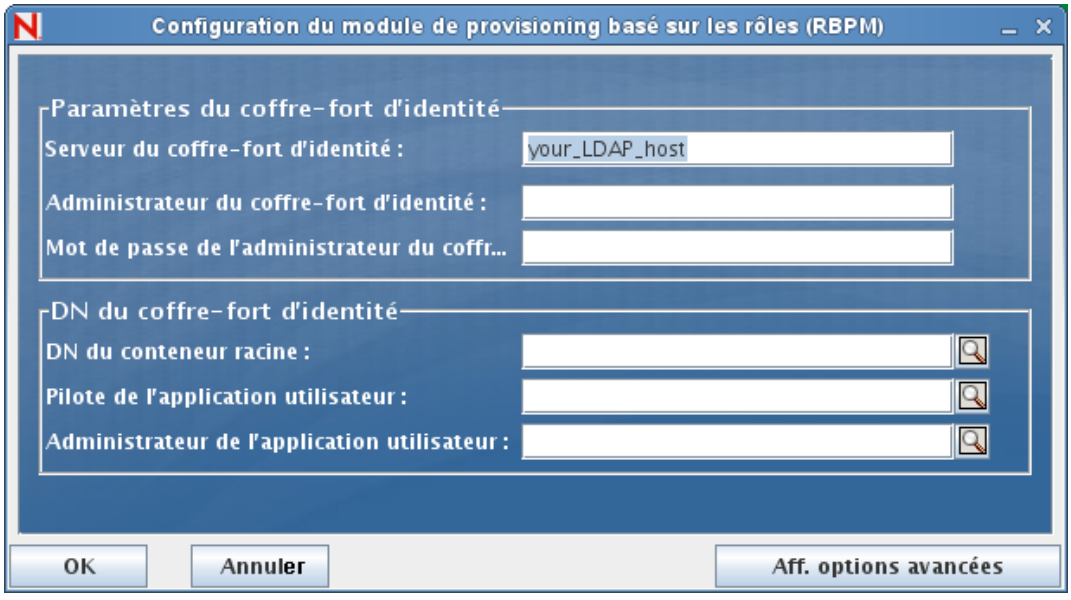
Écran d'installation	Description
Sécurité : clé principale	*Oui* : vous permet d'importer une clé principale existante. Si vous choisissez d'importer une clé maîtresse codée existante, coupez et collez la clé dans la fenêtre de procédure d'installation. *Non* : crée une clé principale. Une fois l'installation terminée, vous devez enregistrer manuellement la clé maîtresse comme décrit dans la Section 9.1, « Enregistrement de la clé maîtresse », page 149.  La procédure d'installation inscrit la clé maîtresse codée dans le fichier `master-key.txt` dans le répertoire d'installation. Voici des raisons d'importer une clé principale existante : • Vous déplacez votre installation d'un système provisoire à un système de production et vous souhaitez conserver l'accès à la base de données que vous avez utilisée avec le système provisoire. • Vous avez installé l'application utilisateur sur le premier membre d'une grappe JBoss et vous l'installez maintenant sur de nouveaux membres de la grappe (qui requièrent la même clé maîtresse). • En raison d'un disque défectueux, vous devez restaurer votre application utilisateur. Vous devez réinstaller l'application utilisateur et indiquer la même clé maîtresse codée que celle qu'utilisait l'installation précédente. Cela vous donne accès aux données codées stockées précédemment.

5 Si vous souhaitez configurer le module RBPM maintenant, sélectionnez *Configurer maintenant*, puis cliquez sur *Suivant*.



(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 32.)

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



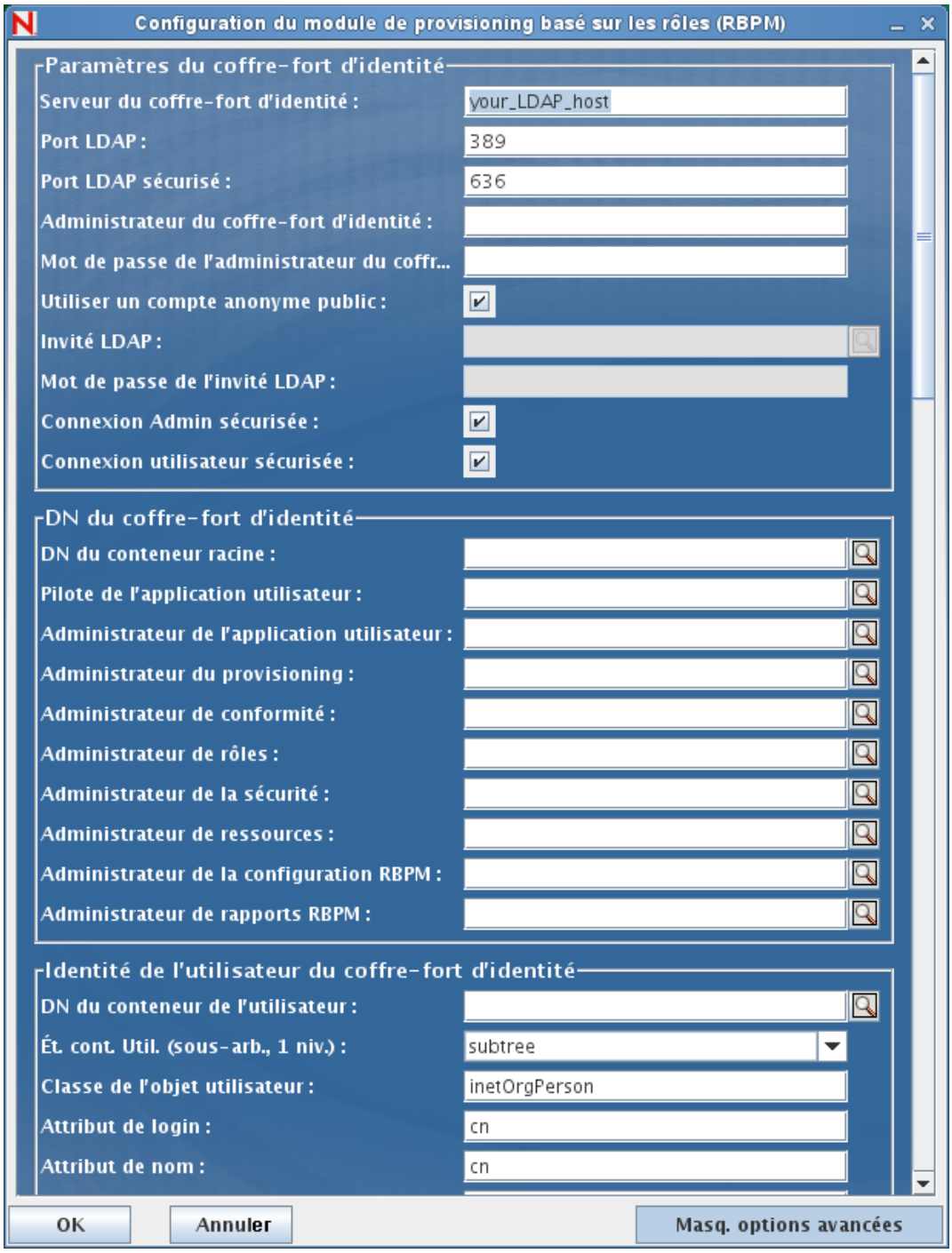
Le programme d'installation utilisera la valeur du champ DN du conteneur racine et l'appliquera aux valeurs suivantes :

- 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 :



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

Reportez-vous à l'Annexe A, « Référence de configuration de l'application utilisateur IDM », page 157 pour obtenir une description des options.

6 Les informations suivantes permettent de terminer l'installation.

Écran d'installation	Description
Résumé pré-installation	Lisez la page de résumé de la pré-installation pour vérifier vos paramètres d'installation. Si nécessaire, utilisez *Retour* pour retourner aux pages d'installation précédentes et modifier les paramètres d'installation. La page de configuration de l'application utilisateur ne sauvegarde pas de valeur. Une fois les pages précédentes de l'installation à nouveau spécifiées, vous devez saisir à nouveau les valeurs de configuration de l'application utilisateur. Lorsque vous êtes satisfait de vos paramètres d'installation et de configuration, retournez à la page Récapitulatif de pré-installation, puis cliquez sur *Installer*.
Installation terminée	Indique que l'installation est terminée.

Le programme d'installation crée l'utilisateur novlua. Le programme d'installation crée un nouvel utilisateur dont le nom est novlua. Le script jboss_init exécute JBoss sous l'identité de cet utilisateur et les autorisations définies dans les fichiers JBoss sont configurées pour ce dernier.

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) :

   `/etc/init.d/jboss_init start` (Linux et Solaris)

   `start-jboss.bat` (Windows)

   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* correspond au nom d'hôte du serveur d'applications (par exemple, monserveur.domaine.com) et au port de votre serveur d'applications (par exemple, 8180, valeur par défaut sur JBoss). La valeur par défaut de *Nom_application* est *IDMProv*. 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 9.9, « Dépannage », page 154.

Installation de l'application utilisateur sur WebSphere

6

Cette section décrit la procédure d'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 81
- Section 6.2, « Configuration de l'environnement WebSphere », page 96
- Section 6.3, « Déploiement du fichier WAR », page 110
- Section 6.4, « Démarrage et accès à l'application utilisateur », page 111

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/idm40/index.html) (Guide de migration de l'application utilisateur).

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

---

Remarque : 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. Vous devez appliquer les fichiers de stratégie non restreints au JDK IBM. Pour accéder à ces fichiers à partir IBM et savoir comment les appliquer, reportez-vous à la documentation de WebSphere. Appliquez ces fichiers à l'environnement JDK d'IBM avant de poursuivre l'installation. Le fichier JAR contenant les fichiers de stratégie non restreints doit être placé dans le dossier JAVA_HOME\jre\lib\security.

   En l'absence de ces fichiers, le message d'erreur « Taille de clé incorrecte » s'affiche. La cause première de ce problème est l'absence de fichiers de stratégie non restreints. Veillez dès lors à utiliser le JDK d'IBM approprié.
3. Lancez le programme d'installation à partir de l'environnement Java d'IBM, comme décrit ci-après :

   Linux ou Solaris

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

   Windows

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

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

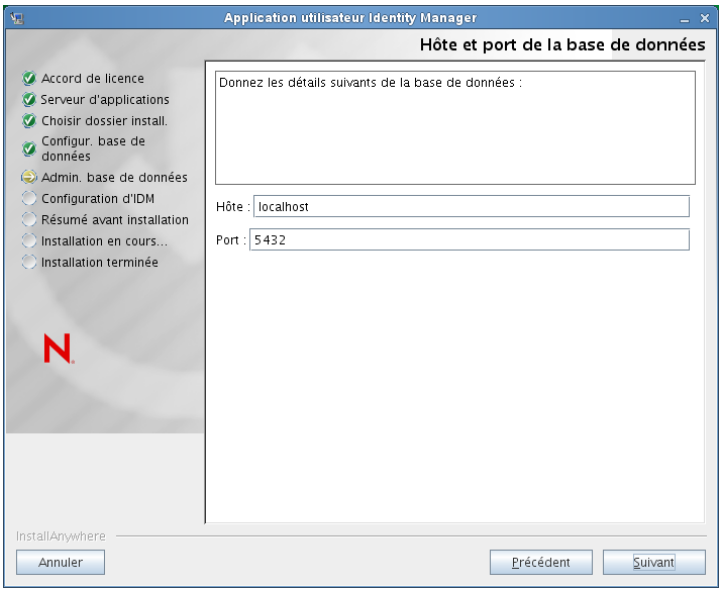
4 Utilisez les informations suivantes pour sélectionner la langue, confirmer l'accord de licence et choisir la plate-forme du serveur d'applications :

Écran d'installation	Description
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 *J'accepte les termes de l'accord de licence*.

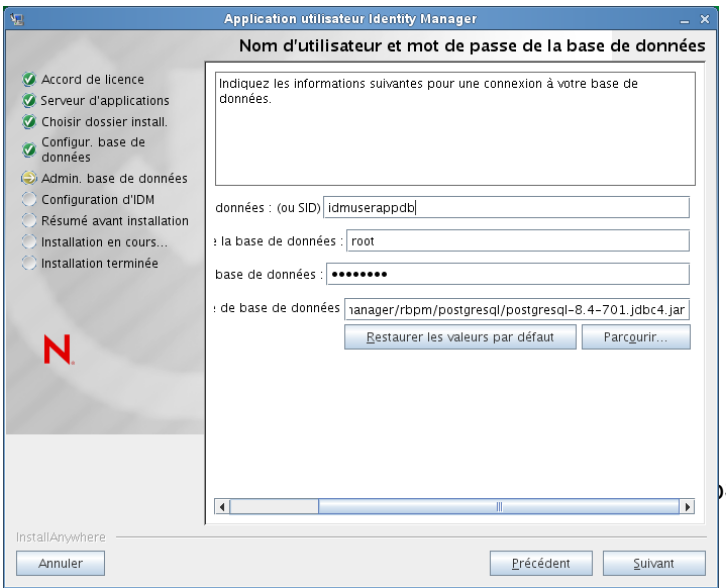
Écran d'installation	Description
Plate-forme du serveur d'applications	Sélectionnez *WebSphere.* Si le fichier WAR de l'application utilisateur est dans un répertoire différent du programme d'installation, ce dernier vous invite à saisir le chemin d'accès au WAR. Si le fichier WAR se trouve à l'emplacement par défaut, vous pouvez cliquez sur *Restaurer le fichier par défaut*. Ou, pour spécifier l'emplacement du fichier WAR, cliquez sur *Choisir* et sélectionnez un emplacement. 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 : 

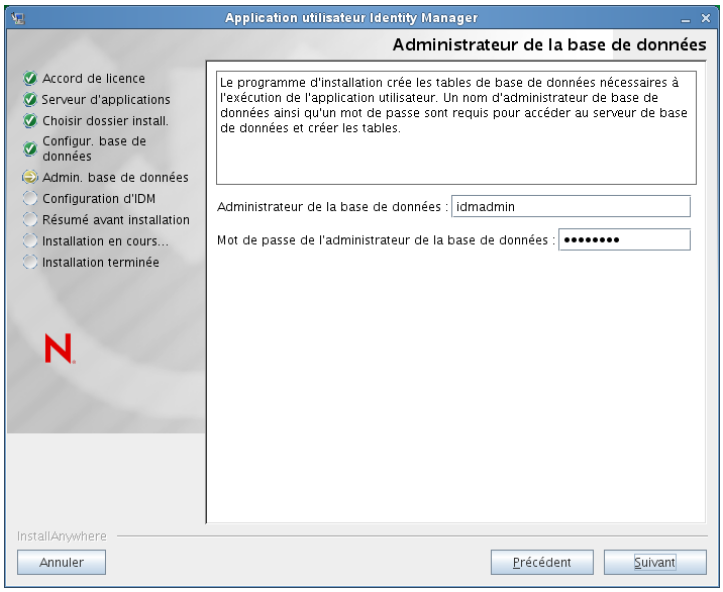
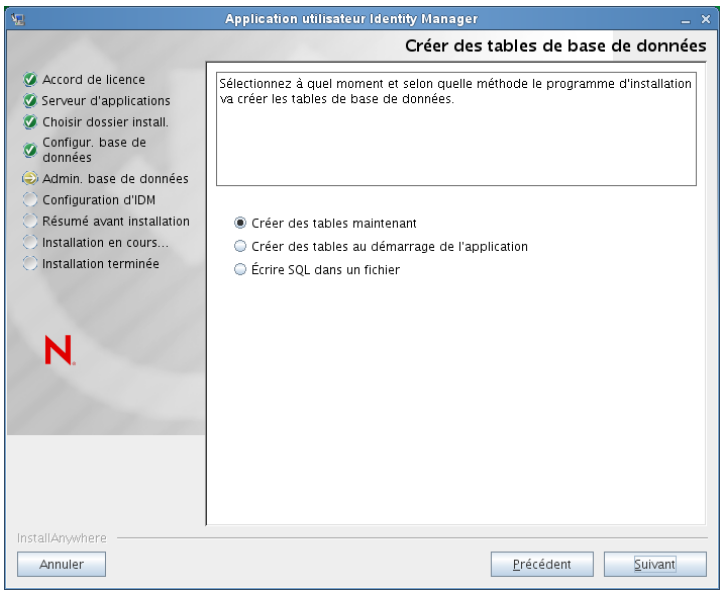
5 Aidez-vous des informations suivantes pour sélectionner le type d'installation, choisir un dossier d'installation et configurer la base de données :

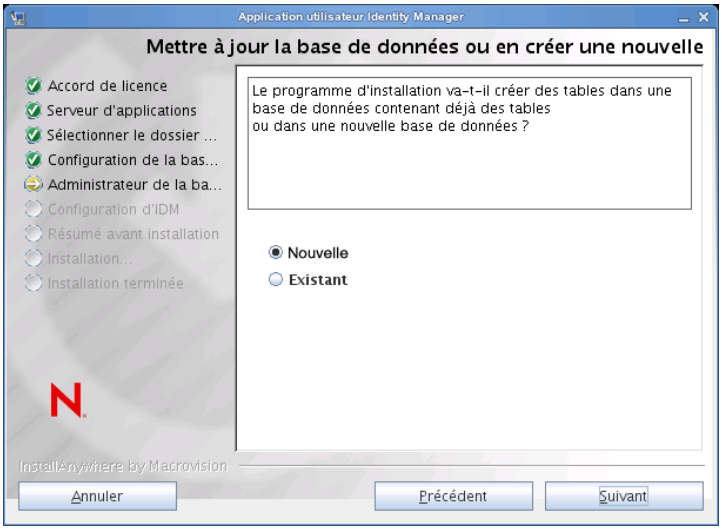
Écran d'installation	Description
Type d'installation	*Provisioning basé sur les rôles* : sélectionnez cette option pour installer le module de provisioning basé sur les rôles. Il s'agit du seul type d'installation pris en charge avec cette version.
Sélectionnez le dossier d'installation	Indiquez l'emplacement auquel le programme d'installation doit mette 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 WebSphere, les options sont les suivantes : ◆ Oracle ◆ Microsoft SQL Server ◆ IBM DB2 ◆ PostgreSQL

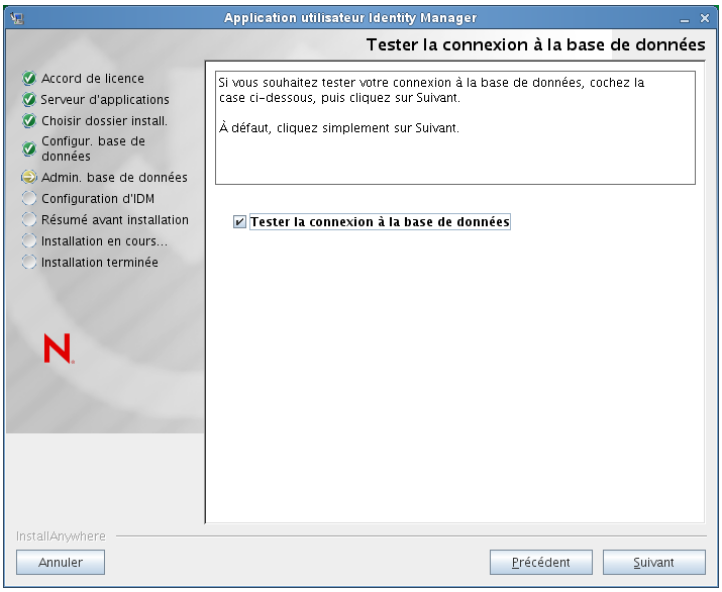
Écran d'installation	Description
Hôte et port de la base de données	*Hôte* : indiquez le nom d'hôte ou l'adresse IP du serveur de bases de données. Pour une grappe, indiquez le même nom d'hôte ou la même adresse IP pour chaque membre de la grappe. *Port* : indiquez le numéro du port d'écoute de la base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

Écran d'installation	Description

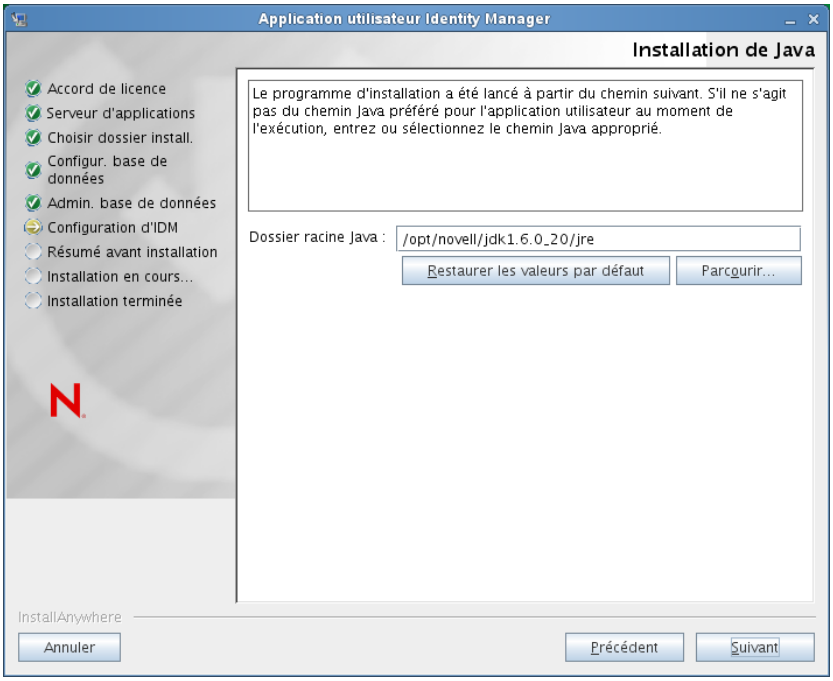
Nom d'utilisateur et mot de passe de la base de données	*Nom de la base de données* (ou SID) : pour DB2, MS SQL Server ou PostgreSQL, indiquez le nom de votre base de données préconfigurée. Pour Oracle, donnez l'identificateur système Oracle (SID) que vous avez créé précédemment. Pour une grappe, indiquez 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`
	
	 

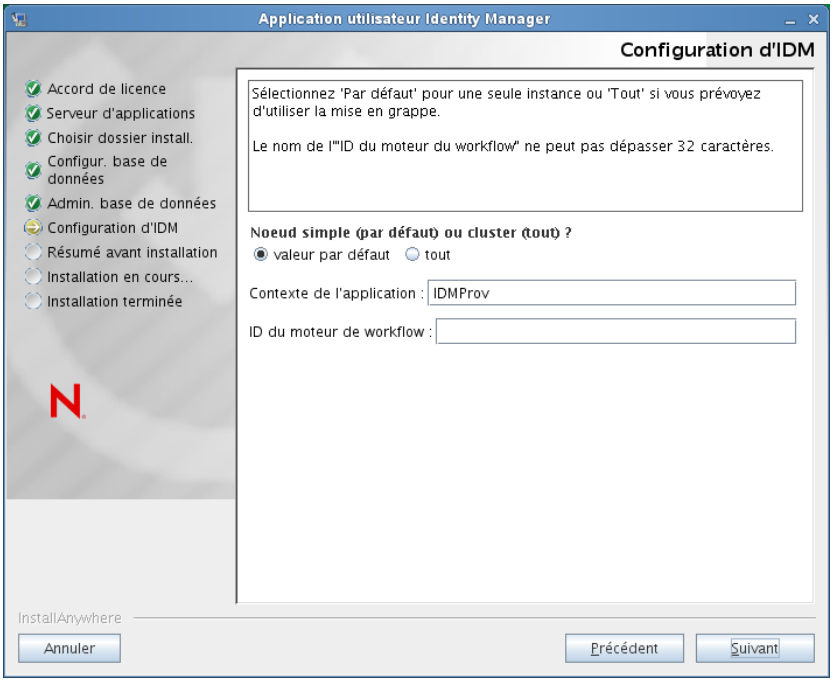
Écran d'installation	Description
Administrateur de la base de données	Cette page est préremplie avec les mêmes nom d'utilisateur et mot de passe que sur la page Nom d'utilisateur et mot de passe de la base de données. Si l'utilisateur de base de données spécifié précédemment ne possède pas les autorisations 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. 
Créer des tables de base de données	Indiquez le moment auquel les tables de base de données doivent être créées : 

Écran d'installation	Description
Nouvelle base de données ou base de données existante	Si la base de données à utiliser est nouvelle ou vide, sélectionnez *Nouvelle base de données*. Si la base de données provient d'une installation précédente, sélectionnez *Base de données existante*. 

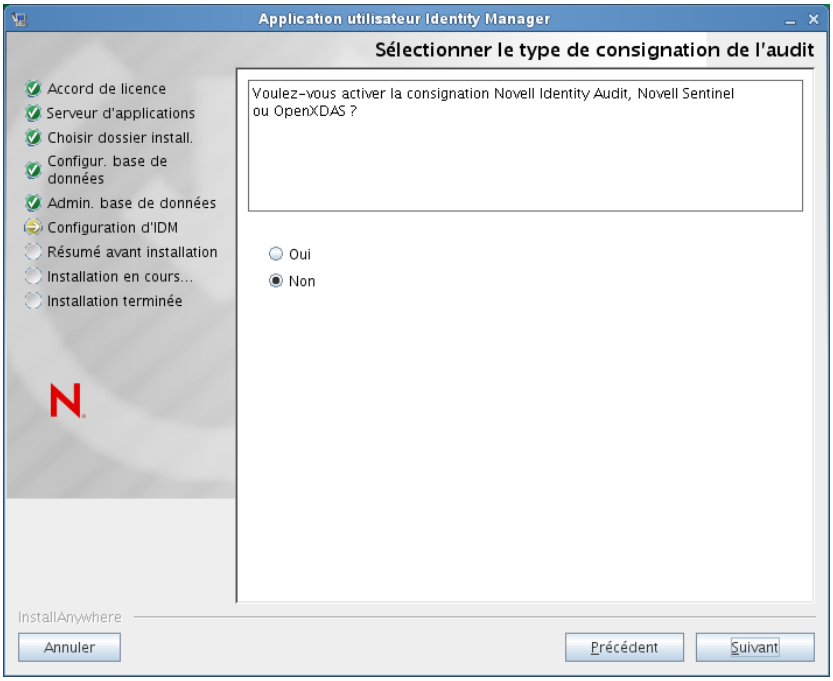
Écran d'installation	Description
Tester la connexion à la base de données	Pour vérifier que les informations fournies dans les écrans précédents sont correctes, vous pouvez tester la connexion à la base de données en cochant la case *Tester la connexion à la base de données* :  Le programme d'installation doit se connecter à la base de données pour créer les tables directement et créer le fichier .SQL. Un échec au test de connexion à la base de données permet néanmoins de poursuivre l'installation. Dans ce cas, vous devrez créer les tables après l'installation, comme décrit dans le *User Application: Administration Guide* (http://www.novell.com/documentation/idm40/agpro/?page=/documentation/idm40/agpro/data/bncf7rj.html) (Guide d'administration de l'application utilisateur).

6 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. 

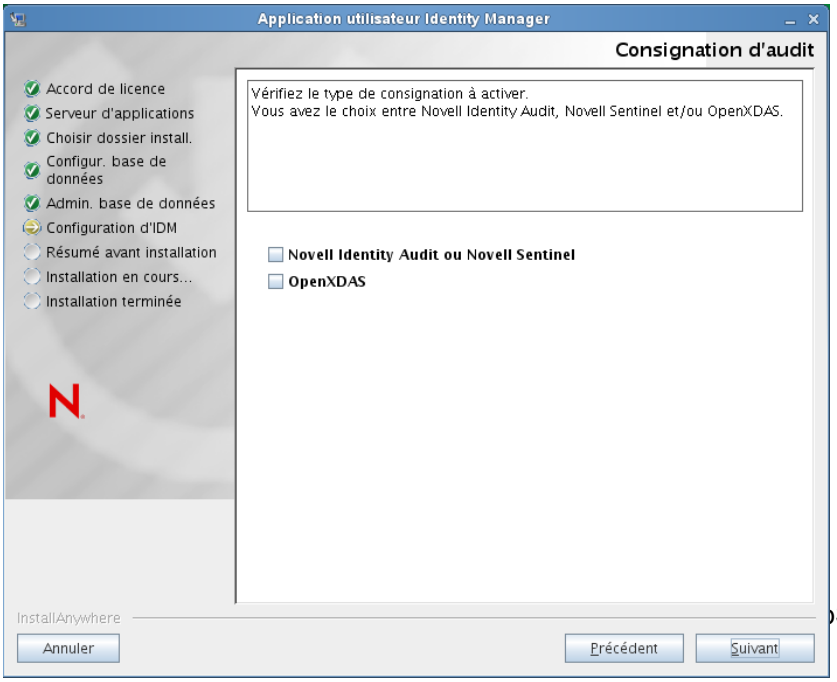
Écran d'installation	Description
Sélectionner le type de consignation de l'audit	Pour activer la consignation, cliquez sur *Oui*. Pour désactiver la consignation, cliquez sur *Non*.



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

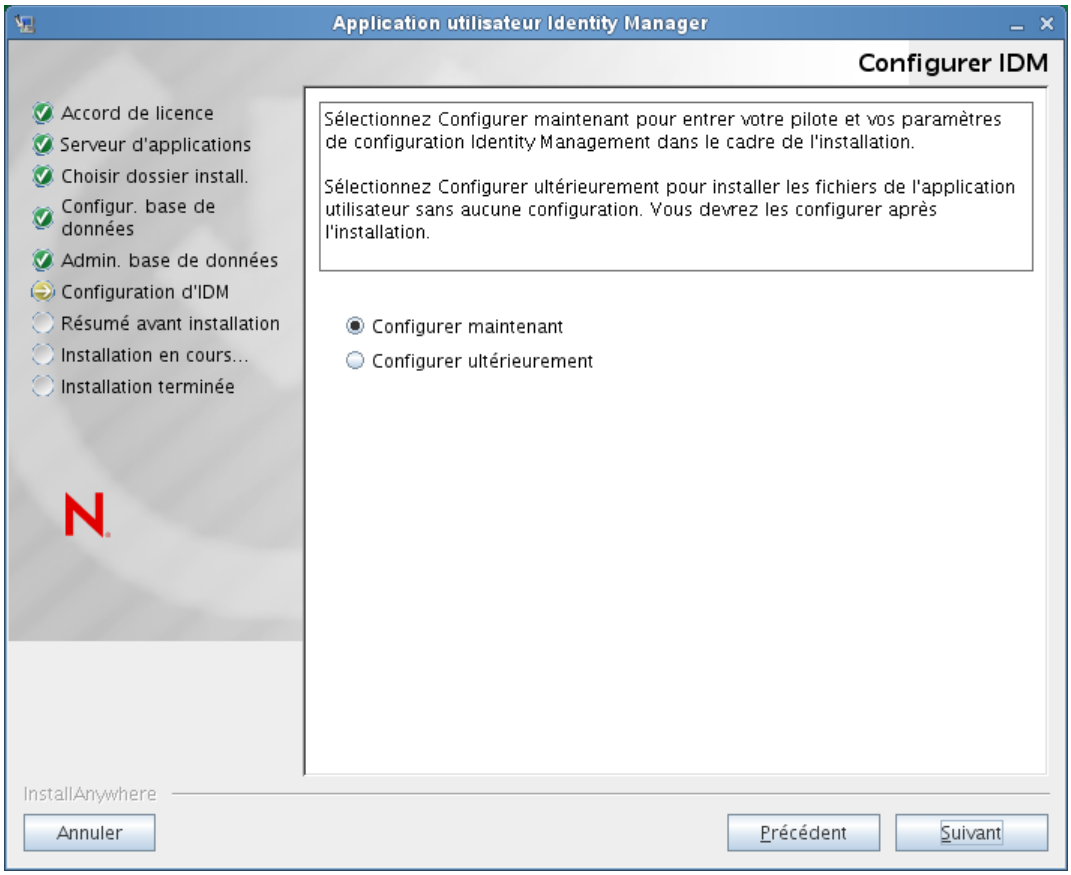
- *Novell Identity Audit ou Novell Sentinel* : permet d'activer la consignation via un client Novell pour l'application utilisateur.
- *OpenXDAS* : les événements sont consignés sur votre serveur de consignation OpenXDAS.

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).



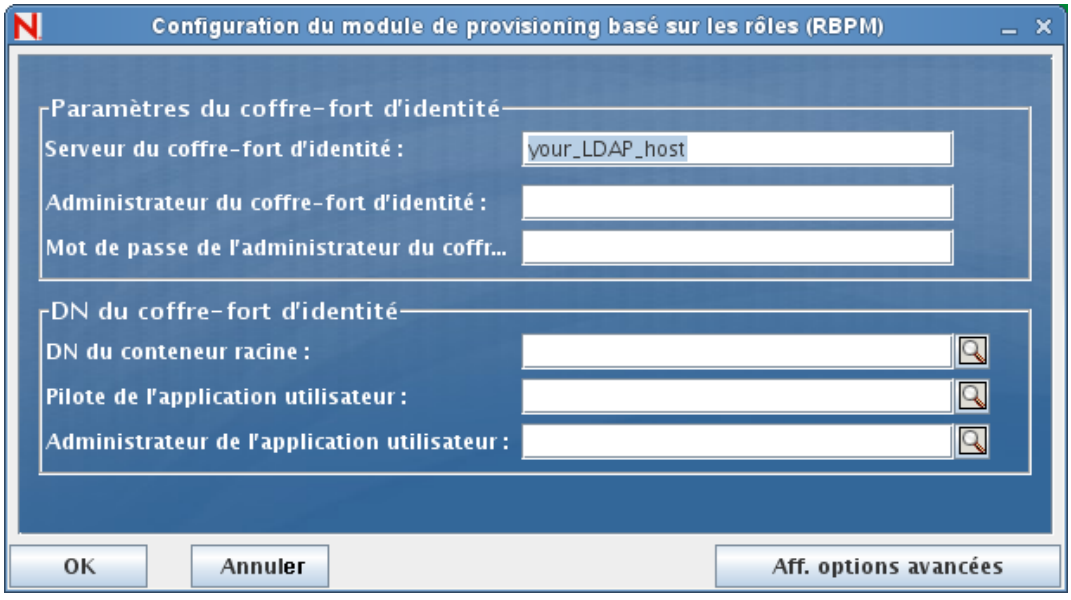
Écran d'installation	Description
Novell Identity Audit ou Novell Sentinel	*Serveur* : si vous activez la consignation, indiquez le nom d'hôte ou l'adresse IP du serveur. Si vous désactivez la consignation, cette valeur est ignorée. *Dossier de cache des journaux* : indiquez le répertoire du cache de consignation.
Sécurité : clé principale	*Oui* : 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. *Non* : 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 149. La procédure d'installation inscrit la clé maîtresse codée dans le fichier `master-key.txt` dans le répertoire d'installation. Voici des raisons d'importer une clé principale existante : ◆ Vous déplacez votre installation d'un système provisoire à un système de production et vous souhaitez conserver l'accès à la base de données que vous avez utilisée avec le système provisoire. ◆ Vous avez installé l'application utilisateur sur le premier membre d'une grappe et vous l'installez maintenant sur de nouveaux membres de la grappe (qui requièrent la même clé maîtresse). ◆ En raison d'un disque défectueux, vous devez restaurer votre application utilisateur. Vous devez réinstaller l'application utilisateur et indiquer la même clé maîtresse codée que celle qu'utilisait l'installation précédente. Cela vous donne accès aux données codées stockées précédemment.

7 Si vous souhaitez configurer le module RBPM maintenant, sélectionnez *Configurer maintenant*, puis cliquez sur *Suivant*.



(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 32.)

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



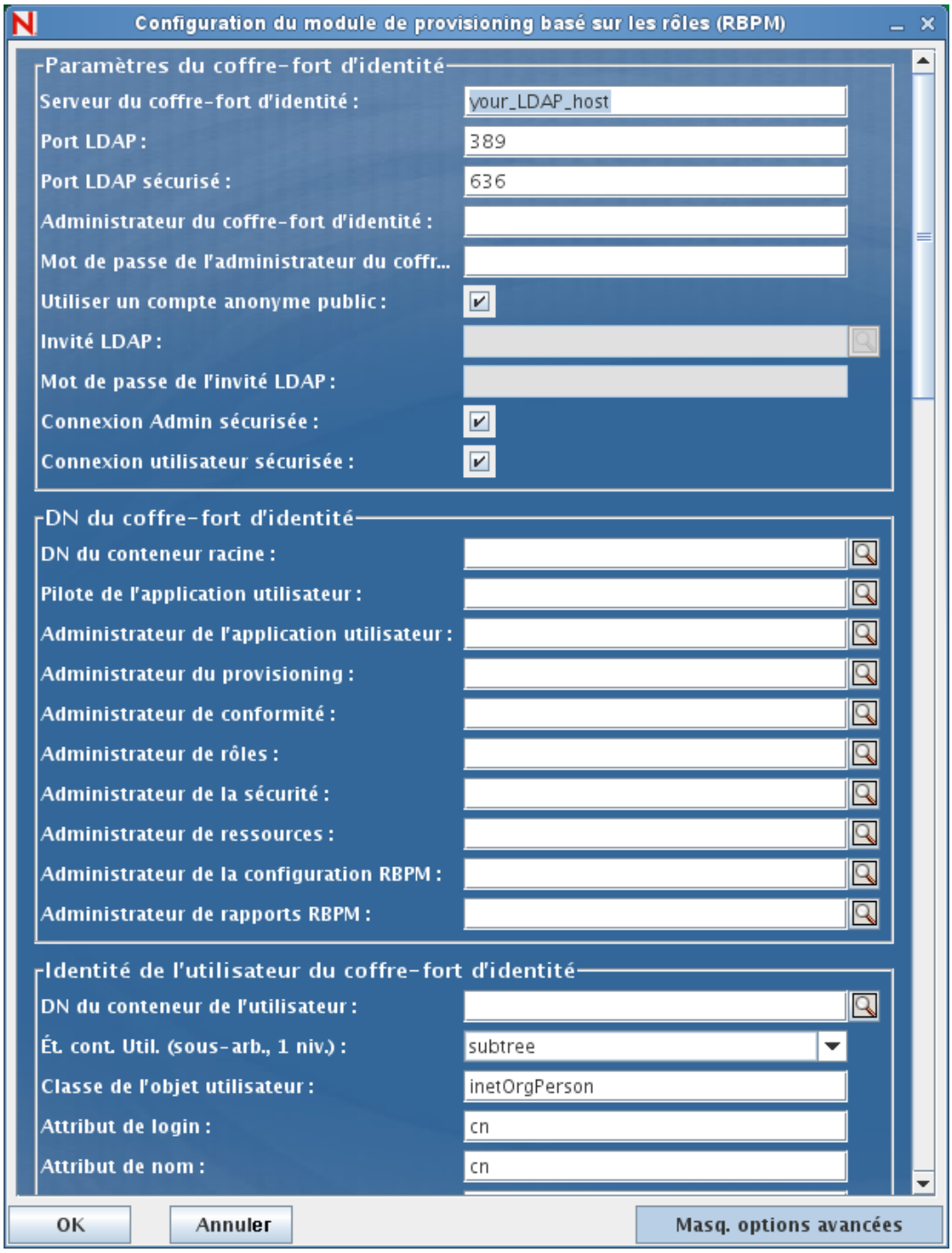
Le programme d'installation utilisera la valeur du champ DN du conteneur racine et l'appliquera aux valeurs suivantes :

- 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 :



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

Reportez-vous à l'Annexe A, « Référence de configuration de l'application utilisateur IDM », page 157 pour obtenir une description des options.

8 Les informations suivantes permettent de terminer l'installation.

Écran d'installation	Description
Résumé pré-installation	Lisez la page de résumé de la pré-installation pour vérifier vos paramètres d'installation. Si nécessaire, utilisez *Retour* pour retourner aux pages d'installation précédentes et modifier les paramètres d'installation. La page de configuration de l'application utilisateur ne sauvegarde pas de valeur. Une fois les pages précédentes de l'installation à nouveau spécifiées, vous devez saisir à nouveau les valeurs de configuration de l'application utilisateur. Lorsque vous êtes satisfait de vos paramètres d'installation et de configuration, retournez à la page Récapitulatif de pré-installation, puis cliquez sur *Installer*.
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 6.2.2, « Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM », page 104.

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

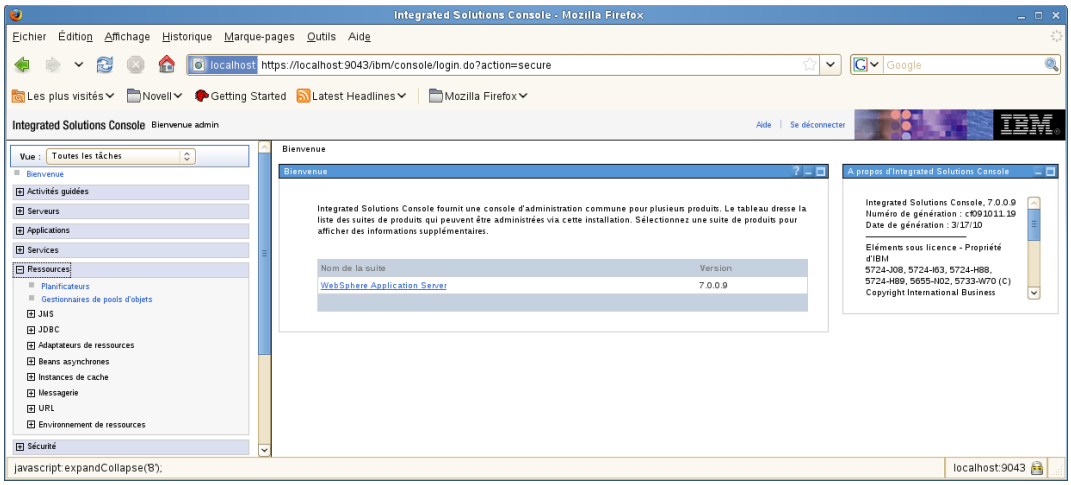
- Section 6.2.1, « Configuration d'une réserve de connexions », page 96
- Section 6.2.2, « Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM », page 104
- Section 6.2.3, « Importation de la racine approuvée d'eDirectory dans le keystore WebSphere », page 109
- Section 6.2.4, « Transmission de la propriété preferIPv4Stack à la JVM », page 110

6.2.1 Configuration d'une réserve de connexions

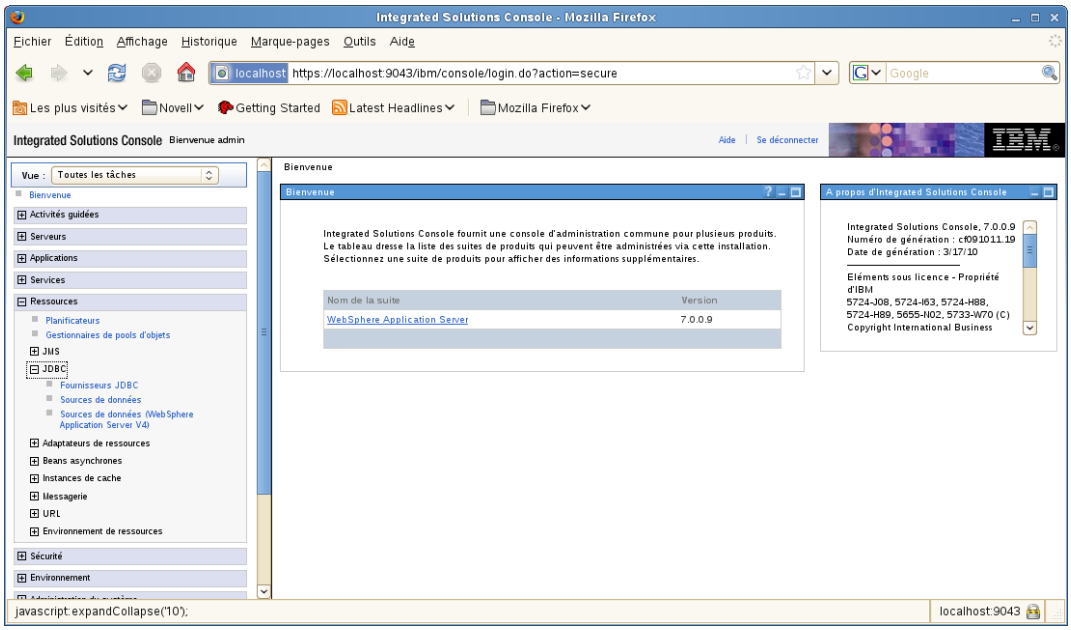
Pour configurer une réserve de connexions à utiliser avec WebSphere, vous devez créer un fournisseur JDBC ainsi qu'une source de données. Cette section fournit des instructions pour la création du fournisseur et de la source de données.

Pour créer un fournisseur JDBC :

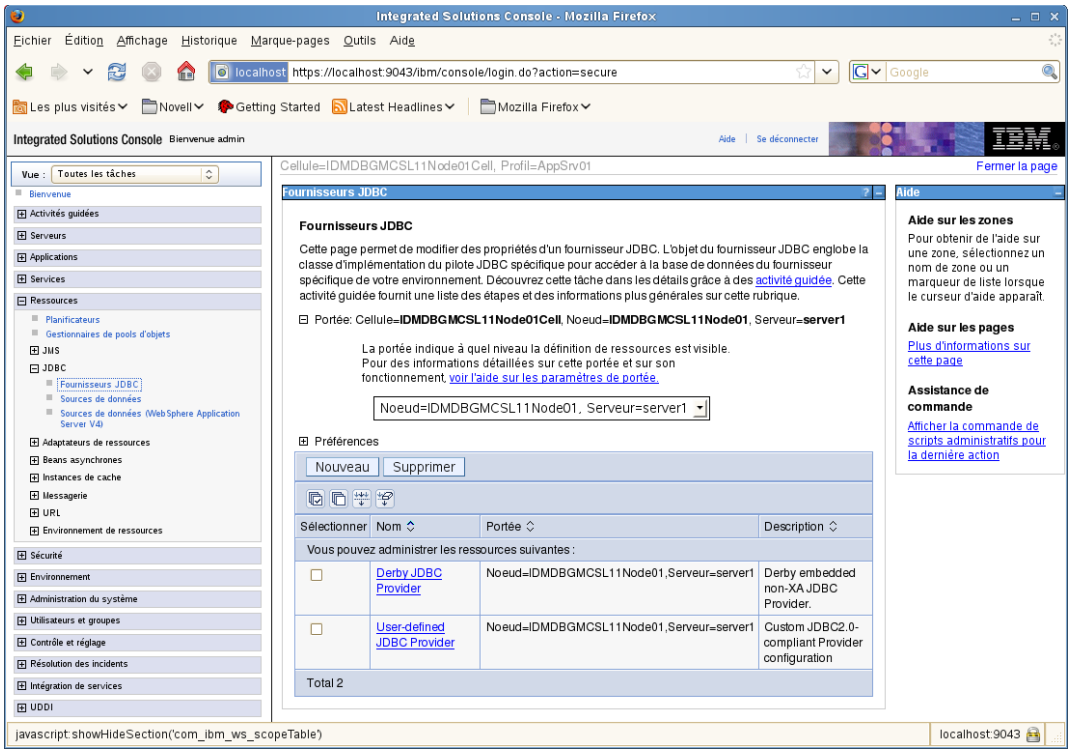
1 Développez *Ressources* sur le côté gauche de la page Integrated Solutions Console :



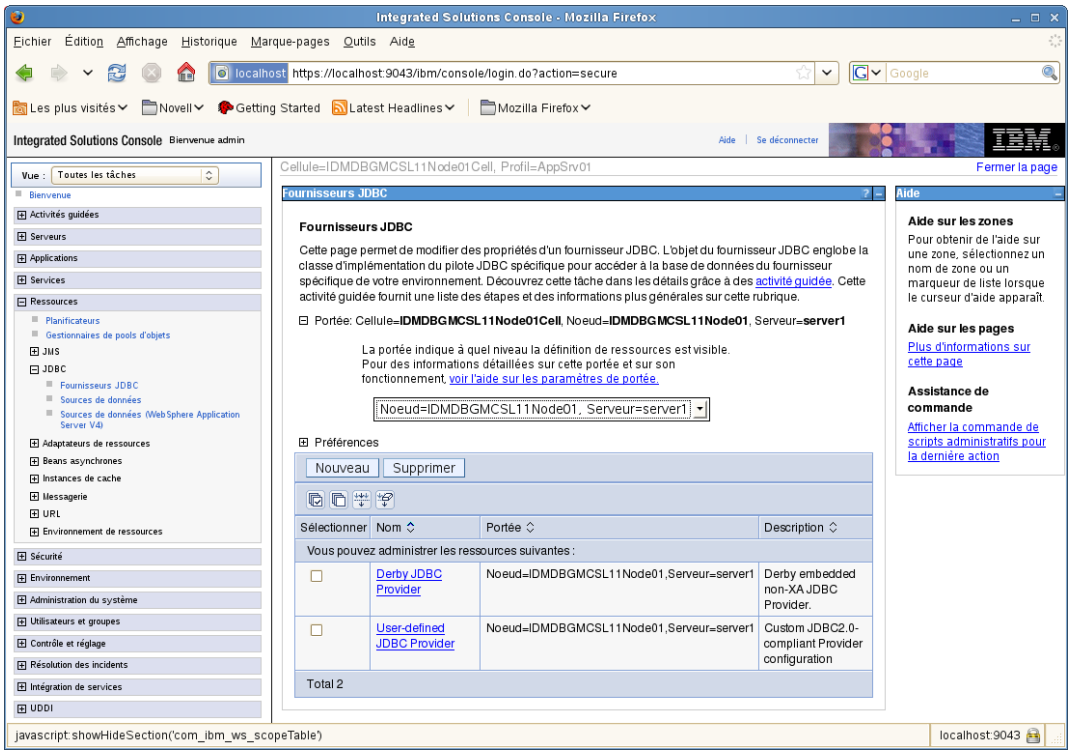
2 Développez *JDBC* :



3 Cliquez sur *Fournisseurs JDBC* :



4 Développez *Étendue* :

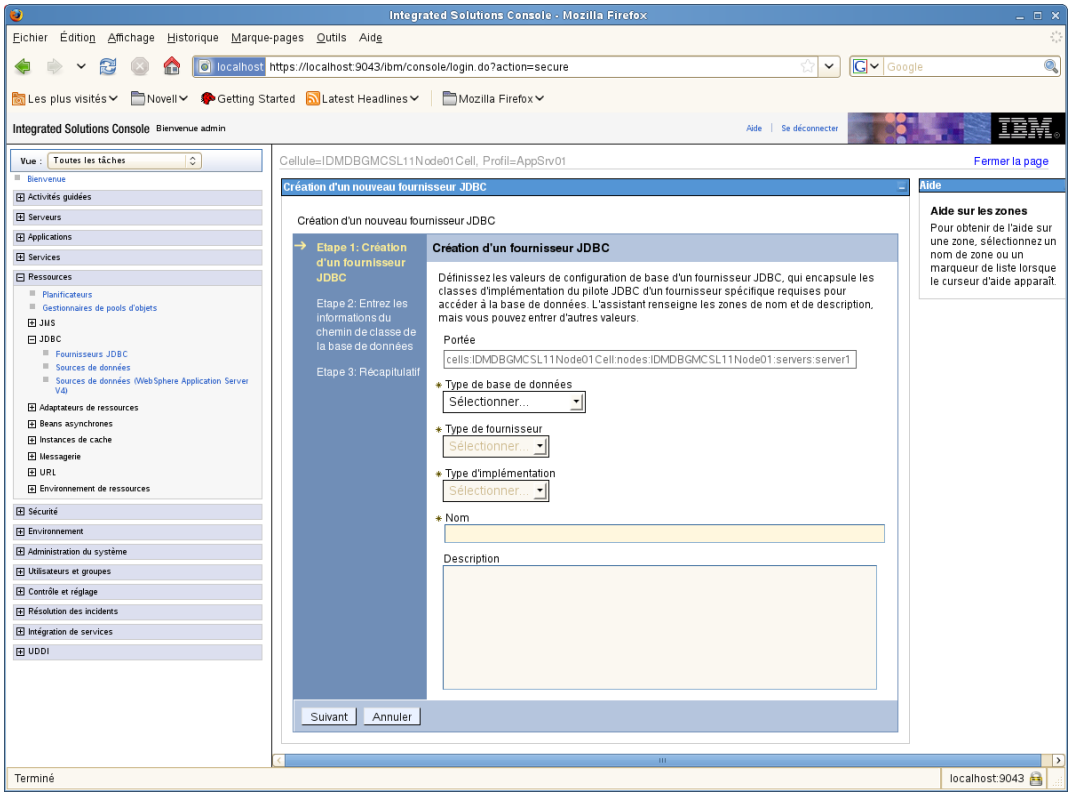


5 Sélectionnez *Node=nom_de_votre_serveur, Server=serveur1*.

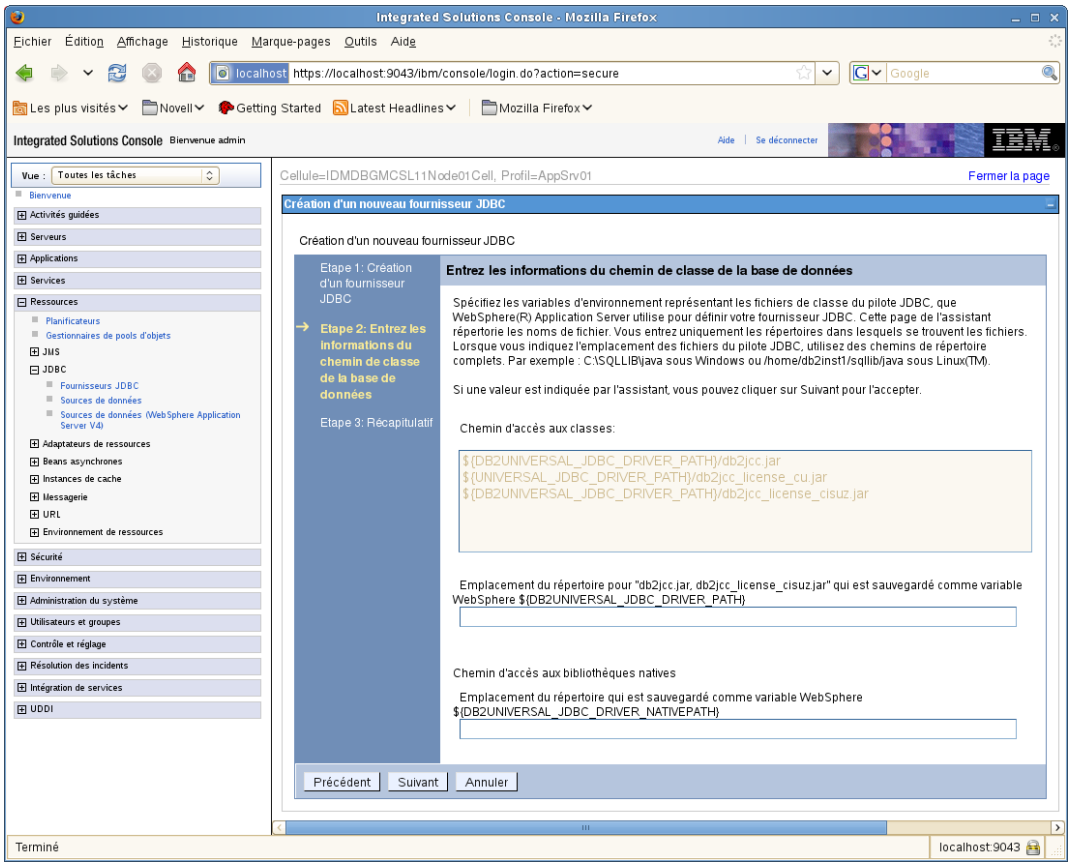
6 Cliquez sur le bouton *Nouveau*.

7 Sélectionnez le *type de base de données* (par exemple, DB2).

8 Cliquez sur *Suivant*.



9 Saisissez les informations du chemin de classe JDBC.



10 Cliquez sur *Suivant*.

11 Cliquez sur *Terminer*.

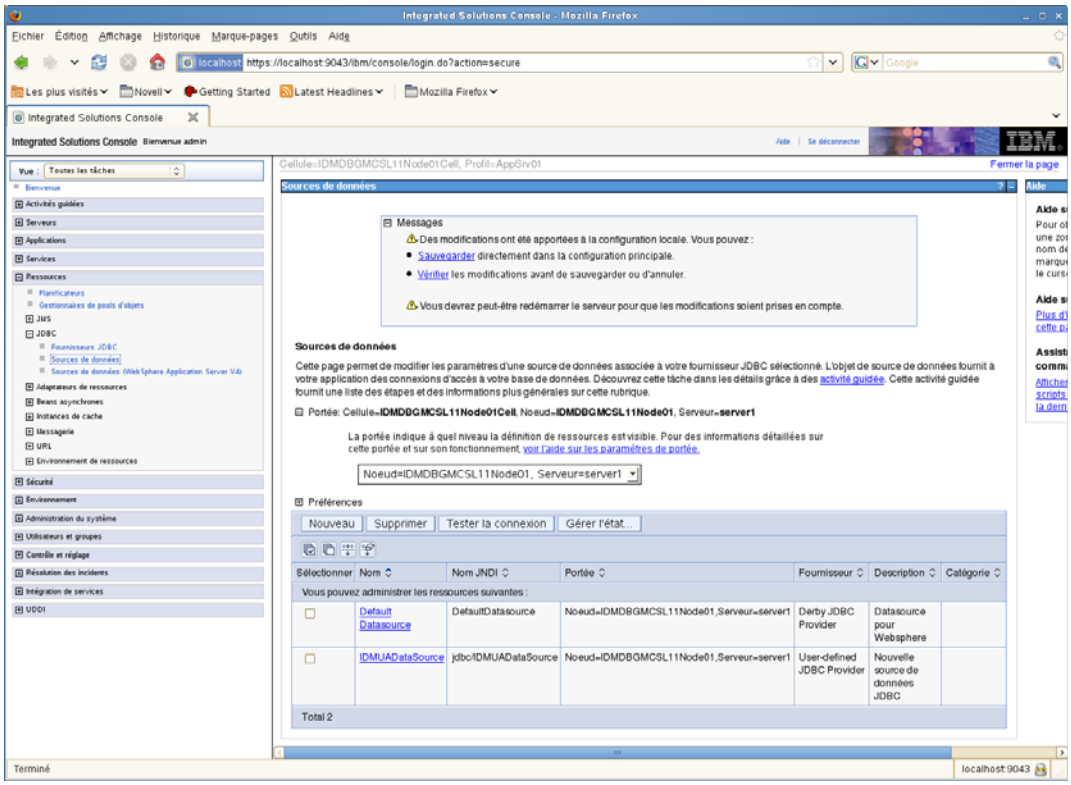
12 Cliquez sur le lien *Enregistrer*.

Pour créer une source de données :

1 Développez *Ressources* sur le côté gauche de la page.

2 Développez *JDBC*.

3 Cliquez sur *Sources de données*.



4 Développez *Étendue*.

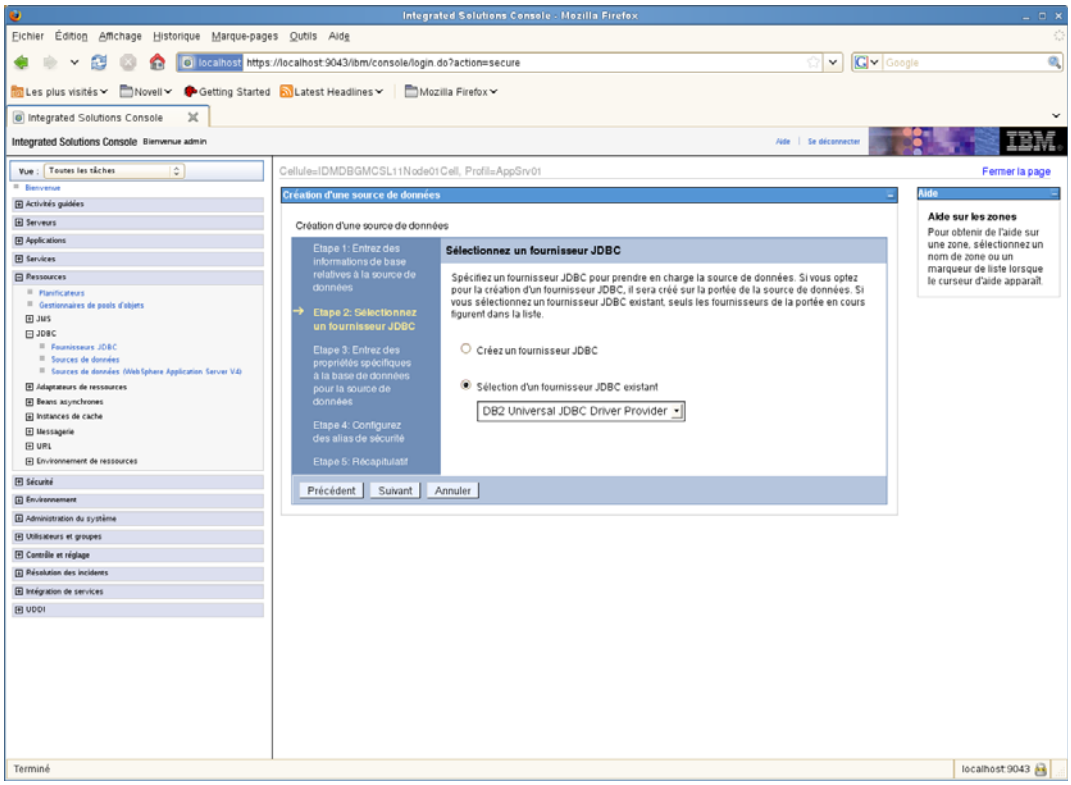
5 Sélectionnez *Node=nom_de_votre_serveur, Server=serveur1*.

6 Cliquez sur le bouton *Nouveau*.

7 Saisissez le nom de la source de données ainsi que le nom JNDI (par exemple, IDMUADataSource pour les deux).

8 Cliquez sur *Suivant*.

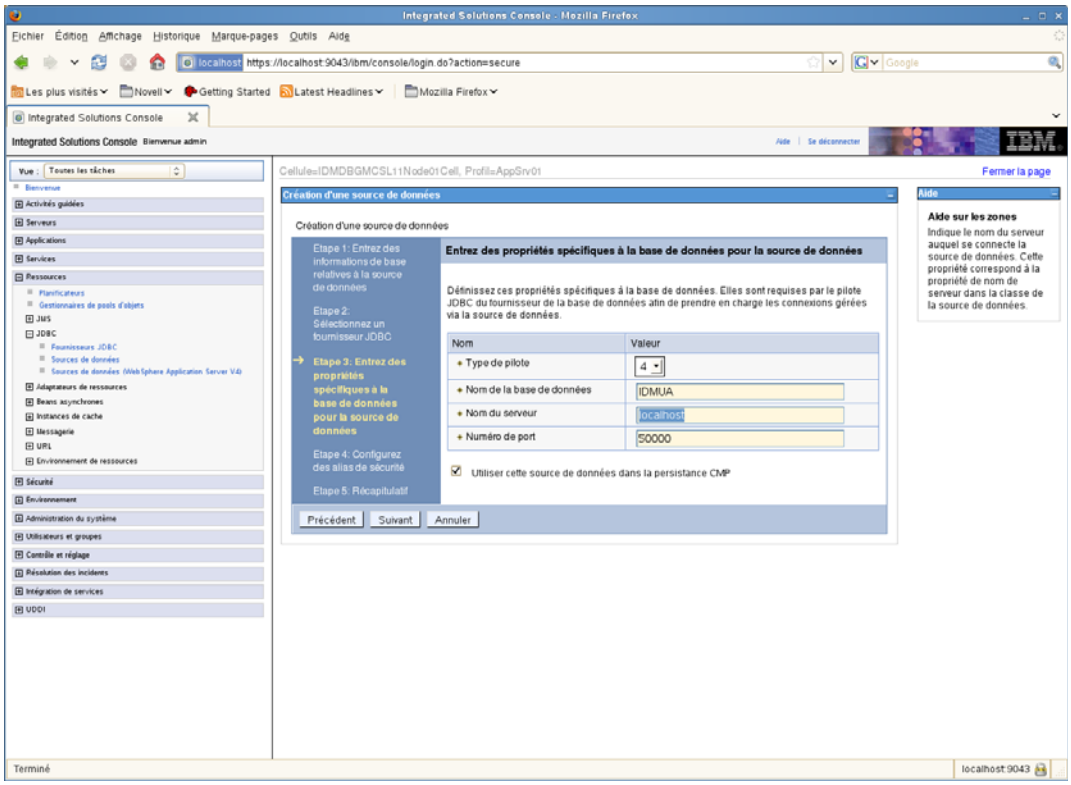
9 Cliquez sur *Sélectionner un fournisseur JDBC existant*.



10 Sélectionnez le fournisseur JDBC que vous venez de créer.

11 Cliquez sur *Suivant*.

12 Saisissez les informations relatives à la base de données demandées par la source de données (nom de la base de données et du serveur, port, nom d'utilisateur et mot de passe).



13 Cliquez sur *Suivant*.

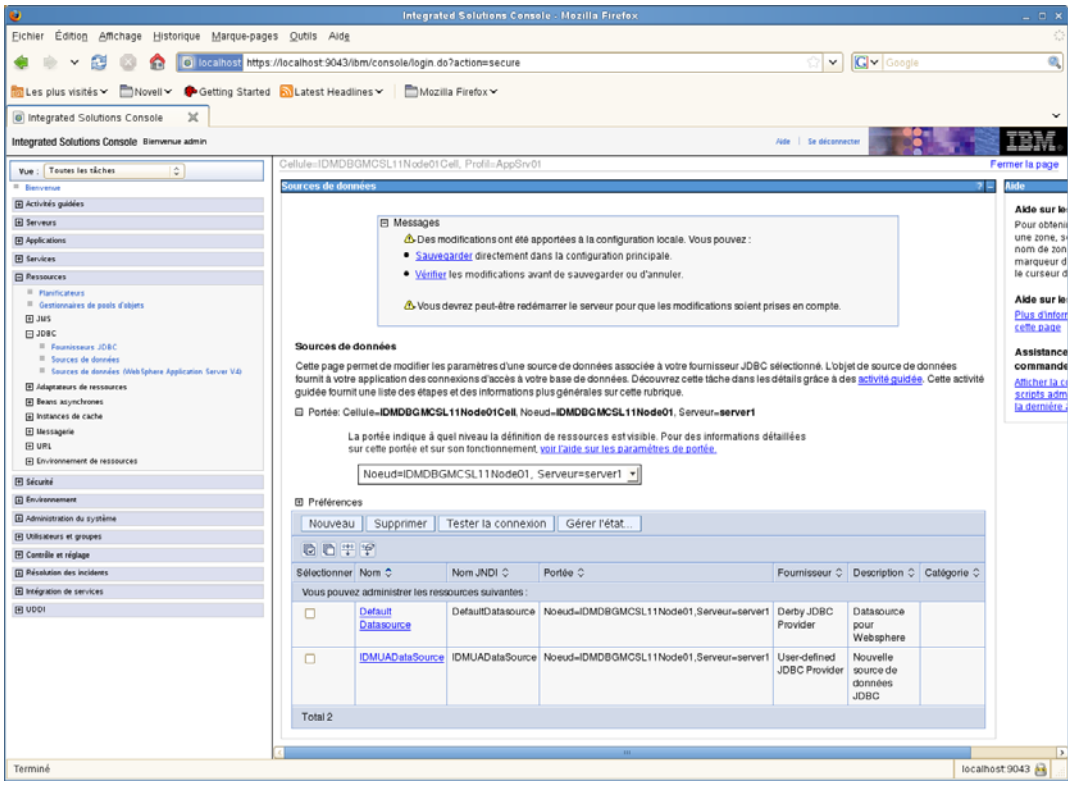
14 Saisissez les informations relatives à l'alias de sécurité ou laissez les valeurs par défaut.

15 Cliquez sur *Suivant*.

16 Cliquez sur *Terminer*.

17 Cliquez sur *Enregistrer*.

18 Sélectionnez votre nouvelle source de données en cochant la case située à gauche du nom.



19 Cliquez sur le bouton *Tester la connexion* et assurez-vous qu'il renvoie bien la valeur *Réussite*.

6.2.2 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 paramètre de droite, accédez à *Java et Gestion de processus* sous *Infrastructure de serveur*.

6 Développez le lien et sélectionnez *Définition du processus*.

7 Sous la liste des *Propriétés supplémentaires*, sélectionnez *Machine virtuelle Java*.

8 Sélectionnez *Propriétés personnalisées* sous le titre *Propriétés supplémentaires* de la page JVM.

9 Cliquez sur *Nouveau* pour ajouter une nouvelle propriété du système JVM.

9a Pour le *Nom*, indiquez `extend.local.config.dir`.

9b Pour la *valeur*, indiquez le 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*.

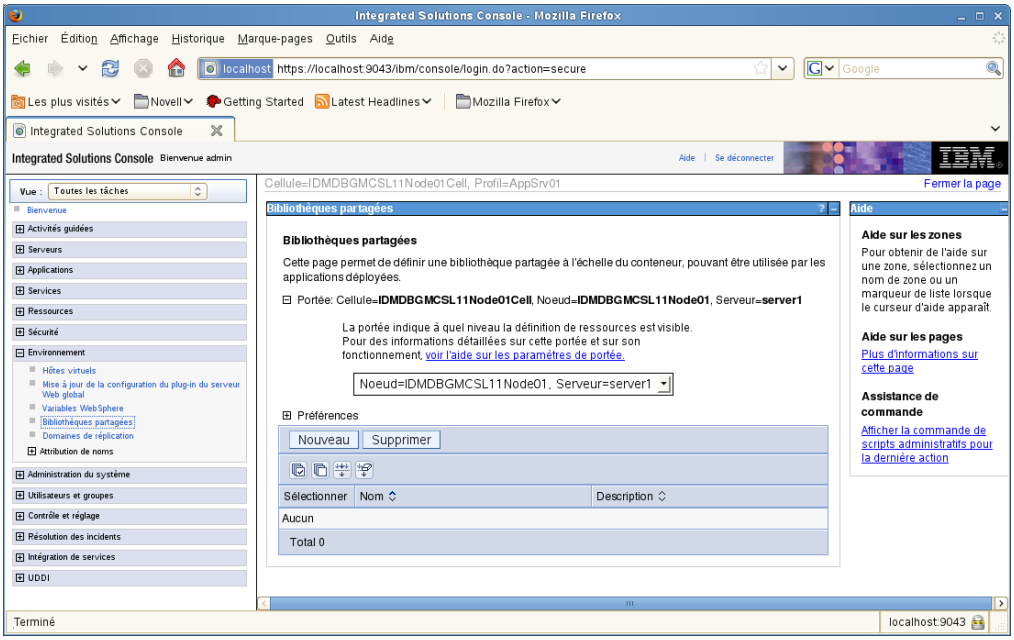
Vous devez également configurer une bibliothèque partagée pour l'application utilisateur sur WebSphere. La bibliothèque partagée définit le comportement de chargement de classes nécessaire à la bonne exécution de l'application.

Pour configurer la bibliothèque partagée :

1 Créez la bibliothèque partagée pour l'application utilisateur :

1a Cliquez sur *Environnement* dans le menu de navigation de gauche.

1b Cliquez sur *Bibliothèques partagées*.



1c Cliquez sur le bouton *Nouveau*.

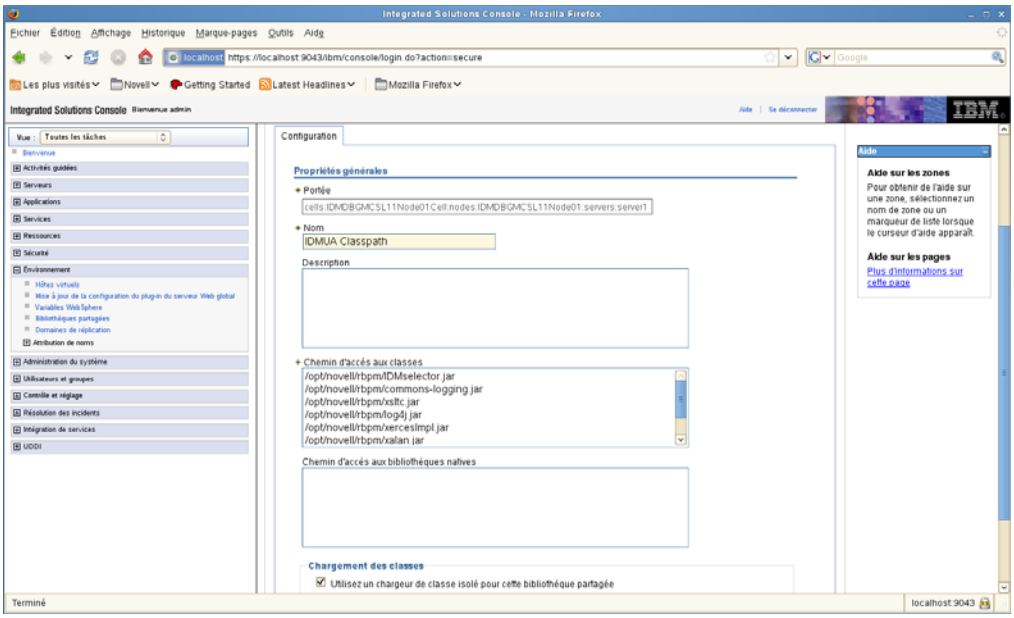
1d Saisissez un nom (comme IDMUA Classloader).

1e Saisissez la liste des fichiers JAR requis dans le champ Chemin de classe :

- `antlr.jar`
- `log4j.jar`
- `commons-logging.jar`

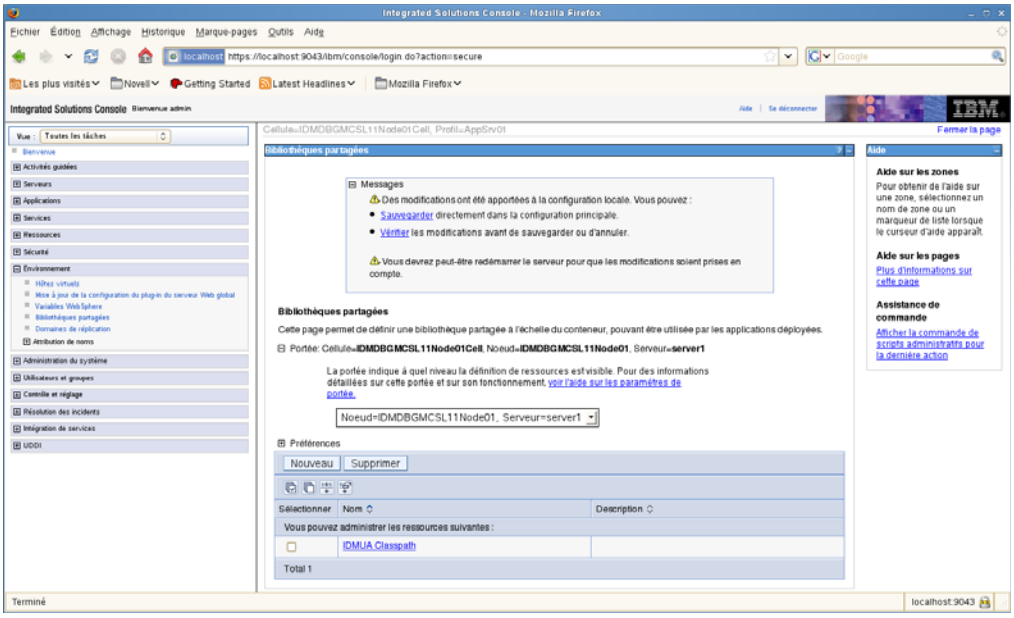
  Remarque : vous devez télécharger ce fichier JAR à partir du site Apache.

- `xalan.jar`
- `xercesImpl.jar`
- `xsltc.jar`
- `serializer.jar`
- `jaxb-impl.jar`
- `IDMselector.jar`



1f Cliquez sur *OK*.

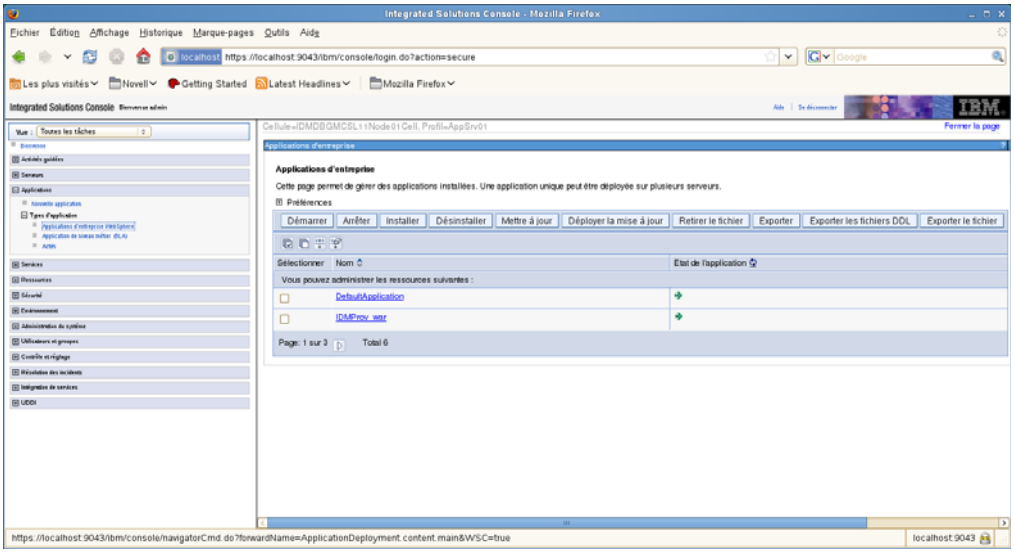
1g Cliquez sur le lien *Enregistrer*.



2 Ajoutez la bibliothèque partagée à IDMProv :

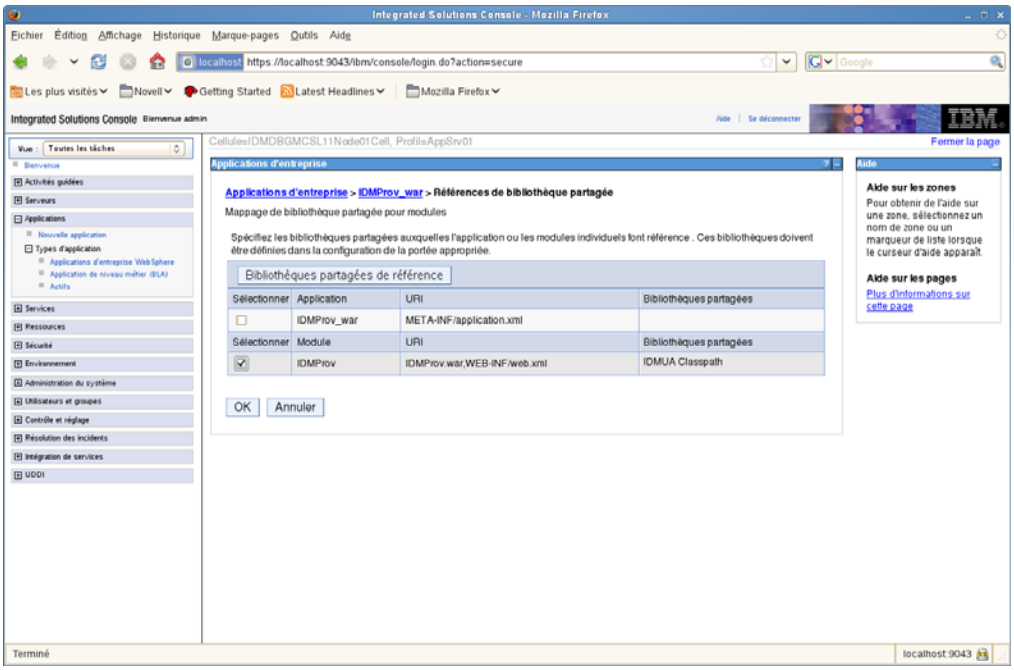
2a Cliquez sur *Applications* à gauche.

2b Cliquez sur *Applications d'entreprise WebSphere*.



2c Cliquez sur le nom *IDMProv_war*.

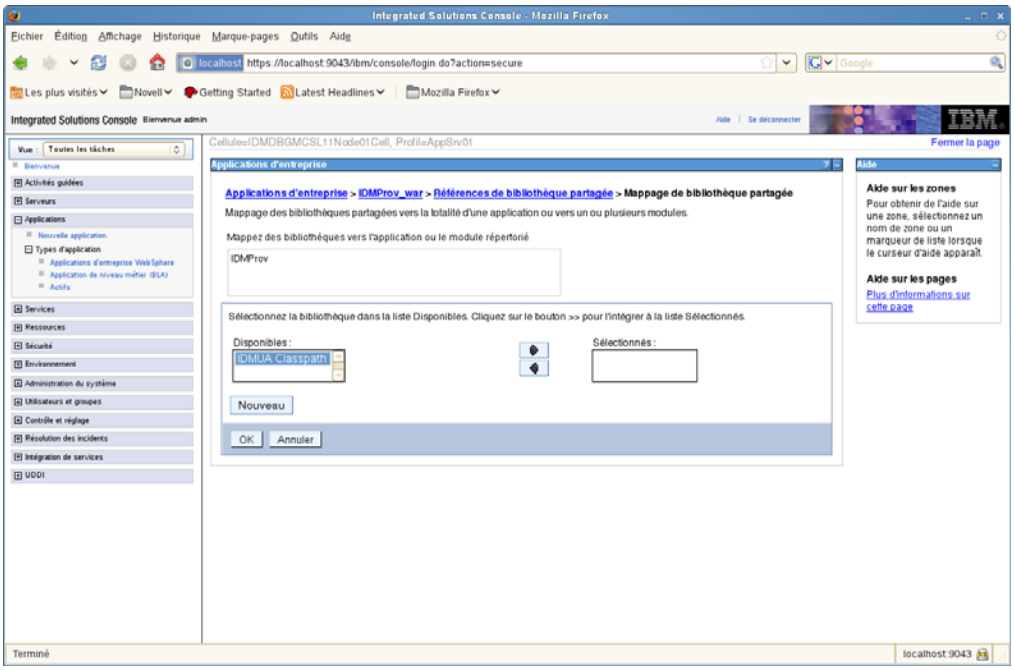
2d En bas de la page, sous *Références*, cliquez sur *Références de bibliothèque partagée*.



2e Cochez la case en regard de *IDMProv* (et non IDMProv_war).

2f Cliquez sur le bouton *Référencer les bibliothèques partagées*.

2g Sélectionnez le nom de la bibliothèque partagée (*Chemin de classe IDMUA*) dans la zone *Disponible*. Cliquez ensuite sur la flèche pointant vers la droite de façon à ce que ce nom passe dans la zone *Sélectionné*.



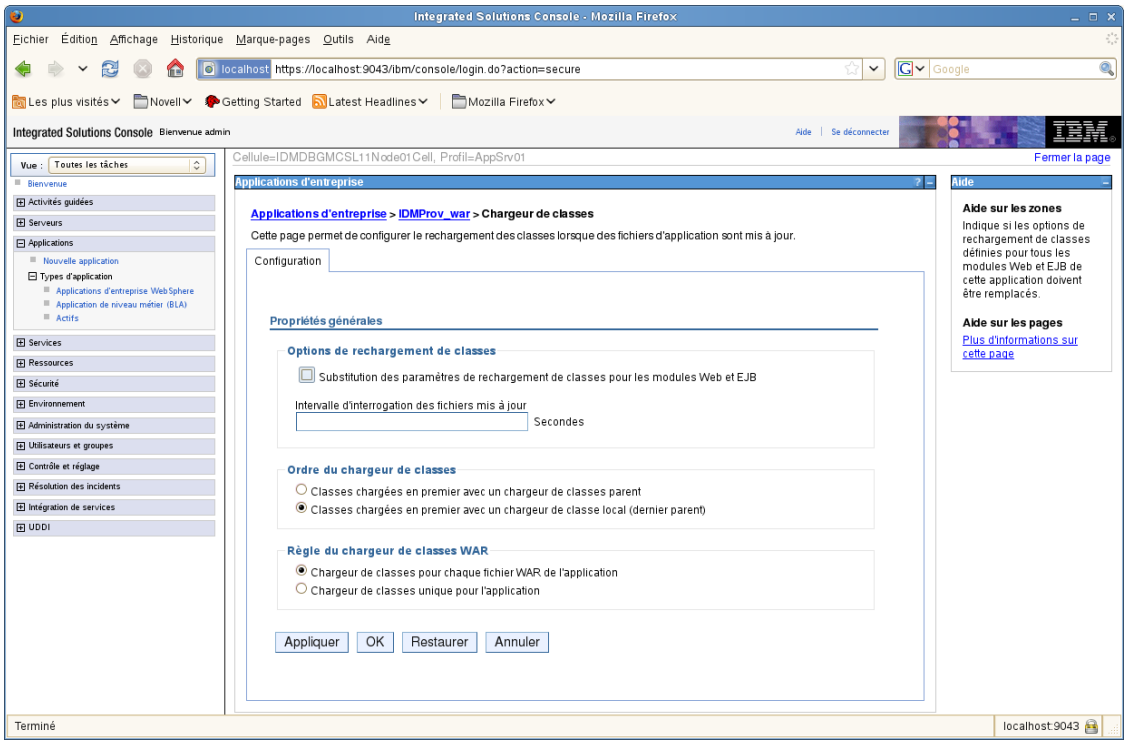
2h Cliquez sur *OK* pour revenir à la page précédente.

2i Cliquez à nouveau sur *OK*.

2j Cliquez sur *Enregistrer* pour conserver les changements apportés à la configuration du serveur.

2k Redémarrez le serveur une fois que toutes les autres étapes de la configuration ont été réalisées.

Notez que le changement de chargement de classe doit être effectué au niveau de l'application et non du module. WebSphere crée un fichier EAR pour le WAR déployé et fait de ce dernier un module au sein du EAR :



6.2.3 Importation de la racine approuvée d'eDirectory dans le keystore WebSphere

1 Copiez les certificats de racine approuvée 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 109) ou la ligne de commande (« Importation de certificats avec la ligne de commande » page 110).

3 Après avoir importé les certificats, passez à la Section 6.3, « Déploiement du fichier WAR », page 110.

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 panneau de gauche, accédez à *Sécurité* > *Gestion des certificats SSL et des clés*.
3. Dans la liste des paramètres à droite, accédez à *Zone de stockage des clés et des certificats* sous *Éléments associés*.
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.
10. Cliquez sur le lien *Enregistrer* en haut de l'écran.

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.

6.2.4 Transmission de la propriété preferIPv4Stack à la JVM

L'application utilisateur utilise JGroups pour l'implémentation du caching. Dans certaines configurations, JGroups requiert que la propriété preferIPv4Stack soit définie sur vrai pour garantir le bon fonctionnement de la liaison mcast_addr. Sans cette option, l'erreur ci-dessous peut se produire et le caching ne fonctionne pas correctement :

```
[10/1/09 16:11:22:147 EDT] 0000000d UDP           W org.jgroups.util.Util
createMulticastSocket could not bind to /228.8.8.8 (IPv4 address); make sure
your mcast_addr is of the same type as the IP stack (IPv4 or IPv6).
```

Le paramètre `java.net.preferIPv4Stack=true` est une propriété système qui peut être configurée de la même façon que les autres propriétés système telles que `extend.local.config.dir`. Pour obtenir les instructions relatives à la configuration des propriétés système, reportez-vous à la Section 6.2.2, « Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM », page 104.

6.3 Déploiement du fichier WAR

Déployez le fichier WAR via les outils de déploiement WebSphere.

6.3.1 Configuration supplémentaire pour WebSphere 7.0

Si vous utilisez WebSphere 7.0 avec la version 4.0 de RBPM, vous devez savoir que dans cette version de RBPM, plusieurs fichiers JAR (tels que commons-digester.jar) ont été mis à niveau vers les dernières versions disponibles. Par conséquent, si vous ne configurez pas votre environnement correctement, des conflits de version sont susceptibles de se produire avec les fichiers JAR fournis avec WebSphere.

Pour vérifier que vous utilisez les fichiers JAR appropriés, vous devez configurer votre serveur WebSphere pour qu'il charge d'abord les classes du fichier IDMProv.war. Pour le fichier IDMProv.war, vous devez sélectionner l'option *D'abord les classes chargées avec le chargeur de classes local (parent en dernier)*.

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 113
- Section 7.2, « Installation et configuration du fichier WAR de l'application utilisateur », page 114
- Section 7.3, « Préparation de l'environnement WebLogic », page 128
- Section 7.4, « Déploiement du fichier WAR de l'application utilisateur », page 131
- Section 7.5, « Accès à l'application utilisateur », page 131

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 133.

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/idm40/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 114.

- ❑ 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 128.

- ❑ Déployez le fichier WAR.

  Reportez-vous à la Section 7.4, « Déploiement du fichier WAR de l'application utilisateur », page 131.

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 JRockit (version 1.6_17) :

   Solaris

   ```
   $ /opt/WL/bea/jrockit_160_17/bin/java -jar IdmUserApp.jar
   ```

   Windows

   ```
   C:\WL\bea\jrockit_160_17\bin\java -jar IdmUserApp.jar
   ```

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

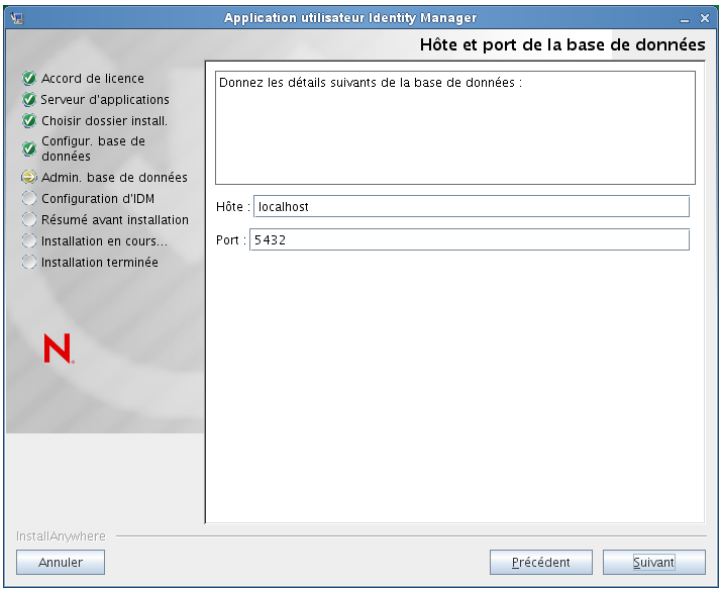
3. Utilisez les informations suivantes pour sélectionner la langue, confirmer l'accord de licence et choisir la plate-forme du serveur d'applications :

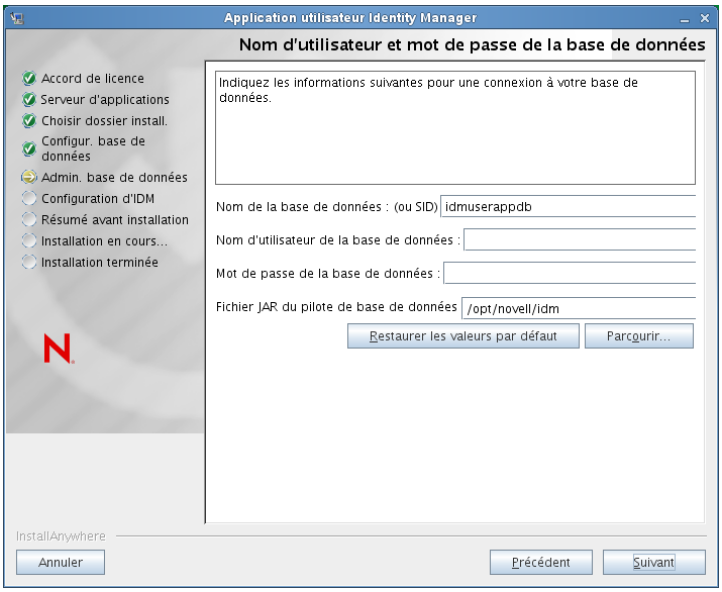
Écran d'installation	Description
Installation de l'application utilisateur	Sélectionnez la langue du programme d'installation. La valeur par défaut est Français.
Accord de licence	Lisez l'accord de licence, puis sélectionnez *J'accepte les termes de l'accord de licence*.

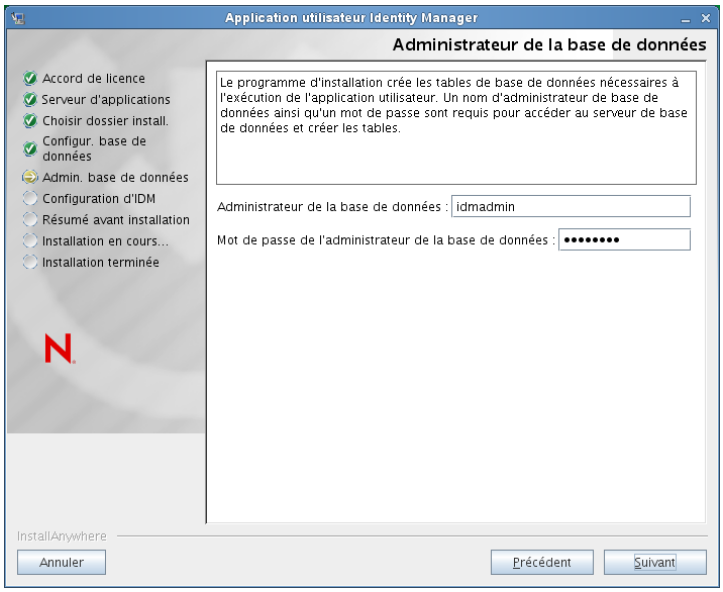
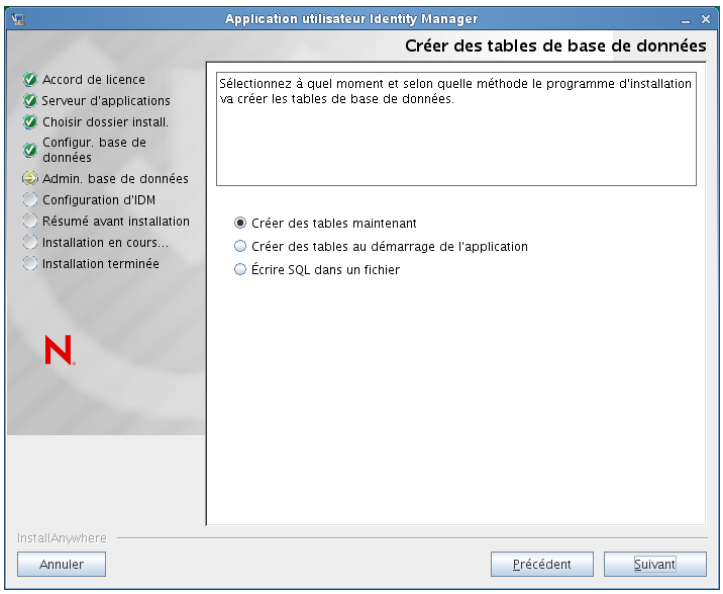
Écran d'installation	Description
Plate-forme du serveur d'applications	Sélectionnez *WebLogic.* Si le fichier WAR de l'application utilisateur est dans un répertoire différent du programme d'installation, ce dernier vous invite à saisir le chemin d'accès au WAR. Si le fichier WAR se trouve à l'emplacement par défaut, vous pouvez cliquez sur *Restaurer le fichier par défaut*. Ou, pour spécifier l'emplacement du fichier WAR, cliquez sur *Choisir* et sélectionnez un emplacement. 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 : 

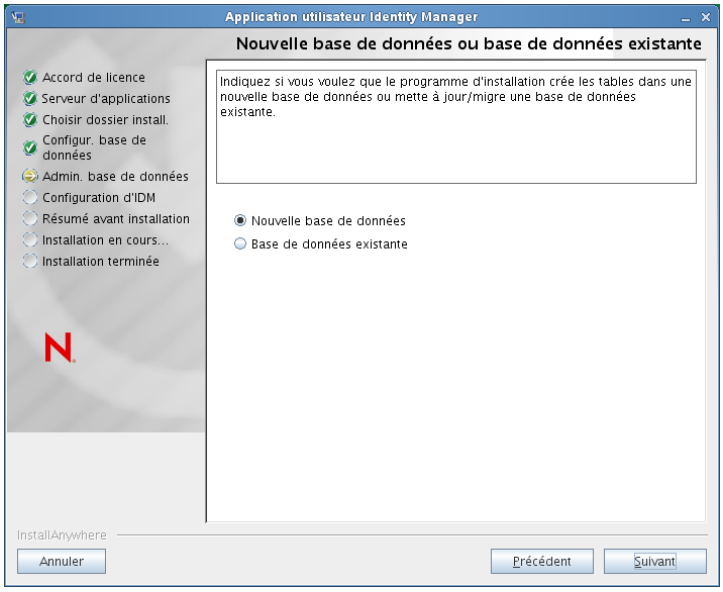
4 Aidez-vous des informations suivantes pour sélectionner le type d'installation, choisir un dossier d'installation et configurer la base de données :

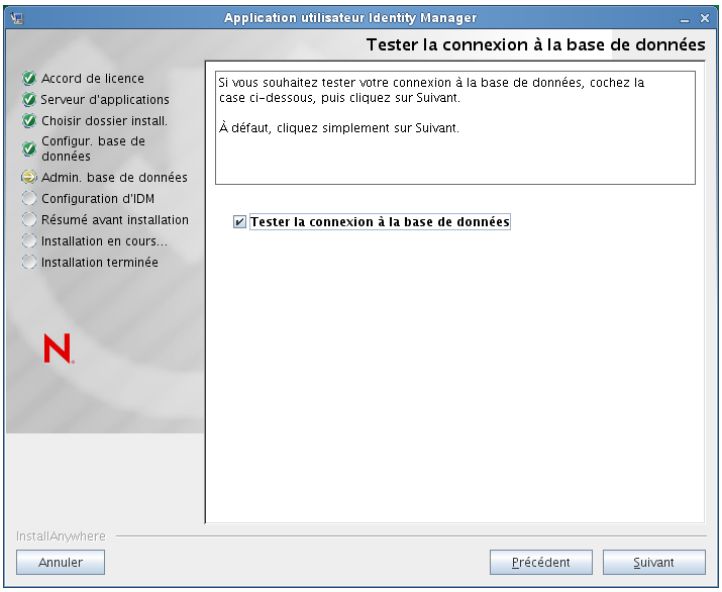
Écran d'installation	Description
Type d'installation	*Provisioning basé sur les rôles* : sélectionnez cette option pour installer le module de provisioning basé sur les rôles. Il s'agit du seul type d'installation pris en charge avec cette version.
Sélectionnez le dossier d'installation	Indiquez l'emplacement 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 WebLogic, les options sont les suivantes : ◆ Oracle ◆ Microsoft SQL Server ◆ PostgreSQL

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

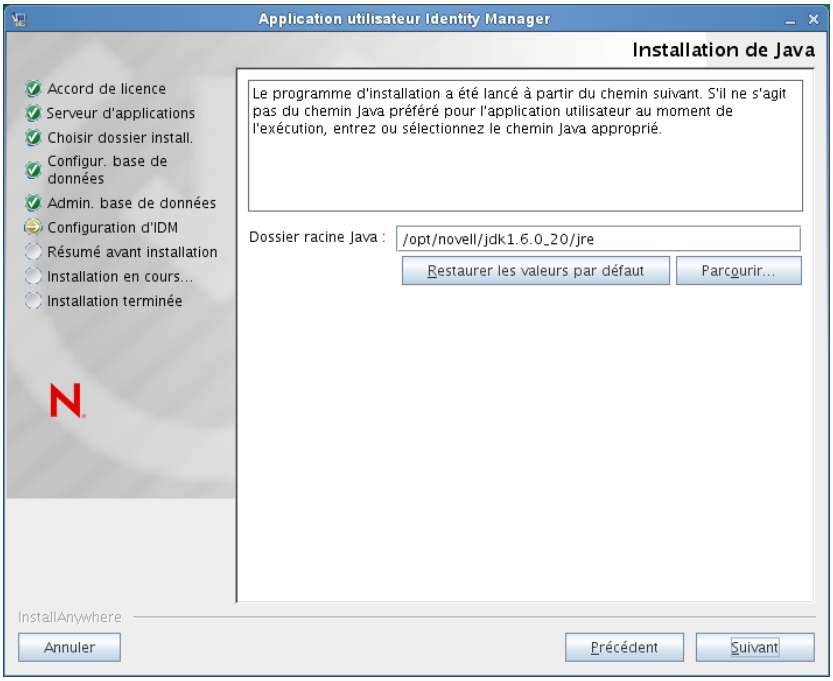
Écran d'installation	Description
Nom d'utilisateur et mot de passe de la base de données	*Nom de la base de données* (ou SID) : pour MS SQL Server ou PostgreSQL, indiquez le nom de votre base de données préconfigurée. Pour Oracle, donnez l'identificateur système Oracle (SID) que vous avez créé précédemment. 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. 

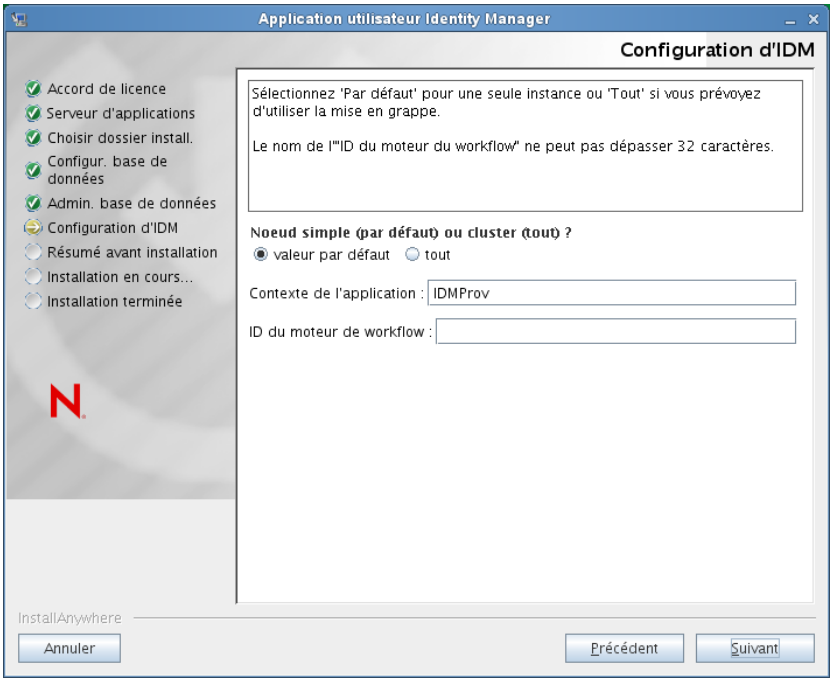
Écran d'installation	Description
Administrateur de la base de données	Cette page est préremplie avec les mêmes nom d'utilisateur et mot de passe que sur la page Nom d'utilisateur et mot de passe de la base de données. Si l'utilisateur de base de données spécifié précédemment ne possède pas les autorisations 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. 
Créer des tables de base de données	Indiquez le moment auquel les tables de base de données doivent être créées : 

Écran d'installation	Description
Nouvelle base de données ou base de données existante	Si la base de données à utiliser est nouvelle ou vide, sélectionnez *Nouvelle base de données*. Si la base de données provient d'une installation précédente, sélectionnez *Base de données existante*. 

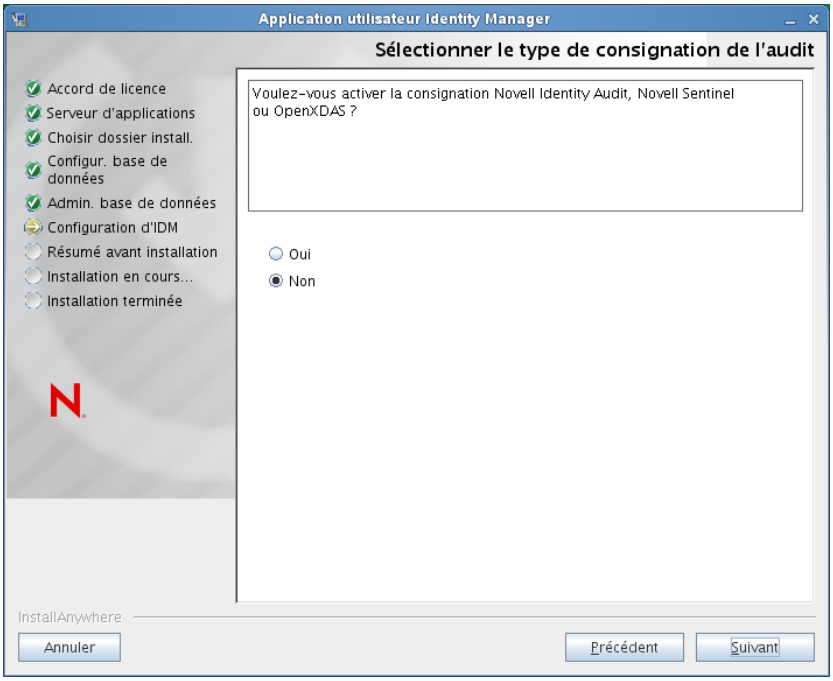
Écran d'installation	Description
Tester la connexion à la base de données	Pour vérifier que les informations fournies dans les écrans précédents sont correctes, vous pouvez tester la connexion à la base de données en cochant la case *Tester la connexion à la base de données* :  Le programme d'installation doit se connecter à la base de données pour créer les tables directement et créer le fichier .SQL. Un échec au test de connexion à la base de données permet néanmoins de poursuivre l'installation. Dans ce cas, vous devrez créer les tables après l'installation, comme décrit dans le *User Application: Administration Guide* (http://www.novell.com/documentation/idm40/agpro/?page=/documentation/idm40/agpro/data/bncf7rj.html) (Guide d'administration de l'application utilisateur).

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. 

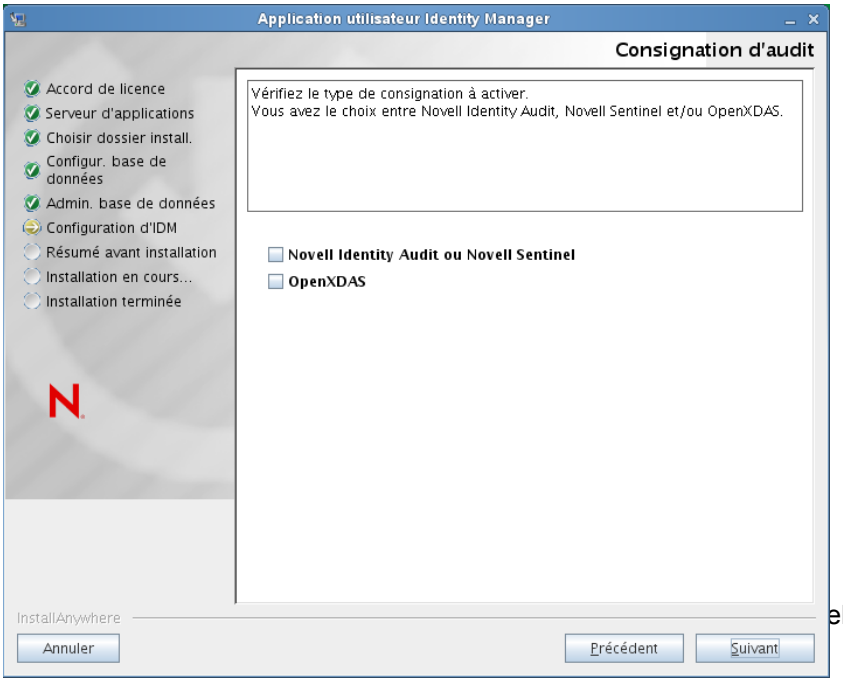
Écran d'installation	Description
Sélectionner le type de consignation de l'audit	Pour activer la consignation, cliquez sur *Oui*. Pour désactiver la consignation, cliquez sur *Non*.



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

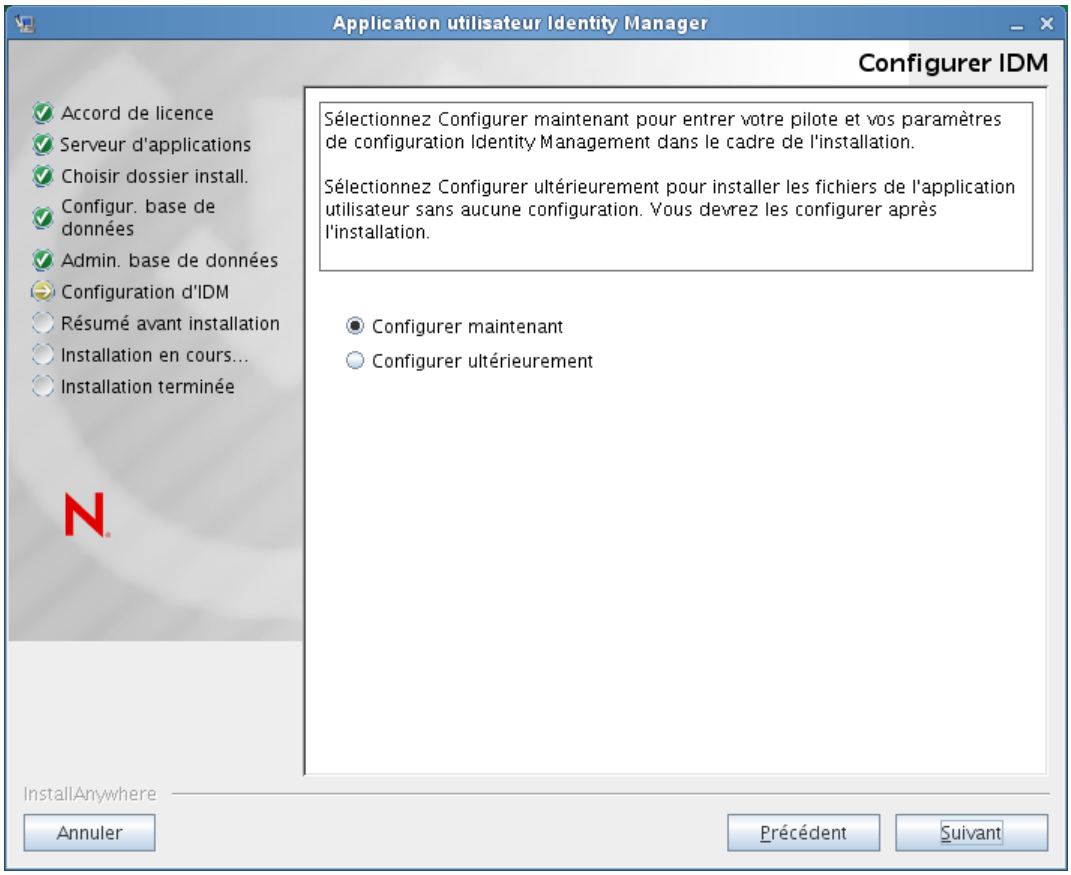
- *Novell Identity Audit ou Novell Sentinel* : permet d'activer la consignation via un client d'audit Novell pour l'application utilisateur.
- *OpenXDAS* : les événements sont consignés sur votre serveur de consignation OpenXDAS.

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).



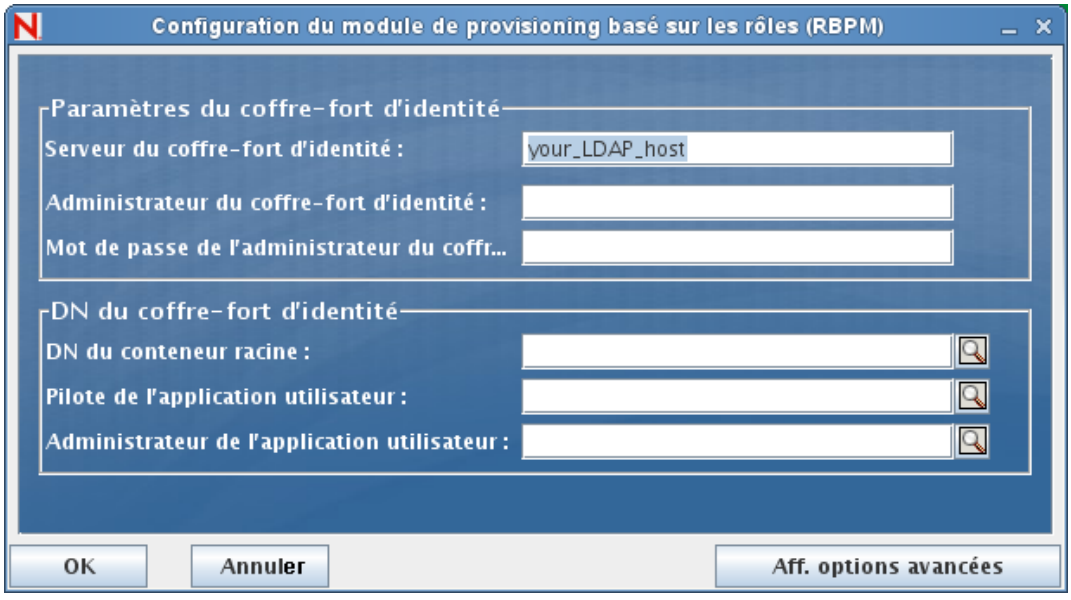
Écran d'installation	Description
Novell Identity Audit ou Novell Sentinel	*Serveur* : si vous activez la consignation, indiquez le nom d'hôte ou l'adresse IP du serveur. Si vous désactivez la consignation, cette valeur est ignorée. *Dossier de cache des journaux* : indiquez le répertoire du cache de consignation.
Sécurité : clé principale	*Oui* : 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. *Non* : 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 149. La procédure d'installation inscrit la clé maîtresse codée dans le fichier `master-key.txt` dans le répertoire d'installation. Voici des raisons d'importer une clé principale existante : ◆ Vous déplacez votre installation d'un système provisoire à un système de production et vous souhaitez conserver l'accès à la base de données que vous avez utilisée avec le système provisoire. ◆ Vous avez installé l'application utilisateur sur le premier membre d'une grappe et vous l'installez maintenant sur de nouveaux membres de la grappe (qui requièrent la même clé maîtresse). ◆ En raison d'un disque défectueux, vous devez restaurer votre application utilisateur. Vous devez réinstaller l'application utilisateur et indiquer la même clé maîtresse codée que celle qu'utilisait l'installation précédente. Cela vous donne accès aux données codées stockées précédemment.

6 Si vous souhaitez configurer le module RBPM maintenant, sélectionnez *Configurer maintenant*, puis cliquez sur *Suivant*.



(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 32.)

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



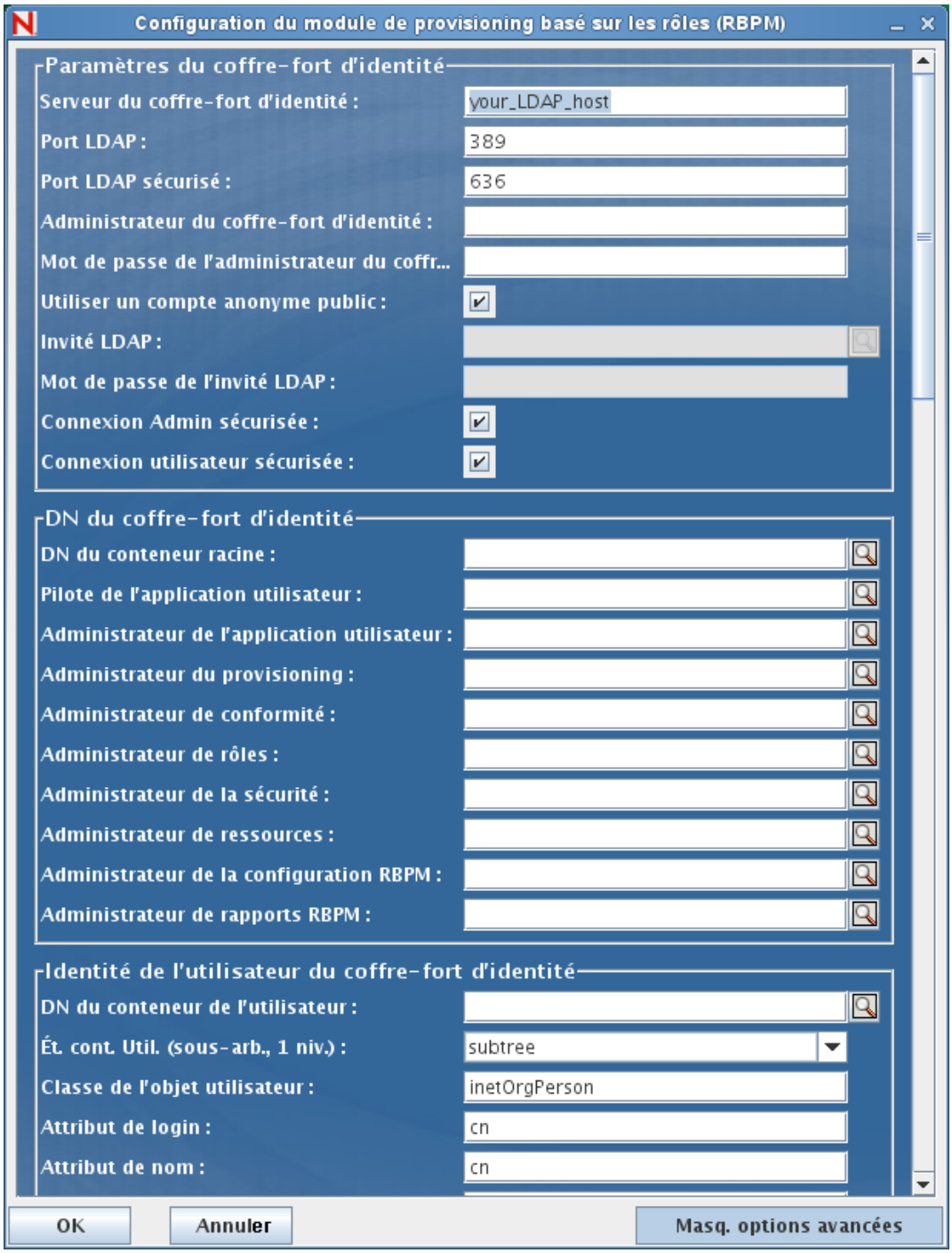
Le programme d'installation utilisera la valeur du champ DN du conteneur racine et l'appliquera aux valeurs suivantes :

- 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 :



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

Reportez-vous à l'Annexe A, « Référence de configuration de l'application utilisateur IDM », page 157 pour obtenir une description des options.

7 Les informations suivantes permettent de terminer l'installation.

Écran d'installation	Description
Résumé pré-installation	Lisez la page de résumé de la pré-installation pour vérifier vos paramètres d'installation. Si nécessaire, utilisez *Retour* pour retourner aux pages d'installation précédentes et modifier les paramètres d'installation. La page de configuration de l'application utilisateur ne sauvegarde pas de valeur. Une fois les pages précédentes de l'installation à nouveau spécifiées, vous devez saisir à nouveau les valeurs de configuration de l'application utilisateur. Lorsque vous êtes satisfait de vos paramètres d'installation et de configuration, retournez à la page Récapitulatif de pré-installation, puis cliquez sur *Installer*.
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, « Configuration de la réserve de connexions », page 128
- Section 7.3.2, « Définition de l'emplacement des fichiers de configuration du module RBPM », page 129
- Section 7.3.3, « Suppression des fichiers JAR OpenSAML », page 131
- Section 7.3.4, « Plug-in de workflow et configuration de WebLogic », page 131

7.3.1 Configuration de la réserve de connexions

- ❑ Copiez les fichiers JAR du pilote de votre base de données dans le domaine où vous voulez déployer l'application utilisateur.
- ❑ 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 module RBPM

L'application utilisateur WebLogic doit pouvoir localiser les fichiers `sys-configuration-xmldata.xml`, `idmuserapp_logging.xml` et `wl_idmuserapp_logging.xml`. Pour cela, vous devez ajouter l'emplacement des fichiers au 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`.
   - `-Dlog.init.file==<nom_fichier>` : indiquez le fichier `wl_idmuserapp_logging.xml` utilisé pour la configuration log4j. Ce fichier gère les configurations appender et logger requises pour l'application utilisateur dans des cas où plusieurs applications sont installées sur le même serveur d'applications.

   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
   set JAVA_OPTIONS=%JAVA_OPTIONS%
   -Dlog.init.file=wl_idmuserapp_logging.xml
   ```

4. Définissez la variable d'environnement `EXT_PRE_CLASSPATH` de façon à ce qu'elle pointe vers les fichiers JAR suivants :

   - `antlr-2.7.6.jar`
   - `log4j.jar`
   - `commons-logging.jar`

     Remarque : vous devez télécharger ce fichier JAR à partir du site Apache.

   - `xalan.jar`
   - `xercesImpl.jar`
   - `xsltc.jar`
   - `serializer.jar`
   - `IDMselector.jar`

Remarque : pour ajouter ces fichiers JAR à la variable EXT_PRE_CLASSPATH, vous pouvez également les copier dans le répertoire WEB-INF/lib du fichier IDMProv.war.

   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;C:\bea\user_projects\domains\base_domain\lib\xalan.jar;C:
\bea\user_projects\domains\base_domain\lib\xercesImpl.jar;C:\bea\user
_projects\domains\base_domain\lib\xsltc.jar;C:\bea\user_projects\doma
ins\base_domain\lib\serializer.jar
```

Par exemple, sous Linux :

```
export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/
lib/antlr-2.7.6.jar:/opt/bea/user_projects/domain/base_domain/lib/
log4j.jar:/opt/bea/user_projects/domains/base_domain/lib/commons-
logging.jar:/opt/bea/user_projects/domains/base_domain/lib/
xalan.jar:/opt/bea/user_projects/domains/base_domain/lib/
xercesImpl.jar:/opt/bea/user_projects/domains/base_domain/lib/
xsltc.jar:/opt/bea/user_projects/domains/base_domain/lib/
serializer.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 le chemin au fichier sys-configuration.xml :

Par exemple, sous Windows :

```
-Dextend.local.config.dir=c:\novell\idm
```

Par exemple, sous Linux :

```
-Dextend.local.config.dir=/opt/novell/idm
```

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 `configupdate`, 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 Suppression des fichiers JAR OpenSAML

Les fichiers JAR OpenSAML utilisés par WebLogic créent des conflits avec ceux requis par l'application utilisateur. Par conséquent, vous devez supprimer les fichiers du répertoire WebLogic / WL103/modules afin de garantir le déploiement correct de l'application utilisateur sur WebLogic. Cette exigence s'applique à toute application utilisateur dont la fonction SSO n'est pas activée.

Veillez à supprimer les fichiers JAR suivants du répertoire WebLogic /WL103/modules :

```
com.bea.core.bea.opensaml_1.0.0.0_5-0-2-0.jar
com.bea.core.bea.opensaml2_1.0.0.0_5-0-2-0.jar
```

7.3.4 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 dans la section `<security-configuration>` juste avant la fin de cette section :

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

À ce stade, vous pouvez déployer le fichier WAR de l'application utilisateur en ayant recours à 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:8180/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 59. Les rubriques sont les suivantes :

- Section 8.1, « Installation de l'application utilisateur à partir de la console », page 133
- Section 8.2, « Installation de l'application utilisateur avec une seule commande », page 134
- Section 8.3, « Exécution de l'utilitaire JBossPostgreSQL en mode console ou silencieux », page 145
- Section 8.4, « Exécution du programme d'installation RIS en mode console ou silencieux », page 146

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 59 : 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 157.
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 149.

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 silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_LDAPHOST=	Paramètres de connexion eDirectory : hôte LDAP. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_LDAPADMIN=	Paramètres de login eDirectory : administrateur LDAP. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer une connexion administrative au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
NOVL_CONFIG_LDAPADMINPASS=	Paramètres de login eDirectory : mot de passe administrateur LDAP. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
NOVL_CONFIG_ROOTCONTAINERNAME=	DN eDirectory : DN du conteneur racine. Indiquez le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire.
NOVL_CONFIG_PROVISIONROOT=	DN eDirectory : DN du pilote de provisioning. Indiquez le nom distinctif du pilote de l'application utilisateur. Par exemple, si votre pilote est UserApplicationDriver et si votre ensemble de pilotes est appelé myDriverSet, et si l'ensemble de pilotes est dans un contexte de o=myCompany, vous saisissez une valeur de : `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_LOCKSMITH=	DN eDirectory : admin. de l'application utilisateur. Un utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs de l'application utilisateur spécifié. Cet utilisateur peut utiliser l'onglet *Administration* de l'application utilisateur pour administrer le portail. Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, Novell Designer pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), 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 *Guide d'administration de l'application utilisateur* pour en savoir plus. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.
NOVL_CONFIG_PROVLOCKSMITH=	DN eDirectory : administrateur de l'application de provisioning. Ce rôle est disponible dans la version de provisioning d'Identity Manager . L'administrateur de l'application de provisioning utilise l'onglet *Provisioning* (sous l'onglet *Administration*) pour gérer les fonctions de workflow du provisioning. Ces fonctions sont accessibles aux utilisateurs en passant par l'onglet *Requêtes et approbations* de l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur de l'application Provisioning. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_ROLECONTAINERDN=	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. Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page *Rôles* > *Assignations de rôles* de l'application utilisateur.
NOVL_CONFIG_COMPLIANCECONTAINERDN	L'administrateur du module de conformité est un rôle système qui permet aux membres d'exécuter toutes les fonctions de l'onglet *Conformité*. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné comme administrateur du module de conformité.
NOVL_CONFIG_USERCONTAINERDN=	Identité utilisateur du méta-annuaire : DN du conteneur utilisateur. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur utilisateur. Cela définit l'étendue de recherche d'utilisateurs et de groupes. Les utilisateurs de ce conteneur (et en-dessous) sont autorisés à se loguer à l'application utilisateur. **Important :** 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.
NOVL_CONFIG_GROUPCONTAINERDN=	Groupes d'utilisateurs du méta-annuaire : DN du conteneur de groupes. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur de groupes. Utilisé par les définitions d'entités au sein de la couche d'abstraction d'annuaire.
NOVL_CONFIG_KEYSTOREPATH=	Certificats eDirectory : chemin d'accès au keystore. Requis. Indiquez le chemin d'accès complet au fichier keystore (`cacerts`) 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.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_KEYSTOREPASSWORD=	Certificats eDirectory : mot de passe du keystore. Indiquez le mot de passe `cacerts`. L'unité par défaut est `changeit`.
NOVL_CONFIG_SECUREADMINCONNECTION=	Paramètres de connexion eDirectory : connexion d'admin. sécurisée. Requis. Indiquez *Vrai* 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. Indiquez *Faux* si le compte administrateur n'utilise pas de communication à socket sécurisé.
NOVL_CONFIG_SECUREUSERCONNECTION=	Paramètres de connexion eDirectory : connexion utilisateur sécurisée. Requis. Indiquez *Vrai* 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. Indiquez *Faux* si le compte utilisateur n'utilise pas de communication par socket sécurisé.
NOVL_CONFIG_SESSIONTIMEOUT=	Divers : timeout de session. Requis. Indiquez un intervalle de timeout de session d'application.
NOVL_CONFIG_LDAPPLAINPORT=	Paramètres de connexion eDirectory : port non sécurisé LDAP. Requis. Indiquez le port non sécurisé de votre serveur LDAP, par exemple 389.
NOVL_CONFIG_LDAPSECUREPORT=	Paramètres de connexion eDirectory : port sécurisé LDAP. Requis. Indiquez le port sécurisé de votre serveur LDAP, par exemple 636.
NOVL_CONFIG_ANONYMOUS=	Paramètres de connexion eDirectory : utiliser un compte anonyme public. Requis. Indiquez *Vrai* pour permettre aux utilisateurs non logués d'accéder au compte anonyme public LDAP. Indiquez *Faux* si vous préférez activer NOVL_CONFIG_GUEST.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_GUEST=	Paramètres de login eDirectory : invité LDAP. Permet aux utilisateurs non logués d'accéder à des portlets autorisés. Vous devez également désélectionner *Utiliser un compte anonyme public*. Le compte utilisateur Guest doit déjà exister dans le coffre-fort d'identité. Pour désactiver l'utilisateur Guest, sélectionnez *Utiliser un compte anonyme public*.
NOVL_CONFIG_GUESTPASS=	Paramètres de connexion eDirectory : mot de passe Guest LDAP.
NOVL_CONFIG_EMAILNOTIFYHOST=	Courrier électronique : jeton HÔTE du modèle de notification. Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple : `myapplication serverServer` Cette valeur remplace le jeton $HOST$ des modèles de courrier électronique. L'URL construite est la liaison aux tâches de requête de provisioning et aux notifications d'approbation.
NOVL_CONFIG_EMAILNOTIFYPORT=	Courrier électronique : jeton du port du modèle de notification. Utilisé pour remplacer le jeton $PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	Courrier électronique : jeton du port sécurisé du modèle de notification. Utilisé pour remplacer le jeton $SECURE_PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
NOVL_CONFIG_NOTFSMTPEMAILFROM=	Courrier électronique : notification SMTP - expéditeur du courrier électronique. Requis. Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
NOVL_CONFIG_NOTFSMTPEMAILHOST=	Courrier électronique : notification SMTP - destinataire du courrier électronique. 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.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_USEEXTPWDWAR=	Gestion des mots de passe : utiliser un WAR de mots de passe externe. Indiquez *Vrai* si vous utilisez un WAR de gestion de mots de passe externe. Si vous indiquez *Vrai*, vous devez également fournir des valeurs pour *NOVL_CONFIG_EXTPWDWARPTH* et *NOVL_CONFIG_EXTPWDWARRTNPATH*. Indiquez *Faux* pour utiliser la fonction de gestion des mots de passe interne par défaut, `/jsps/pwdmgt/ForgotPassword.jsp` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.
NOVL_CONFIG_EXTPWDWARPATH=	Gestion des mots de passe : liaison Mot de passe oublié. Indiquez l'URL de la page de la fonction Mot de passe oublié, `ForgotPassword.jsp`, 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 152.
NOVL_CONFIG_EXTPWDWARRTNPATH=	Gestion des mots de passe : liaison de retour Mot de passe oublié. 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.
NOVL_CONFIG_FORGOTWEBSERVICEURL=	Gestion des mots de passe : URL du service Web de mot de passe oublié. 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 : `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
NOVL_CONFIG_USEROBJECTATTRIBUTE=	Identité utilisateur du méta-annuaire : classe d'objets utilisateur. Requis. La classe d'objets utilisateur LDAP (généralement inetOrgPerson).

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_LOGINATTRIBUTE=	Identité utilisateur du méta-annuaire : attribut de login. Requis. L'attribut LDAP (par exemple, CN) qui représente le nom de login de l'utilisateur.
NOVL_CONFIG_NAMINGATTRIBUTE=	Identité utilisateur du méta-annuaire : attribut d'assignation de nom. 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.
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	Identité utilisateur du méta-annuaire : attribut d'adhésion utilisateur. Facultatif. Requis. L'attribut LDAP qui représente l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	Groupes d'utilisateurs du méta-annuaire : classe d'objets Groupe. Requis. La classe d'objets Groupe LDAP (généralement groupofNames).
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	Groupes d'utilisateurs du méta-annuaire : attribut d'adhésion à un groupe. Requis. Indiquez l'attribut représentant l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.
NOVL_CONFIG_USEDYNAMICGROUPS=	Groupes d'utilisateurs du méta-annuaire : utiliser des groupes dynamiques. Requis. Indiquez *Vrai* si vous souhaitez utiliser les groupes dynamiques. Indiquez *Faux* dans le cas contraire.
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	Groupes d'utilisateurs du méta-annuaire : classe d'objets de groupe dynamique. Requis. Indiquez la classe d'objets de groupe dynamique LDAP (généralement dynamicGroup).
NOVL_CONFIG_TRUSTEDSTOREPATH=	Keystore approuvé : chemin de keystore approuvé. Le keystore approuvé contient les certificats de tous les signataires approuvés. Si ce chemin est vide, l'application utilisateur obtient le chemin à partir de la propriété Système `javax.net.ssl.trustStore`. Si le chemin n'y est pas, il est supposé être `jre/lib/security/cacerts`.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	Keystore approuvé : mot de passe du keystore approuvé.
NOVL_CONFIG_ICSLOGOUTENABLED=	Paramètres Access Manager et IChain : logout simultané activé. Indiquez *Vrai* 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. Indiquez *Faux* pour désactiver le logout simultané.
NOVL_CONFIG_ICSLOGOUTPAGE=	Paramètres Access Manager et IChain : page de logout simultané. 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.
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	Courrier électronique : jeton PROTOCOLE du modèle de notification. Se rapporte à un protocole non sécurisé, HTTP. Utilisé pour remplacer le jeton $PROTOCOL$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	Courrier électronique : jeton du port sécurisé du modèle de notification.
NOVL_CONFIG_OCSPURI=	Divers : OCSP URI. Si l'installation client utilise le protocole OCSP (protocole de propriété d'état de certificat en ligne), fournissez un identificateur de ressource uniforme (URI). Par exemple, le format est http://hstport/ocspLocal. L'URI OCSP met à jour le statut des certificats approuvés en ligne.
NOVL_CONFIG_AUTHCONFIGPATH=	Divers : chemin de configuration d'autorisation. Le nom complet du fichier de configuration de l'autorisation.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_CONFIG_CREATEDIRECTORYINDEX	Divers : créer un index eDirectory. Indiquez Vrai si vous souhaitez que le programme d'installation silencieux crée des index sur les attributs manager, ismanager et srvprvUUID sur le serveur eDirectory indiqué dans NOVL_CONFIG_SERVERDN. Si ce paramètre est défini sur Vrai, NOVL_CONFIG_REMOVEEDIRECTORYINDEX ne peut pas être Vrai. 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.
NOVL_CONFIG_REMOVEDIRECTORYINDEX	Divers : supprimer un index eDirectory. Indiquez Vrai si vous souhaitez que le programme d'installation silencieux supprime des index sur le serveur indiqué dans NOVL_CONFIG_SERVERDN. Si ce paramètre est défini sur Vrai, NOVL_CONFIG_CREATEEDIRECTORYINDEX ne peut pas être Vrai.
NOVL_CONFIG_SERVERDN	Divers : DN de serveur. Indiquez le serveur eDirectory sur lequel les index doivent être créés ou duquel ils doivent être supprimés.
NOVL_CREATE_DB	Indique la méthode de création de la base de données. Vous avez le choix entre : ◆ maintenant : crée la base de données immédiatement ◆ fichier : écrit la sortie SQL dans un fichier ◆ démarrage : crée la base de données au démarrage de l'application
NOVL_DATABASE_NEW	Indique si la base de données est nouvelle ou existe déjà. Choisissez *Vrai* dans le cas d'une nouvelle base de données. Choisissez *Faux* dans le cas d'une base de données existante.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
NOVL_RBPM_SEC_ADMINDN	Administrateur de la sécurité. Ce rôle permet aux membres d'accéder à toutes les fonctionnalités du domaine Sécurité. L'administrateur de la sécurité peut effectuer toutes les opérations possibles sur tous les objets au sein du domaine Sécurité. 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.
NOVL_RBPM_RESOURCE_ADMINDN	Administrateur de ressources. 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.
NOVL_RBPM_CONFIG_ADMINDN	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 proxy et de délégation, l'interface utilisateur de provisioning et le moteur de workflow.
RUN_LDAPCONFIG=	Indique à quel moment vous souhaitez configurer les paramètres LDAP, à savoir maintenant ou ultérieurement. Valeurs : ◆ Maintenant : exécute la configuration LDAP immédiatement en remplissant le fichier WAR avec les paramètres de configuration LDAP fournis. ◆ Ultérieurement : installe simplement les fichiers de l'application utilisateur sans configurer les paramètres LDAP.

8.3 Exécution de l'utilitaire JBossPostgreSQL en mode console ou silencieux

Vous pouvez exécuter l'utilitaire JBossPostgreSQL en mode console ou silencieux. Avant d'exécuter l'utilitaire JBossPostgreSQL en mode silencieux, vous devez éditer son fichier de propriétés. Une fois le fichier de propriétés édité, lancez-le à l'aide de la commande suivante :

```
JBossPostgreSQL -i silent -f <path to the properties file>
```

Par exemple :

```
JBossPostgreSQL -i silent -f /home/jdoe/idm-install-files/silent.properties
```

Voici les propriétés d'une installation JBossPostgreSQL en mode silencieux :

Tableau 8-2 *Propriétés de configuration JBossPostgreSQL*

Propriété	Description
USER_INSTALL_DIR	Chemin d'installation de JBoss et du JRE. Requis en cas d'installation de JBoss ; dans le cas contraire, ne pas renseigner.
NOVL_DB_NAME	Nom de la base de données à utiliser. Le nom de la base de données par défaut est idmuserappdb. Requis en cas d'installation de PostgreSQL. Si vous n'installez pas PostgreSQL, cette valeur est ignorée.
NOVL_DB_PASSWORD	Mot de passe root de la base de données. Requis en cas d'installation de PostgreSQL. Si vous n'installez pas PostgreSQL, cette valeur est ignorée.
NOVL_DB_PASSWORD_CONFIRM	Confirme le mot de passe root de la base de données. Requis en cas d'installation de PostgreSQL. Si vous n'installez pas PostgreSQL, cette valeur est ignorée.

CHOSEN_INSTALL_FEATURE_LIST	Ensembles d'installation à installer
	
	Requis. Vous pouvez choisir d'installer JBoss et PostgreSQL ou uniquement l'un de ces deux produits.
	
	Exemples :
	
	`CHOSEN_INSTALL_FEATURE_LIST=JBoss, PostgreSQL`
	
	`CHOSEN_INSTALL_FEATURE_LIST=JBoss,""`

Propriété	Description
NOVL_POSTGRESQL_INSTALL_DIR	Nom du répertoire d'installation de PostgreSQL. Requis en cas d'installation de PostgreSQL. Si CHOSEN_INSTALL_FEATURE_LIST n'inclut pas PostgreSQL, cette propriété est ignorée.
START_DB	Indique si le programme d'installation lance la base de données au moment de l'installation. Indiquez la valeur Démarrer si vous souhaitez que le programme d'installation lance la base de données ; dans le cas contraire, ne renseignez pas cette propriété. Facultatif.

8.4 Exécution du programme d'installation RIS en mode console ou silencieux

Cette version inclut un programme d'installation distinct que vous pouvez utiliser pour configurer la fonction RIS (Rest Information Services). Cette fonction permet de configurer le fichier RIS.war, qui prend en charge les ressources REST. Les ressources REST exposées via RIS passent des appels SOAP pour collecter des informations à partir de différents systèmes RBPM.

Vous pouvez exécuter le programme d'installation RIS en mode console ou silencieux. Avant d'exécuter le programme d'installation RIS, vous devez éditer son fichier de propriétés. Une fois le fichier de propriétés édité, lancez-le à l'aide de la commande suivante :

```
RisUpdateWar -i silent -f <path to the properties file>
```

Par exemple :

```
RisUpdateWar -i silent -f /home/jdoe/idm-install-files/silent.properties
```

Le programme d'installation requiert les informations suivantes :

- Emplacement du fichier RIS.war
- Port d'exécution de l'application utilisateur
- Contexte défini pour l'application utilisateur
- Nom de l'hôte sur lequel le fichier RIS.war sera déployé

Voici les propriétés d'une installation RIS :

Tableau 8-3 *Propriétés de configuration RIS*

Propriété	Description
NOVL_INSTALL_HOST	Nom de l'hôte sur lequel le fichier RIS.war sera déployé. Ce nom ne peut pas être localhost. Requis.

Propriété	Description
NOVL_USERAPP_PORT	Port sur lequel s'exécute l'application utilisateur RBPM. Requis.
NOVL_CONTEXT_NAME	Nom du contexte de l'application utilisateur Requis.
RIS_INSTALL_DIRECTORY	Répertoire d'installation du fichier RIS.war Requis.
RIS_WAR_FILE	Nom du fichier RIS.war. Ne modifiez pas cette valeur.
RIS_INSTALL_LOG	Nom du fichier journal du programme d'installation. Vous pouvez choisir un nom pour le fichier. Le programme d'installation écrit le fichier à l'emplacement spécifié dans la propriété RIS_INSTALL_DIR. Si vous ne renseignez pas cette propriété, le fichier journal par défaut est RIS-Install.log. Facultatif.

Tâches post-installation

9

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

- Section 9.1, « Enregistrement de la clé maîtresse », page 149
- Section 9.2, « Configuration de l'application utilisateur », page 149
- Section 9.3, « Configuration d'eDirectory », page 150
- Section 9.4, « Reconfiguration du fichier WAR de l'application utilisateur après l'installation », page 152
- Section 9.5, « Configuration de la gestion externe des mots de passe oubliés », page 152
- Section 9.6, « Mise à jour des paramètres de mot de passe oublié », page 153
- Section 9.7, « Considérations relatives à la sécurité », page 154
- Section 9.8, « Augmentation de la taille du tas Java d'IDM », page 154
- Section 9.9, « Dépannage », page 154

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/idm40/index.html) (Guide d'administration de l'application utilisateur).

9.3 Configuration d'eDirectory

- Section 9.3.1, « Création d'index dans eDirectory », page 150
- Section 9.3.2, « Installation et configuration de la méthode d'authentification SAML », page 150

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 160). 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 d'*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 157 et au Tableau 8-1 page 134.

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 152
- Section 9.5.2, « Spécification d'un WAR de mot de passe interne », page 153
- Section 9.5.3, « Test de la configuration du fichier WAR externe pour les mots de passe oubliés », page 153
- Section 9.5.4, « Configuration de la communication SSL entre serveurs JBoss », page 153

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:8180/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 153.

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 fichier WAR de mots de passe externe, par exemple `http://localhost:8180/ExternalPwd/jsps/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:8180/ExternalPwd/jsps/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 Augmentation de la taille du tas Java d'IDM

Dans un environnement d'entreprise, le pilote du service de rôles et de ressources requiert une taille maximale de tas Java supérieure à la quantité par défaut définie dans IDM. Une taille maximale de segment Java de 256 Mo est recommandée afin d'éviter les situations OutOfMemoryError.

La taille du segment Java peut être spécifiée dans iManager, sous la section Divers des propriétés de l'ensemble de pilotes, ou en configurant les variables d'environnement DHOST_JVM_INITIAL_HEAP et DHOST_JVM_MAX_HEAP. Pour plus d'informations sur la configuration des options de la machine virtuelle Java, reportez-vous au Identity Manager Common Driver Administration Guide (http://www.novell.com/documentation/idm40/idm_common_driver/index.html?page=/documentation/idm40/idm_common_driver/data/front.html) (Guide d'administration des pilotes communs d'Identity Manager).

9.9 Dépannage

Votre représentant Novell vous aidera à régler tout problème d'installation et de configuration. En attendant, voici quelques points à vérifier en cas de problème.

Point	Actions suggérées

Vous souhaitez modifier les paramètres de configuration de l'application utilisateur définis lors de l'installation. Cela comprend la configuration des éléments suivants par exemple :
◆ Connexions et certificats du coffre-fort d'identité
◆ Paramètres de messagerie électronique
◆ Identité utilisateur du méta-annuaire, groupes d'utilisateurs
◆ Paramètres Access Manager ou iChain
	Exécutez l'utilitaire de configuration indépendamment du programme d'installation.
	Sous Linux et Solaris, exécutez la commande suivante depuis le répertoire d'installation (par défaut, `/opt/novell/idm`) :
	`configupdate.sh`
	Sous Windows, exécutez la commande suivante depuis le répertoire d'installation (par défaut, `c:\opt\novell\idm`) :
	`configupdate.bat`

Des exceptions sont renvoyées au démarrage du serveur d'applications, avec un message de journal indiquant `port 8180 already in use`.	Arrêtez toutes les instances de Tomcat (ou autre logiciel de serveur) qui pourraient déjà être en cours d'exécution. Si vous décidez de reconfigurer le serveur d'applications de façon à ce qu'il utilise un autre port que le port 8180, n'oubliez pas de modifier les paramètres `config` du pilote de l'application utilisateur.
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 loguer à la page d'administration du portail.	Assurez-vous que le compte administrateur de l'application utilisateur existe. Ne le confondez pas avec votre compte administrateur iManager. Il s'agit de deux objets admin. différents (normalement).
Vous pouvez vous loguer en tant qu'administrateur, mais vous ne pouvez pas créer de nouveaux utilisateurs.	L'administrateur de l'application utilisateur doit être un ayant droit du conteneur maître et doit avoir des droits de superviseur. En attendant, vous pouvez essayer de configurer les droits administrateur de l'application utilisateur équivalents aux droits administrateur LDAP (via iManager).
Vous rencontrez des erreurs de keystore lors du démarrage du serveur d'applications.	Votre serveur d'applications n'exécute pas le JDK spécifié à l'installation de l'application utilisateur. Utilisez la commande `keytool` pour importer le fichier de certificat : `keytool -import -trustcacerts -alias` *`aliasName`* `-file` *`certFile`* `-keystore ..\lib\security\cacerts -storepass changeit` ◆ Remplacez *aliasName* par un nom unique de votre choix pour ce certificat. ◆ Remplacez *certFile* par le chemin complet et le nom de votre fichier de certificat. ◆ Le mot de passe du keystore par défaut est `changeit` (si vous avez un mot de passe différent, indiquez-le).

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`) :
	
	`configupdate.sh`
	
	Sous Windows, exécutez la commande suivante depuis le répertoire d'installation (par défaut, `c:\opt\novell\idm`) :
	
	`configupdate.bat`

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 157
- Section A.2, « Configuration de l'application utilisateur : tous les paramètres », page 160

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

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

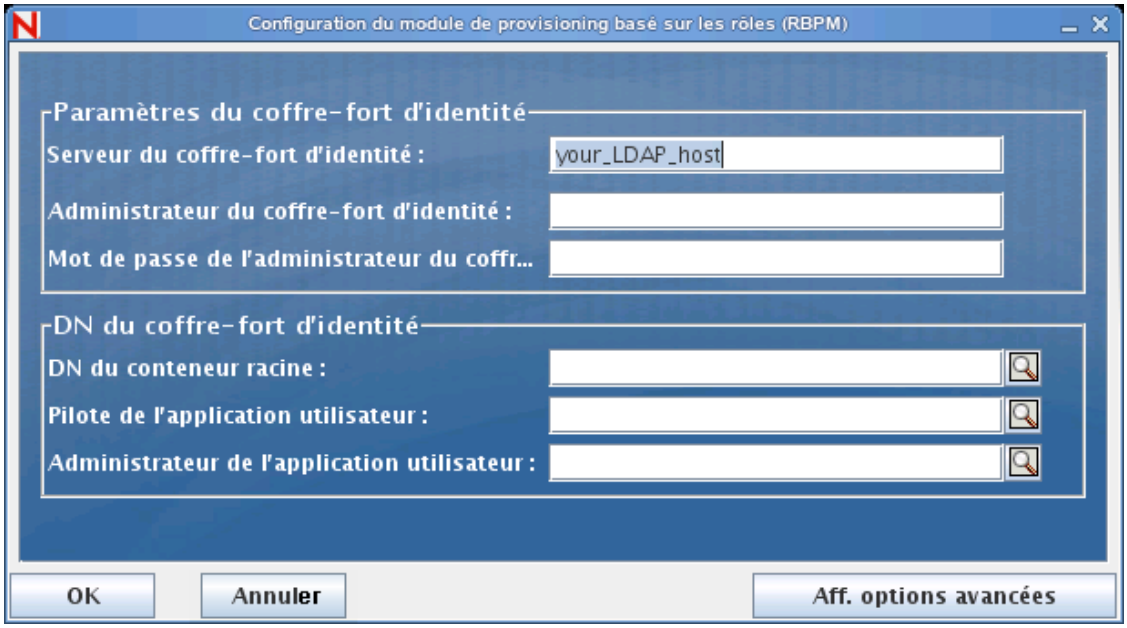


Tableau A-1 *Options de base de configuration de l'application utilisateur*

Type de paramètre	Option	Description
Paramètres du coffre-fort d'identité	*Serveur du coffre-fort d'identité*	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP et son port sécurisé. Par exemple : `myLDAPhost`
	Administrateur du coffre-fort d'identité	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.
	Mot de passe de l'administrateur du coffre-fort d'identité	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	*DN du conteneur racine*	Requis. Indiquez le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire.
	DN du pilote de l'application utilisateur	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur. Par exemple, si votre pilote est UserApplicationDriver, que votre ensemble de pilotes est appelé myDriverSet et que l'ensemble de pilotes est dans un contexte o=myCompany, vous saisissez la valeur suivante : `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Administrateur de l'application utilisateur	Requis. Un utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs de l'application utilisateur spécifié. Cet utilisateur peut utiliser l'onglet *Administration* de l'application utilisateur pour administrer le portail. Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, Novell Designer pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), 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 *Guide d'administration de l'application utilisateur* pour en savoir plus. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur. Vous ne pouvez pas modifier ce paramètre via ConfigUpdate si vous avez démarré le serveur d'applications qui héberge l'application utilisateur.
	Nom du contexte RBPM	Affiche le nom actuel du contexte
	Administrateur de rapports RBPM	Pointe vers l'administrateur de rapports. Par défaut, le programme d'installation définit cette valeur sur le même utilisateur que celui renseigné dans les autres champs de sécurité.

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	*Serveur du coffre-fort d'identité*	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP. Par exemple : myLDAPhost
	Port LDAP	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	Port LDAP sécurisé	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	Administrateur du coffre-fort d'identité	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.
	Mot de passe de l'administrateur du coffre-fort d'identité	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
	Utiliser le compte anonyme public	Permet aux utilisateurs non logués d'accéder au compte anonyme public LDAP.
	Guest LDAP	Permet aux utilisateurs non logués d'accéder à des portlets autorisés. Ce compte utilisateur doit déjà exister dans le coffre-fort d'identité. Pour activer Guest LDAP, vous devez désélectionner *Utiliser le compte anonyme public*. Pour désactiver l'utilisateur Guest, sélectionnez *Utiliser le compte anonyme public*.
	Mot de passe Guest LDAP	Indiquez le mot de passe Guest LDAP.
	Connexion Admin sécurisée	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.
	Login utilisateur sécurisé	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	*DN du conteneur racine*	Requis. Indiquez le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire.
	DN du pilote d'application utilisateur	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur. Par exemple, si votre pilote est UserApplicationDriver, que votre ensemble de pilotes est appelé myDriverSet et que l'ensemble de pilotes est dans un contexte o=myCompany, vous saisissez la valeur suivante : `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Administrateur de l'application utilisateur	Requis. Un utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs de l'application utilisateur spécifié. Cet utilisateur peut utiliser l'onglet *Administration* de l'application utilisateur pour administrer le portail. Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, Novell Designer pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), 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 *User Application: Administration Guide* (Guide d'administration de l'application utilisateur). Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur. Vous ne pouvez pas modifier ce paramètre via ConfigUpdate si vous avez démarré le serveur d'applications qui héberge l'application utilisateur.
	Administrateur du provisioning	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 *Administration* > *Assignations de l'administrateur* de l'application utilisateur.

Type de paramètre	Option	Description
	Administrateur de conformité	L'administrateur de conformité est un rôle système qui permet aux membres d'exécuter toutes les fonctions de l'onglet *Conformité*. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné comme administrateur du module de conformité. 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. Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page *Administration* > *Assignations de l'administrateur* de l'application utilisateur.
	Administrateur de rôles	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. Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page *Administration* > *Assignations de l'administrateur* de l'application utilisateur. 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.
	Administrateur de la sécurité	Ce rôle permet aux membres d'accéder à toutes les fonctionnalités du domaine Sécurité. L'administrateur de la sécurité peut effectuer toutes les opérations possibles sur tous les objets au sein du domaine Sécurité. 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. Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page *Administration* > *Assignations de l'administrateur* de l'application utilisateur.
	Administrateur de ressources	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. Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page *Administration* > *Assignations de l'administrateur* de l'application utilisateur.

Type de paramètre	Option	Description
	Administrateur de la configuration RBPM	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 proxy et de délégation, l'interface utilisateur de provisioning et le moteur de workflow. Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page *Administration* > *Assignations de l'administrateur* de l'application utilisateur.
	Administrateur de rapports RBPM	Pointe vers l'administrateur de rapports. Par défaut, le programme d'installation définit cette valeur sur le même utilisateur que celui renseigné dans les autres champs de sécurité.
	Réinitialiser la sécurité RBPM	Case à cocher vous permettant de réinitialiser la sécurité.
	URL IDMReport	URL qui pointe vers l'interface utilisateur du module de création de rapports Identity.

Type de paramètre	Option	Description
Identité de l'utilisateur du coffre-fort d'identité	*DN du conteneur d'utilisateurs*	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur d'utilisateurs. Les utilisateurs de ce conteneur (et en-dessous) sont autorisés à se loguer à l'application utilisateur. Vous ne pouvez pas modifier ce paramètre via ConfigUpdate si vous avez démarré le serveur d'applications qui héberge l'application utilisateur. **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.
	Étendue du conteneur d'utilisateurs	Cela définit l'étendue de recherche d'utilisateurs.
	Classe d'objets Utilisateur	La classe d'objets utilisateur LDAP (généralement inetOrgPerson).
	Attribut de login	L'attribut LDAP (par exemple, CN) qui représente le nom de login de l'utilisateur.
	Attribut de nom	L'attribut LDAP utilisé comme identifiant lors de la consultation d'utilisateurs ou de groupes. Il est différent de l'attribut de login, qui n'est utilisé que lors du login, et non pas lors des recherches d'utilisateurs/de groupes.
	Attribut de l'adhésion utilisateur	Facultatif. L'attribut LDAP qui représente l'adhésion à un groupe de l'utilisateur. N'utilisez pas d'espace pour ce nom.

Type de paramètre	Option	Description
Groupes d'utilisateurs du coffre-fort d'identité	*DN de conteneur de groupes*	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur de groupes. Utilisé par les définitions d'entités au sein de la couche d'abstraction d'annuaire. Vous ne pouvez pas modifier ce paramètre via ConfigUpdate si vous avez démarré le serveur d'applications qui héberge l'application utilisateur.
	Étendue du conteneur de groupes	Cela définit l'étendue de recherche des groupes.
	Classe d'objets Groupe	La classe d'objets Groupe LDAP (généralement groupofNames).
	Attribut d'adhésion à un groupe	L'attribut qui représente l'adhésion d'un utilisateur à un groupe. N'utilisez pas d'espaces pour le nom.
	Utiliser des groupes dynamiques	Sélectionnez cette option si vous souhaitez utiliser des groupes dynamiques.
	Classe d'objets Groupe dynamique	La classe d'objets Groupe dynamique LDAP (généralement dynamicGroup).
Certificats du coffre-fort d'identité	*Chemin d'accès au Keystore*	Requis. Indiquez le chemin d'accès complet au fichier keystore (`cacerts`) du JRE utilisé par le serveur d'applications pour s'exécuter, ou cliquez sur le petit bouton du navigateur pour accéder au fichier `cacerts`. L'installation de l'application utilisateur modifie le fichier keystore. Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier. **Remarque concernant WebSphere.** Le champ relatif au chemin du fichier Keystore doit être défini sur le répertoire d'installation du module RBPM et non l'emplacement du fichier cacerts du JDK, comme c'est le cas pour les installations JBoss. La valeur par défaut est définie sur l'emplacement correct.
	Mot de passe Keystore	Requis. Indiquez le mot de passe `cacerts`. L'unité par défaut est `changeit`.
	Confirmer le mot de passe Keystore	

Type de paramètre	Option	Description
Banque de clés approuvée	*Chemin d'accès à la banque approuvée*	Le keystore approuvé contient les certificats de tous les signataires approuvés. Si ce chemin est vide, l'application utilisateur obtient le chemin à partir de la propriété Système `javax.net.ssl.trustStore`. Si le chemin n'y est pas, il est supposé être `jre/lib/security/cacerts`.
	Mot de passe de la banque approuvée	Si ce champ est vierge, l'application utilisateur obtient le mot de passe à partir de la propriété système `javax.net.ssl.trustStorePassword`. S'il n'y a aucune valeur, `changeit` est utilisé. Ce mot de passe est codé, en fonction de la clé maîtresse.
	Keystore de type JKS	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.
	Keystore de type PKCS12	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.
Clé de certificat et signature numérique Novell Audit		Contient la clé de signature numérique et le certificat pour le service d'audit.
	Certificat de signature numérique Novell Audit	Affiche le certificat de signature numérique pour le service d'audit.
	Clé privée de signature numérique Novell Audit	Affiche la clé privée de signature numérique. Cette clé est codée, en fonction de la clé maîtresse.
Paramètres Access Manager	*Logout simultané activé*	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.
	Page de Logout simultané	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 consignation 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	*HÔTE du modèle de notification*	Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple : `myapplication serverServer` Cette valeur remplace le jeton $HOST$ des modèles de courrier électronique. L'URL construite est la liaison aux tâches de requête de provisioning et aux notifications d'approbation.
	PORT du modèle de notification	Utilisé pour remplacer le jeton $PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	PORT SÉCURISÉ du modèle de notification	Utilisé pour remplacer le jeton $SECURE_PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	PROTOCOLE du modèle de notification	Se rapporte à un protocole non sécurisé, HTTP. Utilisé pour remplacer le jeton $PROTOCOL$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	PROTOCOLE SÉCURISÉ du modèle de notification	Se rapporte à un protocole sécurisé, HTTPS. Utilisé pour remplacer le jeton $SECURE_PROTOCOL$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Notification SMTP - expéditeur du courrier électronique	Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
	Nom du serveur SMTP	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		
	Utiliser le WAR de mots de passe externe	Cette fonction permet d'indiquer une page Mot de passe oublié qui réside dans un WAR Mot de passe oublié externe et une URL que le WAR Mot de passe oublié externe utilise pour rappeler l'application utilisateur grâce à un service Web. Si vous sélectionnez *Utiliser le WAR de mot de passe externe*, vous devez indiquer des valeurs pour les paramètres *Lien Mot de passe oublié*, *Lien Retour mot de passe oublié* et *URL du service Web de mot de passe oublié*. Si vous ne sélectionnez pas *Utiliser le WAR de mot de passe externe*, IDM utilise la fonction de gestion des mots de passe interne par défaut, `/jsps/pwdmgt/ForgotPassword.jsp` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.
	Liaison Mot de passe oublié	Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier `ForgotPassword.jsp` dans un fichier WAR de gestion des mots de passe externe ou interne.
	Lien Retour mot de passe oublié	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.
	URL du service Web de mot de passe oublié	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 : `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
Divers	*Timeout de session*	Le timeout de session de l'application.
	OCSP URI	Si l'installation client utilise le protocole OCSP (protocole de propriété d'état de certificat en ligne), fournissez un identificateur de ressource uniforme (URI). Par exemple, le format est http://host:port/ocspLocal. L'URI OCSP met à jour le statut des certificats approuvés en ligne.
	Chemin de configuration d'autorisation	Nom complet du fichier de configuration de l'autorisation.

Type de paramètre	Option	Description
	Créer un index de coffre-fort d'identité	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 150. 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.
	Supprimer l'index de coffre-fort d'identité	Supprime des index des attributs manager, ismanager et srvprvUUID.
	DN du serveur	Sélectionnez le serveur eDirectory sur lequel les index doivent être créés ou duquel ils doivent être supprimés. **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.
Objet Conteneur	*Sélectionné*	Sélectionnez chaque type d'objet Conteneur à utiliser.
	Type d'objet Conteneur	Sélectionnez parmi les conteneurs standard suivants : lieu, pays, unité organisationnelle, organisation et domaine. Vous pouvez également définir vos propres conteneurs dans iManager et les ajouter sous *Ajouter un nouvel objet Conteneur*.
	Nom de l'attribut Conteneur	Indique le nom de type d'attribut associé au type d'objet Conteneur.
	Ajouter un nouvel objet Conteneur : type d'objet Conteneur	Indiquez le nom LDAP d'une classe d'objets du coffre-fort d'identité pouvant servir de conteneur.
	Ajouter un nouvel objet Conteneur : nom d'attribut Conteneur	Donnez le nom d'attribut de l'objet Conteneur.