Guide d'installation de l'application utilisateur

Novell®
Module de provisioning basé sur les rôles Identity Manager

3.6.1

23 juillet 2008

www.novell.com

Mentions légales

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

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

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

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

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

Marques de Novell

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

Éléments tiers

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

Table des matières

À propos de ce guide 7

1 Présentation de l'installation du module de provisioning basé sur les rôles 9

1.1 Liste de contrôle de l'installation . . . 9
1.2 À propos du programme d'installation . . . 10
1.3 Configuration système requise . . . 11

2 Conditions préalables 17

2.1 Installation du méta-annuaire Identity Manager . . . 17
2.2 Téléchargement du module de provisioning basé sur les rôles . . . 17
2.3 Installation d'un serveur d'applications . . . 19
2.3.1 Installation du serveur d'applications JBoss . . . 19
2.3.2 Installation du serveur d'applications WebLogic . . . 21
2.3.3 Installation du serveur d'applications WebSphere . . . 21
2.4 Installation d'une base de données . . . 21
2.4.1 Configuration d'une base de données MySQL . . . 22
2.5 Installation du kit de développement Java . . . 23
2.6 Installation des fichiers supplémentaires pour le méta-annuaire 3.5.1 . . . 23
2.6.1 Installation du pilote de service de rôles à l'aide de l'interface graphique . . . 24
2.6.2 Installation du pilote du service de rôles depuis la console . . . 25
2.6.3 Copie des icônes iManager . . . 25
2.6.4 Copie d'afadmin.jar . . . 26

3 Création de pilotes 27

3.1 Création du pilote d'application utilisateur dans iManager . . . 27
3.2 Création du pilote de service de rôle dans iManager . . . 29

4 Installation sur JBoss à l'aide du programme d'installation de l'interface graphique 33

4.1 Installation et configuration du fichier WAR de l'application utilisateur . . . 33
4.1.1 Affichage des fichiers journaux et d'installation . . . 39
4.2 Tester l’installation . . . 39

5 Installation sur un serveur d'applications WebSphere à l'aide du programme d'installation de l'interface graphique 41

5.1 Installation et configuration du fichier WAR de l'application utilisateur . . . 41
5.1.1 Affichage des fichiers journaux d'installation . . . 46
5.2 Configuration de l'environnement WebSphere . . . 46
5.2.1 Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM . . . 46
5.2.2 Importation de la racine approuvée d'eDirectory dans la zone de stockage des clés WebSphere . . . 47
5.3 Déploiement du fichier WAR . . . 48
5.4 Démarrage et accès à l'application utilisateur . . . 48

6 Installation sur un serveur d'applications WebSphere à l'aide du programme d'installation de l'interface graphique 51

6.1 Liste de contrôle de l'installation de WebLogic 51
6.2 Installation et configuration du fichier WAR de l'application utilisateur 52
6.2.1 Affichage des fichiers journaux et d'installation 56
6.3 Préparation de l'environnement WebLogic 56
6.3.1 Configurez la réserve de connexions 56
6.3.2 Indiquez l'emplacement des fichiers de configuration de l'application utilisateur. . . . 56
6.3.3 Plug-in de workflow et configuration de WebLogic 58
6.4 Déploiement du fichier WAR de l'application utilisateur 58
6.5 Accès à l'application utilisateur 58

7 Installation depuis la console ou à l'aide d'une commande unique 59

7.1 Installation de l'application utilisateur à partir de la console 59
7.2 Installation de l'application utilisateur avec une seule commande 60

8 Tâches post-installation 71

8.1 Enregistrement de la clé maîtresse 71
8.2 Configuration de l'application utilisateur 71
8.2.1 Configuration de Novell Audit 71
8.3 Configuration d'eDirectory 72
8.3.1 Création d'index dans eDirectory 72
8.3.2 Installation et configuration de la méthode d'authentification SAML 72
8.4 Reconfiguration du fichier WAR de l'application utilisateur après l'installation. 73
8.5 Configuration de la gestion de mots de passe externe 74
8.5.1 Spécification d'un WAR de gestion des mots de passe externe 74
8.5.2 Spécification d'un WAR de mot de passe interne 75
8.5.3 Essai de la configuration du fichier WAR de mots de passe externe 75
8.5.4 Configuration de la communication SSL entre serveurs JBoss 75
8.6 Mise à jour des paramètres Mot de passe oublié 75
8.7 dépannage 76

A Référence de configuration de l'application utilisateur IDM 79

A.1 Configuration de l'application utilisateur : paramètres de base 79
A.2 Configuration de l'application utilisateur : tous les paramètres 84

À propos de ce guide

Ce guide explique la procédure d'installation du module de provisioning basé sur les rôles Novell® Identity Manager 3.6.1. Il comprend les sections :

- Chapitre 1, « Présentation de l'installation du module de provisioning basé sur les rôles », page 9
- Chapitre 2, « Conditions préalables », page 17
- Chapitre 3, « Création de pilotes », page 27
- Chapitre 4, « Installation sur JBoss à l'aide du programme d'installation de l'interface graphique », page 33
- Chapitre 5, « Installation sur un serveur d'applications WebSphere à l'aide du programme d'installation de l'interface graphique », page 41
- Chapitre 6, « Installation sur un serveur d'applications WebSphere à l'aide du programme d'installation de l'interface graphique », page 51
- Chapitre 7, « Installation depuis la console ou à l'aide d'une commande unique », page 59
- Chapitre 8, « Tâches post-installation », page 71
- Annexe A, « Référence de configuration de l'application utilisateur IDM », page 79

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 des utilisateurs au bas de chaque page de la documentation en ligne ou saisissez vos commentaires dans la page www.novell.com/documentation/feedback.html.

Documentation supplémentaire

Pour plus d'informations sur le module de provisioning basé sur les rôles d'Identity Manager, reportez-vous au site Web de documentation d'Identity Manager (http://www.novell.com/documentation/lg/dirxmldrivers/index.html).

Conventions relatives à la documentation

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

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

Lorsqu'un nom de chemin peut s'écrire avec une barre oblique pour certaines plates-formes et une barre oblique inverse pour d'autres, il sera toujours présenté avec une barre oblique inverse. Les utilisateurs de plates-formes qui requièrent une barre oblique normale, comme Linux* ou UNIX*, doivent utiliser ces barres obliques comme l'exige leur logiciel.

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

1

Cette section présente les étapes de l'installation du module de provisioning basé sur les rôles. Elle peut également vous aider lors de l'installation et la configuration supplémentaires de l'édition standard de l'application utilisateur, qui a lieu lors de l'installation du serveur méta-annuaire. Les rubriques sont les suivantes :

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

Si vous migrez depuis une version antérieure de l'application utilisateur ou du module de provisioning basé sur les rôles, reportez-vous au *Guide de migration de l'application utilisateur* (http://www.novell.com/documentation/idmrbpm361/index.html).

1.1 Liste de contrôle de l'installation

Pour installer le module de provisioning basé sur les rôles Novell® Identity Manager ou l'édition standard de l'application utilisateur, vous devez réaliser les tâches suivantes :

- ❑ Vérifiez que votre logiciel dispose de la configuration système requise. Reportez-vous à Section 1.3, « Configuration système requise », page 11.
- ❑ Téléchargez la version 3.6.1 du module de provisioning basé sur les rôles Identity Manager. Reportez-vous à 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 Section 2.1, « Installation du méta-annuaire Identity Manager », page 17.
  - ❑ Installez et configurez un serveur d'applications. Reportez-vous à Section 2.3, « Installation d'un serveur d'applications », page 19.
  - ❑ Installez une base de données et configurez-la. Reportez-vous à Section 2.4, « Installation d'une base de données », page 21.
  - ❑ Si vous migrez depuis version antérieure de l'application utilisateur et que continuez d'utiliser le méta-annuaire Identity Manager version 3.5.1, exécutez les tâches suivantes :
    - ❑ Exécutez l'utilitaire d'installation du pilote de l'application utilisateur et du service de rôles pour étendre le schéma de coffre-fort d'identité et installer les fichiers de configuration du pilote de l'application utilisateur et du service de rôles. Copiez les fichiers supplémentaires le cas échéant. Pour plus d'informations, reportez-vous à Section 2.6, « Installation des fichiers supplémentaires pour le méta-annuaire 3.5.1. », page 23.

Remarque : le méta-annuaire Identity Manager 3.6 exécute l'utilitaire d'installation du pilote de l'application utilisateur et du service de rôles en silence. Ceci permet de garantir que vous disposez de tous les fichiers nécessaires.

- ❑ Copiez le contenu du fichier `iManager_icons_for_roles.zip` à l'emplacement iManager correct. Reportez-vous à Section 2.6.3, « Copie des icônes iManager », page 25.
- ❑ Copiez le fichier `afadmin.jar` à l'emplacement correct. Reportez-vous à « Copie d'afadmin.jar » page 26.

❑ Créez le pilote de l'application utilisateur dans iManager ou Designer pour Identity Manager 3.0.

- Pour iManager : Section 3.1, « Création du pilote d'application utilisateur dans iManager », page 27.
- Pour Designer : Guide de conception de l'application utilisateur (http://www.novell.com/documentation/idmrbpm361/index.html).

❑ Créez le pilote de service de rôles dans iManager ou Designer pour Identity Manager 3.0.

- Pour iManager : Section 3.2, « Création du pilote de service de rôle dans iManager », page 29.
- Pour Designer : Guide de conception de l'application utilisateur (http://www.novell.com/documentation/idmrbpm361).

❑ Installez et configurez l'application utilisateur ou le module de provisioning basé sur les rôles Novell Identity Manager. (Vous devez avoir installé le JDK* correct avant de démarrer le programme d'installation. Reportez-vous à la section Section 2.5, « Installation du kit de développement Java », page 23.)

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

- Interface Utilisateur Graphique. Consultez l'une des sections suivantes :
  - Chapitre 4, « Installation sur JBoss à l'aide du programme d'installation de l'interface graphique », page 33.
  - Chapitre 5, « Installation sur un serveur d'applications WebSphere à l'aide du programme d'installation de l'interface graphique », page 41.
  - Chapitre 6, « Installation sur un serveur d'applications WebSphere à l'aide du programme d'installation de l'interface graphique », page 51.
- Interface de console (ligne de commande). Reportez-vous à Section 7.1, « Installation de l'application utilisateur à partir de la console », page 59.
- Installation en mode silencieux. Reportez-vous à Section 7.2, « Installation de l'application utilisateur avec une seule commande », page 60.

❑ Procédez aux tâches post-installation décrites dans Chapitre 8, « Tâches post-installation », page 71.

1.2 À propos du programme d'installation

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

- Désigne une version existante d'un serveur d'applications à utiliser.

- Désigne une version existante d'une base de données à utiliser, par exemple MySQL*, Oracle*, DB2* ou Microsoft* SQL Server*. La base de données stocke les données de l'application utilisateur et les informations de configuration de l'application utilisateur.
- Configure le fichier des certificats de JDK pour que l'application utilisateur (exécutée sur le serveur d'applications) puisse communiquer avec le coffre-fort d'identité et le pilote de l'application utilisateur de façon sécurisée.
- Configure et déploie le fichier d'archive de l'application Web Java* (fichier WAR) pour l'application utilisateur Novell Identity Manager sur le serveur d'applications. Sous WebSphere* et WebLogic*, vous devez déployer le fichier WAR manuellement.
- Active la consignation Novell Audit ou OpenXDAS si vous la sélectionnez.
- Permet d'importer une clé maîtresse existante pour restaurer une installation particulière de module Provisioning basé sur les rôles et pour prendre des grappes en charge.
- Migre les données existantes d'un module de provisioning version 3.5.1 ou d'un module de provisioning basé sur les rôles version 3.6 vers le format de données requis pour la version 3.6.2.

1.3 Configuration système requise

Vous ne pouvez utiliser la version 3.6.1 du module de provisioning basé sur les rôles d'Identity Manager que si vous avez installé chacun des composants requis indiqués au Tableau 1-1.

Tableau 1-1 *Configuration système requise*

Composant système requis	Configuration système requise
Identity Manager 3.5.1 (système de méta-annuaire)	SUSE® Linux Enterprise Server (SLES) 10 avec le dernier Support Pack (prise en charge 32 bits et 64 bits) eDirectory™ : 8.8.2 Security Services 2.0.5 (NMAS™ 3.1.3)
Identity Manager 3.6 (système de méta-annuaire)	L'un des systèmes d'exploitation suivants : ◆ Windows Server* 2003 SP2 (32 bits) ◆ Linux Red Hat 5.0 (32 bits) avec le dernier Support Pack ◆ SLES* 10 SP2 (32 bits) avec le dernier Support Pack ◆ Solaris* 10 (32 bits) ◆ AIX* 5L v5.3 (32 bits) eDirectory : 8.8.3

Composant système requis	Configuration système requise
Serveur d'administration basé sur le Web ◆ iManager 2.6 et les plug-ins (avec le méta-annuaire version 3.5.1 uniquement) ◆ iManager 2.7 et les plug-ins	L'un des systèmes d'exploitation suivants : ◆ Novell Open Enterprise Server (OES) 1.0 sur NetWare avec le dernier Support Pack ◆ Novell Open Enterprise Server 2.0 ◆ NetWare 6.5 avec le dernier Support Pack ◆ Windows 2000 Server avec le dernier Service Pack (32 bits) ◆ Windows Server 2003 avec le dernier Service Pack (32 bits) ◆ Microsoft Windows Vista* ◆ Red Hat Linux 3.0, 4.0 ou 5.0 ES ou AS (prise en charge 32 bits et 64 bits) ◆ Solaris 9 ou 10 avec le dernier Support Pack ◆ SUSE Linux Enterprise Server 9 ou 10 avec le dernier Support Pack (prise en charge 32 bits et 64 bits) Systèmes d'exploitation pris en charge via le poste de travail iManager : ◆ Windows 2000 Professionnel avec le dernier Service Pack ◆ Windows XP avec SP2 ◆ Windows Vista éditions Ultimate et Business (iManager 2.7 uniquement) ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 ◆ openSUSE® 10.3 (iManager 2.7 uniquement) Le logiciel suivant : ◆ Novell iManager 2.6 ou 2.7 avec les derniers Support Pack et plug-ins

Composant système requis	Configuration système requise
Service de consignation sécurisée ◆ Le serveur de consignation sécurisée ◆ L'agent de plate-forme (composant client) ◆ Novell Audit 2.0.2, Sentinel™ 5.1.3 ou Sentinel 6.1 (méta-annuaire version 3.6 uniquement)	Pour le serveur de consignation sécurisée, un des systèmes d'exploitation suivants : ◆ Novell Open Enterprise Server 1.0 ou 2.0 avec le dernier Support Pack ◆ NetWare 6.5 avec le dernier Support Pack ◆ Windows 2000 Server avec le dernier Service Pack (32 bits) ◆ Windows Server 2003 avec le dernier Service Pack (32 bits) ◆ Red Hat Linux 3.0, 4.0 ou 5.0 AS et ES (32 bits ou 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits) ◆ Solaris 9 ou 10 avec le dernier Support Pack ◆ SUSE Linux Enterprise Server 9 ou 10 (32 bits ou 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits) avec le dernier Support Pack ◆ Novell eDirectory 8.7.3.6 ou 8.8 avec le Support Pack le plus récent (doit être installé sur le serveur de consignation sécurisée) Pour l'agent de plate-forme, un des systèmes d'exploitation suivants : ◆ Novell Open Enterprise Server 1.0 SP1 ou le dernier Support Pack ◆ NetWare 6.5 avec le dernier Support Pack ◆ Serveur Windows 2000 ou 2000, XP ou Windows Server 2003 avec le dernier Service Pack (32 bits) ◆ Red Hat Linux 3 ou 4 AS ou ES (32 bits ou 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits) ◆ Solaris 8, 9 ou 10 ◆ SUSE Linux Enterprise Server 9 ou 10 (32 bits ou 64 bits, bien que Novell Audit ne fonctionne qu'en mode 32 bits) iManager 2.6 ou 2.7 avec le Support Pack et les plug-ins les plus récents

Composant système requis	Configuration système requise
Serveur d'applications de l'application utilisateur	L'application utilisateur s'exécute sur JBoss*, WebSphere* et WebLogic* (voir ci-dessous). L'application utilisateur avec JBoss 4.2.2 GA requiert JRE* 1.5.0_15 et est prise en charge sous : ◆ Novell Open Enterprise Server (OES) 1.0 SP2 ou le dernier Support Pack (Linux uniquement) ◆ SUSE Linux Enterprise Server 9 SP2 (inclus dans OES 1.0 SP2) ou 10.1.x (JVM* 64 bits;) ◆ Windows 2003 Server avec SP1 (64 bits) ◆ Solaris 10 Support Pack daté du 6/06 ◆ Red Hat Linux 5 (32 bits) L'application utilisateur sous WebSphere 6.1 requiert le JDK d'IBM. Le niveau du pack de correctifs minimum est 6.1.0.9 ; les fichiers de stratégie non limités doivent être appliqués. Il est pris en charge sur les plates-formes suivantes : ◆ Solaris 10 (64 bits) ◆ Windows 2003 SP1 (64 bits) L'application utilisateur sous WebLogic 10 requiert JRockit* 1.5.0_06 et est prise en charge sur les plates-formes suivantes. ◆ Solaris 10 (32 bits ou 64 bits) ◆ Windows 2003 SP1
Navigateur de l'application utilisateur	L'application utilisateur prend en charge Firefox* et Internet Explorer (voir ci-dessous). Firefox* 2 est pris en charge sous : ◆ Windows XP avec SP2 ◆ Windows Vista ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ openSUSE 10 Internet Explorer 7 est pris en charge sur : ◆ Windows XP avec SP2 ◆ Windows Vista Enterprise Internet Explorer 6 SP1 est pris en charge sous : ◆ Windows XP avec SP2

Composant système requis	Configuration système requise
Serveur de base de données pour l'application utilisateur	Les bases de données suivantes sont prises en charge avec JBoss : ◆ MySQL version 5.0.51 ◆ Oracle 9i (9.2.0.1.4) ◆ Oracle 10g version 2 (10.2.0.1.0) ◆ MS SQL 2005 avec SP1 Les bases de données suivantes sont prises en charge avec WebSphere : ◆ Oracle 10g version 2 (10.2.0) ◆ MS SQL 2005 avec SP1 ◆ DB2 DV2 v9.1.0.0 Les bases de données suivantes sont prises en charge avec WebLogic : ◆ Oracle 10g version 2 (10.2.0) ◆ MS SQL 2005 avec SP1 Les pilotes JDBC suivants sont pris en charge : Serveur MS SQL version 1.2.2828.100 Serveur léger Oracle : pilote JDBC Oracle, version 10.2.0.1.0. Pilote OCI Oracle : pilote JDBC Oracle, version 10.2.0.2.0. MySQL Connector/J 5.0.8 Pilote DB2 version 1.4.2
Postes de travail ◆ Designer 3.0 pour Identity Manager 3.6 ◆ Accès en ligne à iManager	Le concepteur a été testé sur les plates-formes suivantes : Windows : ◆ Windows XP SP2 ◆ Microsoft Windows Vista Linux : ◆ SUSE Linux Enterprise Server 10 (concepteur uniquement) ◆ SUSE Linux Enterprise Desktop 10 ◆ openSUSE 10
Audit	Novell Audit 2.0.2
OpenXDAS	OpenXDAS version 0.5.257
Intégration SSO de l'application utilisateur	Nécessite Novell Access Manager 3.0.1

Conditions préalables

2

Cette section décrit les logiciels et les composants que vous devez installer ou configurer avant de pouvoir installer le module de provisioning basé sur les rôles Identity Manager ou l'édition standard de l'application utilisateur. 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 21
- Section 2.5, « Installation du kit de développement Java », page 23
- Section 2.6, « Installation des fichiers supplémentaires pour le méta-annuaire 3.5.1. », page 23

2.1 Installation du méta-annuaire Identity Manager

Le module de provisioning basé sur les rôles version 3.6.1 peut être utilisé avec le méta-annuaire Identity Manager 3.5.1 ou 3.6.

Pour les instructions d'installation du méta-annuaire Identity Manager 3.6, reportez-vous au *Guide d'installation de Novell Identity Manager 3.6* (http://www.novell.com/documentation/idm36/).

Si vous avez installé le méta-annuaire Identity Manager 3.5.1, vous devez mettre plusieurs fichiers à jour avant que le module de provisioning basé sur les rôles version 3.6.1 fonctionne. Pour plus d'informations, reportez-vous à Section 2.6, « Installation des fichiers supplémentaires pour le méta-annuaire 3.5.1. », page 23. Ceci n'est pas nécessaire pour le méta-annuaire Identity Manager 3.6 car les fichiers sont installés automatiquement dans le cadre de son installation.

2.2 Téléchargement du module de provisioning basé sur les rôles

Le module de provisioning basé sur les rôles Identity Manager est accessible via la page des téléchargements Novell (http://download.novell.com/index.jsp). Téléchargez les fichiers d'images `.iso` correspondant à votre produit, conformément aux indications fournies dans le Tableau 2-1.

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

Pour ce produit	Téléchargez ce fichier .iso
Module de provisioning basé sur les rôles	`Identity_ Manager_3_6_1_User_Application_Provisioning.iso`
Édition standard de l'application utilisateur	`Identity_Manager_3_6_1_User_Application_NON_Provisioning.iso`

Si vous avez installé le méta-annuaire Identity Manager 3.5.1, vous devez également télécharger le fichier `Roles_Driver_Install_Utility.iso`. Il est inutile de télécharger le fichier `Roles_Driver_Install_Utility.iso` si vous utilisez un méta-annuaire Identity Manager 3.6 car les fichiers contenus dans ce fichier `.iso` sont déjà inclus dans l'installation du méta-annuaire Identity Manager 3.6.

Le Tableau 2-2 décrit les fichiers d'installation du fichier `.iso` du module de provisioning basé sur les rôles ou de l'édition standard de l'application utilisateur.

Tableau 2-2 *Fichiers et scripts inclus dans le fichier .iso*

Fichier	Description
`IDMProv.war`	Fichier WAR du module de provisioning basé sur les rôles. Il contient l'application utilisateur Identity Manager 3.6.1 avec les fonctions self-service d'identité et le module de provisioning basé sur les rôles.
`IDM.war`	Fichier WAR de l'édition standard de l'application utilisateur. Il comprend l'application utilisateur Identity Manager 3.6.1, qui prend en charge les fonctions self-service d'identité.
`IDMUserApp.jar`	Programme d'installation de l'application utilisateur et du module de provisioning basé sur les rôles.
`silent.properties`	Fichier contenant les paramètres requis pour une installation silencieuse. Ceux-ci correspondent aux paramètres d'installation que vous avez définis dans les procédures d'installation de l'interface utilisateur graphique ou de la console. Vous devez copier ce fichier et en modifier le contenu pour l'adapter à votre environnement d'installation.
`JBossMySQL.bin` ou `JBossMySQL.exe`	Utilitaire pratique permettant d'installer le serveur d'applications JBoss et la base de données MySQL.
`nmassaml.zip`	Contient une méthode eDirectory de prise en charge de SAML. Nécessaire uniquement si vous n'utilisez pas Access Manager.
`afadmin.jar`	Requis uniquement pour le méta-annuaire Identity Manager 3.5.1.
`prerequisitefiles.zip`	Requis uniquement pour le méta-annuaire Identity Manager 3.5.1. Contient d'autres fichiers que vous devez copier manuellement à l'emplacement correct.

Le système sur lequel vous installez le module de provisioning basé sur les rôles Identity Manager ou l'édition standard de l'application utilisateur doit disposer d'au moins 320 Mo d'espace de stockage, 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 différent durant l'installation, mais celui-ci doit avoir été créé avant le démarrage de l'installation et être accessible en écriture. Sous Linux et Solaris, les utilisateurs non-`root` doivent également y avoir un accès en écriture.

2.3 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 21
- Section 2.3.3, « Installation du serveur d'applications WebSphere », page 21

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

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

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

Composant	Recommandation
RAM	La mémoire vive recommandée pour le serveur d'applications JBoss lors de l'exécution du module de provisioning basé sur les rôles Identity Manager est de 512 Mo.
Port	La valeur par défaut pour le serveur d'applications est 8080. Notez le port que votre serveur d'applications utilise.
SSL	Activez SSL si vous prévoyez utiliser la gestion de mots de passe externe. ◆ 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 Section 8.5, « Configuration de la gestion de mots de passe externe », page 74 et au *Guide d'administration de l'application utilisateur* (http://www.novell.com/documentation/idmrbpm361/index.html) .

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

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

1 Localisez et exécutez `JBossMySQL.bin` ou `JBossMySQL.exe` depuis le fichier .iso.

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

Cet utilitaire n'est pas disponible avec Solaris.

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
Sélectionnez les paramètres d'installation	Choisissez les produits à installer. ◆ *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 « Installation du serveur d'applications JBoss en tant que service ou un daemon » page 21. ◆ *MySQL*: installe MySQL et crée une base de données MySQL dans le répertoire que vous indiquez, ainsi que les scripts permettant de le démarrer et de l'arrêter.
Sélectionnez le dossier parent JBoss.	Cliquez sur *Sélectionner* pour choisir un dossier d'installation autre que le dossier par défaut.
Sélectionnez le dossier parent MySQL.	Cliquez sur *Sélectionner* pour choisir un dossier d'installation autre que le dossier par défaut.
Infos sur MySQL	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 : notez-le, ainsi que l'emplacement. ◆ *Mot de passe utilisateur 'root'* (et confirmation du mot de passe) : indiquez le mot de passe root (et confirmez-le) pour cette base de données.
Résumé de la pré-installation	Consultez la page Résumé. Si les indications sont correctes, cliquez sur *Installer.*

L'utilitaire affiche un message dès qu'il a fini d'installer les produits que vous avez sélectionnés. Si vous avez installé la base de données MySQL, passez à Section 2.4.1, « Configuration d'une base de données MySQL », page 22.

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

Pour démarrer l'application JBoss comme daemon, reportez-vous aux instructions de JBoss (http://wiki.jboss.org/wiki/Wiki.jsp?page=StartJBossOnBootWithLinux).

Utilisation de JavaServiceWrapper Vous pouvez utiliser JavaServiceWrapper (wrapper de service Java) pour installer, démarrer et arrêter le serveur d'applications JBoss comme service Windows ou comme processus daemon Linux ou UNIX. Reportez-vous aux indications JBoss à la page http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows (http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows). Un tel wrapper est disponible à la page http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html) : vous pouvez le gérer via JMX (reportez-vous pour cela à 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 utiliser 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 à http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService (http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService).

2.3.2 Installation du serveur d'applications WebLogic

Si vous prévoyez d'utiliser le serveur d'applications WebLogic 10, téléchargez-le et installez-le. Reportez-vous à Section 1.3, « Configuration système requise », page 11 pour en savoir plus sur les versions prises en charge.

2.3.3 Installation du serveur d'applications WebSphere

Si vous prévoyez d'utiliser le serveur d'applications WebSphere 6.1, téléchargez-le et installez-le. Reportez-vous à Section 1.3, « Configuration système requise », page 11 pour en savoir plus sur les versions prises en charge.

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.). Avant de pouvoir installer le module de provisioning basé sur les rôles ou 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.
- ❑ Consignation des paramètres suivants de la base de données : vous en aurez besoin lors de l'installation du module de provisioning basé sur les rôles Identity Manager.
  - 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 du module de provisioning basé sur les rôles d'Identity Manager crée un fichier source de données du serveur d'applications qui pointe vers la base de données et nomme le fichier en fonction du fichier WAR du module de provisioning basé sur les rôles d'Identity Manager. Dans le cas de WebSphere et WebLogic, configurez la source de données manuellement avant l'installation.

- ❑ Les bases de données doivent être compatibles UTF-8.

Remarque : si vous migrez 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 Configuration d'une base de données MySQL

L'application utilisateur requiert certaines options de configuration pour MySQL. Si vous installez MySQL vous-même, vous devez configurer ces paramètres. Si vous installez MySQL à l'aide de l'utilitaire JbossMysql, celui-ci définit les valeurs qui vous conviennent, mais vous devez connaître les valeurs à maintenir pour ce qui suit :

- « Moteur de stockage et types de tables INNODB » page 22
- « Ensemble de caractères » page 22
- « Distinction de la casse » page 23

Moteur de stockage et types de tables INNODB

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

```
default-table-type=innodb
```

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

Ensemble de caractères

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

```
character_set_server=utf8
```

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

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

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

```
<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&amp;characterEncoding=utf8&amp;connectionCollation=ut
f8_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.

2.5 Installation du kit de développement Java

Les programmes d'installation de l'édition standard de l'application utilisateur ou du module de provisioning basé sur les rôles requièrent que vous utilisiez au moins la version 1.5 du kit de développement de la plate-forme Java 2, Standard Edition.

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

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

2.6 Installation des fichiers supplémentaires pour le méta-annuaire 3.5.1.

Si vous utilisez le méta-annuaire Identity Manager 3.5.1, vous devez suivre les étapes supplémentaires décrites dans ces sections :

- Section 2.6.1, « Installation du pilote de service de rôles à l'aide de l'interface graphique », page 24
- Section 2.6.2, « Installation du pilote du service de rôles depuis la console », page 25
- Section 2.6.3, « Copie des icônes iManager », page 25
- Section 2.6.4, « Copie d'afadmin.jar », page 26

Si vous utilisez Linux/Unix, procédez à l'installation en tant qu'utilisateur root.

2.6.1 Installation du pilote de service de rôles à l'aide de l'interface graphique

Ceci est nécessaire uniquement lorsque vous utilisez le méta-annuaire Identity Manager 3.5.1. Si vous avez installé le méta-annuaire Identity Manager 3.6, ces fichiers ont déjà été installés.

L'utilitaire d'installation du pilote de l'application utilisateur et du service de rôles fournit les options permettant d'effectuer les tâches suivantes :

- Étendre le schéma de coffre-fort d'identité pour prendre en charge l'application utilisateur et le module de provisioning basé sur les rôles.
- Installer les fichiers de configuration du pilote de l'application utilisateur et du pilote du service de rôles sur le serveur du méta-annuaire.
- Installer les fichiers de configuration du pilote de l'application utilisateur et du service de rôles sur iManager.

Vous devrez exécuter ce programme d'installation sur les machines du méta-annuaire et d'iManager.

Remarque : vous devez installer votre méta-annuaire à l'emplacement par défaut pour pouvoir utiliser ce programme d'installation.

Accédez au fichier `Roles_Driver_Install_Utility.iso`

1. Localisez le programme d'installation correspondant à votre système d'exploitation et exécutez-le.

Système d'exploitation	Programme d'installation du pilote de services de rôles
AIX	`roles_driver_install.aix.bin`
Linux	`roles_driver_install.linux.bin`
Solaris	`roles_driver_install.solaris.bin`
Windows	`roles_driver_install.exe`

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

Écran d'installation	Description
Accord de licence	Lisez l'accord de licence, puis sélectionnez *J'accepte les termes de l'accord de licence*.

Écran d'installation	Description
Sélection des composants	*Pilotes* : installe le pilote du service de rôles et le pilote de l'application utilisateur sur le serveur du méta-annuaire ; met à jour les fichiers JAR de la bibliothèque de prise en charge. *Schéma* : met à jour le schéma du méta-annuaire pour inclure les objets nécessaires au module de provisioning basé sur les rôles et à l'édition standard de l'application utilisateur. Il installe le fichier `nrf-extensions.sch` et le fichier srvprv.sch, puis exécute la commande (`NdsCons.exe` sous Windows et `ndssch` sous UNIX/Linux) pour la plate-forme actuelle. *Fichiers de configuration des pilotes* : installe les fichiers de configuration du pilote du service de rôles et du pilote de l'application utilisateur. Ces fichiers sont utilisés lorsque vous créez les nouveaux pilotes dans iManager. Vous devez l'exécuter sur la machine qui héberge iManager.
Authentification	Lorsque vous sélectionnez *Extensions de schéma*, vous devez indiquer un nom d'utilisateur et un mot de passe. Cet utilisateur doit disposer des droits d'administrateur sur le coffre-fort d'identité. Par exemple, *cn=admin,o=novell*.
Emplacement du pilote	Si vous avez choisi d'installer le pilote du service de rôles et de l'application utilisateur, vous êtes invité à en saisir l'emplacement sur le serveur eDirectory. Il s'agit généralement du répertoire /lib/dirxml/classes du méta-annuaire.
Emplacement d'installation des fichiers de configuration des pilotes	Indiquez l'emplacement auquel le programme d'installation doit mettre les fichiers de configuration du pilote sur la machine iManager. Ceux-ci sont en général installés dans le répertoire /nps/Dirxml.Drivers d'iManager.
Résumé pré-installation	Consultez la page Résumé avant installation pour vérifier les paramètres d'installation que vous avez sélectionnés et terminez l'installation.

2.6.2 Installation du pilote du service de rôles depuis la console

Pour exécuter le programme d'installation au mode console (caractère), émettez la commande suivante :

```
roles_driver_install_<operatingsystemfile> -i console
```

Suivez les étapes décrites pour l'interface graphique sous Section 2.6.1, « Installation du pilote de service de rôles à l'aide de l'interface graphique », page 24, en lisant les invites et en saisissant les réponses sur la ligne de commande.

2.6.3 Copie des icônes iManager

Remarque : cette procédure n'est pas nécessaire si vous avez installé iManager 2.7 ainsi que les derniers plug-ins.

1 Dans l'image `.iso` que vous avez téléchargée, localisez le fichier `prerequisites.zip`.

2 Dézippez-le puis recherchez le fichier `iManager_icons_for_roles.zip`.

   Contient les icônes iManager destinées aux objets de rôle dans eDirectory.

3 Dézippez-le, puis copiez les icônes extraites dans le répertoire `nps/portal/modules/dev/images/dir`.

4 Redémarrez iManager pour qu'il utilise les nouvelles icônes.

2.6.4 Copie d'afadmin.jar

Remarque : cette procédure n'est pas nécessaire si vous avez installé iManager 2.7 ainsi que les derniers plug-ins.

1 Dans l'image `.iso` que vous avez téléchargée, localisez le fichier `prerequisites.zip`.

   Vous le trouverez dans le répertoire `/36MetaDirSupport`.

2 Dézippez le fichier, puis recherchez le fichier `afadmin.jar`.

3 Copiez le fichier `afadmin.jar` dans le répertoire `/iManager/nps/WEB-INF/lib`.

Création de pilotes

3

Cette section décrit la procédure permettant de créer les pilotes nécessaires à l'utilisation du module de provisioning basé sur les rôles. Les rubriques sont les suivantes :

- Section 3.1, « Création du pilote d'application utilisateur dans iManager », page 27
- Section 3.2, « Création du pilote de service de rôle dans iManager », page 29

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

La 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.
- Associer une application utilisateur unique à un pilote d'application utilisateur.

3.1 Création du pilote d'application utilisateur dans iManager

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

Vous devez créer un pilote d'application utilisateur séparé pour chaque module de provisioning basé sur les rôles d'Identity Manager, à l'exception des modules de provisioning basés sur les rôles membres d'une grappe. Les modules de provisioning basés sur les rôles qui font partie de la même grappe doivent partager un seul pilote d'application utilisateur. Pour plus d'informations sur l'exécution du module de provisioning basé sur les rôles dans une grappe, reportez-vous au *Guide d'administration de l'application utilisateur* (http://www.novell.com/documentation/idmrbpm361/index.html).

Important : la configuration d'un ensemble de modules de provisioning basés sur les rôles non mis en grappe pour partager un seul pilote crée une ambiguïté et une configuration incorrecte d'un ou plusieurs des composants exécutés dans le module de provisioning basé sur les rôles. La source des problèmes conséquents est difficile à détecter.

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

1. Ouvrez iManager dans un navigateur Web.

   Utilisez iManager 2.6 (pour Identity Manager 3.5.1) ou iManager 2.7 (pour Identity Manager 3.6).

2. Dans *Rôles et tâches* > *Utilitaires Identity Manager*, sélectionnez *Nouveau pilote* ou *Importer la configuration* (en fonction de la version de vos plug-ins).

   Pour Identity Manager 3.5.1, utilisez le lien *Nouveau pilote*.

   Pour Identity Manager 3.6, utilisez le lien *Importer la configuration*.

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

ou

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

3a Indiquez un nom, un contexte et un serveur pour le nouvel ensemble de pilotes. Le contexte correspond au contexte eDirectory™ dans lequel l'objet serveur se trouve.

3b Cliquez sur *Suivant*.

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

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

UserApplication_3_6_1-IDM3_5_1-V1.xml

Si ce fichier ne figure pas dans la liste, le pilote de service de rôles peut ne pas être installé correctement. Reportez-vous à Section 2.6.1, « Installation du pilote de service de rôles à l'aide de l'interface graphique », page 24.

6 Cliquez sur *Suivant*.

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

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

8 Cliquez sur *Suivant*.

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

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

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

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

12 Cliquez sur *OK* pour fermer la fenêtre Équivalents de sécurité, puis cliquez sur *Suivant* pour afficher la page de résumé.

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

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

3.2 Création du pilote de service de rôle dans iManager

Remarque : vous n'avez pas besoin de réaliser les étapes de cette section si vous utilisez l'édition standard de l'application utilisateur.

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

1 Ouvrez iManager dans un navigateur Web.

Utilisez iManager 2.6 (avec Identity Manager 3.5.1) ou iManager 2.7 (avec Identity Manager 3.6).

2 Sous *Identity Manager* > *Présentation Identity Manager*, sélectionnez l'ensemble de pilotes dans lequel installer le pilote de service de rôles.

Installez le pilote d'application utilisateur avant le pilote de service de rôle. Utilisez la version 3.6.1 du pilote d'application utilisateur (`UserApplication_3_6_1-IDM3_5_1-V1.xml`) avec le pilote de service de rôle. Si vous utilisez une version différente du pilote d'application utilisateur, le catalogue de rôles ne sera pas disponible.

3 Cliquez sur *Ajouter pilote*.

4 Dans l'Assistant, conservez la valeur par défaut *Dans un ensemble de pilotes existant*. Cliquez sur *Suivant*.

5 Sélectionnez *RoleService_3_6_1-IDM3_5_1-V1.xml* dans la liste déroulante. Il s'agit du fichier de configuration du pilote de service de rôle prenant en charge le module de provisioning basé sur les rôles.

S'il ne s'y trouve pas, vous n'avez pas copié ce fichier à l'emplacement correct. Reportez-vous à Section 2.6.1, « Installation du pilote de service de rôles à l'aide de l'interface graphique », page 24.

Cliquez sur *Suivant*.

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

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

Dans ce cas, l'application iManager n'a pas encore récupéré votre nouveau schéma de rôles. Ce dernier est nécessaire au pilote de service de rôle. Essayez de redémarrer iManager et eDirectory pour vérifiez que les nouvelles modifications de schéma sont correctement prises en compte.

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

Option	Description
Nom du pilote	Indiquez le nom du pilote ou conservez le nom par défaut (`Service de rôle`). Si vous installez un pilote dont le nom est identique à celui d'un pilote existant, le nouveau pilote remplace la configuration de l'ancien pilote. Le bouton *Parcourir* permet d'afficher les pilotes existants de l'ensemble sélectionné. Ce champ est obligatoire.
DN du conteneur de base du groupe d'utilisateurs	Le pilote agit uniquement sur les utilisateurs, les conteneurs et les groupes de ce conteneur de base. S'il existe des attributions de rôle de groupe, le pilote de rôles attribue ou révoque uniquement les rôles sur les membres au sein du domaine du conteneur.
DN du pilote de l'application utilisateur	Nom distinctif de l'objet Pilote de l'application utilisateur qui héberge le système du rôle. Utilisez le format eDirectory, par exemple UserApplication.driverset.org, ou recherchez l'objet pilote. Ce champ est obligatoire.
URL de l'application utilisateur	URL utilisée pour se connecter à l'application utilisateur afin de lancer les workflows d'approbation. L'exemple d'URL indiqué est *http://hôte:port/IDM*. Ce champ est obligatoire.
Identité de l'application utilisateur	Nom distinctif de l'objet utilisé pour authentifier l'application utilisateur afin de lancer les workflows d'approbation. Il peut s'agir d'un administrateur de l'application utilisateur à qui vous avez donné le droit de gérer le portail de l'application utilisateur. Utilisez le format eDirectory, par exemple admin.department.org, ou recherchez l'utilisateur. Ce champ est obligatoire.
Mot de passe de l'application utilisateur	Mot de passe de l'administrateur de l'application utilisateur indiqué dans l'ID d'authentification. Mot de passe utilisé pour s'authentifier auprès de l'application utilisateur afin de lancer les workflows d'approbation. Ce champ est obligatoire.
Confirmez le mot de passe	Saisissez de nouveau le mot de passe de l'administrateur de l'application utilisateur.

7. Une fois les informations renseignées, cliquez sur *Suivant*.
8. Cliquez sur *Définir les équivalents de sécurité* pour ouvrir la fenêtre Équivalents de sécurité. Recherchez et sélectionnez un objet administrateur ou autre superviseur, puis cliquez sur *Ajouter*.

   Cette étape donne au pilote les autorisations de sécurité dont il a besoin. Des détails sur le sens de cette étape se trouvent dans votre documentation Identity Manager.
9. (Facultatif, mais recommandé) Cliquez sur *Exclure les rôles administratifs*.
10. Cliquez sur *Ajouter*, sélectionnez les utilisateurs que vous souhaitez exclure des actions de pilote (les rôles administratifs, par exemple), cliquez deux fois sur *OK*, puis cliquez sur *Suivant*.
11. Cliquez sur *OK* pour fermer la fenêtre Équivalents de sécurité, puis cliquez sur *Suivant* pour afficher la page de résumé.
12. Si les informations sont correctes, cliquez sur *Terminer*.

Installation sur JBoss à l'aide du programme d'installation de l'interface graphique

4

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

- Section 4.1, « Installation et configuration du fichier WAR de l'application utilisateur », page 33
- Section 4.2, « Tester l'installation », page 39

Si vous préférez utiliser la ligne de commande, reportez-vous au Chapitre 7, « Installation depuis la console ou à l'aide d'une commande unique », page 59.

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

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

---

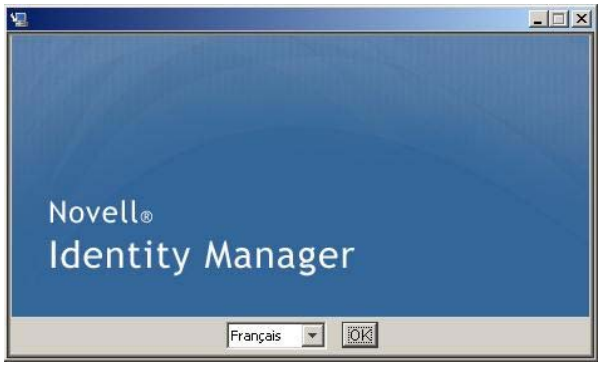
Remarque : le programme d'installation requiert au moins la version 1.5 du kit de développement de la plate-forme Java 2, Standard Edition. Si vous utilisez une version antérieure, la procédure d'installation ne configurera pas correctement le fichier WAR de l'application utilisateur. L'installation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

---

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

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

Lors du lancement du programme d'installation, le programme vous invite à indiquez la langue à utiliser.

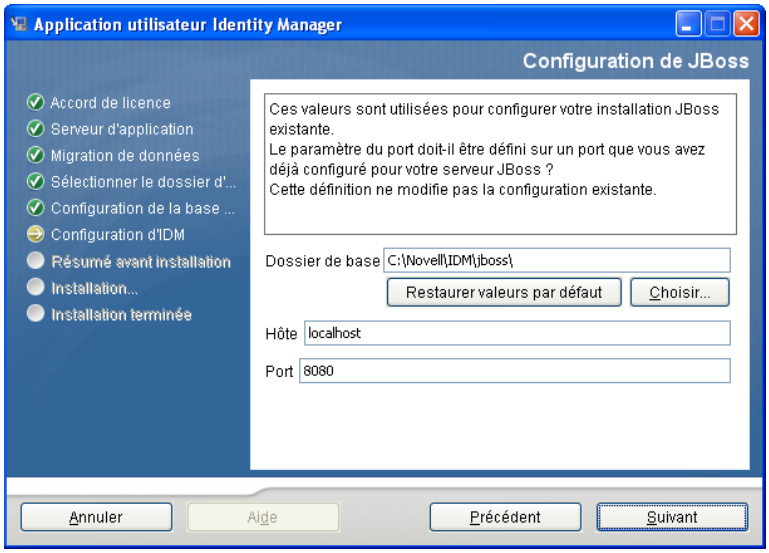


2 Utilisez les informations suivantes, ainsi que les instructions qui figurent sur chaque volet d'installation, pour terminer l'installation :

Écran d'installation	Description
Novell Identity Manager	Sélectionnez la langue du programme d'installation. La valeur par défaut est Français.
Accord de licence	Lisez l'accord de licence, puis sélectionnez *J'accepte les termes de l'accord de licence*.
Plate-forme du serveur d'applications	Sélectionnez *JBoss*.
Standard ou Provisioning	*Standard* : sélectionnez cette option si vous installez l'édition standard de l'application utilisateur. *Provisioning basé sur les rôles* : sélectionnez cette option si vous installez le module de provisioning basé sur les rôles.
Migration de données	Acceptez la valeur par défaut (vérifiez que *Oui* n'est pas sélectionné). **Avertissement :** ne sélectionnez pas *Oui*. Si Oui est sélectionné, des problèmes risquent de se produire au démarrage de l'application utilisateur. Pour en savoir plus sur la migration, reportez-vous au *Guide de migration de l'application utilisateur* (http://www.novell.com/documentation/idmrbpm361/index.html).
Où est le fichier WAR ?	Si le fichier WAR de l'application utilisateur Identity Manager est dans un répertoire différent du programme d'installation, ce dernier vous invite à saisir le chemin d'accès au WAR.
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. Les options disponibles sont les suivantes : ◆ MySQL ◆ Oracle (le programme vous demande la version Oracle) ◆ Serveur MS SQL
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 de la base de données et utilisateur privilégié	*Nom de la base de données* (ou identificateur système) : pour MySQL ou le serveur MS SQL, 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. *Utilisateur de la base de données* : indiquez l'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/Confirmation du mot de passe* : 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.
Installation de Java	Indiquez le dossier d'installation racine de Java.

Vous êtes invité à indiquer l'emplacement d'installation du serveur d'applications JBoss.



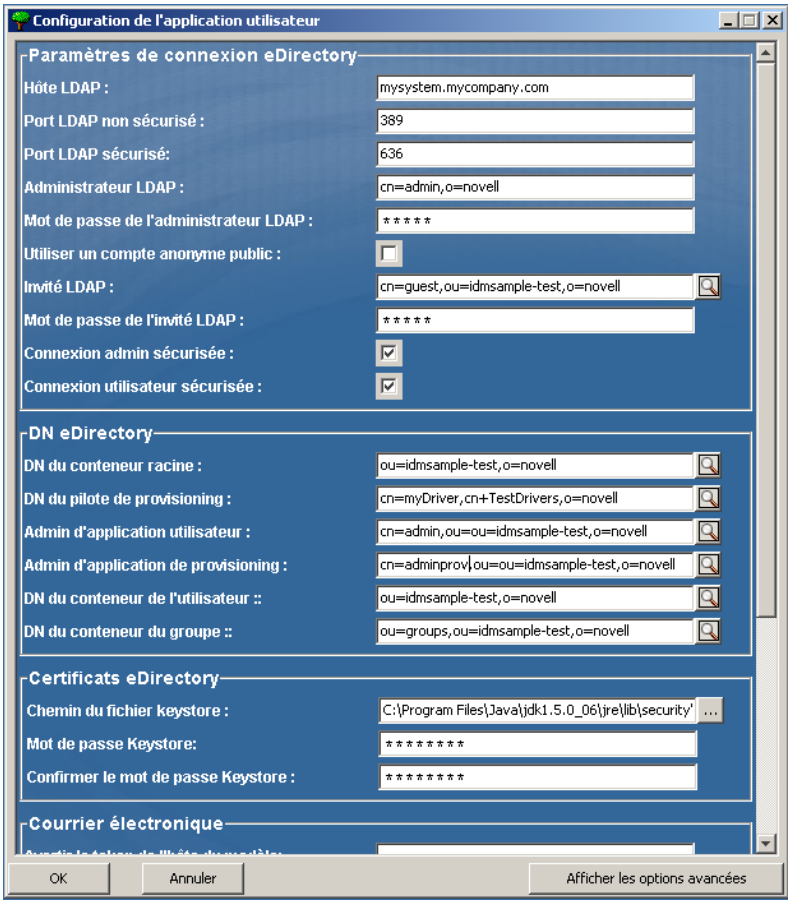
3 Utilisez les informations suivantes pour compléter ce volet et poursuivre l'installation.

Écran d'installation	Description
Configuration de JBoss	Indique à l'application utilisateur où le serveur d'applications JBoss se trouve. La procédure d'installation n'installe pas le serveur d'applications JBoss ; pour obtenir des instructions sur l'installation du serveur d'applications JBoss, reportez-vous à « Installation du serveur d'applications JBoss et de la base de données MySQL » page 20. *Dossier de base* : indiquez l'emplacement du serveur d'applications. *Hôte* : indiquez le nom d'hôte ou l'adresse IP du serveur d'applications. *Port* : indiquez le numéro de port d'écoute du serveur d'applications. Le port JBoss par défaut est 8080.

Écran d'installation	Description
Configuration d'IDM	Sélectionnez le type de configuration du serveur d'applications : ◆ Sélectionnez *tous* si cette installation fait partie d'une grappe ◆ Sélectionnez *par défaut* si cette installation est sur un noeud simple qui ne fait pas partie d'une grappe Si vous sélectionnez *par défaut* et décidez que vous aurez besoin d'une grappe ultérieurement, vous devrez réinstaller l'application utilisateur. *Nom de l'application* : le nom de la configuration du serveur d'applications, le nom du fichier WAR de l'application et le nom du contexte de l'URL. Le script d'installation crée une configuration serveur et par défaut nomme la configuration en fonction du *Nom de l'application*. Notez le nom de l'application et ajoutez-le dans l'URL lorsque vous démarrez l'application utilisateur dans un navigateur. *ID de moteur de workflow* : chaque serveur d'une grappe doit avoir un ID de moteur de workflow unique. Les ID de moteur de workflow sont décrits dans le *Guide d'administration de l'application utilisateur* à la section 3.5.4, « Configuration de workflows pour la mise en grappe .
Consignation Audit	Pour activer la consignation, cliquez sur *Oui*. Le tableau de bord suivant vous invite à indiquer le type de consignation. Choisissez parmi les options suivantes : ◆ *Novell Audit* : active la consignation Novell® Audit 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 Novell Audit ou OpenXDAS, reportez-vous au *Guide d'administration de l'application utilisateur*.
Novell Audit	*Serveur* : si vous activez la consignation Novell Audit, indiquez le nom d'hôte ou l'adresse IP du serveur Novell Audit. Si vous désactivez la consignation, cette valeur est ignorée. *Dossier 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 tel que décrit dans Section 8.1, « Enregistrement de la clé maîtresse », page 71. 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.

4 Le programme d'installation vous invite à saisir les informations qu'il utilise pour configurer le fichier WAR de l'application utilisateur. (Si le programme ne vous invite pas à saisir ces informations, vous n'avez peut-être pas suivi toutes les étapes définies dans Section 2.5, « Installation du kit de développement Java », page 23.



5 Utilisez les informations suivantes pour compléter le tableau de bord et poursuivre l'installation.

Écran d'installation	Description
Configuration de l'application utilisateur	Le programme d'installation de l'application utilisateur permet de configurer les paramètres de configuration de l'application utilisateur. La plupart de ces paramètres sont également éditables avec `configupdate.sh` ou `configupdate.bat` après l'installation ; les exceptions sont notées dans les descriptions des paramètres. Pour une grappe, indiquez les paramètres de configuration identiques de l'application utilisateur pour chaque membre de la grappe. Reportez-vous à Annexe A, « Référence de configuration de l'application utilisateur IDM », page 79 pour obtenir une description des options.

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 Résumé avant installation, puis cliquez sur *Installer*.
Installation terminée	Indique que l'installation est terminée.

4.1.1 Affichage des fichiers journaux et d'installation

Si votre installation s'est terminée sans erreur, passez à 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.

4.2 Tester l'installation

1. Démarrez votre base de données. Reportez-vous à la documentation de votre base de données pour obtenir des directives.
2. Démarrez le serveur de l'application utilisateur (JBoss). Sur la ligne de commande, faites du répertoire d'installation votre répertoire de travail et exécutez le script suivant (fourni par l'installation de l'application utilisateur) :

   `start-jboss.sh` (Linux et Solaris)

   `start-jboss.bat` (Windows)

   Pour arrêter le serveur d'applications, utilisez `stop-jboss.sh` ou `stop-jboss.bat` ou fermez la fenêtre dans laquelle `start-jboss.sh` ou `start-jboss.bat` est exécuté.

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

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

3. Démarrez le pilote d'application utilisateur. Cela active la communication vers le pilote de l'application utilisateur.

   3a Loguez-vous à iManager.

3b Sur l'écran des Rôles et tâches dans la trame de navigation de gauche, sélectionnez *Présentation Identity Manager* sous *Identity Manager*.

3c Sur l'affichage du contenu, spécifiez l'ensemble de pilotes qui contient le pilote de l'application utilisateur, puis cliquez sur *Rechercher*. Un graphique s'affiche, indiquant l'ensemble de pilotes avec ses pilotes associés.

3d Cliquez sur l'icône rouge et blanche sur le pilote.

3e Sélectionnez *Démarrer le pilote*. Le statut du pilote change et passe au symbole du yin et du yang, indiquant que le pilote est démarré.

Le pilote, au démarrage, tente une « reconnaissance mutuelle » avec l'application utilisateur. Si votre serveur d'applications n'est pas en cours d'exécution ou si le WAR n'a pas été correctement déployé, le pilote renvoie une erreur.

4 Pour lancer et se loguer à l'application utilisateur, utilisez votre navigateur Web pour aller sur l'URL suivante :

http://*nomhôte*:*port*/*NomApplication*

nomhôte:*port* représente le nom d'hôte du serveur d'applications (par exemple, monserveur.domaine.com) et le port de votre serveur d'applications (par exemple, 8080, valeur par défaut sur JBoss). La valeur par défaut de *NomApplication* est *IDM*. Vous avez spécifié le nom de l'application lors de l'installation lorsque vous avez fourni les informations de configuration du serveur d'applications.

La page de renvoi de l'application utilisateur Novell Identity Manager s'affiche.

5 Dans le coin supérieur droit de cette page, cliquez sur *Login* pour vous loguer à l'application utilisateur.

Si la page de l'application utilisateur Identity Manager ne s'affiche pas dans votre navigateur à la suite de ces étapes, vérifiez l'absence de messages d'erreur sur la console du terminal et reportez-vous à Section 8.7, « dépannage », page 76.

5 Installation sur un serveur d'applications WebSphere à l'aide du programme d'installation de l'interface graphique

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

- Section 5.1, « Installation et configuration du fichier WAR de l'application utilisateur », page 41
- Section 5.2, « Configuration de l'environnement WebSphere », page 46
- Section 5.3, « Déploiement du fichier WAR », page 48
- Section 5.4, « Démarrage et accès à l'application utilisateur », page 48

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

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

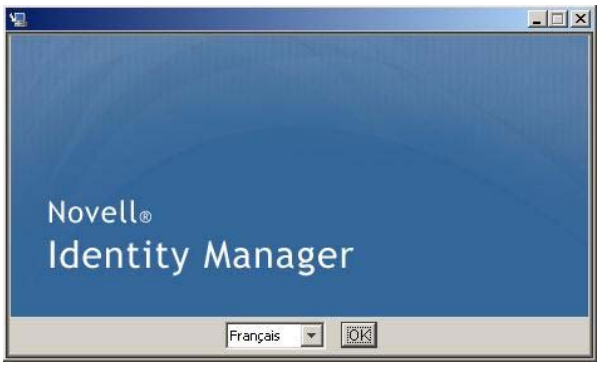
Remarque : le programme d'installation requiert au moins la version 1.5 du kit de développement de la plate-forme Java 2, Standard Edition. Si vous utilisez une version antérieure, la procédure d'installation ne configurera pas correctement le fichier WAR de l'application utilisateur. L'installation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

1. Naviguez jusqu'au répertoire contenant vos fichiers d'installation.
2. Lancez le programme d'installation :

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

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

   Lors du lancement du programme d'installation, le programme vous invite à indiquez la langue à utiliser.



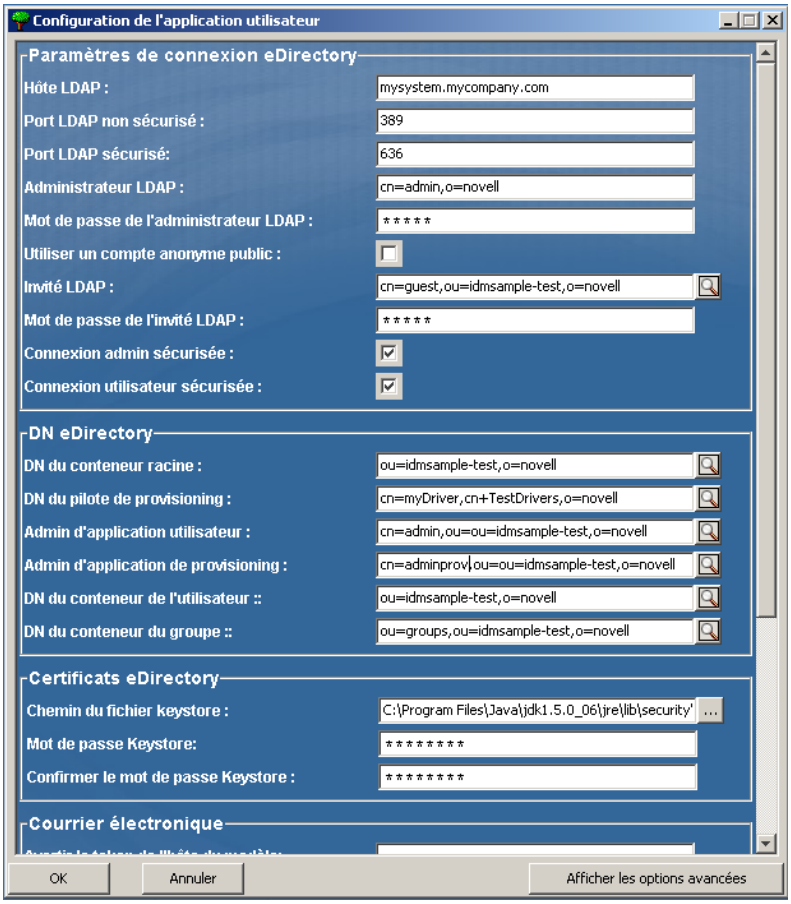
3 Utilisez les informations suivantes, ainsi que les instructions qui figurent sur chaque volet d'installation, pour terminer l'installation :

Écran d'installation	Description
Novell Identity Manager	Sélectionnez la langue du programme d'installation. La valeur par défaut est Français.
Accord de licence	Lisez l'accord de licence, puis sélectionnez *J'accepte les termes de l'accord de licence*.
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.
Standard ou Provisioning	*Standard* : sélectionnez cette option si vous installez l'édition standard de l'application utilisateur. *Provisioning basé sur les rôles* : sélectionnez cette option si vous installez le module de provisioning basé sur les rôles.
Migration de données	Acceptez la valeur par défaut (vérifiez que *Oui* n'est pas sélectionné). **Avertissement :** ne sélectionnez pas *Oui*. Si Oui est sélectionné, des problèmes risquent de se produire au démarrage de l'application utilisateur. Pour en savoir plus sur la migration, reportez-vous au *Guide de migration de l'application utilisateur* (http://www.novell.com/documentation/idmrbpm361/index.html).
Où est le fichier WAR ?	Si le fichier WAR de l'application utilisateur Identity Manager est dans un répertoire différent du programme d'installation, ce dernier vous invite à saisir le chemin d'accès au WAR.
Choisissez 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. Les options disponibles sont les suivantes : ◆ Oracle (le programme vous demande la version Oracle) ◆ Serveur MS SQL ◆ DB2
Installation de Java	Indiquez le dossier d'installation racine de Java. **Remarque :** avec WebSphere, utilisez le JDK d'IBM et appliquez les fichiers de stratégies accessibles.
Configuration d'IDM	Indiquez le contexte d'application.
Consignation Audit	Pour activer la consignation, cliquez sur *Oui*. Le tableau de bord suivant vous invite à indiquer le type de consignation. Choisissez parmi les options suivantes : ◆ *Novell Audit* : active la consignation Novell Audit pour l'application utilisateur. Pour plus d'informations sur la configuration de la consignation Novell Audit, reportez-vous au *Guide d'administration de l'application utilisateur Identity Manager*. ◆ *OpenXDAS* : les événements sont consignés sur votre serveur de consignation OpenXDAS. Pour plus d'informations sur la configuration de la consignation Novell Audit ou OpenXDAS, reportez-vous au *Guide d'administration de l'application utilisateur*.
Novell Audit	*Serveur* : si vous activez la consignation Novell Audit, indiquez le nom d'hôte ou l'adresse IP du serveur Novell Audit. Si vous désactivez la consignation, cette valeur est ignorée. *Dossier 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. Vous devez enregistrer manuellement la clé principale à l'issue de l'installation. La procédure d'installation inscrit la clé maîtresse codée dans le fichier `master-key.txt` dans le répertoire d'installation. Voici des exemples de raisons d'importer une clé maîtresse existante : ◆ Vous déplacez votre installation d'un système provisoire à un système de production et vous souhaitez conserver l'accès à la base de données que vous avez utilisée avec le système provisoire. ◆ Vous avez installé l'application utilisateur sur le premier membre d'une grappe et vous l'installez maintenant sur de nouveaux membres de la grappe (qui requièrent la même clé maîtresse). ◆ En raison d'un disque défectueux, vous devez restaurer votre application utilisateur. Vous devez réinstaller l'application utilisateur et indiquer la même clé maîtresse codée que celle qu'utilisait l'installation précédente. Cela vous donne accès aux données codées stockées précédemment.

4 Le programme d'installation vous invite à saisir les informations qu'il utilise pour configurer le fichier WAR de l'application utilisateur. (Si le programme ne vous invite pas à saisir ces informations, vous n'avez peut-être pas suivi toutes les étapes définies dans Section 2.5, « Installation du kit de développement Java », page 23.



5 Utilisez les informations suivantes pour compléter le tableau de bord et poursuivre l'installation.

Écran d'installation	Description
Configuration de l'application utilisateur	Le programme d'installation de l'application utilisateur permet de configurer les paramètres de configuration de l'application utilisateur. La plupart de ces paramètres sont également éditables avec `configupdate.sh` ou `configupdate.bat` après l'installation ; les exceptions sont notées dans les descriptions des paramètres. Pour plus d'informations, reportez-vous à Annexe A, « Référence de configuration de l'application utilisateur IDM », page 79.

Écran d'installation	Description
Résumé pré-installation	Lisez la page Résumé avant installation pour vérifier vos choix de 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 Résumé avant installation, puis cliquez sur *Installer*.
Installation terminée	Indique que l'installation est terminée.

5.1.1 Affichage des fichiers journaux d'installation

Si votre installation s'est terminée sans erreur, passez à Section 5.2.1, « Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM », page 46.

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 Configuration de l'environnement WebSphere

- Section 5.2.1, « Ajout de fichiers de configuration de l'application utilisateur et des propriétés JVM », page 46
- Section 5.2.2, « Importation de la racine approuvée d'eDirectory dans la zone de stockage des clés WebSphere », page 47

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

Les étapes suivantes permettent l'installation sous WebSphere.

1 Copiez le fichier `sys-configuration-xmldata.xml` du répertoire d'installation de l'application utilisateur dans un répertoire de la machine hébergeant le serveur WebSphere, par exemple `/UserAppConfigFiles`.

Le répertoire d'installation de l'application utilisateur est celui dans lequel vous avez installé l'application utilisateur.

2. Définissez le chemin d'accès du fichier `sys-configuration-xmldata.xml` dans les propriétés du système JVM. Loguez-vous à la console d'administration WebSphere en tant qu'utilisateur administrateur pour ce faire.
3. Dans le panneau de gauche, accédez à *Serveurs* > *Serveur d'application*
4. Cliquez sur le nom du serveur dans la liste, par exemple serveur1.
5. Dans la liste des paramètres de droite, accédez à *Java et Gestion de processus* sous *Infrastructure de serveur*.
6. Développez le lien et sélectionnez *Définition du processus*.
7. Sous la liste des *Propriétés supplémentaires*, sélectionnez *Machine virtuelle Java*.
8. Sélectionnez *Propriétés personnalisées* sous le titre *Propriétés supplémentaires* de la page JVM.
9. Cliquez sur *Nouveau* pour ajouter une nouvelle propriété du système JVM.
   - **9a** Pour le *Nom*, indiquez `extend.local.config.dir`.
   - **9b** Pour la *valeur*, indiquez le nom du répertoire d'installation que vous avez spécifié lors de l'installation.

     Le programme d'installation y a écrit le fichier `sys-configuration-xmldata.xml`.
   - **9c** *Description* permet de saisir la description de la propriété. (exemple : `chemin vers sys-configuration-xmldata.xml`).
   - **9d** Cliquez sur *OK* pour enregistrer la propriété.
10. Cliquez sur *Nouveau* pour ajouter une autre propriété nouvelle du système JVM.
    - **10a** Pour le *Nom*, indiquez `idmuserapp.logging.config.dir.`
    - **10b** Pour la *valeur*, indiquez le nom du répertoire d'installation que vous avez spécifié lors de l'installation.
    - **10c** *Description* permet de saisir la description de la propriété (exemple : `chemin vers idmuserapp_logging.xml`).
    - **10d** Cliquez sur *OK* pour enregistrer la propriété.

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

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

1. Copiez les certificats racine approuvés eDirectory™ sur la machine qui héberge le serveur WebSphere.

   La procédure d'installation de l'application utilisateur exporte les certificats vers le répertoire dans lequel vous installez l'application utilisateur.

2 Importez les certificats dans la zone de stockage de clés WebSphere. Pour cela, utilisez la console de l'administrateur WebSphere (« Importation de certificats avec la console de l'administrateur WebSphere » page 48) ou la ligne de commande (« Importation de certificats avec la ligne de commande » page 48).

3 Après avoir importé les certificats, passez à Section 5.3, « Déploiement du fichier WAR », page 48.

Importation de certificats avec la console de l'administrateur WebSphere

1 Loguez-vous à la console d'administration WebSphere en tant qu'utilisateur administrateur.

2 Dans le tableau de bord de gauche, accédez à *Sécurité* > *Gestion des certificats SSL et des clés*

3 Dans la liste des paramètres de droite, accédez à *Zone se stockage des clés et des certificats* sous *Propriétés supplémentaires*.

4 Sélectionnez *NodeDefaultTrustStore* (ou la zone de stockage fiable que vous utilisez).

5 Sous *Propriétés supplémentaires*, sur la droite, sélectionnez *Certificats du signataire*.

6 Cliquez sur *Ajouter*.

7 Saisissez le nom de l'alias et le chemin d'accès complet au fichier de certificat.

8 Modifiez le type de donnée dans la liste déroulante en sélectionnant *Données DER binaires*.

9 Cliquez sur *OK*. À présent, le certificat doit apparaître dans la liste des certificats du signataire.

Importation de certificats avec la ligne de commande

Dans la ligne de commande de la machine qui héberge le serveur WebSphere, exécutez l'outil clé pour importer le certificat dans la zone de stockage de clés de WebSphere.

Remarque : vous devez utiliser l'outil clé de WebSphere pour que cela fonctionne. Vérifiez en outre que la zone de stockage est de type PKCS12.

L'outil clé WebSphere se trouve dans `/IBM/WebSphere/AppServer/java/bin`.

Exemple de commande d'outil clé :

```
keytool -import -trustcacerts -file servercert.der -alias
myserveralias -keystore trust.p12 -storetype PKCS12
```

Si votre système contient plusieurs fichiers `trust.p12`, il se peut que vous deviez indiquer le chemin complet du fichier.

5.3 Déploiement du fichier WAR

Déployez le fichier WAR via les outils de déploiement WebSphere.

5.4 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 sur un serveur d'applications WebSphere à l'aide du programme d'installation de l'interface graphique

6

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 6.1, « Liste de contrôle de l'installation de WebLogic », page 51
- Section 6.2, « Installation et configuration du fichier WAR de l'application utilisateur », page 52
- Section 6.3, « Préparation de l'environnement WebLogic », page 56
- Section 6.4, « Déploiement du fichier WAR de l'application utilisateur », page 58
- Section 6.5, « Accès à l'application utilisateur », page 58

Pour en savoir plus sur l'installation avec une interface utilisateur non graphique, reportez-vous à Chapitre 7, « Installation depuis la console ou à l'aide d'une commande unique », page 59.

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

6.1 Liste de contrôle de l'installation 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 Section 6.2, « Installation et configuration du fichier WAR de l'application utilisateur », page 52.

- ❑ Préparez l'environnement WebLogic afin de déployer le fichier WAR en copiant les fichiers de configuration aux emplacements WebLogic appropriés.

  Reportez-vous à Section 6.3, « Préparation de l'environnement WebLogic », page 56.

- ❑ Déployez le fichier WAR.

  Reportez-vous à Section 6.4, « Déploiement du fichier WAR de l'application utilisateur », page 58.

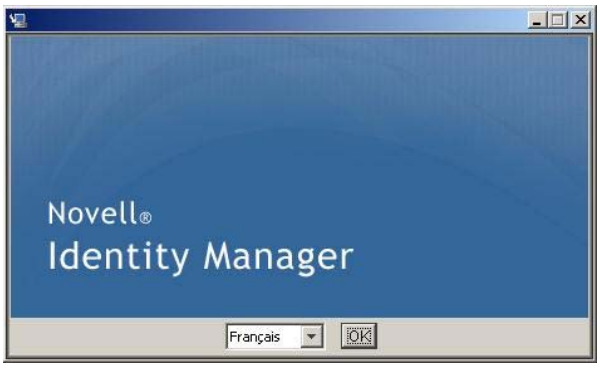
6.2 Installation et configuration du fichier WAR de l'application utilisateur

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. Naviguez jusqu'au répertoire contenant vos fichiers d'installation.
2. Lancez le programme d'installation correspondant à votre plate-forme à partir de la ligne de commande :

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

   Lors du lancement du programme d'installation, le programme vous invite à indiquez la langue à utiliser.

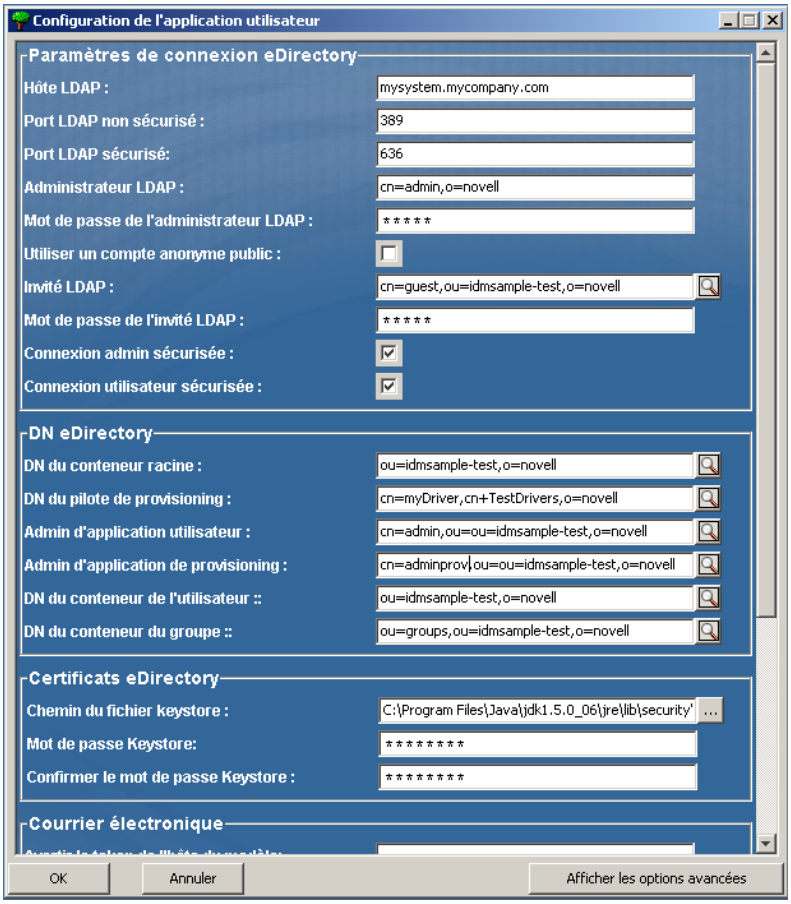
   

3. Utilisez les informations suivantes, ainsi que les instructions qui figurent sur chaque volet d'installation, pour terminer l'installation :

Écran d'installation	Description
Novell Identity Manager	Sélectionnez la langue du programme d'installation. La valeur par défaut est Français.
Accord de licence	Lisez l'accord de licence, puis sélectionnez *J'accepte les termes de l'accord de licence*.
Plate-forme du serveur d'applications	Sélectionnez *WebLogic* pour le serveur d'applications.
Standard ou Provisioning	*Standard* : sélectionnez cette option si vous installez l'édition standard de l'application utilisateur. *Provisioning basé sur les rôles* : sélectionnez cette option si vous installez le module de provisioning basé sur les rôles.
Migration de données	Acceptez la valeur par défaut (vérifiez que *Oui* n'est pas sélectionné). **Avertissement :** ne sélectionnez pas *Oui*. Si Oui est sélectionné, des problèmes risquent de se produire au démarrage de l'application utilisateur. Pour en savoir plus sur la migration, reportez-vous au *Guide de migration de l'application utilisateur* (http://www.novell.com/documentation/idmrbpm361/index.html).
Où est le fichier WAR ?	Si le fichier WAR de l'application utilisateur Identity Manager est dans un répertoire différent du programme d'installation, ce dernier vous invite à saisir le chemin d'accès au WAR.
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. Les options disponibles sont les suivantes : ◆ Oracle (le programme vous demande la version Oracle) ◆ Serveur MS SQL
Installation de Java	Indiquez le dossier d'installation racine de Java.
Configuration d'IDM	Indiquez le contexte d'application. Celui-ci fera partie de l'URL lorsque vous démarrerez l'application utilisateur depuis un navigateur.
Consignation Audit	Pour activer la consignation, cliquez sur *Oui*. Le tableau de bord suivant vous invite à indiquer le type de consignation. Choisissez parmi les options suivantes : ◆ *Novell Audit* : active la consignation Novell® Audit 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 Novell Audit ou OpenXDAS, reportez-vous au *Guide d'administration de l'application utilisateur*.

Écran d'installation	Description
Novell Audit	*Serveur* : si vous activez la consignation Novell Audit, indiquez le nom d'hôte ou l'adresse IP du serveur Novell Audit. Si vous désactivez la consignation, cette valeur est ignorée. *Dossier 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 tel que décrit dans Section 8.1, « Enregistrement de la clé maîtresse », page 71. 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.

4 Le programme d'installation vous invite à saisir les informations qu'il utilise pour configurer le fichier WAR de l'application utilisateur. (Si le programme ne vous invite pas à saisir ces informations, vous n'avez peut-être pas suivi toutes les étapes définies dans Section 2.5, « Installation du kit de développement Java », page 23.



Écran d'installation	Description
Configuration de l'application utilisateur	Le programme d'installation de l'application utilisateur permet de configurer les paramètres de configuration de l'application utilisateur. La plupart de ces paramètres sont également éditables avec `configupdate.sh` ou `configupdate.bat` après l'installation ; les exceptions sont notées dans les descriptions des paramètres. Pour plus d'informations, reportez-vous à Annexe A, « Référence de configuration de l'application utilisateur IDM », page 79
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 Résumé avant installation, puis cliquez sur *Installer*.
Installation terminée	Indique que l'installation est terminée.

6.2.1 Affichage des fichiers journaux et d'installation

Si votre installation s'est terminée sans erreur, passez à 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.

6.3 Préparation de l'environnement WebLogic

- Section 6.3.1, « Configurez la réserve de connexions », page 56
- Section 6.3.2, « Indiquez l'emplacement des fichiers de configuration de l'application utilisateur. », page 56
- Section 6.3.3, « Plug-in de workflow et configuration de WebLogic », page 58

6.3.1 Configurez la réserve de connexions

- ❑ Copiez les fichiers JAR du pilote de votre base de données vers le domaine où vous déploierez l'application utilisateur.
- ❑ Créez votre source de données.

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

  Le nom JNDI de la source de données doit être identique à celui de la base de données que vous avez indiquée pendant la création du fichier WAR de l'application utilisateur (exemple : `jdbc/IDMUADataSource`).
- ❑ Copiez `antlr-2.7.6.jar` depuis le répertoire d'installation de l'application utilisateur vers le dossier de la bibliothèque de domaine.

6.3.2 Indiquez l'emplacement des fichiers de configuration de l'application utilisateur.

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

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

1. Ouvrez le fichier `setDomainEnv.cmd` ou `setDomainEnv.sh`.
2. Localisez la ligne qui ressemble à ce qui suit :

```
set JAVA_PROPERTIES

export JAVA_PROPERTIES
```

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

- `-Dextend.local.config.dir` : indiquez le dossier (et non le fichier lui-même) qui contient le fichier `sys-configuration.xml`.
- `-Didmuserapp.logging.config.dir` : indiquez le dossier (et non le fichier lui-même) qui contient le fichier `idmuserapp_logging.xml`.

Par exemple, sous Windows :

```
set JAVA_OPTIONS=-Dextend.local.config.dir=c:/bea/user_projects/domains/
base_domain/idm.local.config.dir
-Didmuserapp.logging.config.dir=c:/bea/user_projects/domains/base_domain/
idm.local.config.dir
```

4 Définissez la variable d'environnement `EXT_PRE_CLASSPATH` de façon à ce qu'elle pointe vers le fichier `antlr.jar`.

4a Recherchez cette ligne :

```
ADD EXTENSIONS TO CLASSPATH
```

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

```
set EXT_PRE_CLASSPATH=C:\bea\user_projects\domains\base_domain\lib\antlr-
2.7.6.jar
```

Par exemple, sous Linux :

```
export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/lib/
antlr-2.7.6.jar
```

5 Enregistrez le fichier et quittez l'application.

Les fichiers XML sont également utilisés par l'utilitaire de mise à jour de la configuration ; 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 Ajoutez l'entrée suivante en dessous :

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

4 Enregistrez et fermez le fichier.

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

Lorsque vous exécutez une `mise à jour de la configuration`, le programme vous invite à indiquer le fichier `cacerts` sous le JDK que vous utilisez. Si vous n'utilisez pas le JDK que vous avez indiqué pendant l'installation, vous devez exécuter la `mise à jour de la configuration` 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.

6.3.3 Plug-in de workflow et configuration de WebLogic

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

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

1. Ouvrez le fichier `Config.xml` dans le dossier *<WLHome>*`/user_projects/domains/base_domain/config/` .
2. Ajoutez la ligne suivante à la section `<security-configuration>` :

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
   ```
3. Enregistrez le fichier et redémarrez le serveur.

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

6.4 Déploiement du fichier WAR de l'application utilisateur

- Déployez le fichier jsf-ri-1.1.1.war comme bibliothèque.
- Copiez le fichier WAR mis à jour de l'application utilisateur depuis le répertoire d'installation (en général `Novell\IDM` vers le domaine d'application. Par exemple :

  ```
  bea\user_projects\domains\base_domain\servers\AdminServer\upload
  ```
- Déploie le fichier WAR de l'application utilisateur à l'aide de la procédure de déploiement WebLogic standard.

6.5 Accès à l'application utilisateur

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

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

  Par exemple :

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

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

7

Cette section décrit les méthodes d'installation dont vous disposez si vous ne souhaitez pas utiliser l'interface graphique décrite au Chapitre 4, « Installation sur JBoss à l'aide du programme d'installation de l'interface graphique », page 33. Les rubriques sont les suivantes :

- Section 7.1, « Installation de l'application utilisateur à partir de la console », page 59
- Section 7.2, « Installation de l'application utilisateur avec une seule commande », page 60

7.1 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 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 sous Chapitre 4, « Installation sur JBoss à l'aide du programme d'installation de l'interface graphique », page 33 : 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 Section A.1, « Configuration de l'application utilisateur : paramètres de base », page 79.
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 à Chapitre 8, « Tâches post-installation », page 71.

7.2 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 7-1 pour obtenir une description de chaque paramètre de configuration de l'application utilisateur. Les paramètres de configuration de l'application utilisateur sont les mêmes que ceux que vous pouvez configurer dans les procédures d'installation de l'interface utilisateur graphique ou de la console ou avec l'utilitaire configupdate.
5. Lancez l'installation silencieuse de la façon suivante :

   ```
   java -jar IdmUserApp.jar -i silent -f / yourdirectorypath/
   silent.properties
   ```

   Saisissez le chemin d'accès complet à `silent.properties` si ce fichier est dans un répertoire différent du script du programme d'installation. Le script décondense les fichiers nécessaires vers un répertoire temporaire et lance l'installation en mode silencieux.

Tableau 7-1 *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 à eDirectory™ : hôte LDAP. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP.

Nom du paramètre de l'application utilisateur dans 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 que vous avez créé auparavant dans Section 3.1, « Création du pilote d'application utilisateur dans iManager », page 27. 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, le concepteur Novell pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), vous devez accorder à cet administrateur des droits d'ayant droit sur les instances d'objets contenues dans le pilote de l'application utilisateur. Reportez-vous au *Guide d'administration de l'application utilisateur* 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.

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_KEYSTOREPATH=	Certificats eDirectory : chemin d'accès au keystore. Requis. Indiquez le chemin d'accès complet au fichier (`cacerts`) de votre keystore du JRE que le serveur d'applications utilise. L'installation de l'application utilisateur modifie le fichier keystore. Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier.
NOVL_CONFIG_KEYSTOREPASSWORD=	Certificats eDirectory : mot de passe du keystore. 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.

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_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.
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.

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_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.
NOVL_CONFIG_USEEXTPWDWAR=	Gestion des mots de passe : utiliser un WAR de mots de passe externe. Indiquez *Vrai* si vous utilisez un WAR de gestion de mots de passe externe. Si vous indiquez *Vrai*, vous devez également fournir des valeurs pour *NOVL_CONFIG_EXTPWDWARPTH* et *NOVL_CONFIG_EXTPWDWARRTNPATH*. Indiquez *Faux* pour utiliser la fonction de gestion des mots de passe interne par défaut. `/jsps/pwdmgt/ForgotPassword.jsf` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.
NOVL_CONFIG_EXTPWDWARPATH=	Gestion des mots de passe : liaison Mot de passe oublié. Indiquez l'URL de la page de la fonction Mot de passe oublié, `ForgotPassword.jsf`, dans un WAR de gestion de mots de passe externe ou interne. Vous pouvez également accepter le WAR de gestion des mots de passe interne par défaut. Pour plus de détails, reportez-vous au « Configuration de la gestion de mots de passe externe » page 74.

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_EXTPWDWARRTNPATH=	Gestion des mots de passe : liaison de retour Mot de passe oublié. Si vous utilisez un WAR de gestion des mots de passe externe, indiquez le chemin d'accès que le WAR de gestion des mots de passe externe utilise pour rappeler l'application utilisateur par des services Web, par exemple `https://idmhost:sslport/idm`.
NOVL_CONFIG_USEROBJECTATTRIBUTE=	Identité utilisateur du méta-annuaire : classe d'objets utilisateur. Requis. La classe d'objets utilisateur LDAP (généralement inetOrgPerson).
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.

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_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_PRIVATESTOREPATH=	Keystore privé : chemin du keystore privé. Indiquez le chemin d'accès au keystore privé qui contient la clé privée et les certificats de l'application utilisateur. Réservé. Si vous laissez ce champ vierge, ce chemin d'accès est `/jre/lib/security/cacerts` par défaut.
NOVL_CONFIG_PRIVATESTOREPASSWORD=	Keystore privé : mot de passe du keystore privé.
NOVL_CONFIG_PRIVATEKEYALIAS=	Keystore privé : alias de clé privée. Cet alias est `novellIDMUserApp` à moins d'indication contraire.
NOVL_CONFIG_PRIVATEKEYPASSWORD=	Keystore privé : mot de passe de clé privée.
NOVL_CONFIG_TRUSTEDSTOREPATH=	Keystore approuvé : chemin de keystore approuvé. Le keystore approuvé contient tous les certificats approuvés des signataires utilisés pour valider les signatures numériques. Si ce chemin est vide, l'application utilisateur obtient le chemin à partir de la propriété Système `javax.net.ssl.trustStore`. Si le chemin n'y est pas, il est supposé être `jre/lib/security/cacerts`.
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	Keystore approuvé : mot de passe du keystore approuvé.
NOVL_CONFIG_AUDITCERT=	Certificat de signature numérique Novell Audit
NOVL_CONFIG_AUDITKEYFILEPATH=	Chemin de fichier du keystore privé de signatures numériques Novell Audit.

Nom du paramètre de l'application utilisateur dans silent.properties	Nom du paramètre équivalent dans le fichier des paramètres de configuration de l'application utilisateur
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 connexion à ICS est activée et si un utilisateur se délogue de l'application utilisateur, il est réacheminé vers cette page.
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	Courrier électronique : jeton PROTOCOLE du modèle de notification. Se rapporte à un protocole non sécurisé, HTTP. Utilisé pour remplacer le jeton $PROTOCOL$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	Courrier électronique : jeton du port sécurisé du modèle de notification.
NOVL_CONFIG_OCSPURI=	Divers : OCSP URI. Si l'installation client utilise le protocole OCSP (protocole de propriété d'état de certificat en ligne), fournissez un identificateur de ressource uniforme (URI). Par exemple, le format est http://hstport/ocspLocal. L'URI OCSP met à jour le statut des certificats approuvés en ligne.
NOVL_CONFIG_AUTHCONFIGPATH=	Divers : chemin de configuration d'autorisation. Le nom complet du fichier de configuration de l'autorisation.

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.

Tâches post-installation

8

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

- Section 8.1, « Enregistrement de la clé maîtresse », page 71
- Section 8.2, « Configuration de l'application utilisateur », page 71
- Section 8.3, « Configuration d'eDirectory », page 72
- Section 8.4, « Reconfiguration du fichier WAR de l'application utilisateur après l'installation », page 73
- Section 8.5, « Configuration de la gestion de mots de passe externe », page 74
- Section 8.6, « Mise à jour des paramètres Mot de passe oublié », page 75
- Section 8.7, « dépannage », page 76

8.1 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.

8.2 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 3.6.1 Administration Guide (Guide d'administration de Novell IDM Roles Based Provisioning Module 3.6)*.
- Le manuel *Novell IDM Roles Based Provisioning Module 3.6.1 Design Guide (Guide de conception de Novell IDM Roles Based Provisioning Module 3.6)*

8.2.1 Configuration de Novell Audit

Copiez le fichier `dirxml.lsc` (situé dans le fichier prerequisites.zip) sur le serveur Audit en suivant les instructions de la section intitulée « Configuration de la consignation » du Guide d'administration de l'application utilisateur (http://www.novell.com/documentation/idmrbpm361/index.html).

8.3 Configuration d'eDirectory

- Section 8.3.1, « Création d'index dans eDirectory », page 72
- Section 8.3.2, « Installation et configuration de la méthode d'authentification SAML », page 72

8.3.1 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 tableau de bord Configuration de l'application utilisateur (décrit dans Tableau A-2 page 85). Reportez-vous au *Guide d'administration de Novell eDirectory* pour obtenir des instructions sur l'utilisation du gestionnaire d'index en vue de créer des index. (http://www.novell.com/documentation)

8.3.2 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.)

8.4 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 Section A.1, « Configuration de l'application utilisateur : paramètres de base », page 79, Tableau 7-1 page 60.

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.

8.5 Configuration de la gestion de mots de passe externe

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 8.5.1, « Spécification d'un WAR de gestion des mots de passe externe », page 74
- Section 8.5.2, « Spécification d'un WAR de mot de passe interne », page 75
- Section 8.5.3, « Essai de la configuration du fichier WAR de mots de passe externe », page 75
- Section 8.5.4, « Configuration de la communication SSL entre serveurs JBoss », page 75

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

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

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

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

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

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

La liaison de retour doit utiliser SSL pour assurer une communication sécurisée des services Web vers l'application utilisateur. Reportez-vous également à Section 8.5.4, « Configuration de la communication SSL entre serveurs JBoss », page 75.

5 Effectuez l'une des opérations suivantes :

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

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

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

8.5.2 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*.

8.5.3 Essai de la configuration du fichier WAR de mots de passe externe

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. Allez sur la page Mot de passe oublié dans le WAR de mots de passe externe, par exemple `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`.
- Dans la page de login de l'application utilisateur, cliquez sur le lien *Mot de passe oublié*.

8.5.4 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 WAR de l'application utilisateur et le fichier `IDMPwdMgt.war`. Reportez-vous à votre documentation JBoss pour obtenir des directives.

8.6 Mise à jour des paramètres Mot de passe oublié

Vous pouvez modifier les valeurs de la *liaison Mot de passe oublié* et de la *liaison retour Mot de passe oublié* après l'installation. Utilisez l'utilitaire configupdate ou l'application utilisateur.

Utilisation de l'utilitaire configupdate. Sur une ligne de commande, naviguez jusqu'au répertoire d'installation et saisissez `configupdate.sh` (Linux ou Solaris) ou `configupdate.bat` (Windows). Si vous créez ou modifiez un WAR de gestion de mots de passe externe, vous devez alors renommer manuellement le WAR avant de le copier sur le serveur distant JBoss.

Utilisation de l'application utilisateur. Loguez-vous en tant qu'administrateur de l'application utilisateur et allez dans *Administration* > *Configuration application* > *Configuration module mot de passe* > *Login*. Modifiez les champs suivants :

- *Liaison Mot de passe oublié* (par exemple : `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`)
- *Liaison retour Mot de passe oublié* (par exemple : `https://idmhost:sslport/idm`)

8.7 dépannage

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

Point	Actions suggérées

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 et 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 apparaissent lorsque le serveur d'application démarre, avec un message de journal `port 8080 déjà en cours d'utilisation`.	Arrêter toute instance de Tomcat (ou autre logiciel de serveur) qui pourrait déjà être en cours d'exécution. Si vous décidez de reconfigurer le serveur d'applications de façon à ce qu'il utilise un port autre que 8080, n'oubliez pas de modifier les paramètres `config` pour le pilote de l'application utilisateur dans iManager.
Au démarrage du serveur d'applications, un message s'affiche indiquant qu'aucun certificat approuvé n'a été trouvé.	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).

Point	Actions suggérées
Au démarrage du serveur d'applications, il y a des erreurs de connexion à MySQL.	N'exécutez rien en tant qu'utilisateur `root`. (La survenue de ce problème est cependant peu probable si vous exécutez la version de MySQL fournie avec Identity Manager.) Assurez-vous que MySQL fonctionne (et que la copie correcte est exécutée). Détruisez toute autre instance de MySQL. Exécutez `/idm/mysql/start-mysql.sh`, puis `/idm/start-jboss.sh`. Examinez `/idm/mysql/setup-mysql.sh` dans un éditeur de texte et corrigez toute valeur qui semble suspecte. Exécutez ensuite le script, puis `/idm/start-jboss.sh`.
Vous rencontrez des erreurs de keystore lors du démarrage du serveur d'applications.	Votre serveur d'applications n'exécute pas le JDK spécifié à l'installation de l'application utilisateur. Utilisez la commande `keytool` pour importer le fichier de certificat : `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ Remplacez *aliasName* par un nom unique de votre choix pour ce certificat. ◆ Remplacez *certFile* par le chemin complet et le nom de votre fichier de certificat. ◆ Le mot de passe du keystore par défaut est `changeit` (si vous avez un mot de passe différent, indiquez-le).

Aucune notification n'a été envoyée par courrier électronique.	Exécutez l'utilitaire configupdate pour vérifier 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 79
- Section A.2, « Configuration de l'application utilisateur : tous les paramètres », page 84

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

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

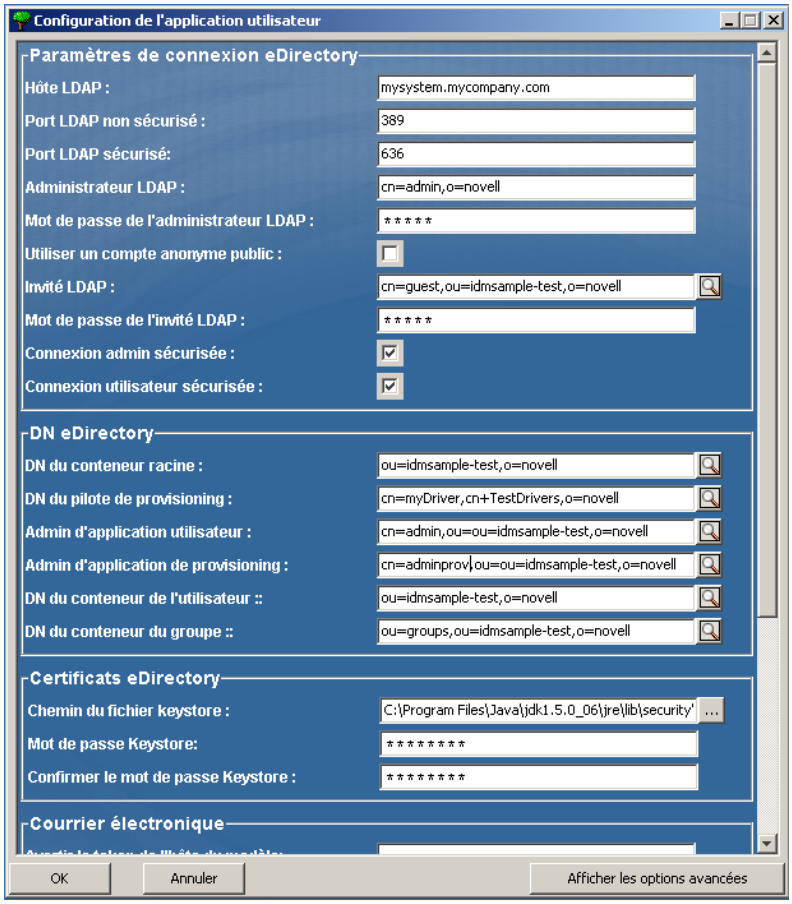


Tableau A-1 *Options de base de configuration de l'application utilisateur*

Type de paramètre	Option	Description
Paramètres de connexion à eDirectory®	*Hôte LDAP*	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP et son port sécurisé. Par exemple : `myLDAPhost`
	Port non sécurisé LDAP	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	Port sécurisé LDAP	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	Administrateur LDAP	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer 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 administrateur LDAP	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.
	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 l'invité LDAP, vous devez désactiver *Utiliser un compte anonyme public*. Pour désactiver l'utilisateur invité, sélectionnez *Utiliser un 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 utilisant le compte de l'utilisateur logué soient effectuées à l'aide d'un socket sécurisé (cette option peut nuire aux performances). Cette configuration permet également d'exécuter des opérations qui ne nécessitent pas SSL.

Type de paramètre	Option	Description
DN eDirectory	*DN du conteneur racine*	Requis. Indiquez le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire.
	DN du pilote de provisioning	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur (décrit dans Section 3.1, « Création du pilote d'application utilisateur dans iManager », page 27). Par exemple, si votre pilote est UserApplicationDriver et si votre ensemble de pilotes est appelé myDriverSet, et si l'ensemble de pilotes est dans un contexte de o=myCompany, vous saisiriez une valeur de : `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Admin. application utilisateur	Requis. Un utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs de l'application utilisateur spécifié. Cet utilisateur peut utiliser l'onglet *Administration* de l'application utilisateur pour administrer le portail. Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, le concepteur Novell pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), vous devez accorder à cet administrateur des droits d'ayant droit sur les instances d'objets contenues dans le pilote de l'application utilisateur. Reportez-vous au *Guide d'administration de l'application utilisateur* 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.
	Admin de l'application de provisioning	L'administrateur de l'application de provisioning utilise l'onglet *Provisioning* (sous l'onglet *Administration*) pour gérer les fonctions de workflow du provisioning. Ces fonctions sont accessibles aux utilisateurs en passant par l'onglet *Requêtes et approbations* de l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur de l'application Provisioning. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.

Type de paramètre	Option	Description
	Admin de conformité	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. 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 module de conformité valide existe, vos modifications ne sont pas enregistrées. Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page *Rôles* > *Assignations de rôles* de l'application utilisateur.
DN eDirectory (suite)	*Administrateur de rôles*	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. 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.
	DN du conteneur d'utilisateurs	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur utilisateur. Cela définit l'étendue de recherche d'utilisateurs et de groupes. Les utilisateurs de ce conteneur (et en dessous) sont autorisés à se loguer à l'application utilisateur. **Important :** 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. Vous ne pouvez pas modifier ce paramètre via ConfigUpdate si vous avez démarré le serveur d'applications qui héberge l'application utilisateur.

Type de paramètre	Option	Description
	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.
Certificats eDirectory	*Chemin d'accès au Keystore*	Requis. Indiquez le chemin d'accès complet au fichier (`cacerts`) de votre keystore du JDK que le serveur d'applications utilise pour fonctionner ou cliquez sur le petit bouton du navigateur pour trouver le fichier `cacerts .` Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier.
	Mot de passe Keystore/Confirmer mot de passe Keystore	Requis. Indiquez le mot de passe `cacerts`. L'unité par défaut est `changeit`.
E-mail	*Jeton de l'hôte du modèle de notification*	Indiquez le serveur d'applications hébergeant l'application utilisateur Identity Manager. Par exemple : `myapplication serverServer` Cette valeur remplace le jeton $HOST$ des modèles de courrier électronique. L'URL construite est la liaison aux tâches de requête de provisioning et aux notifications d'approbation.
	Jeton du port du modèle de notification	Utilisé pour remplacer le jeton $PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Jeton du port sécurisé du modèle de notification	Utilisé pour remplacer le jeton $SECURE_PORT$ des modèles de courrier électronique utilisés dans les tâches de requête de provisioning et les notifications d'approbation.
	Notification SMTP - expéditeur du courrier électronique	Indiquez l'utilisateur expéditeur du courrier électronique dans le message de provisioning.
	Notification SMTP - destinataire du courrier électronique	Indiquez l'utilisateur destinataire du courrier électronique dans le message de provisioning. Il peut s'agir d'une adresse IP ou d'un nom DNS.

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 fournir des valeurs pour *Lien Mot de passe oublié* et *Lien Retour mot de passe oublié*. Si vous ne sélectionnez pas *Utiliser le WAR de mot de passe externe*, IDM utilise la fonction de gestion des mots de passe interne par défaut. `/jsps/pwdmgt/ForgotPassword.jsf` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.
	Liaison Mot de passe oublié	Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier `ForgotPassword.jsf` dans un WAR de gestion des mots de passe externe ou interne. Pour plus de détails, reportez-vous à « Configuration de la gestion de mots de passe externe » page 74.
	Liaison de retour Mot de passe oublié	Si vous utilisez un WAR de gestion des mots de passe externe, indiquez le chemin d'accès que le WAR de gestion des mots de passe externe utilise pour rappeler l'application utilisateur par des services Web, par exemple `https://idmhost:sslport/idm`.

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 de connexion eDirectory	*Hôte LDAP*	Requis. Indiquez le nom d'hôte ou l'adresse IP de votre serveur LDAP. Par exemple : myLDAPhost
	Port non sécurisé LDAP	Indiquez le port non sécurisé de votre serveur LDAP. Par exemple : 389.
	Port sécurisé LDAP	Indiquez le port sécurisé de votre serveur LDAP. Par exemple : 636.
	Administrateur LDAP	Requis. Indiquez les références de l'administrateur LDAP. Cet utilisateur doit déjà exister. L'application utilisateur utilise ce compte pour effectuer une connexion administrative au coffre-fort d'identité. Cette valeur est codée, en fonction de la clé maîtresse.
	Mot de passe administrateur LDAP	Requis. Indiquez le mot de passe administrateur LDAP. Ce mot de passe est codé, en fonction de la clé maîtresse.
	Utiliser le compte anonyme public	Permet aux utilisateurs non logués d'accéder au compte anonyme public LDAP.
	Guest LDAP	Permet aux utilisateurs non logués d'accéder à des portlets autorisés. Ce compte utilisateur doit déjà exister dans le coffre-fort d'identité. Pour activer Guest LDAP, vous devez désélectionner *Utiliser le compte anonyme public*. Pour désactiver l'utilisateur Guest, sélectionnez *Utiliser le compte anonyme public*.
	Mot de passe Guest LDAP	Indiquez le mot de passe Guest LDAP.
	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 eDirectory	*DN du conteneur racine*	Requis. Indiquez le nom distinctif LDAP du conteneur racine. Celui-ci est utilisé comme racine de recherche de définition d'entité par défaut lorsqu'aucune racine n'est indiquée dans la couche d'abstraction d'annuaire.
	DN du pilote de provisioning	Requis. Indiquez le nom distinctif du pilote de l'application utilisateur (décrit dans Section 3.1, « Création du pilote d'application utilisateur dans iManager », page 27). Par exemple, si votre pilote est UserApplicationDriver et si votre ensemble de pilotes est appelé myDriverSet, et si l'ensemble de pilotes est dans un contexte de o=myCompany, vous saisissez une valeur de : `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Admin. application utilisateur	Requis. Un utilisateur existant dans le coffre-fort d'identité qui dispose des droits pour effectuer des tâches administratives pour le conteneur d'utilisateurs de l'application utilisateur spécifié. Cet utilisateur peut utiliser l'onglet *Administration* de l'application utilisateur pour administrer le portail. Si l'administrateur de l'application utilisateur participe aux tâches d'administration du workflow exposées dans iManager, le concepteur Novell pour Identity Manager ou l'application utilisateur (onglet *Requêtes et approbations*), vous devez accorder à cet administrateur des droits d'ayant droit sur les instances d'objets contenues dans le pilote de l'application utilisateur. Reportez-vous au *Guide d'administration de l'application utilisateur* 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.
	Admin de l'application de provisioning	L'administration de l'application de provisioning gère les fonctions de workflow du provisioning accessibles par l'onglet *Requêtes et approbations* de l'application utilisateur. Cet utilisateur doit exister dans le coffre-fort d'identité avant d'être désigné administrateur de l'application Provisioning. Pour modifier cette assignation après avoir déployé l'application utilisateur, vous devez utiliser les pages *Administration* > *Sécurité* de l'application utilisateur.

Type de paramètre	Option	Description
	Admin de conformité	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. 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 module de conformité valide existe, vos modifications ne sont pas enregistrées. Pour modifier cette assignation après avoir déployé l'application utilisateur, utilisez la page *Rôles* > *Assignations de rôles* de l'application utilisateur.
	Administrateur de rôles	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. 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.

Type de paramètre	Option	Description
Identité utilisateur du méta-annuaire	*DN du conteneur d'utilisateurs*	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur d'utilisateurs. 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 méta-annuaire	*DN de conteneur de groupes*	Requis. Indiquez le nom distinctif (DN) LDAP ou le nom LDAP complet du conteneur de groupes. Utilisé par les définitions d'entités au sein de la couche d'abstraction d'annuaire. 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 eDirectory	*Chemin d'accès au Keystore*	Requis. Indiquez le chemin d'accès complet au fichier (`cacerts`) de votre keystore du JRE que le serveur d'applications utilise pour fonctionner ou cliquez sur le petit bouton du navigateur pour trouver le fichier `cacerts` . L'installation de l'application utilisateur modifie le fichier keystore. Sous Linux ou Solaris, l'utilisateur doit avoir une autorisation pour écrire sur ce fichier.
	Mot de passe Keystore	Requis. Indiquez le mot de passe `cacerts`. L'unité par défaut est `changeit`.
	Confirmer le mot de passe Keystore	
Keystore privé	*Chemin d'accès au keystore privé*	Le keystore privé contient la clé privée et les certificats de l'application utilisateur. Réservé. Si vous laissez ce champ vierge, ce chemin d'accès est `/jre/lib/security/cacerts` par défaut.
	Mot de passe Keystore privé	Ce mot de passe est `changeit`, à moins d'indication contraire. Ce mot de passe est codé, en fonction de la clé maîtresse.
	Alias de clé privée	Cet alias est `novellIDMUserApp`, à moins d'indication contraire.
	Mot de passe de la clé privée	Ce mot de passe est `novellIDM`, à moins d'indication contraire. Ce mot de passe est codé, en fonction de la clé maîtresse.

Type de paramètre	Option	Description
Banque de clés approuvée	*Chemin d'accès à la banque approuvée*	La banque de clés approuvées contient tous les certificats approuvés des signataires utilisés pour valider les signatures numériques. Si ce chemin est vide, l'application utilisateur obtient le chemin à partir de la propriété Système `javax.net.ssl.trustStore`. Si le chemin n'y est pas, il est supposé être `jre/lib/security/cacerts`.
	Mot de passe de la banque approuvée	Si ce champ est vierge, l'application utilisateur obtient le mot de passe à partir de la propriété système `javax.net.ssl.trustStorePassword`. S'il n'y a aucune valeur, `changeit` est utilisé. Ce mot de passe est codé, en fonction de la clé maîtresse.
Clé de certificat et signature numérique Novell Audit		Contient le certificat et la clé de signature numérique Novell Audit.
	Certificat de signature numérique Novell Audit	Affiche le certificat de signature numérique.
	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 et iChain	*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 connexion à ICS est activée et si un utilisateur se délogue de l'application utilisateur, il est redirigé vers cette page.

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

Type de paramètre	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 fournir des valeurs pour *Lien Mot de passe oublié* et *Lien Retour mot de passe oublié*. Si vous ne sélectionnez pas *Utiliser le WAR de mot de passe externe*, IDM utilise la fonction de gestion des mots de passe interne par défaut. `/jsps/pwdmgt/ForgotPassword.jsf` (sans le protocole http(s) au début). Cela redirige l'utilisateur vers la fonction Mot de passe oublié intégrée à l'application utilisateur, plutôt que vers un WAR externe.
	Liaison Mot de passe oublié	Cette URL pointe vers la page de fonction Mot de passe oublié. Indiquez un fichier `ForgotPassword.jsf` dans un WAR de gestion des mots de passe externe ou interne.
	Liaison de retour Mot de passe oublié	Si vous utilisez un WAR de gestion des mots de passe externe, indiquez le chemin d'accès que le WAR de gestion des mots de passe externe utilise pour rappeler l'application utilisateur par des services Web, par exemple `https://idmhost:sslport/idm`.
Divers	*Timeout de session*	Le timeout de session de l'application.
	OCSP URI	Si l'installation client utilise le protocole OCSP (protocole de propriété d'état de certificat en ligne), fournissez un identificateur de ressource uniforme (URI). Par exemple, le format est http://host:port/ocspLocal. L'URI OCSP met à jour le statut des certificats approuvés en ligne.
	Chemin de configuration d'autorisation	Nom complet du fichier de configuration de l'autorisation.
	Créer un index eDirectory	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 Section 8.3.1, « Création d'index dans eDirectory », page 72. 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 un index eDirectory	Supprime des index des attributs manager, ismanager et srvprvUUID.

Type de paramètre	Option	Description
	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. Pour plus d'informations sur les conteneurs, reportez-vous au *Guide d'administration de Novell iManager 2.6 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*.
	Ajouter un nouvel objet Conteneur : nom d'attribut Conteneur	Donnez le nom d'attribut de l'objet Conteneur.