ユーザアプリケーション：インストールガイド

Novell® Identity Manager Roles Based Provisioning Module

3.7

2009 年 9 月 18 日

www.novell.com

保証と著作権

米国 Novell, Inc., およびノベル株式会社は、本書の内容または本書を使用した結果について、いかなる保証、表明または約束も行っていません。また、本書の商品性、および特定の目的への適合性について、いかなる明示的または黙示的な保証も否認し、排除します。また、本書の内容は予告なく変更されることがあります。

米国 Novell, Inc., およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っていません。また、ノベル製ソフトウェアの商品性、および特定の目的への適合性について、いかなる明示的または黙示的な保証も否認し、排除します。米国 Novell, Inc., およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。

本契約の下で提供される製品または技術情報はすべて、米国の輸出規制および他国の商法の制限を受けます。お客様は、すべての輸出規制を遵守し、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。ノベル製ソフトウェアの輸出に関する詳細については、「Novell International Trade Services (http://www.novell.com/info/exports/)」の Web ページを参照してください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとします。

本書に記載された製品で使用されている技術に関連する知的所有権は、弊社に帰属します。これらの知的所有権は、Novell Legal Patents (http://www.novell.com/company/legal/patents/) の Web ページに記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

オンラインマニュアル: 本製品とその他の Novell 製品の最新のオンラインマニュアルにアクセスするには、Novell マニュアルの Web ページ (http://www.novell.com/documentation) を参照してください。

Novell の商標

Novell の商標一覧については、「商標とサービスの一覧 (http://www.novell.com/company/legal/trademarks/tmlist.html)」を参照してください。

サードパーティ資料

サードパーティの商標は、それぞれの所有者に帰属します。

目次

このガイドについて

このガイドでは、Novell® Identity Manager Roles Based Provisioning Module 3.7.0. のインストール方法について説明します。主なセクションは次のとおりです。

対象読者

このガイドは、Novell Identity Manager Roles Based Provisioning Module の計画および実装を行う管理者やコンサルタントを対象にしています。

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインマニュアルの各ページの下部にあるユーザコメント機能を使用するか www.novell.com/documentation/feedback.html にアクセスしてコメントを記入してください。

追加のマニュアル

Identity Manager Roles Based Provisioning Module に関する追加のマニュアルについては、Identity Manager マニュアルの Web サイト (http://www.novell.com/documentation/lg/dirxmldrivers/index.html) を参照してください。

マニュアルの表記規則

Novell のマニュアルでは、「より大きい」記号 (>) を使用して手順内の操作と相互参照パス内の項目の順序を示します。

商標記号 (®、™ など) は、Novell の商標を示します。アスタリスク (*) は、サードパーティの商標を示します。

パス名の表記に円記号 (\) を使用するプラットフォームとスラッシュ (/) を使用するプラットフォームがありますが、このマニュアルでは円記号を使用します。Linux* または UNIX* などのようにスラッシュを使用するプラットフォームの場合は、必要に応じて円記号をスラッシュに置き換えてください。

1 Roles Based Provisioning Module インストール概要

このセクションでは、Roles Based Provisioning Module をインストールするステップの概要を説明します。主なトピックは次のとおりです。

ユーザアプリケーションまたは Roles Based Provisioning Module の以前のバージョンから移行する場合、『*ユーザアプリケーション : マイグレーションガイド* (http://www.novell.com/documentation/idmrbpm37/index.html)』を参照してください。

1.1 インストールのチェックリスト

Novell® Identity Manager Roles Based Provisioning Module をインストールするには、次のタスクを実行する必要があります。

- ❑ ソフトウェアがシステム要件を満たしているかどうかを確認します。詳細については、11 ページのセクション 1.3「システム要件」を参照してください。
- ❑ Identity Manager Roles Based Provisioning Module をダウンロードします。詳細については、17 ページのセクション 2.2「Roles Based Provisioning Module のダウンロード」を参照してください。
- ❑ 以下のサポートコンポーネントを設定します。
  - ❑ サポートされている Identity Manager のメタディレクトリがインストールされていることを確認します。詳細については、17 ページのセクション 2.1「Identity Manager メタディレクトリのインストール」を参照してください。
  - ❑ アプリケーションサーバをインストールおよび設定します。詳細については、19 ページのセクション 2.3「アプリケーションサーバのインストール」を参照してください。
  - ❑ データベースをインストールおよび設定します。詳細については、23 ページのセクション 2.4「データベースのインストール」を参照してください。
- ❑ Roles Based Provisioning Module Metadirectory コンポーネントをインストールします。詳細については、31 ページの第 3 章「Roles Based Provisioning Module をメタディレクトリにインストールします。」を参照してください。
- ❑ iManager または Designer for Identity Manager 3.5 でユーザアプリケーションドライバを作成します。
  - iManager の場合 : 45 ページのセクション 4.1「iManager でのユーザアプリケーションドライバの作成」
  - Designer の場合 : ユーザアプリケーション : 設計ガイド (http://www.novell.com/documentation/idmrbpm37/index.html)

- ❑ iManager または Designer for Identity Manager 3.5 で役割とリソースサービスドライバを作成します。
  - iManager の場合 : 47 ページのセクション 4.2「iManager での役割サービドライバおよびリソースサービスドライバの作成」
  - Designer の場合 : ユーザアプリケーション : 設計ガイド (http://www.novell.com/documentation/idmrbpm37)
- ❑ Novell Identity Manager ユーザアプリケーションをインストールし設定します。(インストールプログラムを開始する前に、正しい JDK* がインストールされている必要があります。詳細については、29 ページのセクション 2.5「Java Development Kit のインストール」を参照してください)。

  インストールプログラムは、次の 3 つのモードのいずれかで起動できます。
  - グラフィカルユーザインタフェース 以下のいずれかを参照してください。
    - 51 ページの第 5 章「JBoss でのユーザアプリケーションのインストール」
    - 67 ページの第 6 章「WebSphere でのユーザアプリケーションのインストール」
    - 85 ページの第 7 章「WebLogic でのユーザアプリケーションのインストール」
  - コンソール (コマンドライン) インタフェース詳細については、103 ページのセクション 8.1「コンソールからのユーザアプリケーションのインストール」を参照してください。
  - サイレントインストール。詳細については、104 ページのセクション 8.2「単一コマンドによるユーザアプリケーションのインストール」を参照してください。
- ❑ 115 ページの第 9 章「インストール後のタスク」で説明されているインストール後のタスクを実行します。

重要 : 本書では、セキュリティ環境の設定手順は説明していません。セキュリティの詳細については、『ユーザアプリケーション : 管理ガイド (http://www.novell.com/documentation/idmrbpm37/index.html)』を参照してください。

1.2 インストーラプログラムの概要

ユーザアプリケーションのインストールプログラムは次の処理を実行します。

- 使用する既存のバージョンのアプリケーションサーバを指定する。
- 使用する既存のバージョンのデータベースを指定する (MySQL*、Oracle*、DB2*、Microsoft* SQL Server*、または PostgreSQL* など)。データベースには、ユーザアプリケーションのデータとユーザアプリケーションの設定情報が保存されます。
- ユーザアプリケーション(アプリケーションサーバ上で実行されている)が識別ボールトおよびユーザアプリケーションドライバと安全に通信できるように、JDK の証明書ファイルを設定する。
- Novell Identity Manager ユーザアプリケーション用の Java* Web アプリケーションアーカイブ (WAR) ファイルを設定し、アプリケーションサーバに展開する。WebSphere* および WebLogic* では、WAR を手動で展開する必要があります。
- 必要な場合、Novell または OpenXDAS の監査クライアントを使用してログを有効にします。
- 既存のマスタキーをインポートして、特定の Roles Based Provisioning Module のインストールを復元し、クラスタをサポートできるようにします。

1.3 システム要件

Novell Identity Manager Roles Based Provisioning Module 3.7.0 を使用するには、表 1-1 に記述されている必要な各コンポーネントの 1 つが存在している必要があります。

表 1-1 *システム要件*

必須システムコンポーネント	システム要件
Identity Manager 3.6 および eDirectory	サポートされているオペレーティングシステムのリストは、Identity Manager および eDirectory のマニュアルを参照してください。
Identity Manager 3.6.1 および eDirectory	サポートされているオペレーティングシステムのリストは、Identity Manager および eDirectory のマニュアルを参照してください。
Web ベースの管理サーバ ◆ iManager 2.7 SP2 およびプラグイン	サポートされているオペレーティングシステムのリストは、iManager のマニュアルを参照してください。 次のプラグインは必須です。 ◆ iManager 2.7 用 Identity Manager 3.6.1b プラグイン ◆ iManager 2.7 用 Password Management 3.6.1b プラグイン
Audit Service ◆ Sentinel™ 6.1 ◆ Novell Identity Audit 1.0	サポートされているオペレーティングシステムのリストは、Sentinel または Novell Identity Audit のマニュアルを参照してください。

必須システムコンポーネント	システム要件
ユーザアプリケーションのアプリケーションサーバ	ユーザアプリケーションは、以下に説明するように JBoss*、WebSphere*、および WebLogic* 上で動作します。 JBoss 5.0.1 を持つユーザアプリケーションは Sun から提供されている JRE* 1.6.0-14 を必要とし、以下でサポートされます。 ◆ Windows 2003 Server (32 ビットおよび 64 ビット) ◆ Windows 2008 Server (32 ビットおよび 64 ビット) ◆ Novell Open Enterprise Server (OES) SP1 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 10 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 11 (32 ビットおよび 64 ビット) ◆ Red Hat Linux 5 (32 ビットおよび 64 ビット) ◆ Solaris 10 (32 ビットおよび 64 ビット) WebSphere 6.1 のユーザアプリケーションは IBM J9 VM (build 2.3, J2RE 1.5.0) を必要とします。これらのプラットフォームでサポートされています。 ◆ Windows 2003 Server (32 ビットおよび 64 ビット) ◆ Windows 2008 Server (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 10 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 11 (32 ビットおよび 64 ビット) ◆ Red Hat Linux 5 (32 ビットおよび 64 ビット) ◆ AIX 5.3 (64 ビット) (データベースとしてはOracle 10g asでのみサポートされています) ◆ Solaris 10 (32 ビットおよび 64 ビット) WebSphere 7.0 のユーザアプリケーションは IBM J9 VM (build 2.4, J2RE 1.6.0) を必要とします。これらのプラットフォームでサポートされています。 ◆ Windows 2003 Server (32 ビットおよび 64 ビット) ◆ Windows 2008 Server (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 10 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 11 (32 ビットおよび 64 ビット) ◆ Red Hat Linux 5 (32 ビットおよび 64 ビット) ◆ Solaris 10 (32 ビットおよび 64 ビット) WebLogic 10.3 のユーザアプリケーションは JRockit* JVM 1.6.0_05 を必要とし、次のプラットフォームでサポートされています。 ◆ Windows 2003 Server (32 ビットおよび 64 ビット) ◆ Windows 2008 Server (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 10 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 11 (32 ビットおよび 64 ビット) ◆ Red Hat Linux 5 (32 ビットおよび 64 ビット) ◆ Solaris 10 (32 ビットまたは 64 ビット) **注 :** ゲストオペレーティングシステムがユーザアプリケーションによってサポートされているものである限り、ユーザアプリケーションは仮想化である Xen および VMW がをサポートします。

必須システムコンポーネント	システム要件
ユーザアプリケーションのブラウザ	ユーザアプリケーションは、以下に説明するように Firefox* および Internet Explorer* の両方をサポートしています。 Firefox 3* は次でサポートされています。 ◆ Windows XP SP3 ◆ Windows Vista ◆ SUSE Linux Enterprise Desktop 11 ◆ Novell OpenSuSE 10 ◆ Novell OpenSuSE 11 ◆ Apple Mac Firefox* 2 (Version 2.0.0.20 のみ) は次でサポートされています。 ◆ Novell SUSE Linux Enterprise Desktop 10 ◆ Novell SUSE Linux Enterprise Server 10 ◆ Novell OpenSuSE 10 Internet Explorer 8 は次のプラットフォームでサポートされています。 ◆ Windows XP SP3 ◆ Windows Vista Internet Explorer 7 は次のプラットフォームでサポートされています。 ◆ Windows XP SP3

必須システムコンポーネント	システム要件
ユーザアプリケーション用のデータベースサーバ	JBoss では次のデータベースがサポートされています。 ◆ MS SQL 2005 ◆ MySQL バージョン 5.1 ◆ Oracle 10g ◆ Oracle 11g ◆ PostgreSQL 8.8.3 WebSphere 6.1 では次のデータベースがサポートされています。 ◆ DB2 9.5 ◆ MS SQL 2005 ◆ Oracle 10g ◆ Oracle 11g WebSphere 7.0 では次のデータベースがサポートされています。 ◆ DB2 9.5 ◆ MS SQL 2005 ◆ Oracle 10g ◆ Oracle 11g WebLogic 10.3 では次のデータベースがサポートされています。 ◆ MS SQL 2005 ◆ Oracle 10g ◆ Oracle 11g 次の JDBC ドライバがサポートされています。 MS SQL Server: sqljdbc_1.0 (sqljdbc.jar)、sqljdbc_1.1 (sqljdbc.jar)、sqljdbc_1.2 (sqljdbc.jar)、sqljdbc_2.0 (sqljdbc.jar および sqljdbc4.jar) WebLogic を持つ Oracle10g または Oracle11g : ojdbc6.jar (WebLogic で組み込み) Oracle シンドライバ : Oracle JDBC ドライババージョン 10.2.0.1.0 Oracle OCI ドライバ : Oracle JDBC ドライババージョン 10.2.0.2.0 MySQL: mysql-connector-java.jar v. 5.1.7 IBM DB2 9.5: DB2 JDBC Universal Driver Architecture 3.52.95 PostgreSQL: PostgreSQL8.1JBDC3
Designer	Designer 3.5
OpenXDAS	OpenXDAS バージョン 0.8.345 SLES10 には次の OpenXDAS バージョンが必要です。 ◆ openxdas-0.8.351-1.1.i586.rpm ◆ openxdas-0.8.351-1.1.x86_64.rpm

必須システムコンポーネント	システム要件
ユーザアプリケーションの SSO 統合	Novell Access Manager 3.1.1 または 3.1.1 IR1 Novell Secure Login 6.1
ドメインサービス	Windows 用 OES 2 SP1 ドメインサービス
パスワード管理確認回答	パスワード管理確認回答機能には、NMAS Challenge Response Login Method バージョン : 2770 ビルド : 20080603 以降が必要です。

前提条件

2

このセクションでは、Identity Manager Roles Based Provisioning Module (RBPM) をインストールする前にインストールまたは設定する必要があるソフトウェアおよびコンポーネントを説明します。主なトピックは次のとおりです。

2.1 Identity Manager メタディレクトリのインストール

Roles Based Provisioning Module 3.7 は、Identity Manager 3.6 または 3.6.1 のメタディレクトリと共に使用できます。

Identity Manager メタディレクトリのインストール手順については、『*Novell Identity Manager インストールガイド* (http://www.novell.com/documentation/idm36/)』を参照してください。

2.2 Roles Based Provisioning Module のダウンロード

Novell ダウンロード (http://download.novell.com/index.jsp) から、Identity Manager Roles Based Provisioning Module 3.7 製品を入手します。表 2-1 に示す製品の .iso イメージファイルをダウンロードします。

表 2-1 *.iso ダウンロードファイル*

本製品について	この .iso をダウンロード
ユーザアプリケーション	Identity_Manager_RBPM_3_7_0_User_Application.iso
メタディレクトリ用 Roles Based Provisioning Module コンポーネント	Identity_Manager_RBPM_3_7_0_Driver_Install_Utility.iso

表 2-2 では、ユーザアプリケーションおよび Roles Based Provisioning Module .iso ファイルに渡されるインストールファイルを説明しています。

表 2-2 ISO に渡されるファイルおよびスクリプト

ファイル	説明
IDMProv.war	Roles Based Provisioning Module WARIdentity Manager ユーザアプリケーションと、Identity セルフサービス、および役割ベースプロビジョニングモジュール機能が含まれています。
IDMUserApp.jar	ユーザアプリケーションのインストールプログラム。
silent.properties	サイレントインストールに必要なパラメータに含まれるファイルこれらのパラメータは、GUI またはコンソールインストール手順で設定するインストールパラメータに対応します。このファイルをコピーしてから、コンテンツを修正してインストール環境に適合させる必要があります。
JBossMySQL.bin または JBossMySQL.exe	JBoss アプリケーションサーバおよび MySQL データベースをインストールする便利なユーティリティ
nmassaml.zip	SAML をサポートするための eDirectory メソッドが含まれます。Access Manager を使用していない場合のみ必要となります。
rbpm_driver_install.exe	役割ベースプロビジョニングモジュール (役割およびリソースサービスドライバ、ユーザアプリケーションドライバ、および eDirectory スキーマ) のメタディレクトリコンポーネント用 Windows インストールプログラム
rbpm_driver_install_aix.bin	役割ベースプロビジョニングモジュール (役割およびリソースサービスドライバ、ユーザアプリケーションドライバ、および eDirectory スキーマ) のメタディレクトリコンポーネント用 AIX インストールプログラム
rbpm_driver_install_linux.bin	役割ベースプロビジョニングモジュール (役割およびリソースサービスドライバ、ユーザアプリケーションドライバ、および eDirectory スキーマ) のメタディレクトリコンポーネント用 Linux インストールプログラム
rbpm_driver_install_solaris.bin	役割ベースプロビジョニングモジュール (役割およびリソースサービスドライバ、ユーザアプリケーションドライバ、および eDirectory スキーマ) のメタディレクトリコンポーネント用 Solaris インストールプログラム

Identity Manager Roles Based Provisioning Module をインストールするシステムには、少なくとも 320MB の利用可能な保存領域とサポートするアプリケーション (データベース、アプリケーションサーバなど) に対するスペースを持つ必要があります。システムでは、時間の経過に伴って、データベースまたはアプリケーションサーバのログなど、その他のデータの増加を調整するための追加スペースが必要となります。

デフォルトのインストール場所は次のとおりです。

- Linux または Solaris: /opt/novell/idm
- Windows: C:\Novell\IDM

インストール時に別のデフォルトインストールディレクトリを選択することもできます。ただしその場合、ディレクトリがインストール開始以前に存在しており、書き込み可能になっている必要があります (さらに Linux または Solaris の場合は、非 root ユーザが書き込み可能である必要もあります)。

2.3 アプリケーションサーバのインストール

- 19 ページのセクション 2.3.1「JBoss アプリケーションサーバのインストール」
- 23 ページのセクション 2.3.2「WebLogic アプリケーションサーバのインストール」
- 23 ページのセクション 2.3.3「WebSphere アプリケーションサーバのインストール」

2.3.1 JBoss アプリケーションサーバのインストール

Boss アプリケーションサーバの使用を計画している場合、以下のいずれかを実行できます。

- 製造元の指示に従って、JBoss アプリケーションサーバをダウンロードしてインストールします。サポートされているバージョンについては、11 ページのセクション 1.3「システム要件」を参照してください。
- Roles Based Provisioning Module のダウンロードに含まれる JBossMySQL ユーティリティを使用して、JBoss アプリケーションサーバ (およびオプションで MySQL) をインストールします。手順については、20 ページの 「JBoss アプリケーションサーバと MySQL データベースのインストール」を参照してください。

Identity Manager Roles Based Provisioning Module をインストールするまで JBoss サーバを起動しないでください。JBoss サーバの起動はインストール後のタスクです。

表 2-3 *JBoss アプリケーションサーバの最少推奨要件*

コンポーネント	推奨
RAM	Identity Manager Roles Based Provisioning Module を実行する場合、JBoss アプリケーションサーバの最少推奨 RAM は 512MB です。
ポート	8080 は、アプリケーションサーバのデフォルトです。アプリケーションサーバが使用するポートを記録します。
SSL	外部のパスワード管理を使用する予定がある場合、SSL を有効にします。 • Identity Manager Roles Based Provisioning Module および IDMPwdMgt.war ファイルを展開する JBoss サーバの SSL を有効にします。 • SSL ポートがファイアウォール上で開いていることを確認します。 SSL の有効化の詳細については、JBoss の文書を参照してください。 IDMPwdMgt.war ファイルの詳細については、118 ページのセクション 9.5「外部パスワードを忘れた場合の管理の環境設定」を参照してください。また、『*ユーザアプリケーション : 管理ガイド* (http://www.novell.com/documentation/idmrbpm37/index.html)』も参照してください。

JBoss アプリケーションサーバと MySQL データベースのインストール

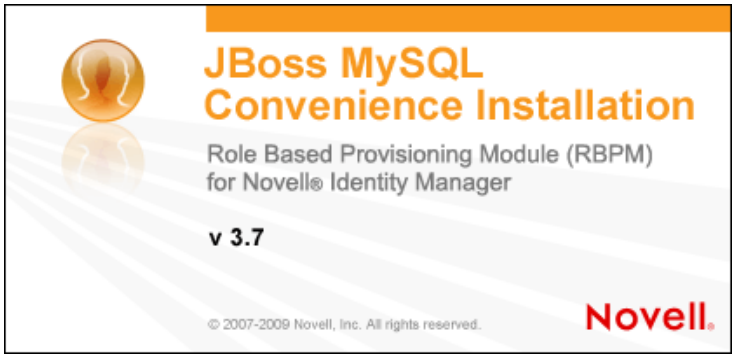
JBossMySQL ユーティリティは JBoss アプリケーションサーバおよび MySQL をシステムにインストールします。このユーティリティではコンソールモードがサポートされていません。グラフィカルユーザインタフェースが必要とされます。Linux/Unix ユーザの場合、これをルート以外のユーザとしてインストールことをお勧めします。

1 JBossMySQL.bin または JBossMySQL.exe を .iso から検索して実行します。

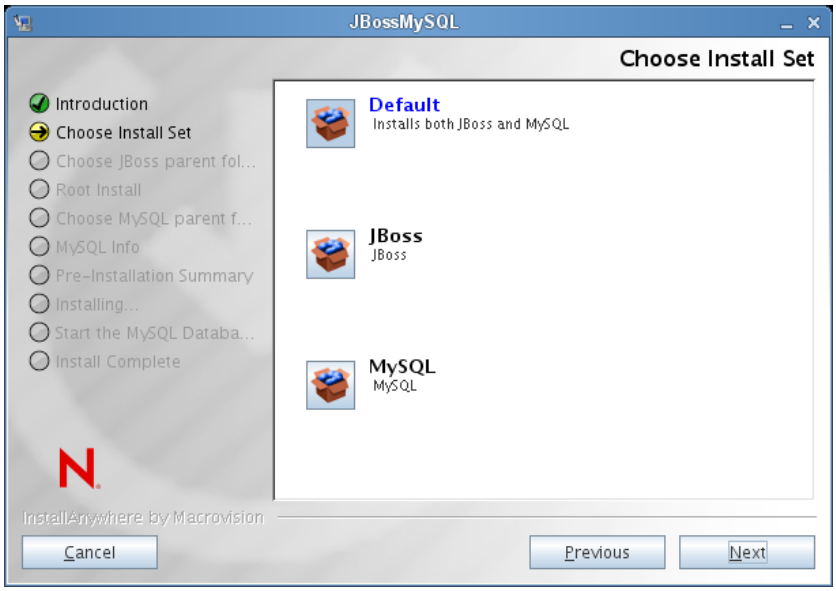
/linux/jboss/JBossMySQL.bin (Linux の場合)
/nt/jboss/JBossMySQL.exe (Windows の場合)

Solaris 用のユーティリティは利用できません。

JBossMySQL ユーティリティでは、スプラッシュスクリーンが表示されます。

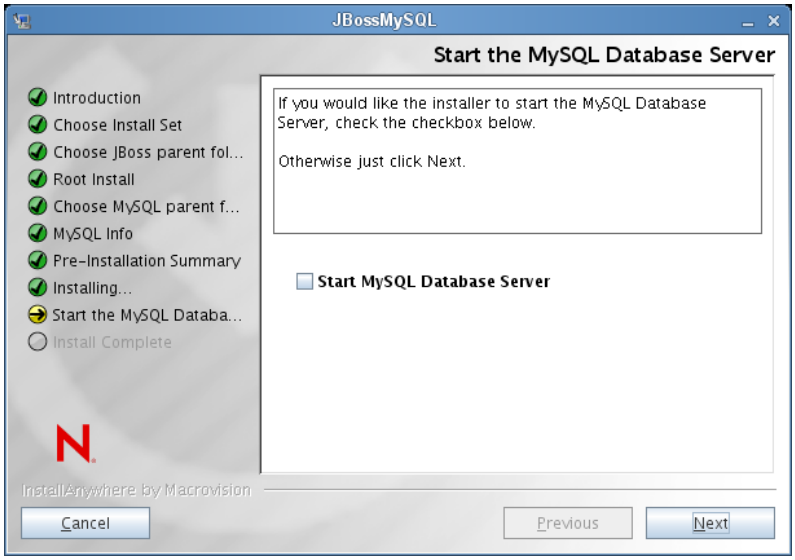


その後、このユーティリティでは *[インストールセットの選択]* 画面が次のように表示されます。



2 画面の指示に従ってユーティティをナビゲートします。追加の情報については、以下の表を参照してください。

インストール画面	説明
インストールセットの選択	インストールする製品を選択します。 ◆ *デフォルト*: 指定したディレクトリに JBoss および MySQL の両方を、それを起動および停止するスクリプトとともに、インストールします。 ◆ *JBoss*: 指定するディレクトリに、起動と停止を行うスクリプトと共に JBoss アプリケーションサーバをインストールします。 **注 :** このユーティリティでは、JBoss アプリケーションサーバは Windows サービスとしてインストールされません。手順については、22 ページの 「JBoss アプリケーションサーバのサーバデーモンとしてのインストール」を参照してください。 ◆ *MySQL*: 指定するディレクトリに、起動と停止を行うスクリプトと一緒に MySQL をインストールし、MySQL データベースを作成します。
JBoss 親フォルダの選択	[*選択*] をクリックし、デフォルト以外のインストールフォルダを選択します。
MySQL 親フォルダの選択	[*選択*] をクリックし、デフォルト以外のインストールフォルダを選択します。
MySQL 情報	以下の内容を指定します。 ◆ *データベース名*: 作成するインストーラのデータベース名を指定します。ユーザアプリケーションインストールユーティリティによりこの名前を入力するようメッセージが表示されるので、名前と場所を書き留めます。 ◆ *「ルート」ユーザパスワード* (および確認パスワード): このデータベースに対してルートパスワードを指定します (また、ルートパスワードを確認します)。
インストール前の概要	概要ページを確認します。仕様が正しい場合、[*インストール*] をクリックします。

インストール画面	説明
MySQL Database サーバを起動します。	MySQL データベースをインストールする場合、このユーティリティはデータベースサーバを起動するように促します。  ユーザアプリケーションのインストールを開始する前に、データベースサーバを起動する必要があります。ユーザアプリケーションをすぐにインストールする場合、*[MySQL データベースサーバの起動]* を選択し、*[次へ]* をクリックします。 MySQL データベースをインストールする場合、24 ページのセクション 2.4.1「MySQL データベース設定上の注意事項」に記述されているとおりデータベースを設定する必要もあります。
インストールの完了	選択した製品がインストールされると、ユーティリティでは正常に完了したことを示す次のメッセージが表示されます。 `The Installer has completed successfully.  Thank you for choosing Novell` **重要 :** JBossMySQL ユーティリティが JMX コンソールまたは JBoss Web コンソールを保護しないことに注意する必要があります。これにより、JBoss 環境は無防備なままになります。セキュリティ上の危険を排除するために、インストールを完了し時点で直ちに環境をロックダウンする必要があります。

JBoss アプリケーションサーバのサーバデーモンとしてのインストール

JBoss アプリケーションをデーモンとして起動するには、JBoss (http://www.jboss.org/community/wiki/StartJBossOnBootWithLinux) からの手順を参照してください。

JavaServiceWrapper の使用 JavaServiceWrapper を使用して、JBoss アプリケーションサーバを Windows サービス、Linux、または UNIX のデーモンプロセスとしてインストール、開始、および停止することができます。http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows (http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows) で JBoss からの指示を参照してください。このような

ラッパの 1 つは、http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html) にあります。これは、JMX (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss) を参照) で管理します。

重要 : 以前のバージョンの場合、JavaService などのサードパーティのユーティリティを使用して、Windows サービスとして JBoss アプリケーションサーバをインストール、開始、および停止することができましたが、現在 JBoss では JavaService を使用することは推奨していません。詳細については、http://www.jboss.org/wiki/JavaService (http://www.jboss.org/community/wiki/JavaService) を参照してください。

2.3.2 WebLogic アプリケーションサーバのインストール

WebLogic アプリケーションサーバの使用を計画している場合、これをダウンロードおよびインストールします。サポートされているバージョンの情報については、11 ページのセクション 1.3「システム要件」を参照してください。

2.3.3 WebSphere アプリケーションサーバのインストール

WebSphere アプリケーションサーバの使用を予定している場合、これをダウンロードおよびインストールします。サポートされているバージョンの情報については、11 ページのセクション 1.3「システム要件」を参照してください。

DB2 設定の注意事項については、27 ページの 「DB2 データベース設定の注意事項」を参照してください。

2.4 データベースのインストール

ユーザアプリケーションは、環境設定データの保存や、ワークフローアクティビティのデータの保存など、さまざまなタスクにデータベースを使用します。Roles Based Provisioning Module およびユーザアプリケーションをインストールする前に、インストールして設定されているプラットフォームに対してサポートされているデータベースが 1 つ存在する必要があります。以下のような機能があります。

- データベースおよびデータベースドライバのインストール
- データベースまたはデータベースインスタンスの作成
- ユーザアプリケーションのインストール手順で使用する次のデータベースパラメータを記録する
  - ホストおよびポート
  - データベース名、ユーザ名、およびユーザパスワード
- データベースをポイントするデータソースファイルの作成

  方法はアプリケーションサーバに応じて変わります。JBoss の場合は、ユーザアプリケーションインストールプログラムが、データベースを指すアプリケーションサーバのデータソースファイルを作成し、Identity Manager Roles Based Provisioning Module WAR ファイルの名前に基づいてファイルに名前を付けます。WebSphere および WebLogic の場合は、インストール前に手動でデータソースを設定します。

- ❑ データベースで Unicode エンコードが有効である必要があります。

  ユーザアプリケーションには、Unicode エンコード方式を使用するデータベース文字セットが必要です。たとえば、UTF-8 は Unicode エンコード方式を使用する文字セットですが、Latin1 は Unicode エンコード方式を使用しません。ユーザアプリケーションをインストールする前に、データベースが Unicode エンコード方式がある文字セットで設定されていることを確認してください。

注 : 新しいバージョンの Roles Based Provisioning Module へマイグレートする場合は、古いインストール (マイグレート元のインストール) で使用していたものと同じユーザアプリケーションデータベースを使用する必要があります。

2.4.1 MySQL データベース設定上の注意事項

ユーザアプリケーションは MySQL の特定の設定オプションを必要とします。MySQL をインストールする場合、これらの設定を行います。JBossMySQL ユーティリティを使用して MySQL をインストールすると、ユーティリティによって正しい値が設定されますが、以下を維持するための値は把握しておく必要があります。

- 24 ページの 「INNODB ストレージエンジンとテーブルタイプ」
- 24 ページの 「文字セット」
- 25 ページの 「大文字と小文字の区別」
- 25 ページの 「Ansi 設定」
- 26 ページの 「ユーザアカウント要件」

INNODB ストレージエンジンとテーブルタイプ

ユーザアプリケーションは INNODB ストレージエンジンを使用します。これにより、MySQL の INNODB テーブルタイプを選択できます。テーブルタイプを指定せずに MySQL テーブルを作成した場合、テーブルはデフォルトで MyISAM テーブルタイプを受け付けます。Identity Manager のインストール手順に従って MySQL をインストールした場合は、この手順で発行される MySQL は、INNODB テーブルタイプが指定された状態で付属します。MySQL サーバが確実に INNODB を使用するようにするには、my.cnf (Linux または Solaris の場合) または my.ini (Windows の場合) に次のオプションが含まれていることを確認します。

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

このファイルには skip-innodb オプションが含まれていてはなりません。

データベースの SQL スクリプトの Create Table 文に default-table-type=innodb オプションを設定する代わりとして ENGINE=InnoDB オプションを付加できます。

文字セット

サーバ全体またはデータベースのみに対し、文字セットとして UTF-8 を指定します。サーバ全体に UTF-8 を指定するには、my.cnf (Linux または Solaris) または my.ini (Windows) に以下のオプションを含めます。

```
character_set_server=utf8
```

次のコマンドを使用して、データベースの作成時にデータベースの文字セットを指定することもできます。

create database databasename character set utf8 collate utf8_bin;

データベースに文字セットを指定した場合、以下の例のように、IDM-ds.xml ファイルの JDBC* URL にも文字セットを指定する必要があります。

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

大文字と小文字の区別

サーバまたはプラットフォーム全体でデータをバックアップおよびリストアする計画の場合は、大文字と小文字の区別がサーバまたはプラットフォーム全体で統一されていることを確認します。統一されているかどうかを確認するには、デフォルトをそのまま使用するのではなく (Windows ではデフォルトで 0 に、Linux ではデフォルトで 1 に設定されます)、すべての my.cnf ファイル (Linux または Solaris の場合) または my.ini ファイル (Windows の場合) の lower_case_table_names に同じ値 (0 または 1) を指定します。データベースを作成して Identity Manager のテーブルを作成する前に、この値を指定します。たとえば、次のように指定します。

lower_case_table_names=1

これは、データベースのバックアップおよびリストアを計画しているすべてのプラットフォームの my.cnf および my.ini ファイルに指定します。

Ansi 設定

MySQL 5.1 に対して独自のインストールプログラムを使用する場合、my.cnf (Linux の場合) または my.ini ファイル (Windows の場合) に ansi エントリを追加する必要があります。このエントリを追加しないと、RBPM テーブルは作成されますがテーブルの初期データロードが実行されず、“ ゲストコンテナページの定義が見つかりません ” というエラーメッセージが表示されます。

ansi エントリの追加後に、my.cnf (または my.ini) ファイルがどのように見えるかここで示します。

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

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

ansi モードを使用する変更が有効になったことを確認するには、MySQL サーバで次の SQL を実行します。

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

ユーザアカウント要件

インストールプロセス時に使用するユーザアカウントはユーザアプリケーションによって使用されるデータベース (の所有者となる) への完全なアクセス権を持っている必要があります。また、このアカウントではシステムのテーブルのへのアクセスが必要です。環境に応じてテーブルは異なります。

MySQL サーバにログインするユーザを作成し、そのユーザに権限を与えます。たとえば次のようにします。

GRANT ALL PRIVILEGES ON <dbname.>* TO <username>@ <host> IDENTIFIED BY ‘ password’

最小の権限のセットは、CREATE、INDEX、INSERT、UPDATE、DELETE、および LOCK TABLES です。GRANT コマンドのマニュアルについては、http://www.mysql.org/doc/refman/5.0/en/grant.html (http://www.mysql.org/doc/refman/5.0/en/grant.html) を参照してください。

重要 : ユーザアカウントは mysql.user テーブルへの選択権を持つ必要があります。ここに、適切な権利を付与するために必要な SQL 構文を示します。

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

2.4.2 Oracle データベース設定上の注意事項

Oracle データベースを作成する場合、必ず AL32UTF8 を使用して Unicode エンコードの文字セットを指定する必要があります。(AL32UTF8 (http://download-east.oracle.com/docs/cd/B19306_01/server.102/b14225/glossary.htm#sthref2039) を参照してください)。

Oracle データベースのユーザを作成する場合、SQL Plus ユーティリティを使用して次の文を発行する必要があります。これらのステートメントにより、ユーザが作成され、ユーザの権限が設定されます。ユーザに CONNECT および RESOURCE 権限を与えます。次を参照してください。

CREATE USER *idmuser* IDENTIFIED BY *password*

GRANT CONNECT, RESOURCE to *idmuser*

Oracle 11g の場合の UTF-8 Oracle 11g の場合、UTF-8 が有効であることを確認するには次のコマンドを発行します。

```
select * from nls_database_parameters;
```

UTF-8 が設定されていない場合、このデータが返されます。

```
NLS_CHARACTERSET
WE8MSWIN1252
```

UTF-8 が設定されている場合、このデータが返されます。

```
NLS_CHARACTERSET
AL32UTF8
```

2.4.3 MS SQL サーバデータベース設定の注意事項

MS SQL サーバデータベースを次のように設定します。

1. MS SQL Server をインストールします。
2. サーバに接続し、データベースとデータベースユーザを作成するアプリケーションを開きます (通常は、SQL Server Management Studio アプリケーション)。
3. データベースを作成します。SQL Server では、データベースの文字セットの選択はできません。IDM ユーザアプリケーションは SQL サーバの文字データを NCHAR カラムタイプ (UTF-8 をサポート) で保存します。
4. ログインを作成します。
5. ログインをデータベースのユーザとして追加します。
6. ログインに次の権限を与えます。CREATE TABLE、CREATE INDEX、SELECT、INSERT、UPDATE、および DELETE。

ユーザアプリケーションには、Microsoft SQL Server 2005 JDBC ドライバのバージョン 1.0.809.102 が必要です。Sun Solaris、Red Hat Linux、および Windows 2000 以降のオペレーティングシステムのみが、この JDBC ドライバで公式にサポートされています。

2.4.4 DB2 データベース設定の注意事項

このセクションでは、DB2 設定についての注意事項について説明します。

データベースドライバ JAR の準備

データベースドライバ JAR ファイルは、*[データベースユーザ名およびパスワード]* 画面でインストールプロセス時に選択する必要があります。ただし、*[データベースドライバ JAR ファイル]* フィールドのブラウズボタンによってのみ、1 つの jar を選択できます。DB2 の場合、2 つの jar を指定する必要があります。

- db2jcc.jar
- db2jcc_license_cu.jar

したがって、WebSphere (DB2 でサポートされる唯一のアプリケーションサーバ) に対してインストールプログラムを実行する場合、1 つの jar を選択できますが、インストールプログラムが実行中のオペレーティングシステムの正しいファイル区切り文字を使用して 2 番目のものを手動で入力する必要があります。または、両方のエントリを手動で入力することもできます。

Windows の場合の例 :

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

Solaris および Linux の場合の例 :

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

デッドロックおよびタイムアウトを防ぐための DB2 データベースの調整

DB2 を使用する際、「デッドロックまたはタイムアウトにより、現在のトランザクションがロールバックされました」という内容のエラーが発生した場合、高いレベルでのユーザおよびデータベースの同時並行性によって問題が発生している可能性があります。

DB2 は、コストベースのオプティマイザの調整を含む、ロック競合を解決するための多くの技術を提供しています。DB2 管理マニュアルに含まれている『*パフォーマンスガイド*』は、調整に関する多くの情報が記載されている優れたソースです。

同時並行性のレベルおよびデータのサイズは異なるため、すべてのインストールに対して使用できる、事前に設定された調整値はありません。ただし、インストールに関連する DB2 調整ヒントはいくつかあります。

- reorgchk update statistics コマンドは、オプティマイザによって使用される統計を更新します。これらの統計の周期的な更新により問題を緩和できます。
- DB2 レジストリパラメータ DB2_RR_TO_RS を使用すると、挿入または更新された行の次のキーをロックしないことによって、同時並行性が向上します。
- データベースの MAXLOCKS パラメータおよび LOCKLIST パラメータを増加します。
- データベース接続プールの currentLockTimeout プロパティを増加します。
- Database Configuration Advisor を使用して、トランザクションの速度を上げるために最適化します。
- すべてのユーザアプリケーションテーブルを VOLATILE に変更して、テーブルの重要性が大幅に異なることをオプティマイザに示します。たとえば、AFACTIVITY テーブルを VOLATILE にするには、ALTER TABLE AFACTIVITY VOLATILE のコマンドを発行します。

  ALTER TABLE コマンドは、ユーザアプリケーションが一度開始されてデータベーステーブルが作成された後で実行する必要があります。このステートメントの詳細については、ALTER TABLE マニュアルを参照してください。すべてのユーザアプリケーションテーブルに対する SQL ステートメントを示します。

```
ALTER TABLE AFACTIVITY VOLATILE
ALTER TABLE AFACTIVITYTIMERTASKS VOLATILE
ALTER TABLE AFBRANCH VOLATILE
ALTER TABLE AFCOMMENT VOLATILE
ALTER TABLE AFDOCUMENT VOLATILE
ALTER TABLE AFENGINE VOLATILE
ALTER TABLE AFENGINESTATE VOLATILE
ALTER TABLE AFMODEL VOLATILE
ALTER TABLE AFPROCESS VOLATILE
ALTER TABLE AFPROVISIONINGSTATUS VOLATILE
ALTER TABLE AFQUORUM VOLATILE
ALTER TABLE AFRESOURCEREQUESTINFO VOLATILE
ALTER TABLE AFWORKTASK VOLATILE
ALTER TABLE AF_ROLE_REQUEST_STATUS VOLATILE
ALTER TABLE ATTESTATION_ATTESTER VOLATILE
ALTER TABLE ATTESTATION_ATTRIBUTE VOLATILE
ALTER TABLE ATTESTATION_QUESTION VOLATILE
ALTER TABLE ATTESTATION_REPORT VOLATILE
ALTER TABLE ATTESTATION_REQUEST VOLATILE
ALTER TABLE ATTESTATION_RESPONSE VOLATILE
ALTER TABLE ATTESTATION_SURVEY_QUESTION VOLATILE
ALTER TABLE ATTESTATION_TARGET VOLATILE
ALTER TABLE AUTHPROPS VOLATILE
ALTER TABLE DATABASECHANGELOG VOLATILE
ALTER TABLE DATABASECHANGELOGLOCK VOLATILE
ALTER TABLE DSS_APPLET_BROWSER_TYPES VOLATILE
ALTER TABLE DSS_APPLET_CFG VOLATILE
ALTER TABLE DSS_APPLET_CFG_MAP VOLATILE
ALTER TABLE DSS_BROWSER_TYPE VOLATILE
```

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

2.5 Java Development Kit のインストール

ユーザアプリケーションインストールプログラムでは、アプリケーションサーバに対応する正しいバージョンの Java 環境を使用することが必要です。

- JBoss 5.01 の場合、Sun から提供されている Java 2 Platform Standard Edition Development バージョン 1.6 (JDK または JRE) を使用する必要があります。

  注 : JBossMySQL ユーティリティは、JBoss に対する正しいバージョンの JRE をインストールします。

- WebSphere 6.1 の場合、IBM から提供されている 1.5 JDK を使用する必要があります。
- WebSphere 7.0 の場合、IBM から提供されている 1.6 JDK を使用する必要があります。
- WebSphere 10.3 の場合、JRockit から提供されている 1.6 JDK を使用する必要があります。

ユーザアプリケーションで使用するために、JAVA_HOME 環境変数を JDK* を指すように設定します。または、ユーザアプリケーションのインストール時に手動でパスを指定して、JAVA_HOME を上書きします。

注 : SUSE Linux Enterprise Server (SLES) ユーザの場合 : SLES に搭載された IBM* JDK は使用しないでください。このバージョンは、インストールの一部の機能との互換性がありません。

3 Roles Based Provisioning Module をメタディレクトリにインストールします。

このセクションでは、Roles Based Provisioning Module (RBPM) のメタディレクトリコンポーネントを Identity Manager にインストールする方法について説明します。主なトピックは次のとおりです。

重要 : このセクションで記述されている手順は、以前のバージョンの Identity Manager (Identity Manager 3.6 または 3.6.1 など) に Roles Based Provisioning Module をインストールする場合に必要です。Identity Manager 3.7 は、自動的に RBPM の基本コンポーネントをインストールします。

3.1 Roles Based Provisioning Module のインストールについて

Identity Manager の Roles Based Provisioning Manager (RBPM) インストールプログラムは複数のコンポーネントを Identity Manager のメタディレクトリにインストールします。これらコンポーネントには次の品目が含まれます。

- 役割ドライバおよびリソースドライバ
- ユーザアプリケーションドライバ
- eDirectory スキーマ

RBPM インストールプログラムは Identity Manager メタディレクトリ環境がインストールされているマシン上で実行する必要があります。

これらの品目が Identity Manager にインストールされると、ユーザアプリケーションを実行するために必要なドライバを作成するために、45 ページの第 4 章「ドライバの作成」で説明されている手順に従う必要があります。

重要 : 以前のバージョンの RBPM で作成された eDirectory ツリーにユーザアプリケーションドライバがある場合、Roles Based Provisioning Module インストールプログラムを実行する前に NrfCaseUpdate ユーティリティを実行する必要があります。実行しないと、インストールが失敗します。

3.2 NrfCaseUpdate ユーティリティの実行

このセクションでは、NrfCaseUpdate ユーティリティの詳細について説明します。主なトピックは次のとおりです。

3.2.1 NrfCaseUpdate の概要

役割とリソースで大文字と小文字が混在する検索をサポートするには、NrfCaseUpdate プロシージャが必要です。このプロシージャは nrfLocalizedDescs および nrfLocalizedNames 属性 (ユーザアプリケーションで使用される) を変更することによってスキーマを更新します。このプロシージャは、RBPM 3.7 のインストール前と Designer 3.5 の既存のドライバを移行する前に、必要です。

3.2.2 インストールの概要

このセクションでは、既存の RBPM 環境を更新し移行するための手順の概要を説明します。この概要は、すべての更新を開始する前にユーザアプリケーションドライバのバックアップを作成する Designer 3.5 の使用法に重点を置きます。この概要は、IDM のバージョンが 3.6 以降であることを前提としています。

1. Designer 3.5 のインストール
2. 識別ボールトのヘルスチェックを実行し、スキーマが適切に拡張されていることを確認します。TID 3564075 を使用してヘルスチェックを完了します。
3. 既存のユーザアプリケーションドライバを Designer 3.5 にインポートします。
4. Designer プロジェクトをアーカイブします。これは RBPM 3.7 以前のドライバの状態を表します。
5. NrfCaseUpdate プロセスを実行します。
6. 新しい Designer 3.5 プロジェクトを作成し、移行に備えてユーザアプリケーションドライバをインポートします。
7. RBPM 3.7 をインストールします。
8. Designer 3.5 を使用してドライバを移行します。
9. 移行したドライバを展開します。

3.2.3 NrfCaseUpdate のスキーマへの影響

NrfCaseUpdate ユーティリティは eDirectory の既存の属性を更新し、これらの属性の既存インスタンスは実質的にすべて削除されます。ユーザアプリケーションはこれらの属性を使用しており、したがってこのスキーマ更新により影響を受けます。特に、役割と権限の分割名と説明、カスタムの構成証明要求、およびレポートなどです。

NrfCaseUpdate プロシージャは、スキーマ更新を実行する前に、既存のユーザアプリケーションドライバを LDIF ファイルにエクスポートするユーティリティを指定することによって、ユーザアプリケーションドライバを更新します。スキーマ更新後に LDIF ファイルをインポートすると、スキーマ更新時に削除されたすべてのオブジェクトは実質的に再作成されます。

既存のユーザアプリケーションドライバを予防措置として必ずバックアップすることは重要です。スキーマ更新は IDM パーティションに影響を与えることを覚えておいてください。したがってユーザアプリケーションドライバをそのツリーにエクスポートするために NrfCaseUpdate を使用することは大変重要です。

3.2.4 ユーザアプリケーションドライバのバックアップの作成

ユーザアプリケーションドライバのバックアップを作成する場合、Designer を使用することをお奨めします。NrfCaseUpdate プロシージャを実行する前に、次の手順に従ってユーザアプリケーションドライバをバックアップしてください。

1. Designer 3.5 をインストールします。これは RBPM 3.7 に同梱されています。
2. 識別ボールトを作成し、それをユーザアプリケーションドライバを含む IDM ドライバにマップします。
3. *[ライブ] > [インポート]* コマンドの順に使用して、ドライバセットとユーザアプリケーションドライバをインポートします。
4. この Designer プロジェクトを保存しアーカイブします。

3.2.5 NrfCaseUpdate の使用

NrfCaseUpdate はドライバをエクスポートするように促してから、スキーマ更新を実行します。既存のユーザアプリケーションドライバの存在または場所について不明確な場合、スキーマ更新がユーザアプリケーションドライバを無効にする可能性があるので、続行しないでください。

IDM インストールディレクトリ (通常 /root/idm/jre) の下に表示される JRE は、NrfCaseUpdate を実行するために使用されます。eDirectory への SSL 接続が必要な場合、36 ページのセクション 3.2.7「SSL 接続の JRE の有効化」の指示に従って SSL 接続の JRE を有効にする必要があります。

あるいは、eDirectory 証明書を含む JRE を持つホスト (ユーザアプリケーションサーバホストなど) からリモートで NrfCaseUpdate ユーティリティを実行することもできます。この場合、すべてのドライバを LDIF にエクスポートした後でスキーマ更新の前に、<CTRL>+<C> を使用して NrfCaseUpdate ユーティリティを終了する必要があります。次に、ndssch コマンドを使用して、次に示すように eDirectory ホストのスキーマを手動で更新します。

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

注 : NrfCaseUpdate はコマンドラインに複数の引数を受け入れることができます。Pass -help or -? を参照してください。

NrfCaseUpdate を実行するには、次の手順に従います。

1. NrfCaseUpdate ユーティリティを実行する前に、識別ボールトのヘルスチェックが完了していることを確認します。TID 3564075 を使用してヘルスチェックを完了します。
2. このユーティリティを起動する前に、既存のユーザアプリケーションドライバのすべての DN を識別します。これらのドライバを LDIF にエクスポートするためには認証資格情報が必要です。
3. NrfCaseUpdate ユーティリティを実行します。必要に応じて -v オプションを渡して、より詳細な出力を取得するすることもできます。

   ```
   /root/idm/jre/bin/java -jar NrfCaseUpdate.jar -v
   ```
4. 既存のユーザアプリケーションドライバを持っているかどうか聞かれます。既存のユーザアプリケーションドライバを持っている場合は、［True］と答えます。そうでなければ、［False］と答えて 34 ページのステップ 6 にスキップします。

   ```
   Do you currently have a User Application Driver configured [DEFAULT true]
   :
   ```
5. 次に、ユーティリティによってユーザアプリケーションドライバを複数持っているかどうか聞かれます。複数のユーザアプリケーションドライバを持っている場合は、［True］と答えます。

   ```
   Do you currently have more than one (1) User Application Driver configured
   [DEFAULT false] :
   ```
6. ユーザアプリケーションドライバをエクスポートする適切な資格情報を持つ管理者の DN を指定します。

   ```
   Specify the DN of the Identity Vault administrator user.
   This user must have inherited supervisor rights to the user application
   driver specified above.
   (e.g. cn=admin,o=acme):
   ```
7. この管理者のパスワードを入力します。

   ```
   Specify the Identity Vault administrator password:
   ```
8. ユーザアプリケーションドライバをホストする IDM サーバのホスト名または IP アドレスを入力します。

   ```
   Specify the DNS address of the Identity Vault (e.g acme.com):
   ```
9. 接続に使用するポートを指定します。

   ```
   Specify the Identity Vault port [DEFAULT 389]:
   ```
10. 次の質問では、接続に SSL を使用するかどうかを聞かれます。SSL を使用する場合、JRE はトラステッドストアに存在するための eDirectory 証明書が必要です。証明書を保持するには、36 ページのセクション 3.2.7「SSL 接続の JRE の有効化」の指示に従ってください。

    ```
    Use SSL to connect to Identity Vault: [DEFAULT false] :
    ```
11. エクスポートするユーザアプリケーションドライバの完全修飾識別名を指定します。

    ```
    Specify the fully qualified LDAP DN of the User Application driver located
    in the Identity Vault
    (e.g. cn=UserApplication,cn=driverset,o=acme):
    ```
12. ユーザアプリケーションをエクスポートする LDIF ファイルの名前を指定します。

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

13 ユーティリティは LDIF に保存されるオブジェクトについての情報をポストします。

14 複数ドライバを持っていることを示した場合、次のプロンプトが表示されます。

```
You indicated you have more than one (1) User Application Driver to
configure.
Do you have another driver to export? [DEFAULT false] :

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

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

15 通常の場所が表示されるとともに、ndssch ユーティリティの場所の入力を促されます。ndssch ユーティリティはスキーマの更新に使用されます。

```
Please enter the path to the schema utility:
For Unix/Linux typically /opt/novell/eDirectory/bin/ndssch
For Windows C:\Novell\NDS\schemaStart.bat:
```

16 このユーティリティは、次のようなスキーマ更新のステータスメッセージをポストします。

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

注 : eDirectory がスキーマの変更と同期する時間を十分に確保します。十分な時間を与えないと、LDIF ファイルのインポートが失敗します。

---

17 識別ボールト上で別のヘルスチェックを実行し、LDIF ファイルのインポート前にスキーマが適切に拡張されていることを確認します。TID 3564075 を使用してヘルスチェックを完了します。

18 すべてのドライバがエクスポートされスキーマ更新が正常に適用された後に、LDIF ファイルをインポートする必要があります。ice コマンドで前方参照を許可することを指示してください。推奨されるコマンドラインは次のとおりです。

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

19 すべてのドライバがインポートし直された後で、NrfCaseUpdate プロセスが正常であったことを確認します。詳細については、35 ページのセクション 3.2.6 「NrfCaseUpdate プロセスの確認」を参照してください。

20 NrfCaseUpdate プロセスが正常であったことを確認した後に、RBPM 3.7 インストールを続行します。

3.2.6 NrfCaseUpdate プロセスの確認

すべてのドライバがインポートし直された後で、ユーザアプリケーションで次の項目を調べることによって、復元が成功したことを確認します。

- 役割名と説明
- 権限の分割名と説明
- カスタム要求を含む、構成証明要求
- レポート機能

確認が完了した後、RBPM 3.7 のインストールを続行し更新できます。

3.2.7 SSL 接続の JRE の有効化

このセクションでは、SSL 接続を使用するために JRE を設定する方法について説明します。

まず、識別ボールトの認証局から自己署名証明書をエクスポートします。

1. iManager から、*［役割とタスク］* ビューで、*［ディレクトリ管理］* > *［オブジェクトの変更］* の順にクリックします。
2. 識別ボールトの認証局オブジェクトを選択してから、*［OK］* をクリックします。これは通常セキュリティコンテナにあり、*TREENAME* CA.Security と名付けられます。
3. *［証明書］* > *［自己署名証明書］* をクリックします。
4. *［エクスポート］* をクリックします。
5. 証明書とともに秘密鍵をエクスポートするかどうか聞かれた場合、*［いいえ］* をクリックしてから、*［次へ］* をクリックします。
6. バイナリの DER フォーマットを選択します。
7. リンク *［エクスポートした証明書の保存］* をクリックします。
8. ファイルを保存するコンピュータの場所をブラウズして *［保存］* をクリックします。
9. *［閉じる］* をクリックします。

次に、自己署名証明書を JRE のトラステッドストアにインポートします。

1. JRE に含まれている keytool ユーティリティを使用します。
2. コマンドプロンプトで次のコマンドを入力することにより役割マッピング管理者の認証ストアに証明書をインポートします。

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

   次に例を示します。

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

3.2.8 無効にされたユーザアプリケーションドライバの復元

NrfCaseUpdate を使用してドライバが処理される前にスキーマ更新が既存のユーザアプリケーションドライバに適用された場合、これは無効にされ、バックアップを使用してそのドライバを復元する必要があります。

重要 : 無効にされたユーザアプリケーションドライバを削除または名前変更 *しない* ことが重要です。そうした場合、すべてのドライバの関連付けが無効になるためです。また、役割およびリソースサービスドライバが実行中で、ユーザアプリケーションドライバを削除した場合、役割およびリソースサービスドライバは役割の削除を検出し、割り当てられたユーザからその役割を削除します。

また、このスキーマの変更この方法で元に戻せないなので、バックアップされているドライバを IDM に展開し直すことは十分ではありません。次のプロシージャは、復元するデータを生成するために、名前変更されたドライバのコピーを展開することによって復元を実行します。

次のプロシージャは Designer 3.5 を使用してユーザアプリケーションドライババックアップを復元するプロセスを概説しています。

1. eDirectory を再起動して、有効にしたスキーマの変更を確認します。
2. ユーザアプリケーションドライバ、UserAppDriver のバックアップを含む、Designer 3.5 プロジェクトのコピーを開きます。このプロシージャはドライバ名を変更するので、プロジェクトのコピーを使用することが重要です。
3. ユーザアプリケーションドライバと識別ボールトの間の接続を選択し、右クリックしてから *[プロパティ]* を選択します。.
4. 「UserAppDriver_restore」などの新しい名前を指定します。*[適用]* および *[OK]* を選択します。
5. *[保存]* をクリックしてプロジェクトを保存します。
6. 識別ボールトを選択することによって識別ボールト同期させ、*[ライブ]* > *[スキーマ]* > *[比較]* を選択し、*[元に戻すアクションのために Designer を更新]* .
7. プロジェクトを保存します。
8. ドライバを選択し、*[ドライバ]* > *[展開]* を選択することによって、名前変更したドライバを展開します。
9. NrfCaseUpdate を実行し、新しく名付けたドライバを LDIF ファイルにエクスポートします。
10. 編集用に LDIF ファイルのコピーを作成します。
11. 復元するユーザアプリケーションドライバを示すために参照する LDIF ファイルを編集し、すべてのドライバを名前変更します。たとえば、元のユーザアプリケーションドライバが「cn=UserAppDriver」の場合、「cn=UserAppDriver_restore」から「cn=UserAppDriver」へ名前変更します。この手順は、本物のユーザアプリケーションドライバを反映する LDIF ファイルを実質的に構築します。
12. ice を使用して、変更した LDIF ファイルをインポートします。

    ```
    ice -l[mylogfile.log] -v -SLDIF -f[your_created_ldif] -c -DLDAP -
    s[hostname] -p[389/636] -d[cn=myadmin,o=mycompany] -w[MYPASSWORD] -F -B
    ```
13. ice を使用したインポートが成功したことを確認するためには、そのステータスに注意してください。
14. ドライバの復元を確認するには、35 ページのセクション 3.2.6「NrfCaseUpdate プロセスの確認」の下の指示に従います。
15. 名前変更したドライバをドライバセットから削除します。

3.3 RBPM インストールプログラムの実行

1. 次のプラットフォームのインストーラを起動します。

   Linux

   ```
   rbpm_driver_install_linux.bin
   ```

   Solaris

rbpm_driver_install_solaris.bin

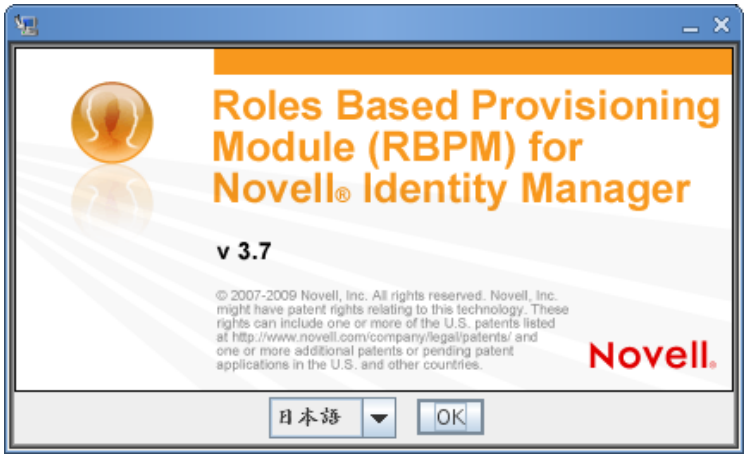
AIX

rbpm_driver_install_aix.bin

Windows

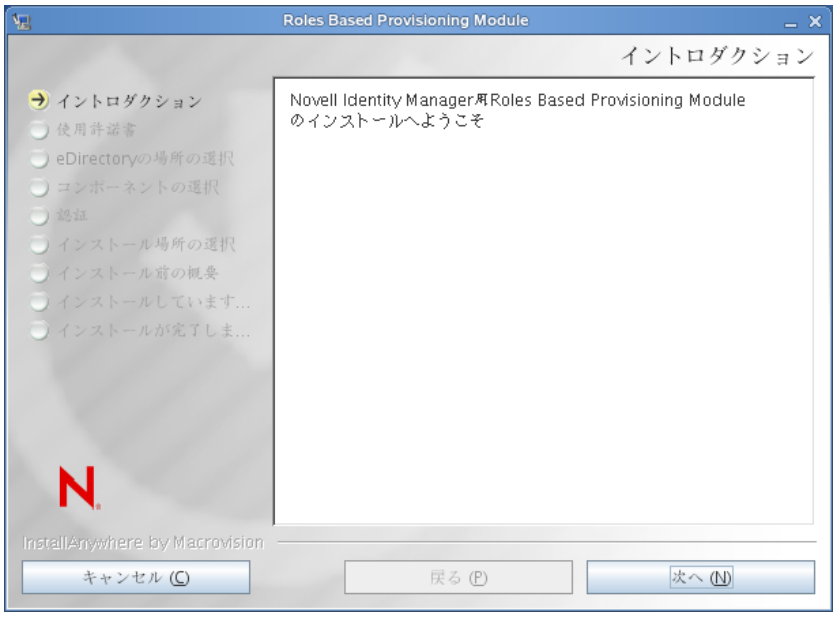
rbpm_driver_install.exe

インストールプログラムを開始すると、言語を入力するよう次のように促されます。



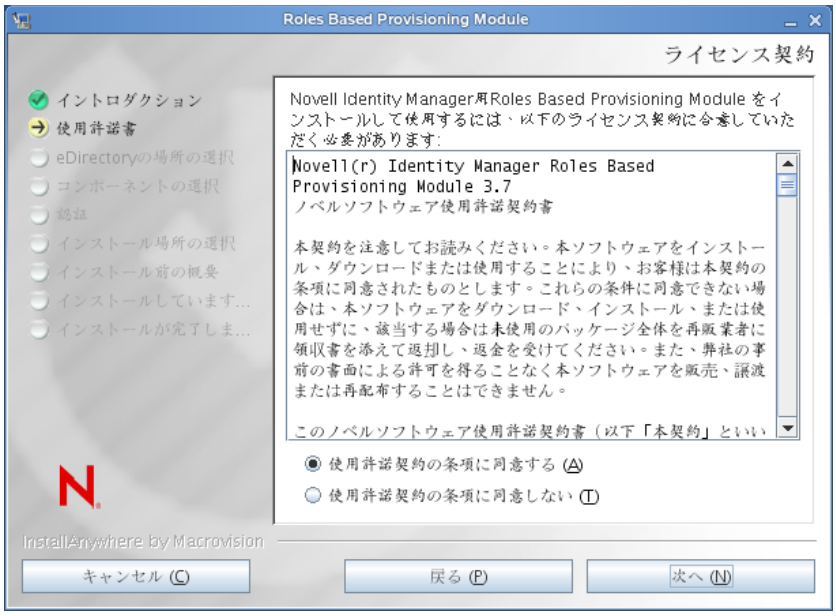
2 インストールする言語を選択して［OK］をクリックします。

インストーラにより、導入画面が表示されます。

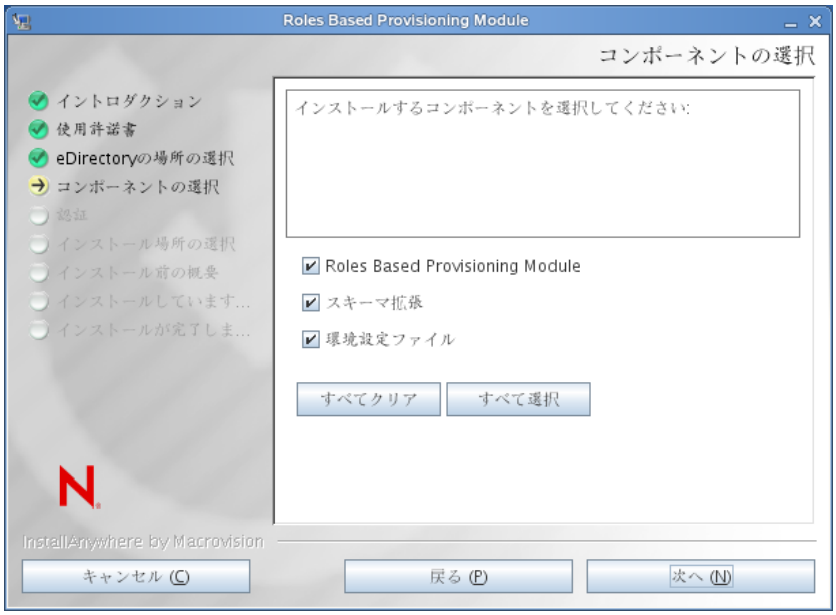


3 *［次へ］*をクリックします。

インストーラにより使用許諾契約画面が表示されます。



4 使用許諾契約に同意したら、*[次へ]* をクリックします。
インストールにより［コンポーネントの選択］画面が表示されます。



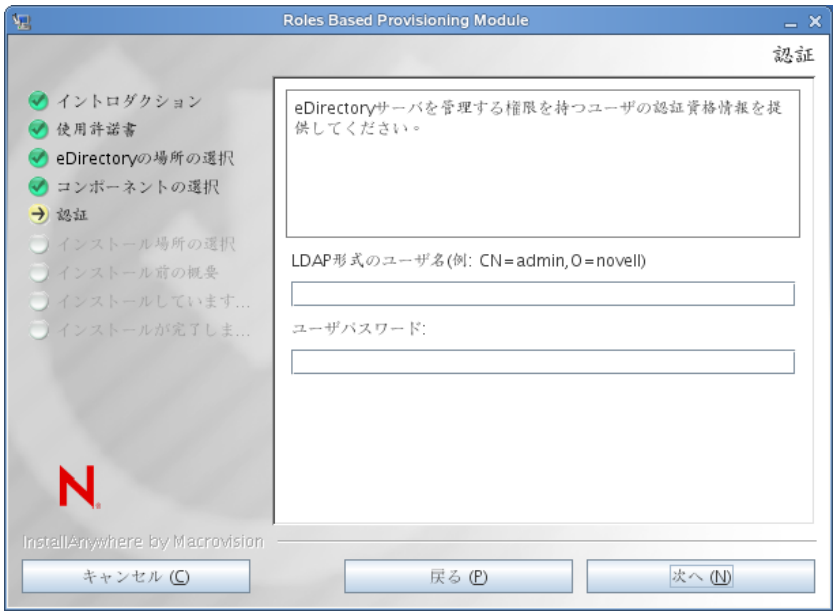
このコンポーネントを次に説明します。

コンポーネント	説明
役割ベースのプロビジョニングモジュール	ユーザアプリケーションドライバおよび役割ドライバとリソースドライバをインストールします。
スキーマ拡張	eDirectory スキーマ拡張をインストールします。

コンポーネント	説明
環境設定ファイル	ドライバ環境設定ファイルをインストールします。

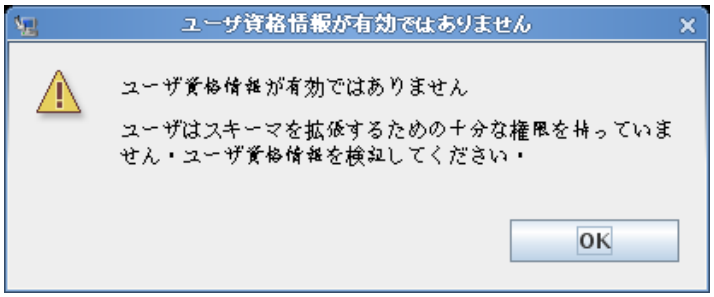
5 インストールするコンポーネントを選択し、*[次へ]* をクリックします。通常、すべてのコンポーネントをインストールします。

インストーラにより、認証画面が表示されます。

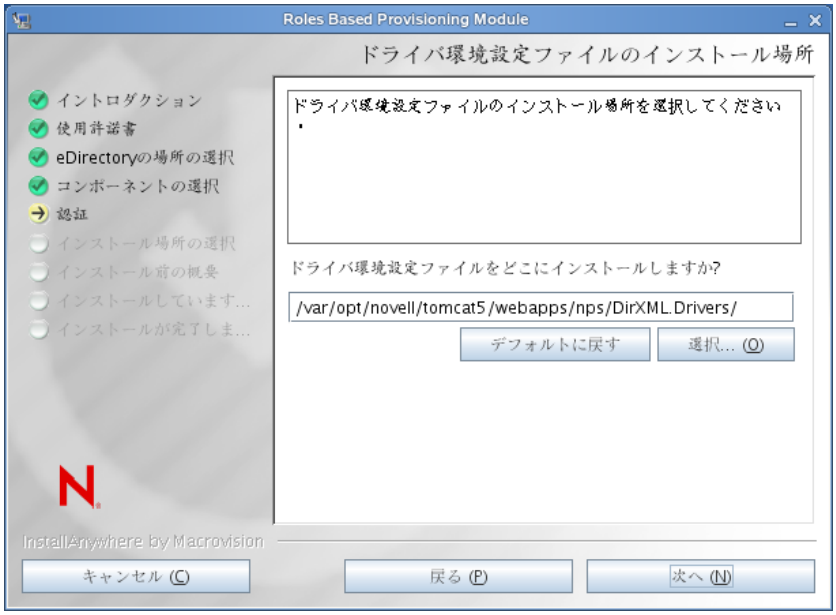


6 ユーザ名を LDAP フォーマットで入力し、パスワードを入力します。次のようにします。

ユーザ資格情報が有効でない場合、またはユーザが必要な権限を持っていない場合、インストーラにより次のようなエラー画面が表示されます。



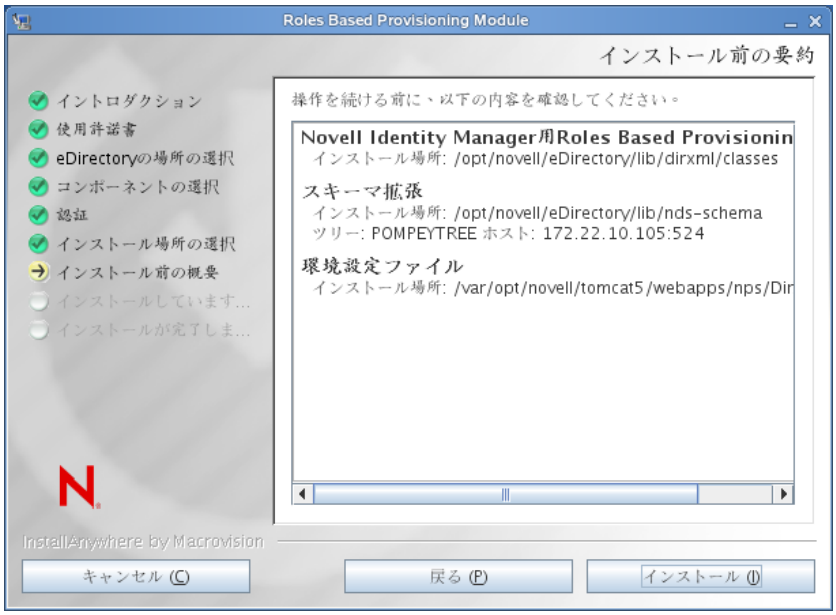
ユーザ資格情報が有効な場合、またはユーザが適切な権限を持っている場合、インストーラにより［ドライバ環境設定ファイル］画面のインストール場所が表示されます。



7 ドライバ環境設定ファイルを保存するディスクの目的の場所を指定するには、*［次へ］*をクリックします。

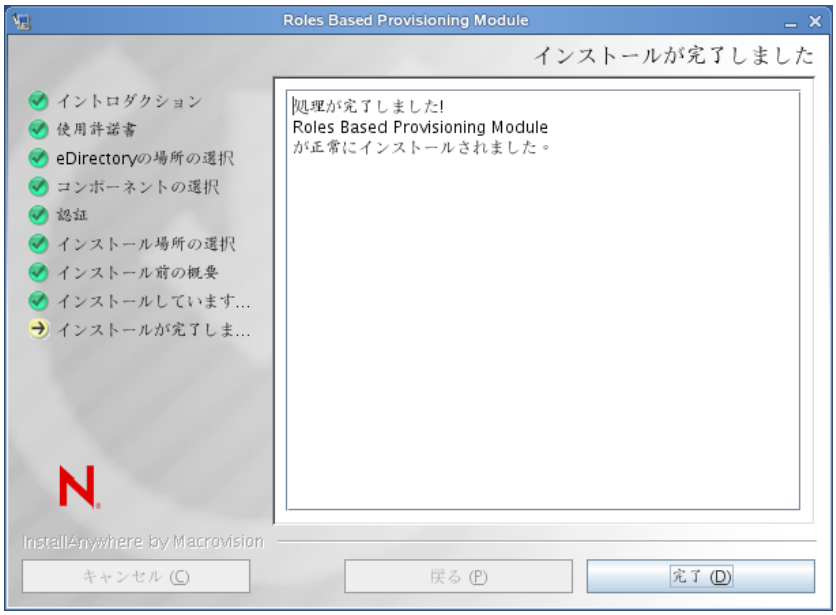
インストーラによりドライバ画面のインストール場所が表示されます。

8 ドライバの目的の場所を指定するには、*[次へ]* をクリックします。
インストーラにより［インストール前の概要］画面が表示されます。



9 概要情報が正しく表示された場合、*[インストール]* をクリックし、インストールプロセスを開始します。

インストールプロセスが完了すると、インストーラにより［インストールが完了しました］画面が表示されます。



ドライバの作成

4

このセクションでは、Roles Based Provisioning Module (RBPM) を使用してドライバを作成する方法について説明します。主なトピックは次のとおりです。

重要 : ユーザアプリケーションドライバは、役割サービスドライバおよびリソースサービスドライバを作成する前に作成する必要があります。ユーザアプリケーションドライバを最初に作成する必要がある理由は、役割サービスおよびリソースサービスドライバがユーザアプリケーションドライバに含まれる役割ボールトコンテナ (RoleConfig.AppConfig) を参照するためです。

ドライバ環境設定サポートでは、次の処理を実行できます。

- 1つのユーザアプリケーションドライバと1つの役割サービスドライバおよびリソースサービスドライバとの関連付け
- 1つのユーザアプリケーションと1つのユーザアプリケーションドライバとの関連付け

4.1 iManager でのユーザアプリケーションドライバの作成

Roles Based Provisioning Module は、アプリケーション環境を制御および設定するためのアプリケーション固有のデータをユーザアプリケーションドライバ内に保存します。たとえば、アプリケーションサーバのクラスタ情報や、ワークフローエンジン環境設定情報などが保持されます。

クラスタのメンバーである RBPM ユーザアプリケーションを除き、各 RBPM ユーザアプリケーションごとに別個のユーザアプリケーションドライバを作成する必要があります。同じクラスタに属するユーザアプリケーションは、単一のユーザアプリケーションドライバを共有する必要があります。クラスタでユーザアプリケーションを実行する場合の詳細については、『*ユーザアプリケーション : 管理ガイド*(http://www.novell.com/documentation/idmrbpm37/index.html)』を参照してください。

重要 : クラスタ以外の RBPM ユーザアプリケーションが単一のドライバを共有するように設定すると、役割ベースプロビジョニングモジュール内で実行されている 1 つ以上のコンポーネントにおいてあいまいな状態が発生してしまいます。発生した問題の原因を突き止めるのは困難です。

ユーザアプリケーションドライバを作成してこれをドライバセットに関連付けるには、以下の処理を実行します。

1. Web ブラウザで iManager を開きます。
2. *［役割とタスク］> ［Identity Manager ユーティリティ］* の順に移動し、*［環境設定のインポート］* を選択します。

3 既存のドライバセット内にドライバを作成するには、［*既存のドライバセットの中*］を選択して、オブジェクトセレクタアイコンをクリックします。続いて、［*次へ*］をクリックしてステップ 4 に進みます。

または

新しいドライバセットを作成する必要がある場合 (たとえば、ユーザアプリケーションドライバを他のドライバとは異なるサーバに配置する場合など)、［*新しいドライバセットの中*］を選択して［*次へ*］をクリックし、新しいドライバセットのプロパティを定義します。

3a 新しいドライバセットの名前、コンテキスト、およびサーバを指定します。コンテキストとは、サーバオブジェクトが存在する eDirectory™ コンテキストのことです。

3b *［次へ］*をクリックします。

4 *［サーバからの環境設定のインポート (.XML ファイル)］*をクリックします。

5 ドロップダウンリストから、ユーザアプリケーションドライバ環境設定ファイルを選択します。ファイル名 :

UserApplication_3_7_0-IDM3_6_0-V1.xml

ファイルがリスト内にない場合、Roles Based Provisioning Module ドライバインストールが正しくインストールされない場合があります。

6 ［*次へ*］をクリックします。

7 ドライバのパラメータを入力するようプロンプトが表示されます (すべてを表示するにはスクロールします)。パラメータを記録します。これらのパラメータは RBPM ユーザアプリケーションをインストールする際に必要になります。

フィールド	説明
ドライバ名	作成するドライバの名前。
認証 ID	ユーザアプリケーション管理者の識別名。これは、ユーザアプリケーションポータルの管理権限を付与するユーザアプリケーション管理者になります。admin.orgunit.novell などの eDirectory™ 形式を使用するか、ユーザを参照して特定します。このフィールドは必須です。
パスワード	［認証 ID］で指定したユーザアプリケーション管理者のパスワード。
アプリケーションコンテキスト	ユーザアプリケーションのコンテキスト。これは、ユーザアプリケーション WAR ファイルのコンテキスト部分です。デフォルトは *IDM* です。
ホスト	Identity Manager ユーザアプリケーションが展開されたアプリケーションサーバのホスト名または IP アドレス。 ユーザアプリケーションがクラスタで実行されている場合は、ディスパッチャのホスト名または IP アドレスを入力します。
ポート	上でリストに表示されているホストのポート。
イニシエータの無効化を許可 :	［*はい*］を選択すると、プロビジョニング管理者は、自分を代理として指定したユーザになりかわってワークフローを開始できます。

8 ［*次へ*］をクリックします。

9 ［*同等セキュリティの定義*］をクリックして、［同等セキュリティ］ウィンドウを表示します。管理者または他のスーパバイザオブジェクトを参照して選択し、［*追加*］をクリックします。

この手順により、ドライバに必要な許可が付与されます。この手順の重要性の詳細については、Identity Manager のマニュアルを参照してください。

10 (オプション、ただし推奨) ［*管理者の役割を除外する*］をクリックします。

11 *［追加］*をクリックして、ドライバアクションから除外するユーザ (管理者の役割など) を選択してから、*［OK］*をクリックします。

12 ［*OK*］をクリックして、［Security Equals］ウィンドウを閉じてから、［*次へ*］をクリックして、概要ページを表示します。

13 情報が正しい場合、［*終了*］をクリックします。

重要 : ドライバはデフォルトでは無効になっています。RBPM ユーザアプリケーションをインストールするまで、ドライバは無効のままにしてください。

4.2 iManager での役割サービドライバおよびリソースサービスドライバの作成

iManager で役割サービスドライバおよびリソースサービスドライバを作成して設定する

1 Web ブラウザで iManager を開きます。

2 *［役割とタスク］> ［Identity Manager ユーティリティ］*の順に移動し、*［環境設定のインポート］*を選択します。

役割サービスドライバおよびリソースサービスドライバをインストールする前に、ユーザアプリケーションドライバをインストールします。役割サービスドライバおよびリソースサービスドライバには、ユーザアプリケーションドライバのバージョン 3.7.0(UserApplication_3_7_0-IDM3_6_0-V1.xml) を使用します。ユーザアプリケーションドライバの他のバージョンを使用すると、役割およびリソースカタログは利用できません。

3 ウィザードで、デフォルトの *［既存のドライバセット内］*を維持します。45 ページのセクション 4.1「iManager でのユーザアプリケーションドライバの作成」で作成されたドライバセットをブラウズします。*［次へ］*をクリックします。

注 : ユーザアプリケーションドライバと役割ドライバおよびリソースドライバは同一ドライバセット内にある必要があります。

---

4 ドロップダウンリストから *［RoleResourceService_3_7_0-IDM3_6_0-V1.xml］*を選択します。これは、ロールベースプロビジョニングモジュールをサポートする役割サービスドライバおよびリソースサービスドライバの設定ファイルです。

ファイルがリスト内にない場合、Roles Based Provisioning Module インストーラは正しくインストールされました。

*［次へ］*をクリックします。

5 ［要求されたインポート情報］ページで、要求された情報を入力します。次の表は、要求される情報について示しています。

オプション	説明
ドライバ名	役割サービスドライバおよびリソースサービスドライバのドライバ名を指定するか、デフォルト名 Role Service および Resource Service をそのまま使用します。既存のドライバと同じ名前の新しいドライバをインストールした場合、既存のドライバの設定は新しいドライバによって上書きされます。 *[参照]* ボタンを使用して、選択したドライバセットにある既存のドライバを表示します。このフィールドは必須です。
ユーザグループベースコンテナ DN	ドライバは、このベースコンテナのユーザ、コンテナ、およびグループでのみ動作します。グループ役割またはリソース割り当てがある場合、役割サービスドライバおよびリソースサービスドライバのみが、コンテナのドメイン内のメンバーの役割またはリソースを許可または取り消します。
ユーザアプリケーションドライバ DN	役割またはリソースシステムをホストするユーザアプリケーションドライバオブジェクトの識別名。UserApplication.driverset.org などの eDirectory フォーマットを使用するか、ドライバオブジェクトを参照して見つけます。このフィールドは必須です。
ユーザアプリケーション URL	ユーザアプリケーションに接続して承認ワークフローを開始するために使用される URL。たとえば、*http://host:port/IDM* のような URL になります。このフィールドは必須です。
ユーザアプリケーションの識別情報	ユーザアプリケーションに対して認証して承認ワークフローを開始するために使用されるオブジェクトの識別名。ここには、ユーザアプリケーションポータルの管理権限を付与するユーザアプリケーション管理者を指定できます。admin.department.org などの eDirectory フォーマットを使用するか、ユーザを参照して見つけます。このフィールドは必須です。
ユーザアプリケーションのパスワード	［認証 ID］で指定したユーザアプリケーション管理者のパスワード。承認ワークフローを開始するためにユーザアプリケーションに対して認証するのに使用されるパスワードです。このフィールドは必須です。
パスワードを再入力	ユーザアプリケーション管理者のパスワードを再入力します。

6 情報を入力したら、［*次へ*］をクリックします。

7 ［*同等セキュリティの定義*］をクリックして、［同等セキュリティ］ウィンドウを表示します。管理者または他のスーパバイザオブジェクトを参照して選択し、［*追加*］をクリックします。

この手順により、ドライバに必要な許可が付与されます。この手順の重要性の詳細については、Identity Manager のマニュアルを参照してください。

8 (オプション、ただし推奨) ［*管理者の役割を除外する*］をクリックします。

9 *［追加］*をクリックして、ドライバアクションから除外するユーザ (管理者の役割など) を選択してから、*［OK］*をクリックします。

10 ［*OK*］をクリックして、［Security Equals］ウィンドウを閉じてから、［*次へ*］をクリックして、概要ページを表示します。

11 情報が正しい場合、［*終了*］をクリックします。

JBoss でのユーザアプリケーションのインストール

5

このセクションでは、グラフィカルユーザインタフェース版のインストーラを使用して、JBoss アプリケーションサーバ上で Roles Based Provisioning Module にユーザアプリケーションをインストールする方法について説明します。次のトピックについて説明します。

- 51 ページのセクション 5.1「ユーザアプリケーション WAR のインストールおよび環境設定」
- 64 ページのセクション 5.2「インストールのテスト」

コマンドラインを使用してインストールする場合は、103 ページの第 8 章「コンソールまたは単一コマンドによるインストール」を参照してください。

ルート以外のユーザとしてインストーラを実行します。

データマイグレーション 移行の詳細については、『*ユーザアプリケーション：マイグレーションガイド* (http://www.novell.com/documentation/idmrbpm37/index.html)』を参照してください。

5.1 ユーザアプリケーション WAR のインストールおよび環境設定

注 : JBoss 5.0.1 の場合、インストールプログラムでは、Sun から提供されている Java 2 Platform Standard Edition Development Kit バージョン 1.6 (JRE または JDK) が必要です。別のバージョンを使用すると、インストールプロシージャはユーザアプリケーション WAR ファイルを正常に設定しません。インストールは成功したかのように見えますが、ユーザアプリケーションの起動を試みるとエラーが発生します。

1 使用しているプラットフォーム用のインストーラをコマンドラインから起動します。

ユーザアプリケーションインストーラを起動するには、以下のプラットフォームで必ず Sun JDK のバージョンを使用してください。

Linux または Solaris

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

Windows

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

インストール手順中に Java インストールのフルパスを入力するよう求められた場合は、Sun JDK のルートパスを入力します。たとえば、Linux におけるルートパスは次のようになります。/opt/jkd1.6.0_14

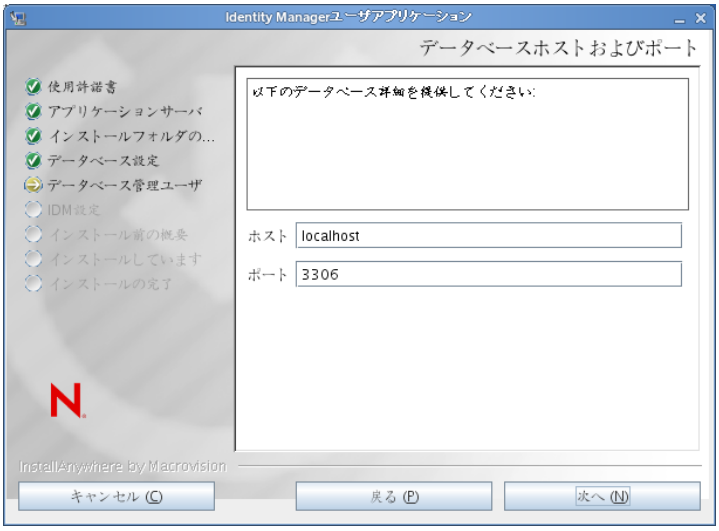
注 : SLES ユーザ : SLES に付属している IBM* JDK は使用しないでください。このバージョンはインストールの一部の機能との互換性がなく、マスタキー破損エラーを起こす可能性があります。

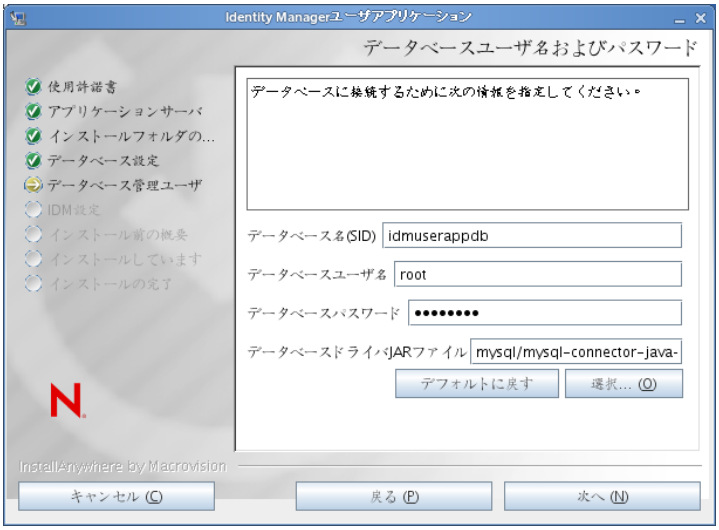
インストールプログラムを開始すると、言語を入力するよう次のように促されます。

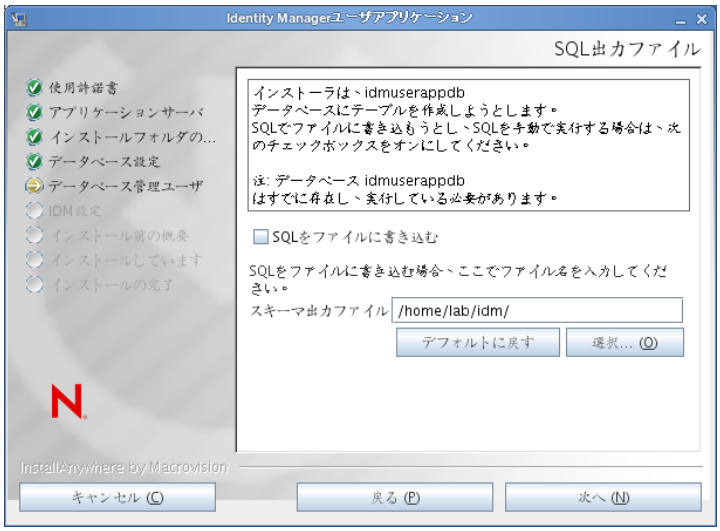
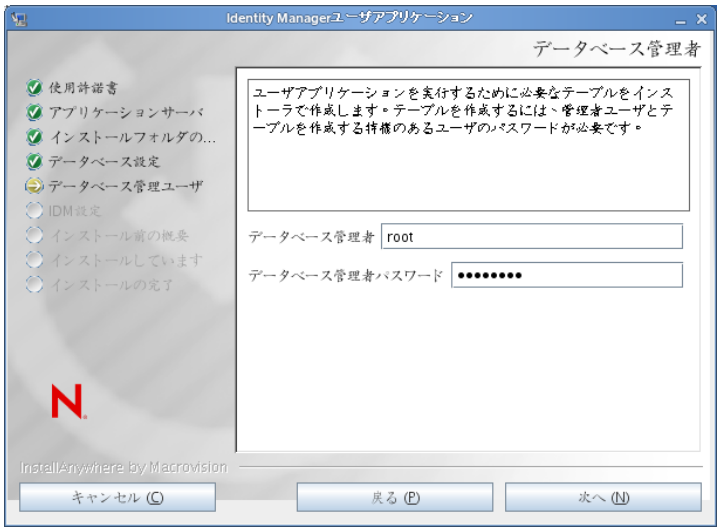
2 次の情報を使用して、言語を選択し、使用許諾契約を確認し、アプリケーションサーバプラットフォームを選択します。

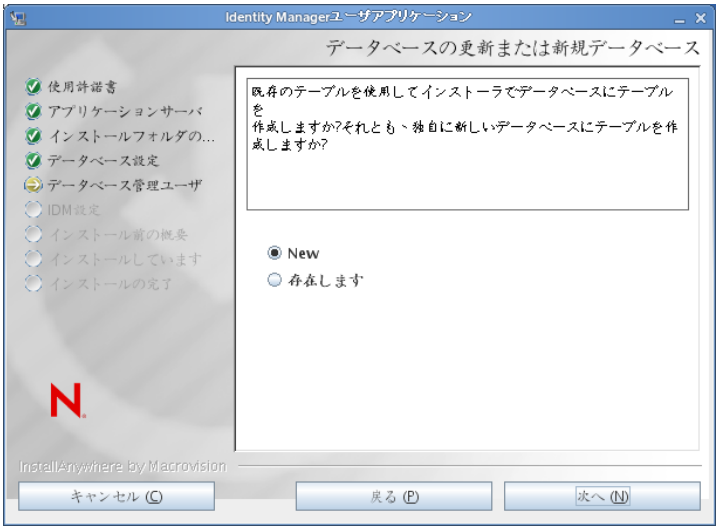
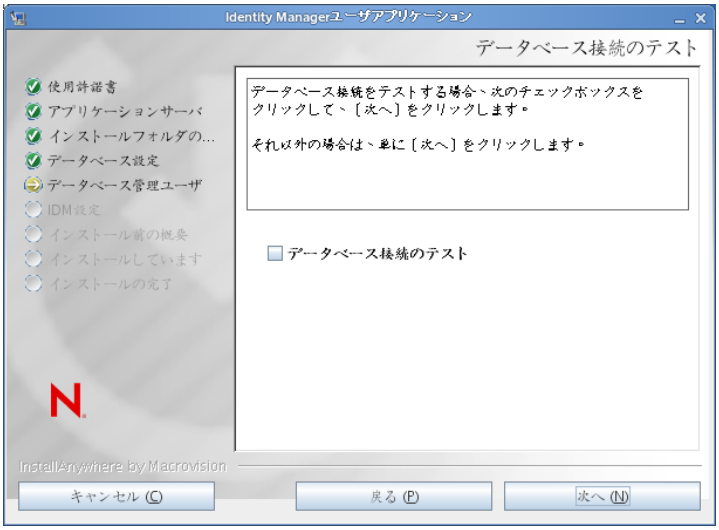
インストール画面	説明
ユーザアプリケーションインストール	インストールプログラムの言語を選択します。デフォルトでは、［英語］が選択されています。
使用許諾契約	使用許諾契約を読み、*［使用許諾契約の条件に同意します］*を選択します。
アプリケーションサーバプラットフォーム	［*JBoss*］を選択します。 JBoss でインストールする場合、Sun の Java 環境を使用することによってインストールプログラムを開始する必要があります。アプリケーションサーバとして JBoss を選択し、インストールの開始に Sun の Java を使用しない場合、次のポップアップエラーメッセージが表示され、インストールは終了します。 

3 次の情報を使用して、インストールタイプを選択し、インストールフォルダを指定し、データベースを設定します。

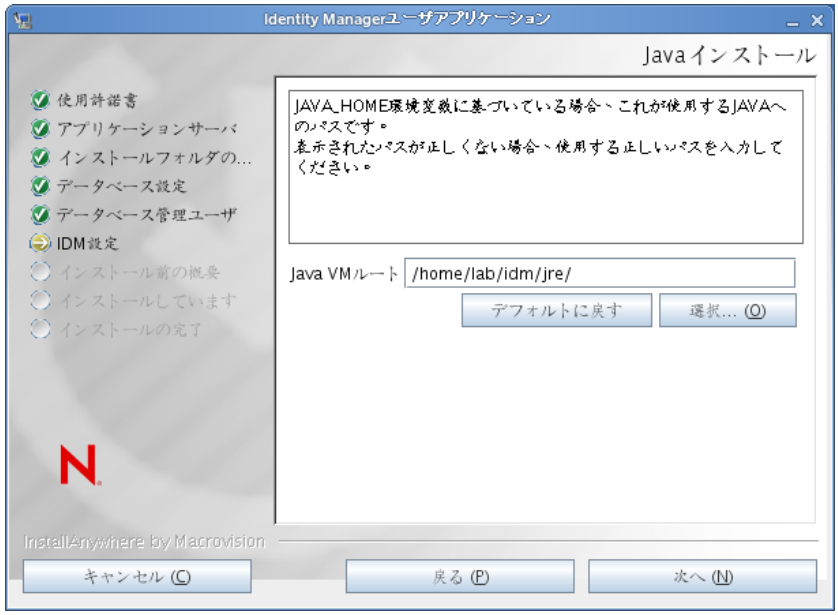
インストール画面	説明
インストールのタイプ	*Roles Based Provisioning*: Roles Based Provisioning Module をインストールするには、このオプションを選択します。これはこのリリースでのみサポートされているインストールタイプです。
インストールフォルダの選択	インストーラがファイルを配置する場所を指定します。
データベースプラットフォーム	データベースプラットフォームを選択します。データベースおよび JDBC ドライバはすでにインストールされている必要があります。JBoss の場合、オプションには次のプラットフォームが含まれます。 ◆ MySQL ◆ Oracle (Oracle 10g および 11g のみサポート。Oracle 9i はサポートされなくなりました。) ◆ PostgreSQL (JBoss にインストール時のみ使用可能) ◆ Microsoft SQL Server ◆ IBM DB2 (バージョン 9.5 のみサポート。バージョン 9.1 はサポートされなくなりました。)
データベースホストおよびポート	*ホスト*: データベースサーバのホスト名または IP アドレスを指定します。クラスタでは、クラスタの各メンバーには同じホスト名または IP アドレスを指定します。 *ポート*: データベースのリスナポート番号を指定します。クラスタの場合は、クラスタの各メンバーに同じポートを指定します。 

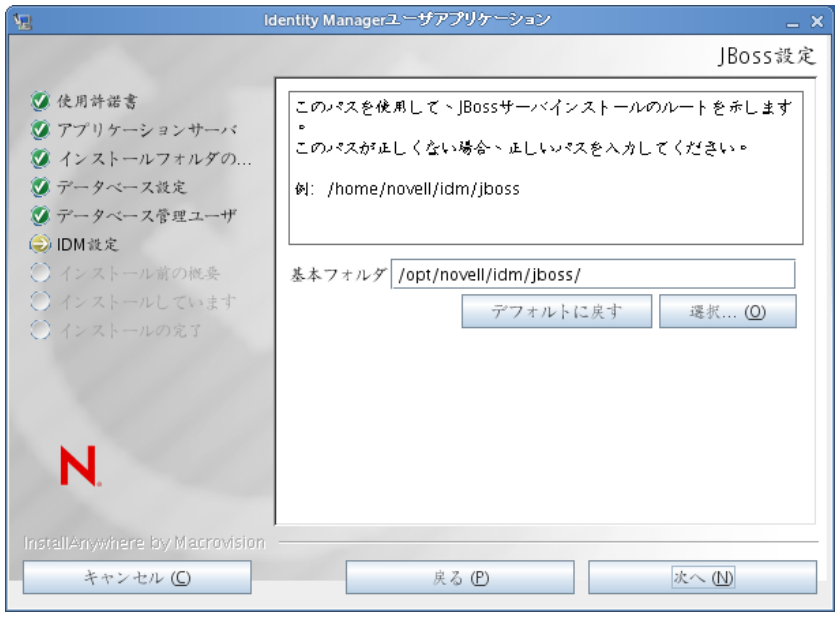
インストール画面	説明
データベースのユーザ名およびパスワード	*データベース名* (または SID): MySQL、MMS SQL Server、または PostgreSQL では、事前に設定したデータベース名を入力します。Oracle の場合は、前に作成した Oracle システム ID (SID) を指定します。クラスタでは、クラスタの各メンバーには同じデータベース名または SID を指定します。 *データベースユーザ名* : データベースユーザを指定します。クラスタでは、クラスタの各メンバーには同じデータベースユーザを指定します。 *データベースパスワード*: データベースパスワードを指定します。クラスタでは、クラスタの各メンバーには同じデータベースパスワードを指定します。 *データベースドライバ JAR ファイル* : データベースサーバにシンクライアント JAR を指定します。これは必須です。 

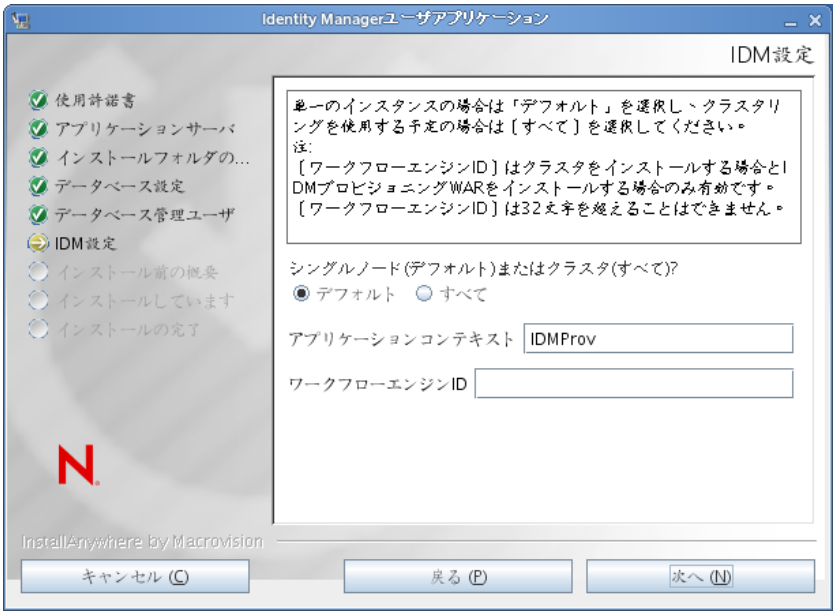
インストール画面	説明
SQL 出力ファイル	このリリースでは、アプリケーションサーバの起動時 (以前のリリースのように) ではなく、ユーザアプリケーションのインストール時にデータベーステーブルが作成できます。 SQL 出力ファイル画面では、スキーマファイルを作成するためのオプションを指定します。データベース管理者は、インストールプログラムでテーブルを作成する代わりに、スキーマファイルを使用してテーブルを作成できます。 スキーマファイルを作成する場合、*[SQL をファイルに書き込む]* チェックボックスをオンにして、*[スキーマ出力ファイル]* フィールドにファイルの名前を入力します。 
データベース管理者	この画面には、[データベースユーザ名およびパスワード] ページから同じユーザ名とパスワードが事前に入力されています。以前に指定したデータベースユーザがデータベースサーバ内にテーブルを作成するための十分な許可を持っていない場合、必要な権限を持つ別のユーザ ID を入力する必要があります。 

インストール画面	説明
データベースの更新または新規データベース	使用するデータベースが新規または空の場合、*[新規]* ボタンを選択します。データベースが以前のインストールからの既存のものである場合、*[存在します]* ボタンを選択します。 
データベース接続のテスト	前の画面で指定した情報が正しかったことを確認するには、*[データベース接続のテスト]* チェックボックスをオンにしてデータベース接続をテストします。 

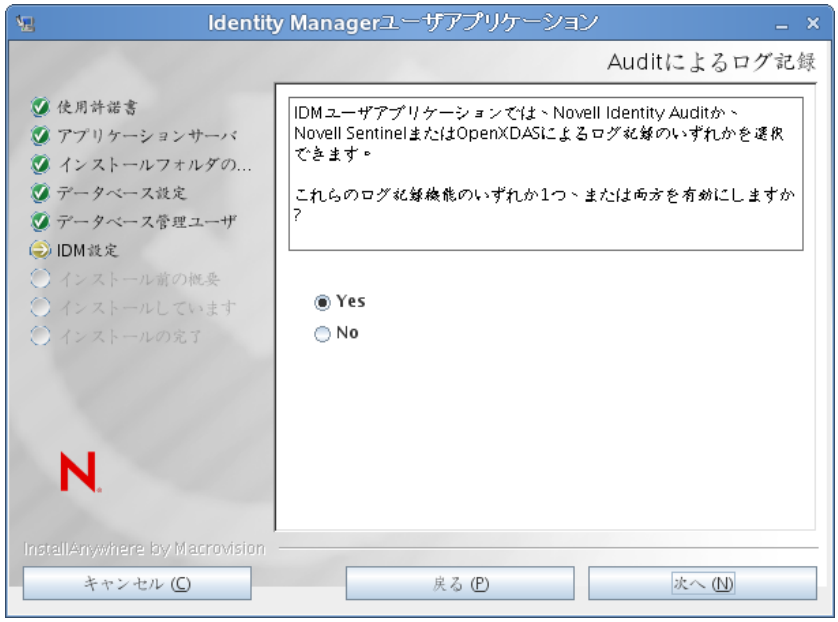
4 次の情報を使用して、Java、JBoss のインストール、および IDM とともに監査設定とセキュリティを設定します。

インストール画面	説明
Java のインストール	Java ルートのインストールフォルダを指定します。Java インストールでは JAVA_HOME 環境変数に基づいて Java へのパスが表示され、それを修正するオプションを選択できます。  この時点で、インストールプログラムは、選択した Java が、選択したアプリケーションサーバに対して正しいものであることも確認します。また、指定されている JRE で CA 証明書に書き込めることも確認します。 JBoss アプリケーションサーバをインストールする場所の情報を入力するよう、次のように促されます。

インストール画面	説明
JBoss 環境設定	JBoss アプリケーションサーバを見つける場所をユーザアプリケーションに伝えます。 このインストール手順では、JBoss アプリケーションサーバはインストールされません。JBoss アプリケーションサーバのインストール手順については、20 ページの 「JBoss アプリケーションサーバと MySQL データベースのインストール」を参照してください。 *ベースフォルダ*: アプリケーションサーバの場所を指定します。 

インストール画面	説明
IDM 環境設定	アプリケーションサーバ設定のタイプを選択します。 ◆ このインストールが、クラスタの一部でない 1 つのノード上の場合は、*［デフォルト］* を選択します。 ［*デフォルト*］を選択し、クラスタを後で必要とすると判断した場合は、ユーザアプリケーションを再インストールする必要があります。 ◆ このインストールがクラスタの一部の場合は、*［すべて］* を選択します。 *アプリケーションコンテキスト*: アプリケーションサーバの環境設定の名前、アプリケーション WAR ファイルの名前、および URL コンテキストの名前です。インストールスクリプトによってサーバの環境設定が作成され、デフォルト名で *アプリケーション名*に基づく環境設定が作成されます。ユーザアプリケーションをブラウザから開始する場合は、アプリケーション名を書き留め、アプリケーション名を URL に含めてください。 *ワークフローエンジン ID*: クラスタ内の各サーバには、一意のワークフローエンジン ID を設定する必要があります。ワークフローエンジン ID はクラスタインストールでのみ、また IDM プロビジョニング WAR をインストールする場合のみ有効です。エンジン ID は 32 文字を越えることはできません。ワークフローエンジン ID については、*『ユーザアプリケーション: 管理ガイド』* のセクション「クラスタ化のワークフローの設定」で説明されています。 

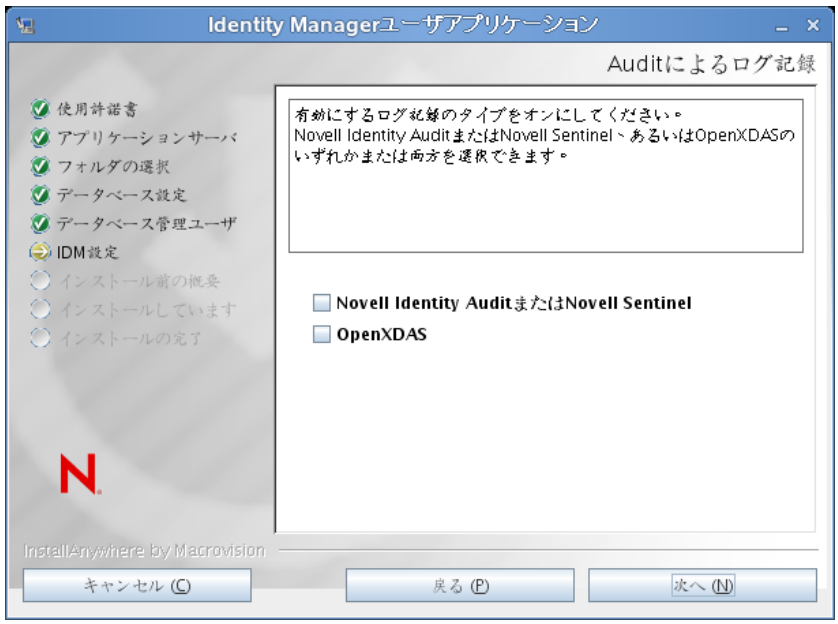
インストール画面	説明
Audit のログ	ログを有効にするには、［*はい*］をクリックします。ログを無効にするには、*［いいえ］*をクリックします。



次のパネルでは、ログのタイプを指定するよう促されます。次のオプションから選択します。

- *Novell Identity Audit または Novell Sentinel*: Novell クライアントを使用してユーザアプリケーションでログを有効にします。
- *OpenXDAS*: OpenXDAS ログサーバにイベントが記録されます。

ログの設定の詳細については、『*ユーザアプリケーション: 管理ガイド*』を参照してください。



インストール画面	説明
Novell Audit	*サーバ*: ログを有効にする場合、サーバのホスト名または IP アドレスを指定します。ログをオフにする場合は、この値は無視されます。 *ログキャッシュフォルダ*: ログキャッシュのディレクトリを指定します。
セキュリティ - マスタキー	*はい*: 既存のマスタキーをインポートできます。既存の暗号化マスタキーをインポートするよう選択した場合は、該当するキーを切り取ってインストール手順のウィンドウに貼り付けます。 *いいえ*: 新規のマスタキーを作成します。インストール終了後、115 ページのセクション 9.1「マスタキーの記録」で示すように、マスタキーを手動で記録します。 インストール手順で、インストールディレクトリにある master-key.txt ファイルに暗号化マスタキーが書き込まれます。 既存のマスタキーをインポートする理由には、次のようなものがあります。 ◆ インストールファイルをステージングシステムから運用システムに移動中で、ステージングシステムで使用したデータベースへのアクセスを保持する場合。 ◆ ユーザアプリケーションを最初の JBoss クラスタのメンバーにインストールしており、現在はクラスタの次のメンバーにインストールしている場合 (同じマスタキーが必要)。 ◆ ディスク故障のため、ユーザアプリケーションを復元する必要がある場合。ユーザアプリケーションを再インストールして、以前のインストールで使用したのと同じ暗号化マスタキーを指定する必要があります。これによって、前に保存した暗号化データにアクセスできます。

5 *[次へ]* をクリックして、[役割ベースプロビジョニングモジュール環境設定] パネルを表示します。(この情報の入力を求められない場合、29 ページのセクション 2.5「Java Development Kit のインストール」で説明したステップを完了していない可能性があります。)

[役割ベースプロビジョニングモジュール環境設定] パネルのデフォルトのビューでは、これらの 6 つのフィールドが表示されます。

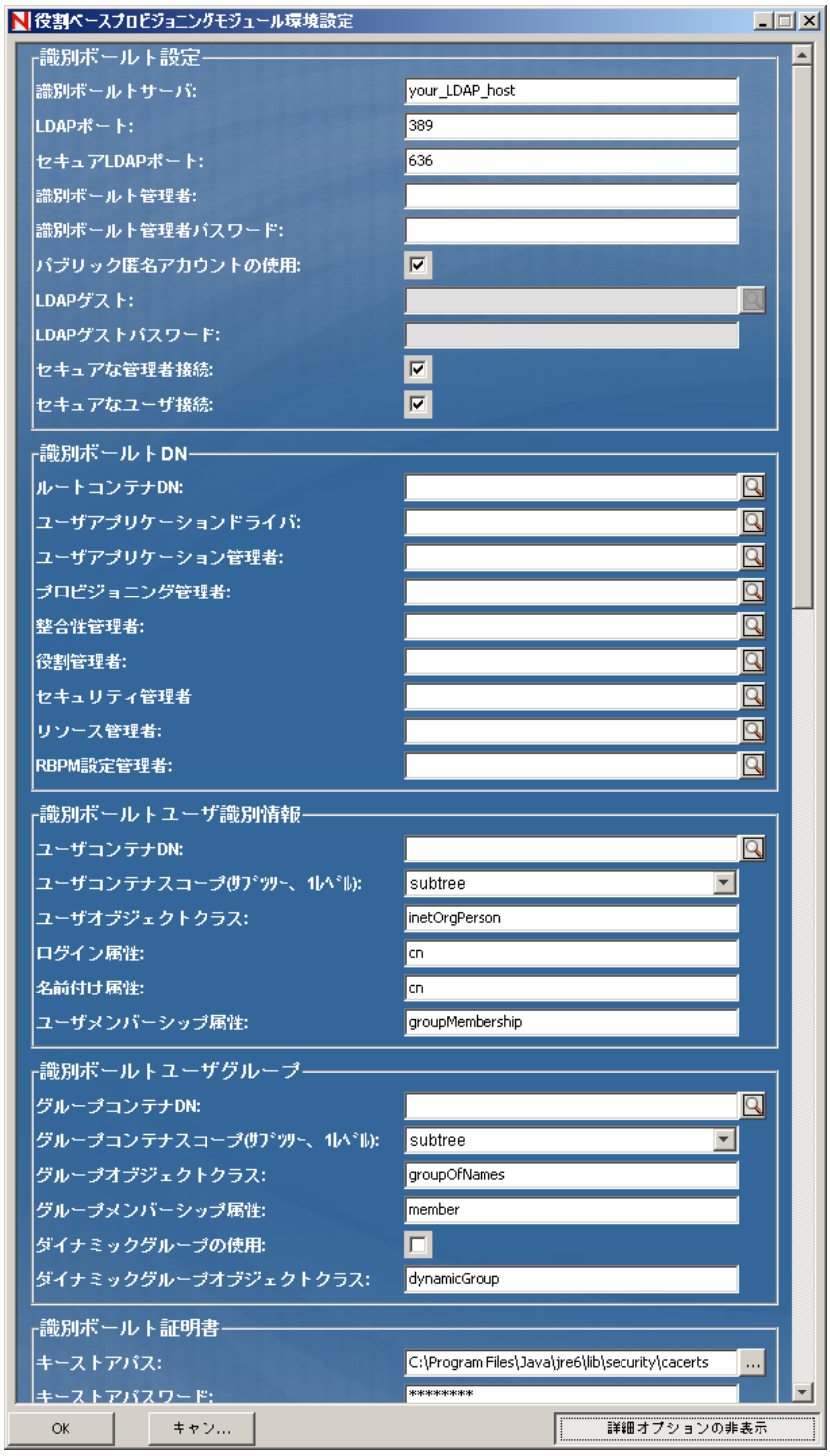
インストールプログラムはルートコンテナ DN から値を取得し、それを次の値に適用します。

- ユーザコンテナ DN
- グループコンテナ DN

インストールプログラムはユーザアプリケーション管理者フィールドから値を取得し、それを次の値に適用します。

- プロビジョニング管理者
- コンプライアンス管理者
- 役割管理者
- セキュリティ管理者
- リソース管理者
- RBPM 設定管理者

これらの値を明示的に指定する場合、*[詳細オプションの表示]* ボタンをクリックしてそれらを変更できます。


役割ベースプロビジョニングモジュール環境設定
識別ボールト設定
識別ボールトサーバ:
your_LDAP_host
LDAPポート:
389
セキュアLDAPポート:
636
識別ボールト管理者:
識別ボールト管理者パスワード:
パブリック匿名アカウントの使用:
LDAPゲスト:
LDAPゲストパスワード:
セキュアな管理者接続:
セキュアなユーザ接続:
識別ボールトDN
ルートコンテナDN:
ユーザアプリケーションドライバ:
ユーザアプリケーション管理者:
プロビジョニング管理者:
整合性管理者:
役割管理者:
セキュリティ管理者
リソース管理者:
RBPM設定管理者:
識別ボールトユーザ識別情報
ユーザコンテナDN:
ユーザコンテナスコープ(サブツリー、1レベル):
subtree
ユーザオブジェクトクラス:
inetOrgPerson
ログイン属性:
cn
名前付け属性:
cn
ユーザメンバーシップ属性:
groupMembership
識別ボールトユーザグループ
グループコンテナDN:
グループコンテナスコープ(サブツリー、1レベル):
subtree
グループオブジェクトクラス:
groupOfNames
グループメンバーシップ属性:
member
ダイナミックグループの使用:
ダイナミックグループオブジェクトクラス:
dynamicGroup
識別ボールト証明書
キーストアパス:
C:\Program Files\Java\jre6\lib\security\cacerts
キーストアパスワード:
****
OK
キャン...
詳細オプションの非表示

6 インストールを完了するには、次の情報を使用します。

インストール画面	説明
ユーザアプリケーション環境設定	ユーザアプリケーションをインストールすると、ユーザアプリケーション環境設定パラメータを設定できます。インストールすると、これらのパラメータの多くは configupdate.sh または configupdate.bat でも編集可能です。例外はパラメータ説明に記述されています。 クラスタの場合は、クラスタの各メンバーに同じユーザアプリケーション環境設定パラメータを指定します。 各オプションの詳細については、123 ページの付録 A「IDM ユーザアプリケーション環境設定の参照」を参照してください。
インストール前の概要	［インストール前の概要］ページを読んで、インストールパラメータの選択を確認します。 必要に応じて、［*戻る*］を使用して前のインストールページに戻り、インストールパラメータを変更します。 ユーザアプリケーション環境設定ページでは値は保存されないため、インストールの前のページを再指定した後に、ユーザアプリケーション環境設定の値を再入力する必要があります。インストールおよび環境設定パラメータで納得いく設定ができたら、［インストール前の概要］ページに戻り、［*インストール*］をクリックします。
インストールの完了	インストールの終了が示されます。

5.1.1 インストールとログファイルの表示

インストールがエラーなしで完了した場合は、インストールのテストに進みます。インストールでエラーまたは警告が発生した場合は、次のようなログファイルを確認して、問題を判断してください。

- Identity_Manager_User_Application_InstallLog.log には、基本的なインストールタスクの結果が格納されています。
- Novell-Custom-Install.log には、インストール中に行ったユーザアプリケーション環境設定についての情報があります。

5.2 インストールのテスト

1 データベースを起動します。手順については、データベースマニュアルを参照してください。

2 ユーザアプリケーションサーバ (JBoss) を起動します。コマンドラインで、インストールディレクトリを作業ディレクトリにして、次のスクリプトを実行します (ユーザアプリケーションのインストールで提供)。

start-jboss.sh(Linux および Solaris)

start-jboss.bat(Windows)

アプリケーションサーバを停止するには、stop-jboss.sh または stop-jboss.bat を使用するか、あるいは start-jboss.sh または start-jboss.bat を実行しているウィンドウを閉じます。

X11 ウィンドウシステム上で実行していない場合は、サーバの起動スクリプトに -Djava.awt.headless=true フラグを含める必要があります。これはレポートの実行に必要です。たとえば、スクリプト内に次の行を含めます。

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

3 ユーザアプリケーションドライバを起動します。これによって、ユーザアプリケーションドライバへの通信は有効になります。

3a iManager にログインします。

3b 左のナビゲーションフレームに表示されている［役割］と［タスク］で、［*Identity Manager*］の下で［*Identity Manager の概要*］を選択します。

3c 表示されたコンテンツビューで、ユーザアプリケーションドライバを含むドライバセットを指定し、［*検索*］をクリックします。ドライバセットとそれに関連付けられたドライバを示すグラフィックが表示されます。

3d ドライバで赤と白のアイコンをクリックします。

3e ［*ドライバの起動*］を選択します。ドライバ状態は陰陽記号に変更され、ドライバが起動されていることが表示されます。

起動時にドライバはユーザアプリケーションと「握手」しようとします。アプリケーションサーバが実行されていないか WAR が正常に展開されなかった場合は、ドライバはエラーを返します。

4 ユーザアプリケーションを起動してログインするには、Web ブラウザを使用して次のアドレスにアクセスします。URL:

http://*hostname*:*port*/*ApplicationName*

この URL では、*hostname*: *port* はアプリケーションサーバのホスト名で (たとえば、「myserver.domain.com」)、ポートはアプリケーションサーバのポートです (たとえば、JBoss のデフォルトは「8080」)。*ApplicationName はデフォルトで IDM です*。アプリケーションサーバの環境設定情報を入力した場合、インストール中にアプリケーション名を指定しています。

Novell Identity Manager のユーザアプリケーションの待ち受けページが表示されます。

5 そのページの右上隅で、［*ログイン*］をクリックしてユーザアプリケーションにログインします。

このようなステップの完了後に、ブラウザに Identity Manager のユーザアプリケーションのページが表示されない場合は、エラーメッセージがないかどうか端末のコンソールを確認して、120 ページのセクション 9.8「トラブルシューティング」を参照します。

WebSphere でのユーザアプリケーションのインストール

6

このセクションでは、グラフィカルユーザインタフェースバージョンのインストーラを使用して、WebSphere アプリケーションサーバに Roles Based Provisioning Module のユーザアプリケーションをインストールする方法について説明します。

- 67 ページのセクション 6.1「ユーザアプリケーション WAR のインストールおよび環境設定」
- 80 ページのセクション 6.2「WebSphere 環境の環境設定」
- 83 ページのセクション 6.3「WAR ファイルの展開」
- 83 ページのセクション 6.4「ユーザアプリケーションの開始およびアクセス」

ルート以外のユーザとしてインストーラを実行します。

データマイグレーション 移行の詳細については、『*ユーザアプリケーション：マイグレーションガイド* (http://www.novell.com/documentation/idmrbpm37/index.html)』を参照してください。

6.1 ユーザアプリケーション WAR のインストールおよび環境設定

注 : WebSphere 6.1 の場合、インストールプログラムでは、IBM から提供されている Java 2 Platform Standard Edition Development Kit バージョン 1.5 JDK が必要です。WebSphere 7.0 の場合、インストールプログラムでは、IBM から提供されている 1.6 JDK が必要です。別のバージョンを使用した場合、このインストール手順ではユーザアプリケーション WAR ファイルは正しく設定されません。インストールは成功したかのように見えますが、ユーザアプリケーションの起動を試みるとエラーが発生します。

1 インストールファイルが含まれるディレクトリに移動します。

2 IBM Java 環境を使用して、次に示すインストーラを開始します。

Solaris

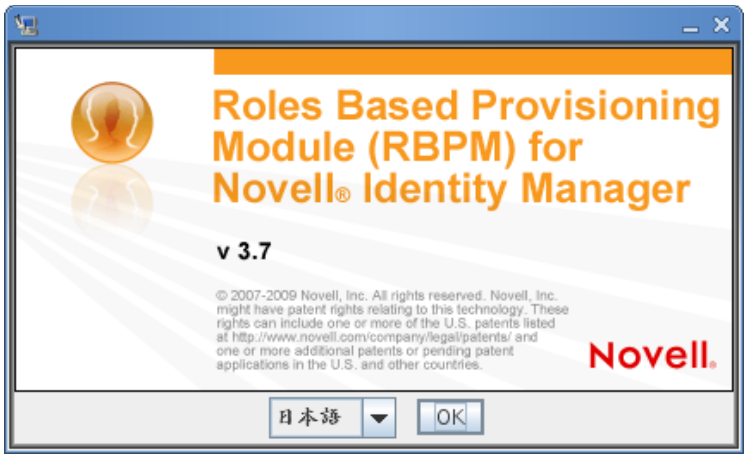
```
$ /opt/WS/IBM/WebSphere/AppServer/java/bin/java -jar IdmUserApp.jar
```

Windows

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

重要 : WebSphere では、制限なしのポリシーファイルが適用された IBM JDK を使用する必要があります。これらの制限なしポリシーファイルがないと、“ 無効なキーサイズ ” というエラーが発生します。このプログラムの根本原因は制限なしポリシーファイル欠如です。したがって必ず正しい IBM JDK を使用してください。

インストールプログラムを開始すると、言語を入力するよう促されます。



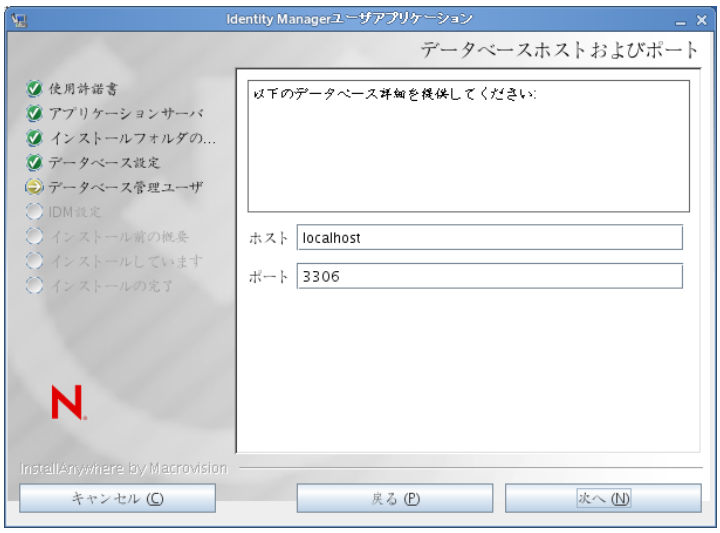
3 言語を選択し、使用許諾契約を確認し、アプリケーションサーバプラットフォームを選択するには、次の情報を使用します。

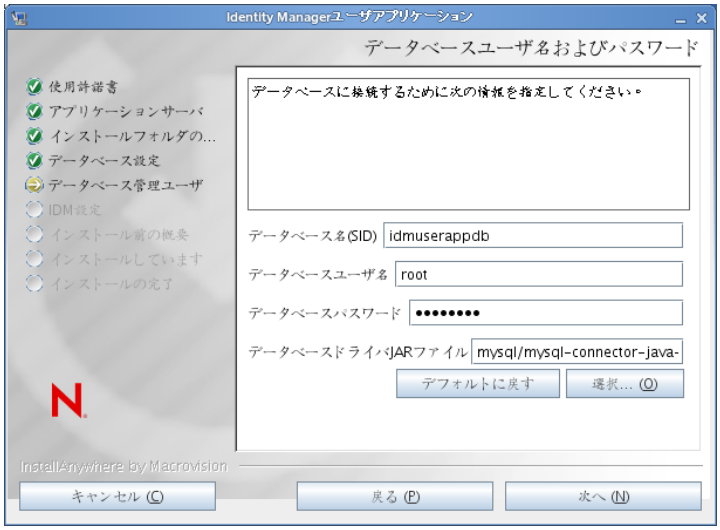
インストール画面	説明
Novell Identity Manager の Roles Based Provisioning Module (RBPM)	インストールプログラムの言語を選択します。デフォルトでは、［英語］が選択されています。
使用許諾契約	使用許諾契約を読み、［*使用許諾契約の条件に同意します*］を選択します。

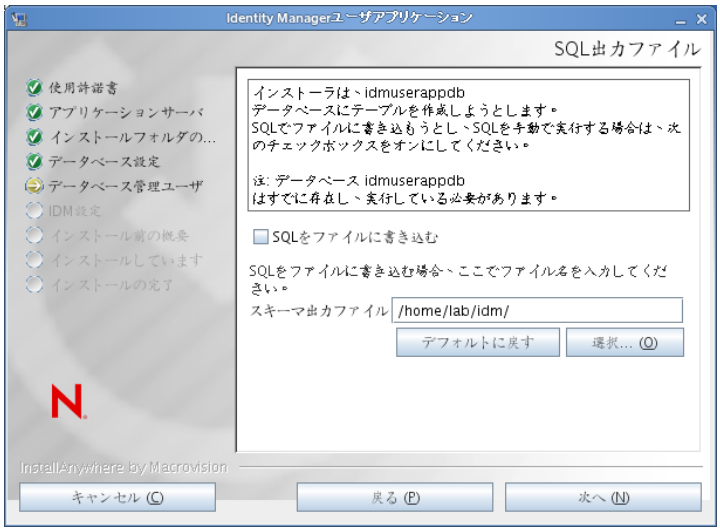
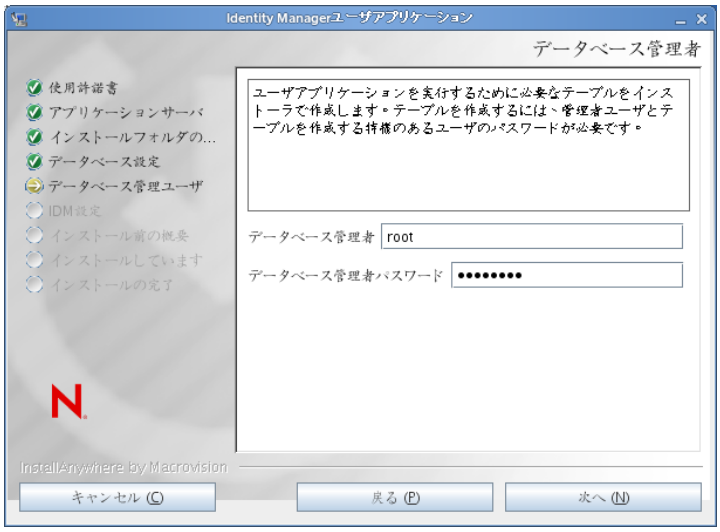
インストール画面	説明
アプリケーションサーバプラットフォーム	*WebSphere* を選択します。 ユーザアプリケーションの WAR ファイルがインストーラとは別のディレクトリにある場合は、インストーラによって WAR へのパスを入力するようメッセージが表示されます。 WAR がデフォルトの場所にある場合は、*[デフォルトのファイルに戻す]* をクリックできます。または、WAR ファイルの場所を指定する場合は、*[選択]* をクリックして場所を選択します。 WebSphere でインストールする場合、IBM Java 環境を使用することによってインストールプログラムを開始する必要があります。アプリケーションサーバとして WebSphere を選択し、インストールの開始に IBM の Java を使用しない場合、次のポップアップエラーメッセージが表示され、インストールは終了します。 

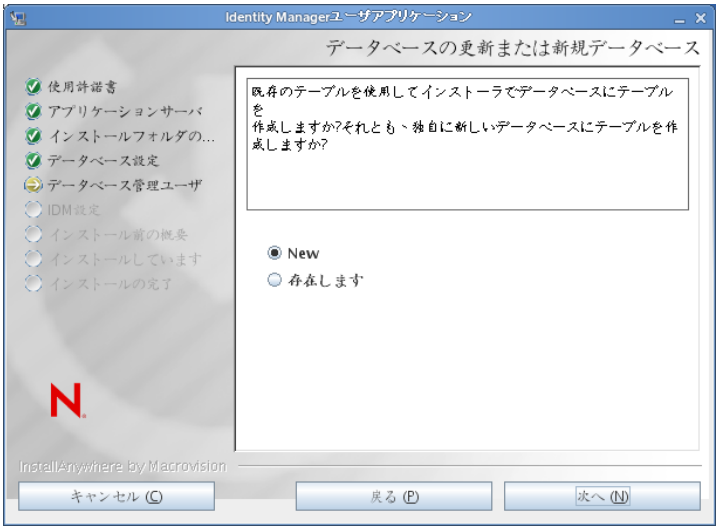
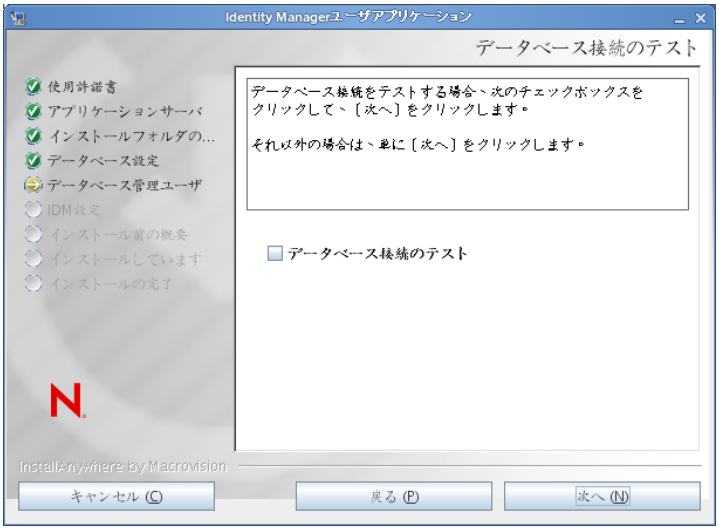
4 次の情報を使用して、インストールタイプを選択し、インストールフォルダを指定し、データベースを設定します。

インストール画面	説明
インストールのタイプ	*Roles Based Provisioning*: Roles Based Provisioning Module をインストールするには、このオプションを選択します。これはこのリリースでのみサポートされているインストールタイプです。
インストールフォルダの選択	インストーラがファイルを配置する場所を指定します。
データベースプラットフォーム	データベースプラットフォームを選択します。データベースおよび JDBC ドライバはすでにインストールされている必要があります。WebSphere の場合、オプションには次のプラットフォームが含まれます。 ◆ MySQL ◆ Oracle (Oracle 10g および 11g のみサポート。Oracle 9i はサポートされなくなりました。) ◆ Microsoft SQL Server ◆ IBM DB2 (バージョン 9.5 のみサポート。バージョン 9.1 はサポートされなくなりました。)

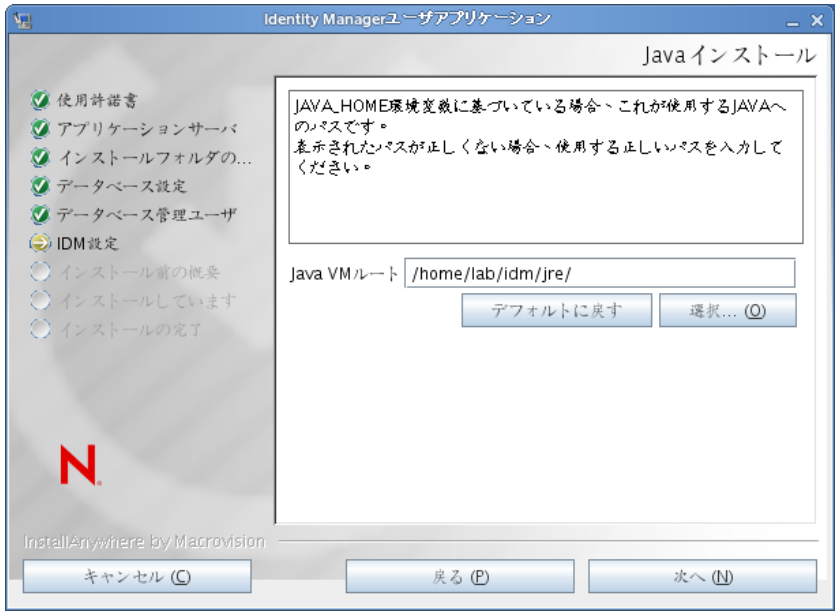
インストール画面	説明
データベースホストおよびポート	*ホスト*: データベースサーバのホスト名または IP アドレスを指定します。クラスタでは、クラスタの各メンバーには同じホスト名または IP アドレスを指定します。 *ポート*: データベースのリスナポート番号を指定します。クラスタの場合は、クラスタの各メンバーに同じポートを指定します。 

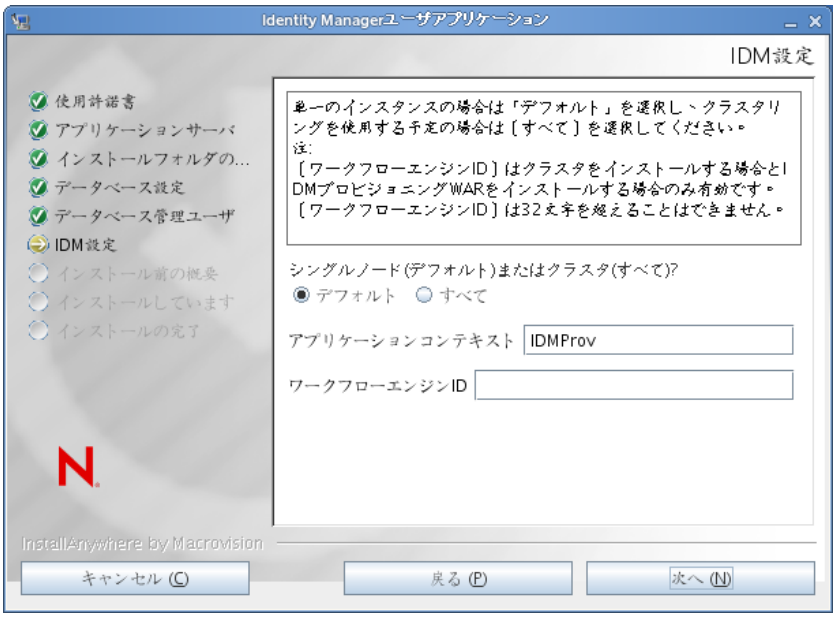
インストール画面	説明
データベースのユーザ名およびパスワード	*データベース名* (または SID): MySQL、MS SQL Server、または PostgreSQL では、事前に設定したデータベース名を入力します。Oracle の場合は、前に作成した Oracle システム ID (SID) を指定します。クラスタでは、クラスタの各メンバーには同じデータベース名または SID を指定します。 *データベースユーザ名* : データベースユーザを指定します。クラスタでは、クラスタの各メンバーには同じデータベースユーザを指定します。 *データベースパスワード*: データベースパスワードを指定します。クラスタでは、クラスタの各メンバーには同じデータベースパスワードを指定します。 *データベースドライバ JAR ファイル* : データベースサーバにシンクライアント JAR を指定します。これは必須です。 **重要 :** *[データベースドライバ JAR ファイル]* フィールドのブラウズボタンによってのみ、1 つの jar を選択できます。DB2 の場合、2 つの jar を指定する必要があります。 ◆ db2jcc.jar ◆ db2jcc_license_cu.jar したがって、1 つの jar を選択できますが、インストールプログラムが実行中のオペレーティングシステムの正しいファイル区切り文字を使用して 2 番目のものを手動で入力する必要があります。または、両方のエントリを手動で入力することもできます。 Windows の場合の例 : `c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar` Solaris および Linux の場合の例 : `/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar` 

インストール画面	説明
SQL 出力ファイル	このリリースでは、アプリケーションサーバの起動時 (以前のリリースのように) ではなく、ユーザアプリケーションのインストール時にデータベーステーブルが作成できます。 SQL 出力ファイル画面では、スキーマファイルを作成するためのオプションを指定します。データベース管理者は、インストールプログラムでテーブルを作成する代わりに、スキーマファイルを使用してテーブルを作成できます。 スキーマファイルを作成する場合、*[SQL をファイルに書き込む]* チェックボックスをオンにし、*[スキーマ出力ファイル]* フィールドにファイルの名前を入力します。 
データベース管理者	この画面には、[データベースユーザ名およびパスワード] ページから同じユーザ名とパスワードが事前に入力されています。以前に指定したデータベースユーザがデータベースサーバ内にテーブルを作成するための十分な許可を持っていない場合、必要な権限を持つ別のユーザ ID を入力する必要があります。 

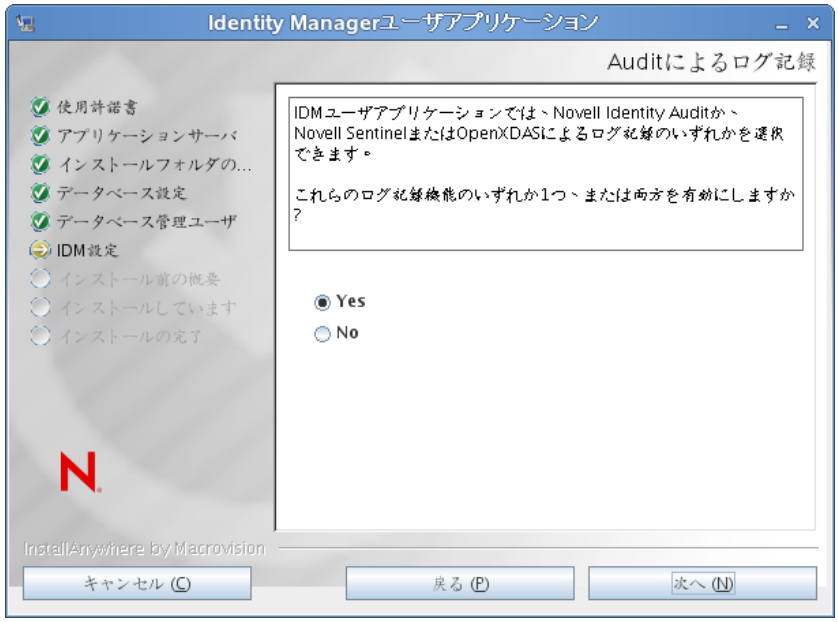
インストール画面	説明
データベースの更新または新規データベース	使用するデータベースが新規または空の場合、*[新規]* ボタンを選択します。データベースが以前のインストールからの既存のものである場合、*[存在します]* ボタンを選択します。 
データベース接続のテスト	前の画面で指定した情報が正しかったことを確認するには、*[データベース接続のテスト]* チェックボックスをオンにしてデータベース接続をテストします。 

5 Java、IDM、監査設定およびセキュリティを設定するには、次の情報を使用します。

インストール画面	説明
Java のインストール	Java ルートのインストールフォルダを指定します。Java インストールでは JAVA_HOME 環境変数に基づいて Java へのパスが表示され、それを修正するオプションを選択できます。  この時点で、インストールプログラムは、選択した Java が、選択したアプリケーションサーバに対して正しいものであることも確認します。また、指定されている JRE で CA 証明書に書き込めることも確認します。

インストール画面	説明
IDM 環境設定	アプリケーションサーバ設定のタイプを選択します。 ◆ このインストールが、クラスタの一部でない 1 つのノード上の場合は、*[デフォルト]* を選択します。 ［*デフォルト*］を選択し、クラスタを後で必要とすると判断した場合は、ユーザアプリケーションを再インストールする必要があります。 ◆ このインストールがクラスタの一部の場合は、*[すべて]* を選択します。 *アプリケーションコンテキスト*: アプリケーションサーバの環境設定の名前、アプリケーション WAR ファイルの名前、および URL コンテキストの名前です。インストールスクリプトによってサーバの環境設定が作成され、デフォルト名で *アプリケーション名*に基づく環境設定が作成されます。ユーザアプリケーションをブラウザから開始する場合は、アプリケーション名を書き留め、アプリケーション名を URL に含めてください。 

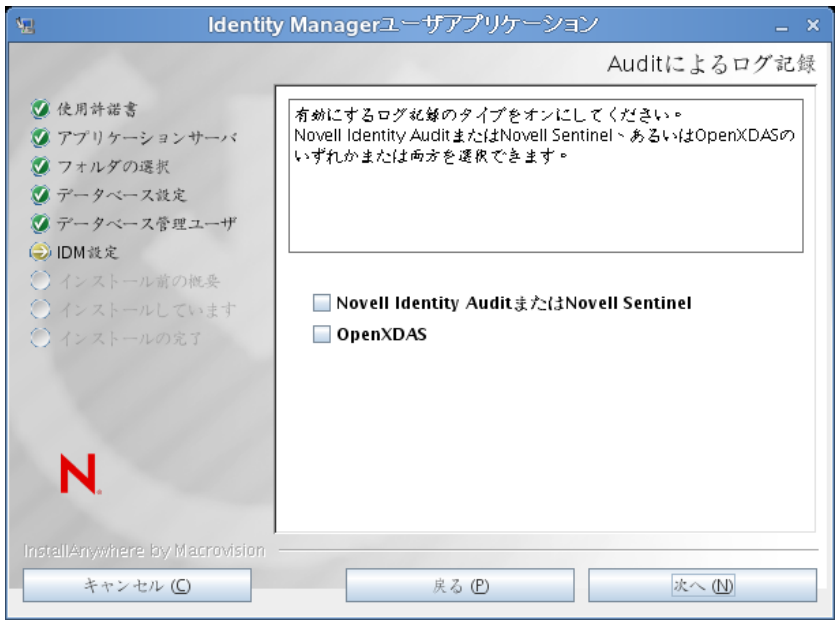
インストール画面	説明
Audit のログ	ログを有効にするには、［*はい*］をクリックします。ログを無効にするには、*［いいえ］*をクリックします。



次のパネルでは、ログのタイプを指定するよう促されます。次のオプションから選択します。

- *Novell Identity Audit または Novell Sentinel*: Novell® Audit がユーザアプリケーションのログを有効にします。
- *OpenXDAS*: OpenXDAS ログサーバにイベントが記録されます。

ログの設定の詳細については、『*ユーザアプリケーション : 管理ガイド*』を参照してください。



インストール画面	説明
Novell Audit	*サーバ*: ログを有効にする場合、サーバのホスト名または IP アドレスを指定します。ログをオフにする場合は、この値は無視されます。 *ログキャッシュフォルダ*: ログキャッシュのディレクトリを指定します。
セキュリティ - マスタキー	*はい*: 既存のマスタキーをインポートできます。既存の暗号化マスタキーをインポートするよう選択した場合は、該当するキーを切り取ってインストール手順のウィンドウに貼り付けます。 *いいえ*: 新規のマスタキーを作成します。インストール終了後、115 ページのセクション 9.1「マスタキーの記録」で示すように、マスタキーを手動で記録します。 インストール手順で、インストールディレクトリにある master-key.txt ファイルに暗号化マスタキーが書き込まれます。 既存のマスタキーをインポートする理由には、次のようなものがあります。 ◆ インストールファイルをステージングシステムから運用システムに移動中で、ステージングシステムで使用したデータベースへのアクセスを保持する場合。 ◆ ユーザアプリケーションを最初のクラスタのメンバーにインストールしており、現在はクラスタの次のメンバーにインストールしている場合 (同じマスタキーが必要)。 ◆ ディスク故障のため、ユーザアプリケーションを復元する必要がある場合。ユーザアプリケーションを再インストールして、以前のインストールで使用したのと同じ暗号化マスタキーを指定する必要があります。これによって、前に保存した暗号化データにアクセスできます。

6 *[次へ]* をクリックして、[役割ベースプロビジョニングモジュール環境設定] パネルを表示します。(この情報の入力を求められない場合、29 ページのセクション 2.5「Java Development Kit のインストール」で説明したステップを完了していない可能性があります。)

[役割ベースプロビジョニングモジュール環境設定] パネルのデフォルトのビューでは、これらの 6 つのフィールドが表示されます。

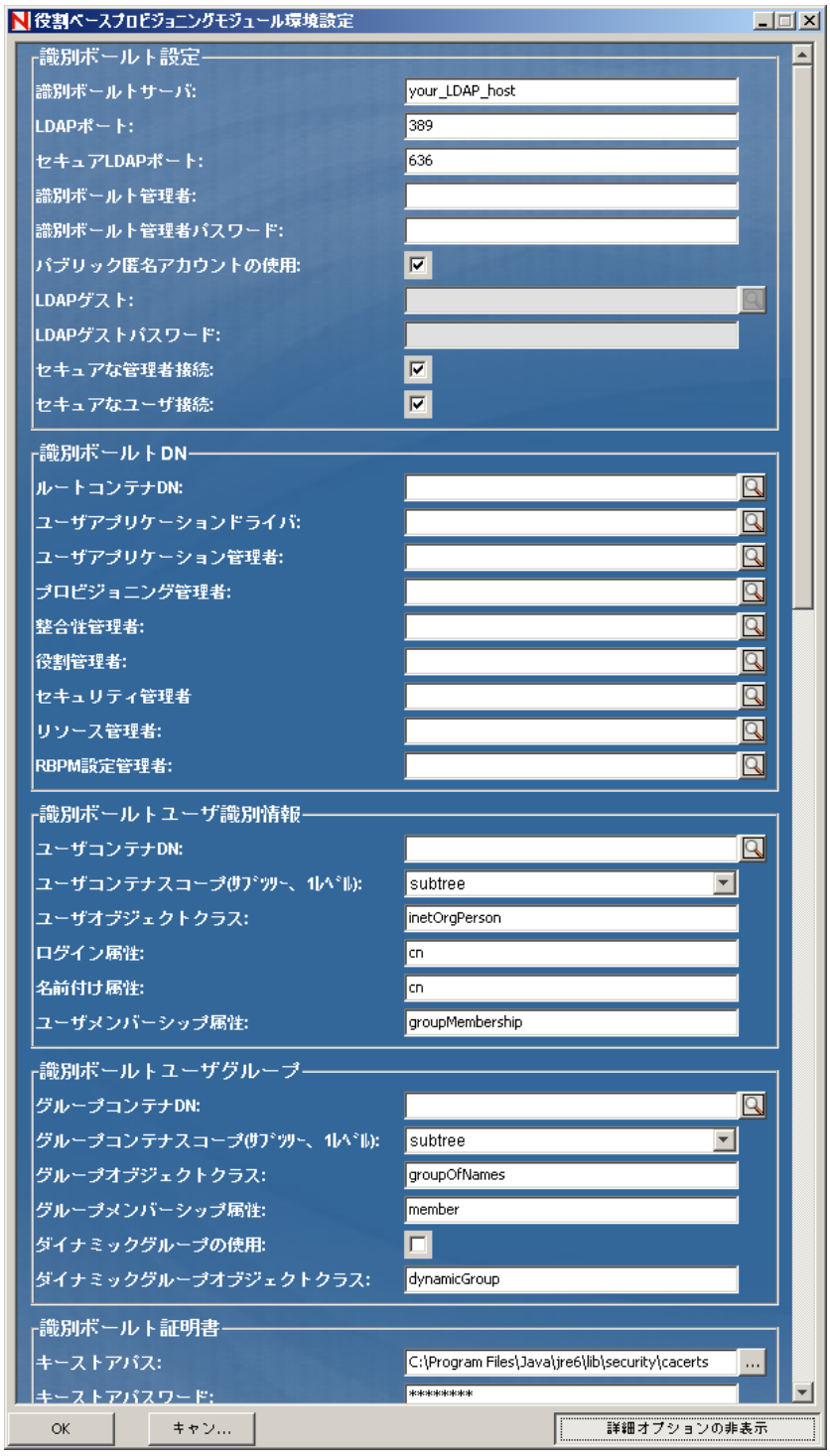
インストールプログラムはルートコンテナ DN から値を取得し、それを次の値に適用します。

- ユーザコンテナ DN
- グループコンテナ DN

インストールプログラムはユーザアプリケーション管理者フィールドから値を取得し、それを次の値に適用します。

- プロビジョニング管理者
- コンプライアンス管理者
- 役割管理者
- セキュリティ管理者
- リソース管理者
- RBPM 設定管理者

これらの値を明示的に指定する場合、*[詳細オプションの表示]* ボタンをクリックしてそれらを変更できます。


役割ベースプロビジョニングモジュール環境設定
識別ボールト設定
識別ボールトサーバ:
your_LDAP_host
LDAPポート:
389
セキュアLDAPポート:
636
識別ボールト管理者:
識別ボールト管理者パスワード:
パブリック匿名アカウントの使用:
LDAPゲスト:
LDAPゲストパスワード:
セキュアな管理者接続:
セキュアなユーザ接続:
識別ボールトDN
ルートコンテナDN:
ユーザアプリケーションドライバ:
ユーザアプリケーション管理者:
プロビジョニング管理者:
整合性管理者:
役割管理者:
セキュリティ管理者
リソース管理者:
RBPM設定管理者:
識別ボールトユーザ識別情報
ユーザコンテナDN:
ユーザコンテナスコープ(サブツリー、1レベル):
subtree
ユーザオブジェクトクラス:
inetOrgPerson
ログイン属性:
cn
名前付け属性:
cn
ユーザメンバーシップ属性:
groupMembership
識別ボールトユーザグループ
グループコンテナDN:
グループコンテナスコープ(サブツリー、1レベル):
subtree
グループオブジェクトクラス:
groupOfNames
グループメンバーシップ属性:
member
ダイナミックグループの使用:
ダイナミックグループオブジェクトクラス:
dynamicGroup
識別ボールト証明書
キーストアパス:
C:\Program Files\Java\jre6\lib\security\cacerts
キーストアパスワード:
****
OK
キャン...
詳細オプションの非表示

7 インストールを完了するには、次の情報を使用します。

インストール画面	説明
ユーザアプリケーション環境設定	ユーザアプリケーションをインストールすると、ユーザアプリケーション環境設定パラメータを設定できます。インストールすると、これらのパラメータの多くは configupdate.sh または configupdate.bat でも編集可能です。例外はパラメータ説明に記述されています。 クラスタの場合は、クラスタの各メンバーに同じユーザアプリケーション環境設定パラメータを指定します。 各オプションの詳細については、123 ページの付録 A「IDM ユーザアプリケーション環境設定の参照」を参照してください。
インストール前の概要	［インストール前の概要］ページを読んで、インストールパラメータの選択を確認します。 必要に応じて、［*戻る*］を使用して前のインストールページに戻り、インストールパラメータを変更します。 ユーザアプリケーション環境設定ページでは値は保存されないため、インストールの前のページを再指定した後に、ユーザアプリケーション環境設定の値を再入力する必要があります。インストールおよび環境設定パラメータで納得いく設定ができたら、［インストール前の概要］ページに戻り、［*インストール*］をクリックします。
インストールの完了	インストールの終了が示されます。

6.1.1 インストールログファイルの表示

エラーが発生せずにインストールが完了した場合は、81 ページのセクション 6.2.1「ユーザアプリケーション環境設定ファイルと JVM システムプロパティの追加」に進みます。

インストールでエラーまたは警告が発生した場合は、次のようなログファイルを確認して、問題を判断してください。

- Identity_Manager_User_Application_InstallLog.log には、基本的なインストールタスクの結果が格納されています。
- Novell-Custom-Install.log には、インストール中に行ったユーザアプリケーション環境設定についての情報があります。

6.2 WebSphere 環境の環境設定

6.2.1 ユーザアプリケーション環境設定ファイルと JVM システムプロパティの追加

WebSphere を正常にインストールするには、次の手順が必要です。

1. ユーザアプリケーションのインストールディレクトリから、sys-configuration-xmldata.xml ファイルを、WebSphere サーバをホストしているマシン上のディレクトリ (例 : / UserAppConfigFiles) にコピーします。

   ユーザアプリケーションのインストールディレクトリとは、ユーザアプリケーションをインストールしたディレクトリです。

2. JVM システムプロパティで、sys-configuration-xmldata.xml ファイルのパスを設定します。これを行うには、WebSphere 管理コンソールに管理者ユーザとしてログインしてください。
3. 左側のパネルから、*［サーバ］*>*［アプリケーションサーバ］* の順に移動します。
4. サーバリストでサーバ名 (例 : server1) をクリックします。
5. 右側の設定リストで、*［Server Infrastructure］* の下にある *［Java and Process Management］* に移動します。
6. リンクを展開して、*［Process Definition］* を選択します。
7. *［Additional Properties］* リストの下にある *［Java Virtual Machine］* を選択します。
8. ［JVM］ページの *［Additional Properties］* という見出しの下にある *［Custom Properties］* を選択します。
9. *［新規］* をクリックして、新しい JVM システムプロパティを追加します。
   - **9a** *［名前］* には、「extend.local.config.dir」を指定します。
   - **9b** *［値］* には、インストール時に指定したインストールフォルダ (ディレクトリ) の名前を入力します。

     インストーラはこのフォルダに sys-configuration-xmldata.xml ファイルを書き込みます。
   - **9c** *［説明］* には、プロパティの説明 (「sys-configuration-xmldata.xm へのパス」など) を指定します。
   - **9d** *［OK］* をクリックしてプロパティを保存します。
10. *［新規］* をクリックして、別の新しい JVM システムプロパティを追加します。
    - **10a** *［名前］* には、「idmuserapp.logging.config.dir」を指定します。
    - **10b** *［値］* には、インストール時に指定したインストールフォルダ (ディレクトリ) の名前を入力します。
    - **10c** *［説明］* には、プロパティの説明 (「idmuserapp_logging.xml へのパス」など) を指定します。
    - **10d** *［OK］* をクリックしてプロパティを保存します。

      idmuserapp-logging.xml ファイルは *［ユーザアプリケーション］*>*［管理］*>*［アプリケーション環境設定］*>*［ログ］* を使用して変更を保持するまでは存在しません。

6.2.2 WebSphere キーストアへの eDirectory ルート認証局のインポート

1 WebSphere サーバをホストするマシンに、eDirectory™ ルート認証局の証明書をコピーします。

ユーザアプリケーションのインストール手順では、ユーザアプリケーションをインストールするディレクトリに証明書がエクスポートされます。

2 証明書を WebSphere のキーストアにインポートします。この作業は、WebSphere の管理者コンソール (82 ページの 「WebSphere 管理者コンソールを使用した証明書のインポート」) またはコマンドライン (82 ページの 「コマンドラインを使用した証明書のインポート」) を使用して実行できます。

3 証明書をインポートしたら、83 ページのセクション 6.3「WAR ファイルの展開」に進みます。

WebSphere 管理者コンソールを使用した証明書のインポート

1 WebSphere 管理者コンソールに管理者ユーザとしてログインします。

2 左側のパネルから、［*セキュリティ*］>［*SSL Certificate and Key Management*］の順に移動します。

3 右側の設定リストで、［*Additional Properties*］の下にある［*Key stores and certificates*］に移動します。

4 ［*NodeDefaultTrustStore*］(または使用している認証ストア) を選択します。

5 右側の［*Signer Certificates*］の下にある［*Additional Properties*］を選択します。

6 ［*追加*］をクリックします。

7 エイリアス名と証明書ファイルへのフルパスを入力します。

8 ドロップダウンリストでデータタイプを［*Binary DER data*］に変更します。

9 ［*OK*］をクリックします。これで、署名者証明書リストに証明書が表示されます。

コマンドラインを使用した証明書のインポート

WebSphere サーバをホストするマシンのコマンドラインから鍵ツールを実行して、WebSphere キーストアに証明書をインポートします。

注 : WebSphere の鍵ツールを使用しないと、この手順は有効ではありません。また、ストアタイプが PKCS12 であることを確認してください。

WebSphere の鍵ツールは /IBM/WebSphere/AppServer/java/bin にあります。

次に鍵ツールコマンドの例を示します。

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

システム上に複数の trust.p12 ファイルがある場合は、ファイルへのフルパスを指定しなければならないことがあります。

6.3 WAR ファイルの展開

WebSphere 展開ツールを使用して、WAR ファイルを展開します。

6.3.1 WebSphere 6.1 用の追加の環境設定

WebSphere 6.1 を使用している場合は、WAR の展開後に ibm-web-ext.xmi ファイルを更新する必要があります。WAR の展開後、ibm-web-ext.xmi ファイル内の次のようなエントリに似た内容を追加する必要があります。

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

名前は jdkSourceLevel にし、値は 15 にする必要があります。JSPAttribute ID には、_3 以上を使用する必要があります。詳細については、次リンクを参照してください。

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

WAR の展開が完了したら、以下の手順を実行します。

1. WebSphere アプリケーションサーバを停止します。
2. 上記の内容に従って、ibm-web-ext.xmi ファイルを変更します。ファイルの場所は、ご使用の IBM のドキュメントに指定する必要があります。たとえば、ファイルは次の場所にあることが考えられます。

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

3. WebSphere アプリケーションサーバを再起動します。

6.4 ユーザアプリケーションの開始およびアクセス

ユーザアプリケーションを起動するには次の処理を行います。

1. WebSphere 管理者コンソールに管理者ユーザとしてログインします。
2. 左側のナビゲーションパネルで、*［アプリケーション］＞［エンタープライズアプリケーション］* の順に移動します。
3. 起動するアプリケーションの横にあるチェックボックスをオンにし、［*起動*］をクリックします。

   起動すると、［*Application status*］カラムに緑色の矢印が表示されます。

ユーザアプリケーションへのアクセス方法

1 展開中に指定したコンテキストを使用してポータルにアクセスします。

WebSphere 上の Web コンテナのデフォルトポートは 9080 です。または、セキュアポートの場合は 9443 です。URL のフォーマットは次のとおりです。http://<*server*>:9080/IDMProv

WebLogic でのユーザアプリケーションのインストール

7

WebLogic インストーラでは、入力内容に基づいてユーザアプリケーション WAR が環境設定されます。このセクションでは次の内容を説明します。

- 85 ページのセクション 7.1「WebLogic インストールチェックリスト」
- 86 ページのセクション 7.2「ユーザアプリケーション WAR のインストールおよび環境設定」
- 98 ページのセクション 7.3「WebLogic 環境の準備」
- 100 ページのセクション 7.4「ユーザアプリケーション WAR の展開」
- 101 ページのセクション 7.5「ユーザアプリケーションへのアクセス」

ユーザグラフィカルインタフェース以外を使用したインストールの方法については、103 ページの第 8 章「コンソールまたは単一コマンドによるインストール」を参照してください。.

ルート以外のユーザとしてインストーラを実行します。

データマイグレーション 移行の詳細については、『*ユーザアプリケーション：マイグレーションガイド* (http://www.novell.com/documentation/idmrbpm37/index.html)』を参照してください。

7.1 WebLogic インストールチェックリスト

- ❑ WebLogic のインストール

  WebLogic マニュアルのインストール手順に従います。

- ❑ WebLogic が有効な WAR を作成します。

  Identity Manager ユーザアプリケーションインストーラを使用してこのタスクを実行します。詳細については、86 ページのセクション 7.2「ユーザアプリケーション WAR のインストールおよび環境設定」を参照してください。

- ❑ WAR を展開するためには、環境設定ファイルを適切な WebLogic ロケーションにコピーして WebLogic 環境を準備します。

  詳細については、98 ページのセクション 7.3「WebLogic 環境の準備」を参照してください。

- ❑ WAR を展開します。

  詳細については、100 ページのセクション 7.4「ユーザアプリケーション WAR の展開」を参照してください。

7.2 ユーザアプリケーション WAR のインストールおよび環境設定

注 : WebLogic 10.3 の場合、インストールプログラムには、JRockit から提供されている Java 2 Platform Standard Edition Development Kit バージョン 1.6 JDK が必要です。別のバージョンを使用した場合、このインストール手順ではユーザアプリケーション WAR ファイルは正しく設定されません。インストールは成功したかのように見えますが、ユーザアプリケーションの起動を試みるとエラーが発生します。

1 インストールファイルが含まれるディレクトリに移動します。

2 JRockit Java 環境を使用して、コマンドラインから次のプラットフォームのインストーラを開始します。

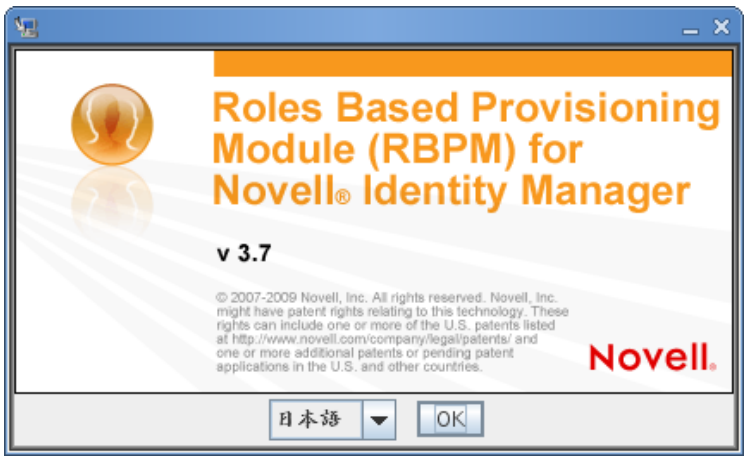
Solaris

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

Windows

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

インストールプログラムを開始すると、言語を入力するよう促されます。



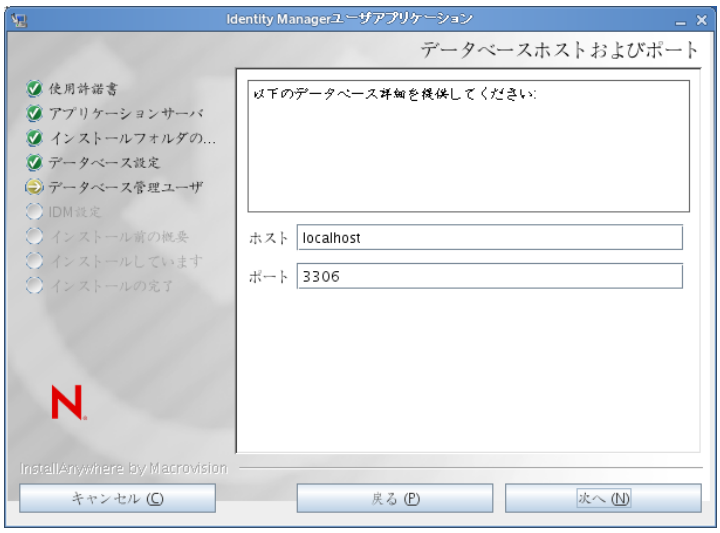
3 言語を選択し、使用許諾契約を確認し、アプリケーションサーバプラットフォームを選択するには、次の情報を使用します。

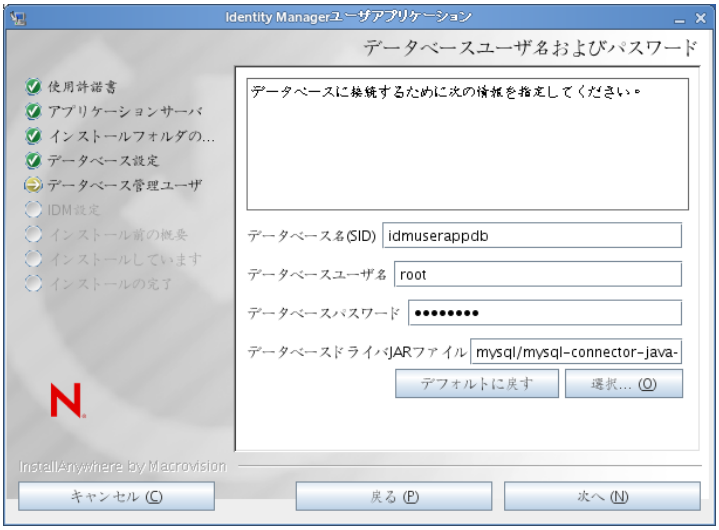
インストール画面	説明
Novell Identity Manager の Roles Based Provisioning Module (RBPM)	インストールプログラムの言語を選択します。デフォルトでは、［英語］が選択されています。
使用許諾契約	使用許諾契約を読み、［*使用許諾契約の条件に同意します*］を選択します。

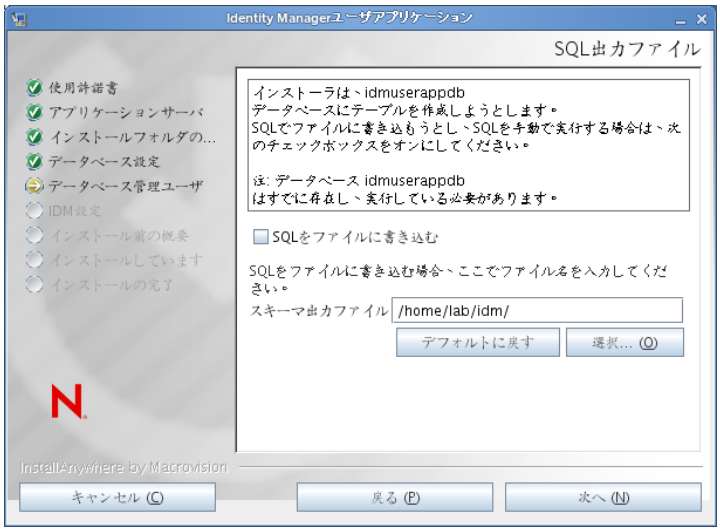
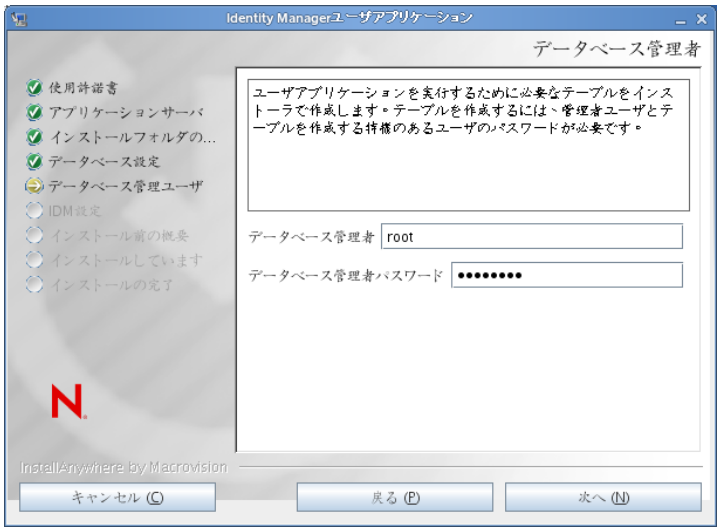
インストール画面	説明
アプリケーションサーバプラットフォーム	*[WebLogic]* を選択します。 ユーザアプリケーションの WAR ファイルがインストーラとは別のディレクトリにある場合は、インストーラによって WAR へのパスを入力するようメッセージが表示されます。 WAR がデフォルトの場所にある場合は、*[デフォルトのファイルに戻す]* をクリックできます。または、WAR ファイルの場所を指定する場合は、*[選択]* をクリックして場所を選択します。 WebLogic でインストールする場合、BEA の Java 環境 (jrockit) を使用することによってインストールプログラムを開始する必要があります。アプリケーションサーバとして WebLogic を選択し、インストールの開始に jrockit を使用しない場合、次のポップアップエラーメッセージが表示され、インストールは終了します。 

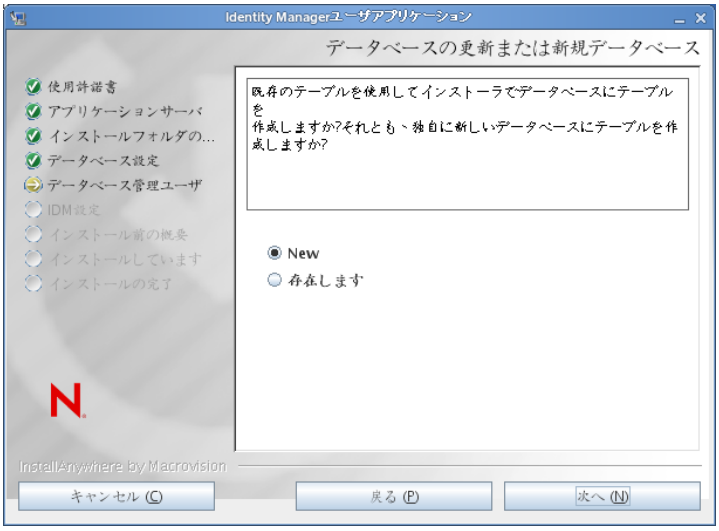
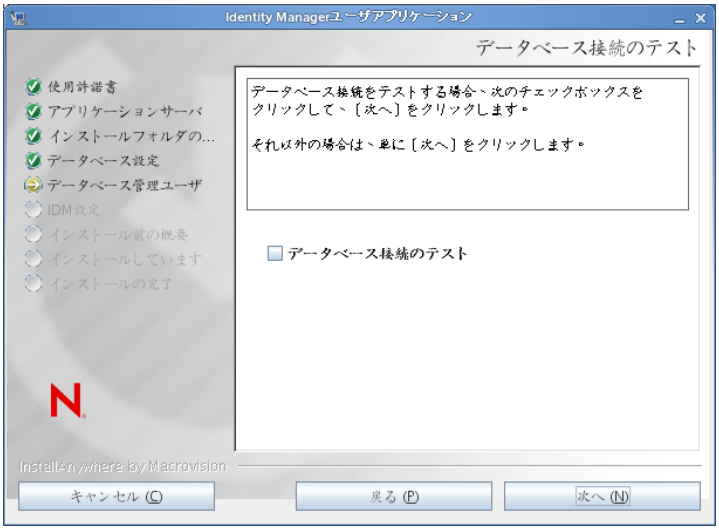
4 次の情報を使用して、インストールタイプを選択し、インストールフォルダを指定し、データベースを設定します。

インストール画面	説明
インストールのタイプ	*Roles Based Provisioning*: Roles Based Provisioning Module をインストールするには、このオプションを選択します。これはこのリリースでのみサポートされているインストールタイプです。
インストールフォルダの選択	インストーラがファイルを配置する場所を指定します。
データベースプラットフォーム	データベースプラットフォームを選択します。データベースおよび JDBC ドライバはすでにインストールされている必要があります。WebLogic の場合、オプションには次のプラットフォームが含まれます。 ◆ Oracle (Oracle 10g および 11g のみサポート。Oracle 9i はサポートされなくなりました。) ◆ Microsoft SQL Server

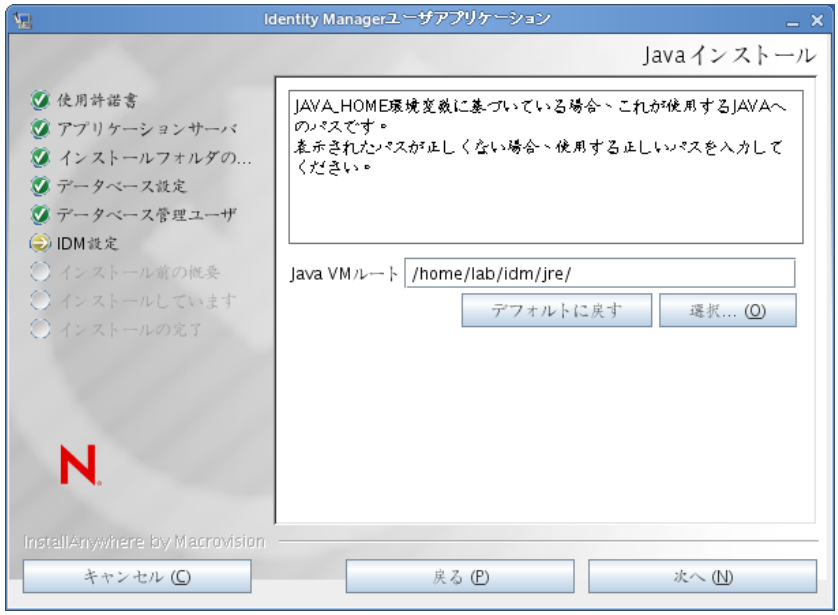
インストール画面	説明
データベースホストおよびポート	*ホスト*: データベースサーバのホスト名または IP アドレスを指定します。クラスタでは、クラスタの各メンバーには同じホスト名または IP アドレスを指定します。 *ポート*: データベースのリスナポート番号を指定します。クラスタの場合は、クラスタの各メンバーに同じポートを指定します。 

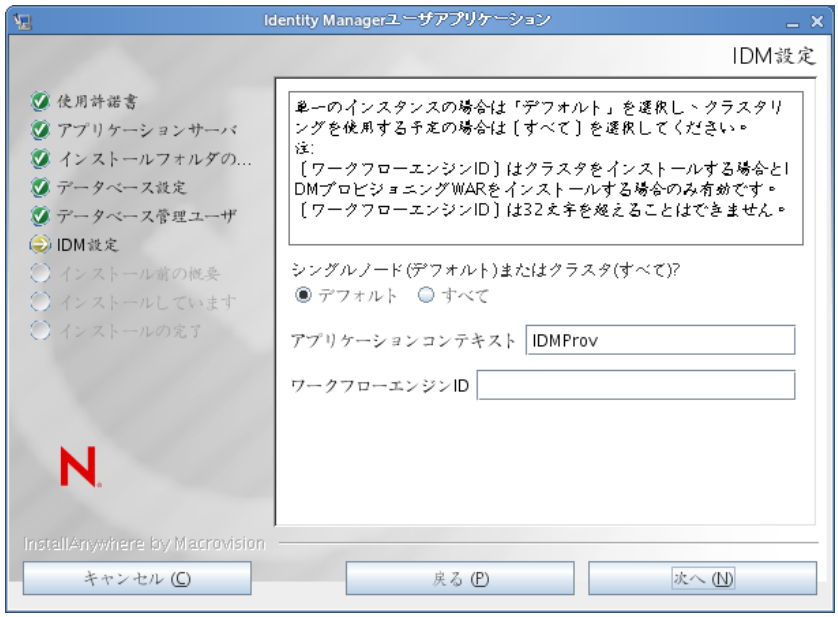
インストール画面	説明
データベースのユーザ名およびパスワード	*データベース名* (または SID): MySQL、MS SQL Server、または PostgreSQL では、事前に設定したデータベース名を入力します。Oracle の場合は、前に作成した Oracle システム ID (SID) を指定します。クラスタでは、クラスタの各メンバーには同じデータベース名または SID を指定します。 *データベースユーザ名* : データベースユーザを指定します。クラスタでは、クラスタの各メンバーには同じデータベースユーザを指定します。 *データベースパスワード*: データベースパスワードを指定します。クラスタでは、クラスタの各メンバーには同じデータベースパスワードを指定します。 *データベースドライバ JAR ファイル* : データベースサーバにシンクライアント JAR を指定します。これは必須です。 

インストール画面	説明
SQL 出力ファイル	このリリースでは、アプリケーションサーバの起動時 (以前のリリースのように) ではなく、ユーザアプリケーションのインストール時にデータベーステーブルが作成できます。 SQL 出力ファイル画面では、スキーマファイルを作成するためのオプションを指定します。データベース管理者は、インストールプログラムでテーブルを作成する代わりに、スキーマファイルを使用してテーブルを作成できます。 スキーマファイルを作成する場合、*[SQL をファイルに書き込む]* チェックボックスをオンにし、*[スキーマ出力ファイル]* フィールドにファイルの名前を入力します。 
データベース管理者	この画面には、[データベースユーザ名およびパスワード] ページから同じユーザ名とパスワードが事前に入力されています。以前に指定したデータベースユーザがデータベースサーバ内にテーブルを作成するための十分な許可を持っていない場合、必要な権限を持つ別のユーザ ID を入力する必要があります。 

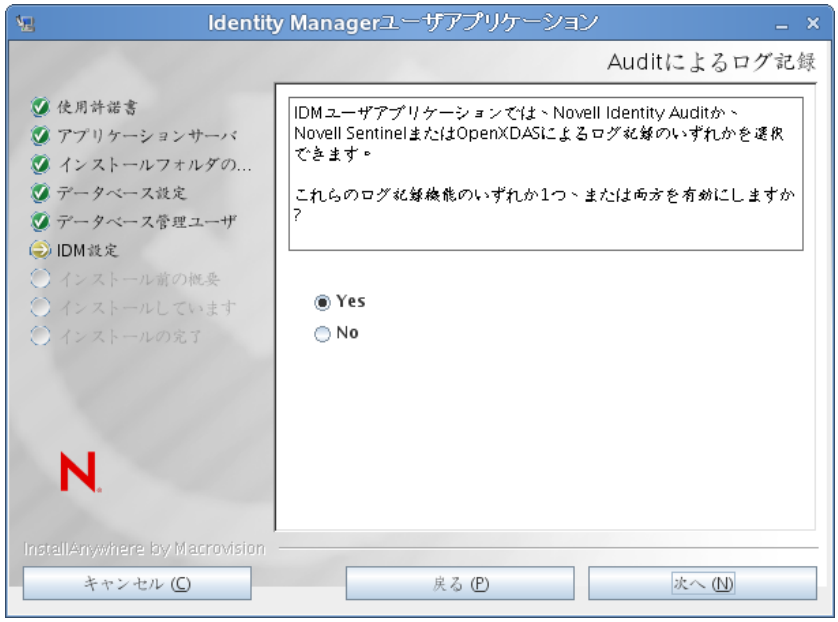
インストール画面	説明
データベースの更新または新規データベース	使用するデータベースが新規または空の場合、*[新規]* ボタンを選択します。データベースが以前のインストールからの既存のものである場合、*[存在します]* ボタンを選択します。 
データベース接続のテスト	前の画面で指定した情報が正しかったことを確認するには、*[データベース接続のテスト]* チェックボックスをオンにしてデータベース接続をテストします。 

5 Java、IDM、監査設定およびセキュリティを設定するには、次の情報を使用します。

インストール画面	説明
Java のインストール	Java ルートのインストールフォルダを指定します。Java インストールでは JAVA_HOME 環境変数に基づいて Java へのパスが表示され、それを修正するオプションを選択できます。  この時点で、インストールプログラムは、選択した Java が、選択したアプリケーションサーバに対して正しいものであることも確認します。また、指定されている JRE で CA 証明書に書き込めることも確認します。

インストール画面	説明
IDM 環境設定	アプリケーションサーバ設定のタイプを選択します。 ◆ このインストールが、クラスタの一部でない 1 つのノード上の場合は、*[デフォルト]* を選択します。 ［*デフォルト*］を選択し、クラスタを後で必要とすると判断した場合は、ユーザアプリケーションを再インストールする必要があります。 ◆ このインストールがクラスタの一部の場合は、*[すべて]* を選択します。 *アプリケーションコンテキスト*: アプリケーションサーバの環境設定の名前、アプリケーション WAR ファイルの名前、および URL コンテキストの名前です。インストールスクリプトによってサーバの環境設定が作成され、デフォルト名で *アプリケーション名*に基づく環境設定が作成されます。ユーザアプリケーションをブラウザから開始する場合は、アプリケーション名を書き留め、アプリケーション名を URL に含めてください。 

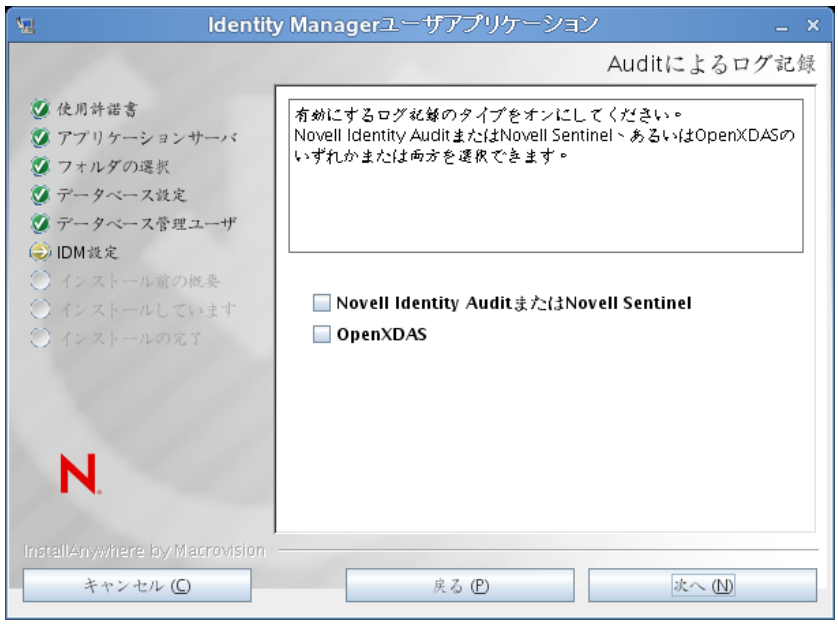
インストール画面	説明
Audit のログ	ログを有効にするには、［*はい*］をクリックします。ログを無効にするには、*［いいえ］*をクリックします。



次のパネルでは、ログのタイプを指定するよう促されます。次のオプションから選択します。

- *Novell Identity Audit または Novell Sentinel*: Novell 監査クライアントを使用してユーザアプリケーションでログを有効にします。
- *OpenXDAS*: OpenXDAS ログサーバにイベントが記録されます。

ログの設定の詳細については、『*ユーザアプリケーション : 管理ガイド*』を参照してください。



インストール画面	説明
Novell Audit	*サーバ*: ログを有効にする場合、サーバのホスト名または IP アドレスを指定します。ログをオフにする場合は、この値は無視されます。 *ログキャッシュフォルダ*: ログキャッシュのディレクトリを指定します。
セキュリティ - マスタキー	*はい*: 既存のマスタキーをインポートできます。既存の暗号化マスタキーをインポートするよう選択した場合は、該当するキーを切り取ってインストール手順のウィンドウに貼り付けます。 *いいえ*: 新規のマスタキーを作成します。インストール終了後、115 ページのセクション 9.1「マスタキーの記録」で示すように、マスタキーを手動で記録します。 インストール手順で、インストールディレクトリにある master-key.txt ファイルに暗号化マスタキーが書き込まれます。 既存のマスタキーをインポートする理由には、次のようなものがあります。 ◆ インストールファイルをステージングシステムから運用システムに移動中で、ステージングシステムで使用したデータベースへのアクセスを保持する場合。 ◆ ユーザアプリケーションを最初のクラスタのメンバーにインストールしており、現在はクラスタの次のメンバーにインストールしている場合 (同じマスタキーが必要)。 ◆ ディスク故障のため、ユーザアプリケーションを復元する必要がある場合。ユーザアプリケーションを再インストールして、以前のインストールで使用したのと同じ暗号化マスタキーを指定する必要があります。これによって、前に保存した暗号化データにアクセスできます。

6 *[次へ]* をクリックして、[役割ベースプロビジョニングモジュール環境設定] パネルを表示します。(この情報の入力を求められない場合、29 ページのセクション 2.5「Java Development Kit のインストール」で説明したステップを完了していない可能性があります。)

[役割ベースプロビジョニングモジュール環境設定] パネルのデフォルトのビューでは、これらの 6 つのフィールドが表示されます。

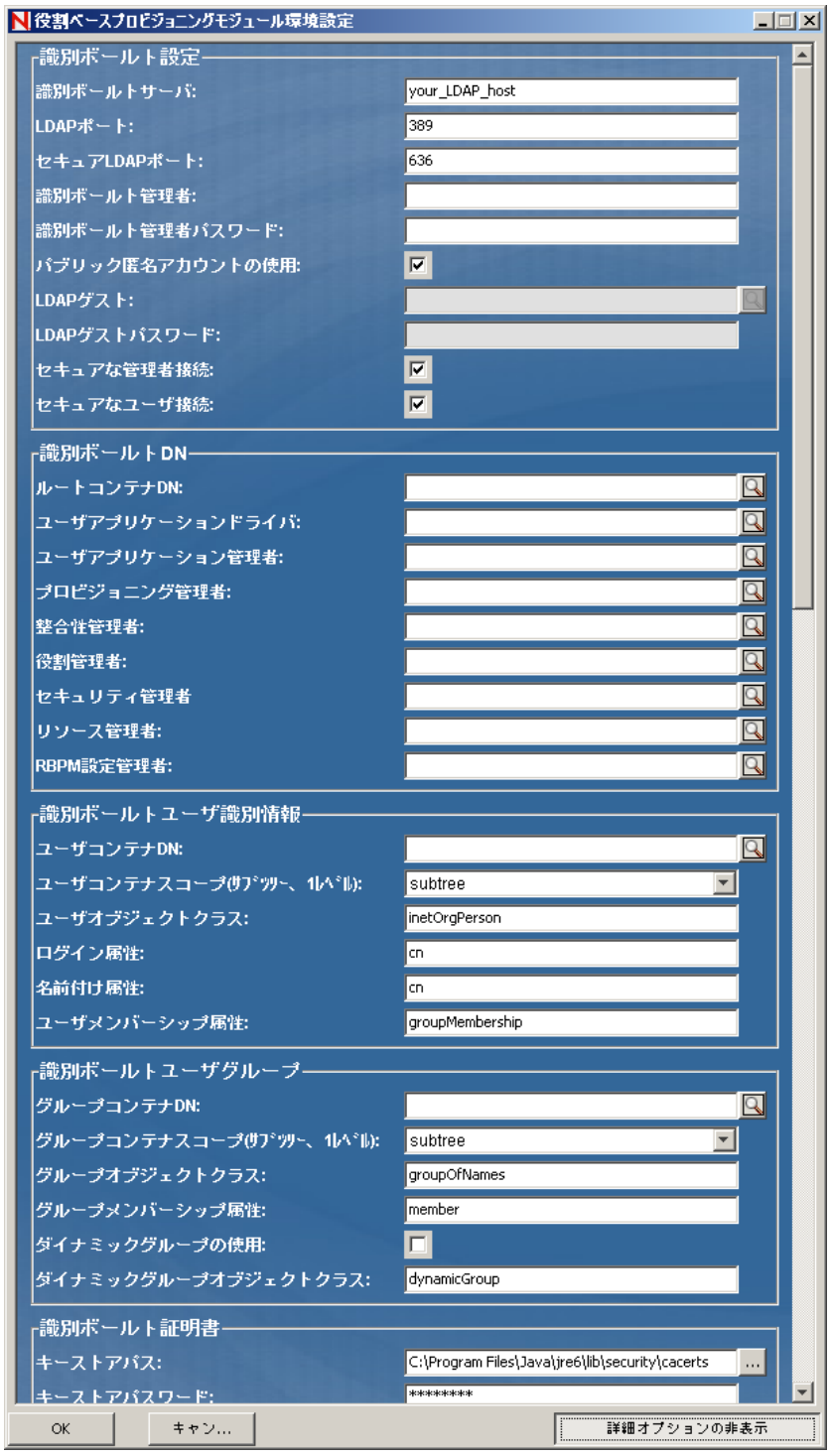
インストールプログラムはルートコンテナ DN から値を取得し、それを次の値に適用します。

- ユーザコンテナ DN
- グループコンテナ DN

インストールプログラムはユーザアプリケーション管理者フィールドから値を取得し、それを次の値に適用します。

- プロビジョニング管理者
- コンプライアンス管理者
- 役割管理者
- セキュリティ管理者
- リソース管理者
- RBPM 設定管理者

これらの値を明示的に指定する場合、*[詳細オプションの表示]* ボタンをクリックしてそれらを変更できます。


役割ベースプロビジョニングモジュール環境設定
識別ボールト設定
識別ボールトサーバ:
your_LDAP_host
LDAPポート:
389
セキュアLDAPポート:
636
識別ボールト管理者:
識別ボールト管理者パスワード:
パブリック匿名アカウントの使用:
LDAPゲスト:
LDAPゲストパスワード:
セキュアな管理者接続:
セキュアなユーザ接続:
識別ボールトDN
ルートコンテナDN:
ユーザアプリケーションドライバ:
ユーザアプリケーション管理者:
プロビジョニング管理者:
整合性管理者:
役割管理者:
セキュリティ管理者
リソース管理者:
RBPM設定管理者:
識別ボールトユーザ識別情報
ユーザコンテナDN:
ユーザコンテナスコープ(サブツリー、1レベル):
subtree
ユーザオブジェクトクラス:
inetOrgPerson
ログイン属性:
cn
名前付け属性:
cn
ユーザメンバーシップ属性:
groupMembership
識別ボールトユーザグループ
グループコンテナDN:
グループコンテナスコープ(サブツリー、1レベル):
subtree
グループオブジェクトクラス:
groupOfNames
グループメンバーシップ属性:
member
ダイナミックグループの使用:
ダイナミックグループオブジェクトクラス:
dynamicGroup
識別ボールト証明書
キーストアパス:
C:\Program Files\Java\jre6\lib\security\cacerts
キーストアパスワード:
****
OK
キャン...
詳細オプションの非表示

7 インストールを完了するには、次の情報を使用します。

インストール画面	説明
ユーザアプリケーション環境設定	ユーザアプリケーションをインストールすると、ユーザアプリケーション環境設定パラメータを設定できます。インストールすると、これらのパラメータの多くは configupdate.sh または configupdate.bat でも編集可能です。例外はパラメータ説明に記述されています。 クラスタの場合は、クラスタの各メンバーに同じユーザアプリケーション環境設定パラメータを指定します。 各オプションの詳細については、123 ページの付録 A「IDM ユーザアプリケーション環境設定の参照」を参照してください。
インストール前の概要	［インストール前の概要］ページを読んで、インストールパラメータの選択を確認します。 必要に応じて、［*戻る*］を使用して前のインストールページに戻り、インストールパラメータを変更します。 ユーザアプリケーション環境設定ページでは値は保存されないため、インストールの前のページを再指定した後に、ユーザアプリケーション環境設定の値を再入力する必要があります。インストールおよび環境設定パラメータで納得いく設定ができたら、［インストール前の概要］ページに戻り、［*インストール*］をクリックします。
インストールの完了	インストールの終了が示されます。

7.2.1 インストールとログファイルの表示

インストールがエラーなしで完了した場合は、WebLogic 環境の準備に進みます。インストールでエラーまたは警告が発生した場合は、次のようなログファイルを確認して、問題を判断してください。

- Identity_Manager_User_Application_InstallLog.log には、基本的なインストールタスクの結果が格納されています。
- Novell-Custom-Install.log には、インストール中に行ったユーザアプリケーション環境設定についての情報があります。

7.3 WebLogic 環境の準備

- 98 ページのセクション 7.3.1「接続プールの環境設定」
- 99 ページのセクション 7.3.2「RBPM 設定ファイルの場所の指定」
- 100 ページのセクション 7.3.3「ワークフロープラグインと WebLogic セットアップ」

7.3.1 接続プールの環境設定

❑ ユーザアプリケーションを展開するドメインに、データベースドライバ JAR ファイルをコピーします。

- ユーザアプリケーションインストールディレクトリからドメイン lib フォルダ (たとえば、c:\bea\user_projects\domains\idm\lib\) へ、antlr-2.7.6.jar および log4j.jar をコピーします。また、commons-logging.jar を c:\bea\tools\eclipse フォルダからドメイン lib フォルダへコピーします。
- データソースを作成します。

  WebLogic マニュアルのデータソース作成の指示に従います。

  ユーザアプリケーション WAR の作成時にデータソースまたはデータベースにどの名前を指定するかにかかわらず、データベースソースの JNDI 名は jdbc/IDMUADataSource の必要があることに注意してください。

7.3.2 RBPM 設定ファイルの場所の指定

WebLogic ユーザアプリケーションでは、sys-configuration-xmldata.xml ファイル、および idmuserapp_logging.xml ファイルの検索方法が分かっている必要があります。これは、setDomainEnv.cmd ファイルにファイルのロケーションを追加して行うことができます。

アプリケーションサーバでこれらを利用できるようにするには、setDomainEnv.cmd または setDomainEnv.sh ファイルで次のようにロケーションを指定します。

1. setDomainEnv.cmd または setDomainEnv.sh ファイルを開きます。
2. 次のような行を見つけます。

   ```
   set JAVA_PROPERTIES
   export JAVA_PROPERTIES
   ```

3. JAVA_PROPERTIES のエントリの下に、次に対してエントリを追加します。
   - Dextend.local.config.dir==<directory-path>: sys-configuration.xml ファイルを含むフォルダ (ファイル自体ではない) を指定します。
   - -Didmuserapp.logging.config.dir==<directory-path>: idmuserapp_logging.xml ファイルを含むフォルダ (ファイル自体ではない) を指定します。

   Windows の場合の例 :

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

4. 環境変数 EXT_PRE_CLASSPATH を設定して、antlr.jar とともに、log4j.jar および commons-logging.jar. をポイントします。

   4a この行を見つけます。

   ```
   ADD EXTENSIONS TO CLASSPATH
   ```

   4b その下に EXT_PRE_CLASSPATH を追加します。Windows の場合の例 :

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

   Linux の場合の例 :

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

5. ファイルを保存して終了します。

XML ファイルは configured ユーティリティでも使用されるため、configupdate.bat または configupdate.sh ファイルを次のように編集する必要があります。

1. configupdate.bat または configupdate.sh を開きます。
2. 次の行をファイル内で探します。

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

3. 次を含む既存の行を更新します。

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

4. ファイルを保存して閉じます。
5. configupdate ユーティリティを実行し、証明書を BEA_HOME 下にある JDK のキーストアにインストールします。

   configupdate を実行する場合、使用中の JDK で cacerts ファイルを入力するよう促されます。インストール中に指定されたものと同じ JDK を使用していない場合、WAR で configupdate を実行する必要があります。このエントリは、WebLogic で使用されている JDK を示す必要があるため、指定されている JDK に注意します。これは、識別ボールトに接続する証明書ファイルをインポートして行われます。これは、eDirectory に接続する証明書をインポートするために実行されます。

   configupdate ユーティリティの識別ボールト証明書の値は、次の場所を指し示す必要があります。

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

7.3.3 ワークフロープラグインと WebLogic セットアップ

enforce-valid-basic-auth-credentials フラグが True に設定されている場合、iManager へのワークフロー管理プラグインは WebLogic で実行しているユーザアプリケーションドライバに接続できません。この接続を正常に行うには、このフラグを無効にする必要があります。

enforce-valid-basic-auth-credentials フラグを無効にするには、以下の手順に従います。

1. <*WLHome*>/user_projects/domains/base_domain/config/ フォルダで、Config.xml ファイルを開きます。
2. 以下の行を <security-configuration> セクションに追加します。

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

3. ファイルを保存して、サーバを再起動します。

この変更を行った後で、ワークフロー管理プラグインにログインできるはずです。

7.4 ユーザアプリケーション WAR の展開

- インストールディレクトリ (一般に Novell\IDM) から、更新されているユーザアプリケーション WAR ファイルをアプリケーションドメインにコピーします 。例を次に示します。

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

- 標準 WebLogic 展開手順を使用してユーザアプリケーション WAR を展開します。

7.5 ユーザアプリケーションへのアクセス

- ユーザアプリケーション URL への移動 :

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

  例を次に示します。

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

コンソールまたは単一コマンドによるインストール

8

このセクションでは、51 ページの第 5 章「JBoss でのユーザアプリケーションのインストール」で説明した GUI を使用したインストール方法の代わりに使用できるインストール方法について説明します。主なトピックは次のとおりです。

- 103 ページのセクション 8.1「コンソールからのユーザアプリケーションのインストール」
- 104 ページのセクション 8.2「単一コマンドによるユーザアプリケーションのインストール」

8.1 コンソールからのユーザアプリケーションのインストール

この手順では、コンソール (コマンドライン) 版のインストーラを使用して Identity Manager ユーザアプリケーションをインストールする方法について説明します。

注 : インストールプログラムには、少なくとも Java 2 プラットフォーム標準エディション Development Kit バージョン 1.5 が必要です。それより前のバージョンを使用している場合、このインストール手順では、ユーザアプリケーション WAR ファイルは正常に環境設定されません。インストールは成功したかのように見えますが、ユーザアプリケーションの起動を試みるとエラーが発生します。

---

1. 18 ページの 図 表 2-2 で説明されている適切なインストールファイルを取得したら、ログインしてターミナルセッションを開きます。
2. 次のように、ご使用のプラットフォーム用のインストーラを Java を使用して起動します。

   java -jar IdmUserApp.jar -i console

3. 51 ページの第 5 章「JBoss でのユーザアプリケーションのインストール」の下にあるグラフィカルユーザインタフェースについて説明されたのと同じステップに従って、コマンドラインのプロンプトを読み、コマンドラインに対する応答を入力して、マスタキーをインポートまたは作成します。
4. ユーザアプリケーション環境設定パラメータを設定するには、手動で configupdate ユーティリティを起動します。コマンドラインで、configupdate.sh (Linux または Solaris) あるいは configupdate.bat (Windows) と入力して、123 ページのセクション A.1「ユーザアプリケーション環境設定 : 基本パラメータ」で説明されている値を入力します。
5. 外部パスワード管理 WAR を使用している場合、これをインストールディレクトリおよび、外部パスワード WAR 機能を実行するリモート JBoss サーバ展開ディレクトリに手動でコピーします。
6. 115 ページの第 9 章「インストール後のタスク」に進みます。

8.2 単一コマンドによるユーザアプリケーションのインストール

この手順では、サイレントインストールの方法について説明します。サイレントインストールには、インストール中のやりとりが必要なく、特に複数のシステムにインストールする場合には、時間を節約できます。サイレントインストールでは、Linux および Solaris がサポートされます。

1. 18 ページの 図 表 2-2 でリストされている手順に従って、適切なインストールファイルを入手します。
2. ログインして、端末のセッションを開きます。
3. Identity Manager プロパティファイルである silent.properties を探します。これはインストールファイルにバンドルされています。CD からインストールしている場合は、このファイルのローカルコピーを作成します。
4. silent.properties を編集して、インストールパラメータおよびユーザアプリケーション環境設定パラメータを指定します。

   各インストールパラメータの例については、silent.properties ファイルを参照してください。インストールパラメータは、GUI またはコンソールインストール手順で設定したインストールパラメータに対応します。

   ユーザアプリケーション環境設定パラメータの説明については、表 8-1 を参照してください。ユーザアプリケーション環境設定パラメータは、GUI またはコンソールインストール手順または configupdate ユーティリティで設定したのと同じパラメータです。
5. サイレントインストールは次の方法で起動します。

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

   そのファイルがインストーラスクリプトとは別のディレクトリにある場合は、silent.properties へのフルパスを入力します。スクリプトによって、必要なファイルが一時ディレクトリに解凍され、サイレントインストールが起動されます。

表 8-1 *サイレントインストール用のユーザアプリケーション環境設定パラメータ*

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_LDAPHOST=	eDirectory™ 接続設定 : LDAP ホスト。 LDAP サーバのホスト名または IP アドレスを指定します。
NOVL_CONFIG_LDAPADMIN=	eDirectory 接続設定 : LDAP 管理者。 LDAP 管理者の資格情報を指定します。このユーザは既に存在している必要があります。ユーザアプリケーションは、このアカウントを使用して識別ボールドへの管理接続を行います。この値は、マスタキーに基づいて暗号化されます。
NOVL_CONFIG_LDAPADMINPASS=	eDirectory 接続設定 : LDAP 管理者パスワード。 LDAP 管理者パスワードを指定します。このパスワードは、マスタキーに基づいて暗号化されます。

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory DN: ルートコンテナ DN。 ルートコンテナの LDAP 識別名を指定します。これは、ディレクトリ抽象化層で検索ルートが指定されない場合に、デフォルトのエンティティ定義検索ルートとして使用されます。
NOVL_CONFIG_PROVISIONROOT=	eDirectory DN: プロビジョニングドライバ DN。 前述の 45 ページのセクション 4.1「iManager でのユーザアプリケーションドライバの作成」で作成したユーザアプリケーションドライバの識別名を指定します。たとえば、ドライバが UserApplicationDriver でドライバセットの名前が myDriverSet であり、ドライバセットが o=myCompany のコンテキストにある場合は、次の値を入力します。 `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
NOVL_CONFIG_LOCKSMITH=	eDirectory DN: ユーザアプリケーション管理者。 指定されたユーザアプリケーションのユーザコンテナについての管理タスクを実行する権限のある、識別ボールト内の既存のユーザ。このユーザは、ユーザアプリケーションの［*管理者*］タブを使用してポータルを管理できます。 ユーザアプリケーション管理者が、iManager、Novell Designer for identity Manager、またはユーザアプリケーション (*［要求と承認］*タブ) に公開されているワークフロー管理タスクに参加する場合は、この管理者に、ユーザアプリケーションドライバに含まれるオブジェクトインスタンスに対する適切なトラスティ権限を与える必要があります。詳細は、『*ユーザアプリケーション : 管理ガイド*』を参照してください。 ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［セキュリティ］*ページを使用する必要があります。

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory DN: プロビジョニングアプリケーション管理者。 この役割は Identity Manager のプロビジョニングバージョンで使用可能です。プロビジョニングアプリケーション管理者は、*［プロビジョニング］*タブ (*［管理］*タブの下) を使用して、プロビジョニングワークフロー機能を管理します。これらの機能は、ユーザアプリケーションの［*要求と承認*］タブでユーザが使用可能です。このユーザは、プロビジョニングアプリケーション管理者に指定される前に、識別ボールトに存在する必要があります。 ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［セキュリティ］*ページを使用する必要があります。
NOVL_CONFIG_ROLECONTAINERDN=	この役割は、Novell Identity Manager Roles Based Provisioning Module で利用可能です。この役割を使用すると、そのメンバーはすべての役割の作成、削除、変更、およびユーザ、グループ、またはコンテナへの役割の付与または取り消しを行うことができます。さらに役割のメンバーは、任意のユーザに対してレポートを実行できます。デフォルトでは、この役割にはユーザアプリケーション管理者が割り当てられています。 ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの *［役割］* > *［役割の割り当て］*ページを使用します。
NOVL_CONFIG_COMPLIANCECONTAINERDN	コンプライアンスモジュール管理者はシステムの役割であり、メンバーはこの［*コンプライアンス*］タブのすべての機能が実行可能です。このユーザは、コンプライアンスモジュール管理者として指定される前に、識別ボールトに存在している必要があります。
NOVL_CONFIG_USERCONTAINERDN=	メタディレクトリユーザ ID: ユーザコンテナ DN。 ユーザコンテナの LDAP 識別名 (DN) または完全修飾 LDAP 名を指定します。これにより、ユーザおよびグループの検索スコープが定義されます。このコンテナ内 (およびその下) のユーザが、ユーザアプリケーションにログインできます。 **重要 :** ユーザによるワークフローの実行を可能とさせる場合は、ユーザアプリケーションドライバの設定中に指定したユーザアプリケーション管理者が、確実にこのコンテナに存在するようにしてください。

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_GROUPCONTAINERDN=	メタディレクトリユーザグループ : グループコンテナ DN。 グループコンテナの LDAP 識別名 (DN) または完全修飾 LDAP 名を指定します。ディレクトリ抽象化レイヤ内のエンティティ定義で使用します。
NOVL_CONFIG_KEYSTOREPATH=	eDirectory 証明書 : キーストア パス。必須。 アプリケーションサーバが使用している JRE の (cacerts) キーストアファイルへのフルパスを指定します。ユーザアプリケーションのインストールによって、キーストアファイルが変更されます。Linux または Solaris では、ユーザにはこのファイルへの書き込み許可が必要です。
NOVL_CONFIG_KEYSTOREPASSWORD=	eDirectory 証明書 : キーストアパスワード。 cacerts のパスワードを指定します。デフォルトは、「changeit」です。
NOVL_CONFIG_SECUREADMINCONNECTION=	eDirectory 接続設定 : セキュア管理者接続。 必須。［*True*］を選択すると、管理者アカウントを使用したすべての通信でセキュアソケットを使用する必要があります (このオプションを使用すると、パフォーマンスに悪影響を及ぼすことがあります)。この設定を行うと、SSL を必要としない他の処理では SSL を使用せずに処理を実行できるようになります。 管理者アカウントがセキュアソケット通信を使用しない場合は、［*False*］を指定します。
NOVL_CONFIG_SECUREUSERCONNECTION=	eDirectory 接続設定 : セキュアユーザ接続。 必須。［*True*］を選択すると、ログインユーザのアカウントを使用したすべての通信でセキュアソケットを使用する必要があります (このオプションを使用すると、パフォーマンスに深刻な悪影響を及ぼすことがあります)。この設定を行うと、SSL を必要としない他の処理では SSL を使用せずに処理を実行できるようになります。 ユーザのアカウントがセキュアソケット通信を使用しない場合は、［*False*］を指定します。
NOVL_CONFIG_SESSIONTIMEOUT=	その他 : セッションのタイムアウト。 必須。アプリケーションセッションのタイムアウト間隔を指定します。
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory 接続設定 : LDAP 非セキュアポート。 必須。LDAP サーバの非セキュアポートを、たとえば「389」のように指定します。

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory 接続設定 : LDAP セキュアポート。 必須。LDAP サーバのセキュアポートを、たとえば「636」のように指定します。
NOVL_CONFIG_ANONYMOUS=	eDirectory 接続設定 : パブリック匿名アカウントの使用 必須。ログインしていないユーザに LDAP パブリック匿名アカウントへのアクセスを許可するには、［*True*］を選択します。 代わりに NOVL_CONFIG_GUEST を有効にするには、［*False*］を指定します。
NOVL_CONFIG_GUEST=	eDirectory 接続設定 : LDAP ゲスト。 ログインしていないユーザに、許可されたポートレットへのアクセスを許可します。［*パブリック匿名アカウントの使用*］の選択も解除する必要があります。ゲストユーザアカウントは、識別ボールトにすでに存在している必要があります。［ゲストユーザ］を無効にするには、［*パブリック匿名アカウントの使用*］を選択します。
NOVL_CONFIG_GUESTPASS=	eDirectory 接続設定 : LDAP ゲストパスワード。
NOVL_CONFIG_EMAILNOTIFYHOST=	電子メール : 通知テンプレートホストトークン。 Identity Manager ユーザアプリケーションをホストしているアプリケーションサーバを指定します。たとえば、次のようにします。 `myapplication serverServer` この値は、電子メールテンプレートの $HOST$ トークンと置き換えられます。作成される url は、プロビジョニング要求タスクと承認通知へのリンクです。
NOVL_CONFIG_EMAILNOTIFYPORT=	電子メール : 通知テンプレートポートトークン。 プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $PORT$ トークンの置き換えに使用されます。
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	電子メール : 通知テンプレートセキュアポートトークン。 プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $SECURE_PORT$ トークンの置き換えに使用します。
NOVL_CONFIG_NOTFSMTPEMAILFROM=	電子メール : 通知 SMTP 電子メール送信者。 必須。プロビジョニング電子メール内のユーザからの電子メールを指定します。

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_NOTFSMTPEMAILHOST=	電子メール : 通知 SMTP 電子メールホスト。 必須。プロビジョニング電子メールを使用している SMTP 電子メールホストを指定します。これは、IP アドレスまたは DNS 名が可能です。
NOVL_CONFIG_USEEXTPWDWAR=	パスワード管理 : 外部パスワード WAR の使用。 外部パスワード管理 WAR を使用している場合は、［*True*］を指定します。［*True*］を指定する場合は、*NOVL_CONFIG_EXTPWDWARPTH* および *NOVL_CONFIG_EXTPWDWARRTNPATH* の値も指定する必要があります。 デフォルトの内部パスワード管理機能を使用するには、*［False］* を指定します。/jsps/pwdmgt/ForgotPassword.jsp(最初は http(s) プロトコルなし)。これは、ユーザを、外部 WAR ではなく、ユーザアプリケーションに組み込まれた［パスワードを忘れた場合］機能にリダイレクトします。
NOVL_CONFIG_EXTPWDWARPATH=	パスワード管理 : パスワードを忘れた場合のリンク。 外部または内部のパスワード管理 WAR で、［パスワードを忘れた場合］機能ページ ForgotPassword.jsp の URL を指定します。または、デフォルトの内部パスワード管理 WAR をそのまま使用します。詳細については、118 ページの 「外部パスワードを忘れた場合の管理の環境設定」を参照してください。
NOVL_CONFIG_EXTPWDWARRTNPATH=	パスワード管理 : パスワードを忘れた場合の返信リンク。 ユーザがパスワードを忘れた場合の操作を実行した後でクリックできるように、パスワードを忘れた場合の返信リンクを指定します。
NOVL_CONFIG_FORGOTWEBSERVICEURL=	パスワード管理 : パスワードを忘れた場合の Web サービス URL これは、外部の［パスワードを忘れた場合］の War がコアのパスワードを忘れた場合の機能を実行するユーザアプリケーションを呼び戻すために使用する URL です。URL のフォーマットは次のとおりです。 `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
NOVL_CONFIG_USEROBJECTATTRIBUTE=	メタディレクトリユーザ ID: ユーザオブジェクトクラス。 必須。LDAP ユーザオブジェクトクラス (通常は inetOrgPerson)。

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_LOGINATTRIBUTE=	メタディレクトリユーザ ID: ログイン属性。 必須。ユーザのログイン名を表す LDAP 属性 (たとえば CN)。
NOVL_CONFIG_NAMINGATTRIBUTE=	メタディレクトリユーザ ID : 名前付け属性。 必須。ユーザまたはグループをルックアップする際に ID として使用する LDAP 属性これはログイン属性と同じではありません。ログイン属性はログイン中にのみ使用し、ユーザおよびグループの検索中には使用しません。
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	メタディレクトリユーザ ID: ユーザメンバーシップ属性。オプション。 必須。ユーザのグループメンバーシップを表す LDAP 属性です。この名前にはスペースを使用しないでください。
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	メタディレクトリユーザグループ : グループオブジェクトクラス。 必須。LDAP オブジェクトクラス (通常は groupofNames)。
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	メタディレクトリユーザグループ : グループメンバーシップ属性。 必須。ユーザのグループメンバーシップを表す属性を指定します。この名前にはスペースを使用しないでください。
NOVL_CONFIG_USEDYNAMICGROUPS=	メタディレクトリユーザグループ : ダイナミックグループ。 必須。ダイナミックグループを使用するには、［*True*］を指定します。使用しない場合は、［*False*］を指定します。
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	メタディレクトリユーザグループ : ダイナミックグループオブジェクトクラス。 必須。LDAP ダイナミックグループオブジェクトクラスを指定します (通常は dynamicGroup)。
NOVL_CONFIG_TRUSTEDSTOREPATH=	トラステッドキーストア : トラステッドストアパス。 トラステッドキーストアには、有効なデジタル署名に使用するすべてのトラステッド署名者の証明書が含まれます。入力しない場合は、ユーザアプリケーションはシステムプロパティ javax.net.ssl.trustStore からパスを取得します。パスがそこではない場合は、jre/lib/security/cacerts と推測されます。
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	トラステッドキーストア : トラステッドストアパスワード。

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_AUDITCERT=	デジタル署名証明書
NOVL_CONFIG_AUDITKEYFILEPATH=	デジタル署名プライベートキーファイルのパス。
NOVL_CONFIG_ICSLOGOUTENABLED=	Access Manager および iChain の設定 : 同時ログアウト有効。 ユーザアプリケーションおよび Novell Access Manager または iChain® の同時ログアウトを有効にするには、［*True*］を指定します。Novell Access Manager または iChain はログアウト時に Cookie をチェックし、Cookie が存在する場合は、ユーザを ICS ログアウトページに再ルーティングします。 同時ログアウトを無効にするには、［*False*］を指定します。
NOVL_CONFIG_ICSLOGOUTPAGE=	Access Manager および iChain 設定 : ［同時ログアウト］ページ。 Novell Access Manager または iChain のログアウトページの URL を指定します。URL は Novell Access Manager または iChain が期待するホスト名です。ICS ログが有効な場合は、ユーザはユーザアプリケーションからログアウトし、ユーザはこのページを再ルーティングします。
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	電子メール : 通知テンプレートプロトコルトークン。 非セキュアプロトコル、HTTP を参照してください。プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $PROTOCOL$ トークンの置き換えに使用します。
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	電子メール : 通知テンプレートセキュアポートトークン。
NOVL_CONFIG_OCSPURI=	その他 : OCSP URI。 クライアントインストールが On-Line Certificate Status Protocol(OCSP) を使用する場合は、Uniform Resource Identifier(URI) を指定します。たとえば、フォーマットは http://hstport/ocspLocal です。OCSP URI によって、トラステッド証明書オンラインの状態は更新されます。
NOVL_CONFIG_AUTHCONFIGPATH=	その他 : 許可設定パス。 許可環境設定ファイルの完全修飾名。

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_CREATEDIRECTORYINDEX	その他 : eDirectory インデックスの作成 サイレントインストーラで、NOVL_CONFIG_SERVERDN で指定した eDirectory サーバ上でマネージャ、ismanager、および srvprvUUID の属性のインデックスが作成されるようにする場合、［true］を指定します。このパラメータが［true］に設定されている場合、NOVL_CONFIG_REMOVEEDIRECTORYINDEX は ［true］に設定できません。 最良のパフォーマンス結果を得るには、インデックス作成が完了している必要があります。ユーザアプリケーションを利用可能な状態にする前にインデックスをオンラインモードにする必要があります。
NOVL_CONFIG_REMOVEDIRECTORYINDEX	その他 : eDirectory インデックスの削除 サイレントインストーラで、NOVL_CONFIG_SERVERDN で指定したサーバのインデックスが削除されるようにする場合、［true］を指定します。このパラメータが ［true］に設定されている場合、NOVL_CONFIG_CREATEEDIRECTORYINDEX は［true］に設定できません。
NOVL_CONFIG_SERVERDN	その他 : サーバ DN インデックスを作成または削除する必要のある eDirectory サーバを指定します。
NOVL_DATABASE_NEW	データベースが新規か既存かを示します。新規データベースの場合、*[True]* を指定します。既存データベースの場合、*[False]* を指定します。
NOVL_RBPM_SEC_ADMINDN	セキュリティ管理者 この役割により、メンバーはセキュリティドメイン内のすべての機能を付与されます。 セキュリティ管理者は、セキュリティドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。セキュリティドメインを使用すると、セキュリティ管理者は Roles Based Provisioning Module 内のすべてのドメインへのアクセス許可を設定できます。セキュリティ管理者はチームを構成でき、またドメイン管理者、委任管理者、およびその他のセキュリティ管理者も割り当てることができます。
NOVL_RBPM_RESOURCE_ADMINDN	リソース管理者 この役割により、メンバーはリソースドメイン内のすべての機能を付与されます。リソース管理者はリソースドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_RBPM_CONFIG_ADMINDN	この役割により、メンバーは構成ドメイン内のすべての機能を付与されます。RBPM 設定管理者は、構成ドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。RBPM 設定管理者は、Roles Based Provisioning Module 内のナビゲーションアイテムへのアクセスを制御します。また、RBPM 設定管理者は委任と代理サービス、デジタル署名サービス、ユーザインタフェースのプロビジョニング、およびワークフローエンジンを設定します。

インストール後のタスク

9

このセクションでは、インストール後のタスクについて説明します。主なトピックは次のとおりです。

9.1 マスタキーの記録

インストール後すぐに、暗号化マスタキーをコピーして安全な場所に記録します。

1. インストールディレクトリで master-key.txt ファイルを開きます。
2. 暗号化マスタキーを、システム障害の場合にアクセスできる安全な場所にコピーします。

警告 : 暗号化マスタキーのコピーは常に保持してください。たとえば装置障害などのためにマスタキーが失われた場合に、暗号化データへのアクセスを回復するために暗号化マスタキーが必要です。

クラスタの最初のメンバーにインストールした場合は、クラスタのほかのメンバーにユーザアプリケーションをインストールする際にこの暗号化マスタキーを使用します。

9.2 ユーザアプリケーションの環境設定

Identity Manager ユーザアプリケーションおよび役割サブシステムの環境設定に関するインストール後の手順については、次を参照してください。

- 『*Novell IDM Roles Based Provisioning Module 管理ガイド*』の「ユーザアプリケーション環境の設定」
- *Novell IDM Roles Based Provisioning Module 設計ガイド*

9.2.1 ログの設定

ログを設定するには、『ユーザアプリケーション : 管理ガイド (http://www.novell.com/documentation/idmrbpm37/index.html)』の「ログの設定」セクションの手順に従います。

9.3 eDirectory の設定

9.3.1 eDirectory でのインデックスの作成

ユーザアプリケーションのパフォーマンスを向上させるには、eDirectory™ 管理者は、マネージャ、ismanager、および srvprvUUID の属性に対してインデックスを作成する必要があります。これらの属性にインデックスがない場合、ユーザアプリケーションのユーザは、特にクラスタ化された環境では低いパフォーマンスの状態にあります。

これらのインデックスは、*［ユーザアプリケーション環境設定］* パネルの *［詳細］* タブの［eDirectory インデックスの作成］が選択されている場合、インストール中に自動的に作成できます (126 ページの 図 表 A-2 で説明されています)。インデックスを作成するためにインデックスマネージャを使用する手順については、『*Novell eDirectory 管理ガイド* (http://www.novell.com/documentation)』を参照してください。

9.3.2 SAML 認証メソッドのインストールおよび環境設定

この環境設定は、SAML 認証メソッドを使用し、アクセスマネージャを使用しない場合にのみ必要となります。アクセスマネージャを使用する場合、eDirectory ツリーには、すでにそのメソッドが含まれています。その手順は次の通りです。

- ❑ eDirectory ツリーに SAML メソッドをインストールします。
- ❑ iManager を使用した eDirectory の属性の編集

eDirectory ツリーにおける SAML メソッドのインストール

1. .iso の nmassaml.zip ファイルを探して、解凍します。
2. SAML メソッドを eDirectory ツリーにインストールします。
   - **2a** authsaml.sch に保存されたスキーマの拡張

     次の例で、Linux 上でこれを実行する方法を説明します。

     ```
     ndssch -h <edir_ip> <edir_admin> authsaml.sch
     ```
   - **2b** SAML メソッドをインストールします。

     次の例で、Linux 上でこれを実行する方法を説明します。

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

eDirectory の属性の編集

1. iManager を開き、*［役割とタスク］* > *［ディレクトリ管理］* > *［オブジェクトの作成］* の順に進みます。
2. ［*すべてのオブジェクトクラスの表示*］を選択します。
3. クラスが authsamlAffiliate である新規のオブジェクトを作成します。
4. ［authsamlAffiliate］を選択して、［*OK*］をクリックします (有効な名前であればこのオブジェクトにどんな名前でも付けられます。)

5 コンテキストを指定するには、ツリーで［*SAML Assertion.Authorized Login Methods.Security*］コンテナオブジェクトを選択して、［*OK*］をクリックします。

6 属性をクラスオブジェクト authsamlAffiliate に追加する必要があります。

6a iManager の *［オブジェクトの表示］>［ブラウズ］* タブに進み、SAML Assertion.Authorized Login Methods.Security コンテナで新しい連携オブジェクトを見つけます。

6b 新しい連携オブジェクトを選択して、［*オブジェクトの修正*］を選択します。

6c 属性 *authsamlProviderID* を新しい連携オブジェクトに追加します。この属性を使用して、アサーションを連携と一致させます。この属性のコンテンツは、SAML アサーションで送られた Issuer の属性と完全に一致している必要があります。

6d［*OK*］をクリックします。

6e 属性 *authsamlValidBefore* および *authsamlValidAfter* を連携オブジェクトに追加します。これらの属性は、アサーションが有効とみなされると、アサーションの *IssueInstant* に基づいて時間を秒で定義します。一般的なデフォルトは 180 秒です。

6f［*OK*］をクリックします。

7 セキュリティコンテナを選択して、［*オブジェクトの作成*］を選択し、セキュリティコンテナで *トラステッドルートコンテナ*を作成します。

8 トラステッドルートコンテナに *トラステッドルート*オブジェクトを作成します。

8a［*役割とタスク］>［ディレクトリ管理*］に戻り、［*オブジェクトの作成*］を選択します。

8b［*すべてのオブジェクトクラスの表示*］を再び選択します。

8c 連携がアサーションを署名するために使用する証明書用の *トラステッドルート*オブジェクトを作成します。これを行うには、証明書の der エンコードしたコピーを持っている必要があります。

8d ルート CA 証明書につながれた署名証明書で、各証明書に対し新規のトラステッドルートオブジェクトを作成します。

8e 以前作成された［トラステッドルートコンテナへのコンテキスト］を設定して、［*OK*］をクリックします。

9 オブジェクトビューアに戻ります。

10 *authsamlTrustedCertDN* 属性を連携オブジェクトに追加し、［*OK*］をクリックします。

この属性は、前のステップで作成した署名証明書に対し、「トラステッドルートオブジェクト」を指し示す必要があります。(連携のアサーションはすべて、この属性によって示される証明書で署名されている必要があります。署名がない場合は拒否されます。)

11 *authsamlCertContainerDN* 属性を連携オブジェクトに追加し、［*OK*］をクリックします。

この属性は、以前作成した「トラステッドルートコンテナ」を指し示す必要があります。(この属性を使用して、署名証明書の証明書チェーンを確認します。)

9.4 インストール後のユーザアプリケーション WAR ファイルの再環境設定

WAR ファイルを更新するには、configupdate ユーティリティを次のように実行できます。

1. configupdate.sh または configupdate.bat を実行して、ユーザアプリケーションのインストールディレクトリにある ConfigUpdate ユーティリティを実行します。これにより、インストールディレクトリの WAR ファイルを更新できます。

   ConfigUpdate ユーティリティのパラメータの詳細については 123 ページのセクション A.1「ユーザアプリケーション環境設定 : 基本パラメータ」、104 ページの 図 表 8-1 を参照してください。

2. 新しい WAR ファイルをアプリケーションサーバに展開します。

   WebLogic および WebSphere では、WAR ファイルをアプリケーションサーバに再展開します。JBoss の単一サーバでは、変更は展開されている WAR に適用されます。JBoss クラスタで実行中の場合、WAR ファイルはこのクラスタの各 JBoss サーバで更新される必要があります。

9.5 外部パスワードを忘れた場合の管理の環境設定

［*パスワードを忘れた場合のリンク*］環境設定パラメータを使用して、［パスワードを忘れた場合］機能を含む WAR の場所を指定します。ユーザアプリケーションの外部または内部の WAR を指定できます。

- 118 ページのセクション 9.5.1「外部パスワードを忘れた場合の管理 WAR の指定」
- 119 ページのセクション 9.5.2「内部パスワード WAR の指定」
- 119 ページのセクション 9.5.3「外部パスワードを忘れた場合の WAR 環境設定のテスト」
- 119 ページのセクション 9.5.4「JBoss サーバ間の SSL 通信の設定」

9.5.1 外部パスワードを忘れた場合の管理 WAR の指定

1. インストール手順または configupdate ユーティリティを使用します。
2. ユーザアプリケーション環境設定パラメータで、*［外部パスワード WAR の使用］*環境設定パラメータチェックボックスをオンにします。
3. *［パスワードを忘れた場合のリンク］*環境設定パラメータには、外部パスワード WAR の場所を指定します。

   ホストおよびポートを含めます。たとえば、http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp。外部パスワード WAR は、ユーザアプリケーションを保護するファイアウォールの外側にできます。
4. *［パスワードを忘れた場合の返信リンク］*では、パスワードを忘れたプロシージャの実行完了後に表示するリンクを指定します。このリンクをクリックすると、指定したリンクにリダイレクトされます。
5. *［パスワードを忘れた場合の Web サービス URL］*では、外部パスワードを忘れた場合の WAR を使用してユーザアプリケーションを呼び戻す Web サービスの URL を指定します。URL のフォーマットは次のとおりです。https://*<idmhost>*:*<sslport>*/*<idm>*/pwdmgt/service.

返信リンクでは、SSL を使用して、ユーザアプリケーションにセキュアな Web サービス通信を確保する必要があります。119 ページのセクション 9.5.4「JBoss サーバ間の SSL 通信の設定」も参照してください。

6 ExternalPwd.war を、外部パスワード WAR 機能を実行するリモート JBoss サーバ展開ディレクトリに、手動でコピーします。

9.5.2 内部パスワード WAR の指定

1 ユーザアプリケーションの設定パラメータで、*［外部パスワード WAR の使用］*を選択しないでください。

2 *［パスワードを忘れた場合のリンク］*のデフォルトの場所を受諾するか、別のパスワード WAR の URL を指定します。

3 *［パスワードを忘れた場合の返信リンク］*のデフォルトの値を受諾します。

9.5.3 外部パスワードを忘れた場合の WAR 環境設定のテスト

外部パスワード WAR があり、これにアクセスして［パスワードを忘れた場合］機能をテストする場合は、次の場所からアクセスできます。

- ブラウザ内で直接アクセスします。外部パスワード WAR で［パスワードを忘れた場合］ページに移動します。たとえば、http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp に移動します。
- ユーザアプリケーションのログインページで、*［パスワードを忘れた場合］*リンクをクリックします。

9.5.4 JBoss サーバ間の SSL 通信の設定

インストール中にユーザアプリケーション環境設定ファイルで *［外部パスワード WAR の使用］*をオンにした場合は、ユーザアプリケーション WAR および外部パスワードを忘れた場合の管理 WAR ファイルを展開する JBoss サーバ間の SSL 通信を設定する必要があります。手順については、JBoss マニュアルを参照してください。

9.6 ［パスワードを忘れた場合の設定］の更新

インストール後に、*［パスワードを忘れた場合のリンク］*、*［パスワードを忘れた場合の返信リンク］*、および *［パスワードを忘れた場合の Web サービス URL］*の値を変更できます。configupdate ユーティリティまたはユーザアプリケーションを使用します。

configupdate ユーティリティの使用 : コマンドラインで、ディレクトリをインストールディレクトリに変更して、configupdate.sh (Linux または Solaris) あるいは configupdate.bat (Windows) と入力します。外部パスワード管理 WAR を作成して編集する場合は、リモートの JBoss サーバにコピーする前に、WAR を手動で名前変更する必要があります。

ユーザアプリケーションの使用 ユーザアプリケーションの管理者としてログインして、*［管理］*>*［アプリケーション環境設定］*>*［パスワードモジュールのセットアップ］*>*［ログイン］*に移動します。これらのフィールドは次のように変更します。

- *［パスワードを忘れた場合のリンク］*(たとえば http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp)

- *［パスワードを忘れた場合のリンク］* (たとえば http://localhost/IDMProv)
- *［パスワードを忘れた場合の Web サービス URL］* (たとえば https://<*idmhost*>:<*sslport*>/<*idm*>/pwdmgt/service)

9.7 セキュリティ上の考慮事項

インストールプロセス中、インストールプログラムによりログファイルがインストールディレクトリに書き込まれます。これらのファイルには、設定に関する情報が含まれています。環境が設定された時点で、これらのログファイルの削除または安全な場所に保存することを考える必要があります。

インストールプロセス中、データベーススキーマをファイルに書き込むことも選択できます。このファイルには、データベースについての説明的な情報が含まれているので、インストールプロセスが完了した後で、安全な場所に移動する必要があります。

9.8 トラブルシューティング

Novell® の担当者は、想定されるセットアップおよび環境設定のあらゆる問題に対応いたします。差し当たり、問題が発生した場合の対処方法をリストします。

項目	推奨されるアクション
インストール中に作成したユーザアプリケーションの環境設定を変更するとします。たとえば、次のような環境設定と仮定します。 ◆ 識別ボールトの接続および証明書 ◆ 電子メール設定 ◆ メタディレクトリのユーザ識別情報、ユーザグループ ◆ Access Manager または iChain® の設定	インストーラとは別に、環境設定ユーティリティを実行します。 Linux および Solaris では、インストールディレクトリ (デフォルトでは、/opt/novell/idm) から次のコマンドを実行します。 `configupdate.sh` Windows では、インストールディレクトリ (デフォルトでは、c:\opt\novell\idm) から次のコマンドを実行します。 `configupdate.bat`
アプリケーションサーバのスタートアップ時に、ログメッセージ「ポート 8080 使用中、使用されている」とともに例外がスローされる。	すでに実行されている Tomcat (または他のサーバソフトウェア) のすべてのインスタンスをシャットダウンします。アプリケーションサーバを再設定して 8080 以外のポートを使用する場合は、必ず iManager のユーザアプリケーションドライバの config 環境設定を編集してください。
アプリケーションサーバの起動時に、トラステッド証明書が見つからないというメッセージが表示される。	ユーザアプリケーションのインストールで指定した JDK を使用して、アプリケーションサーバを起動するようにします。
ポータル管理ページにログインできない。	ユーザアプリケーションの管理者アカウントが存在することを確認します。これを、iManager の管理者アカウントと混同しないでください。2 つの別の管理者オブジェクトがあります (またはある必要があります)。

項目	推奨されるアクション
管理者としてログインできるが、新規ユーザを作成することができない。	ユーザアプリケーションの管理者は、最上位のコンテナのトラスティでなければならず、スーパバイザ権限が必要です。応急処置として、LDAP 管理者と同等の権限を持つ、ユーザアプリケーションの管理者権限の設定を試みることができます (iManager を使用)。
アプリケーションサーバの起動時に、MySQL 接続エラーが発生する。	root として実行しないでください (Identity Manager に同梱されている MySQL のバージョンを実行している場合、この問題が発生することはほとんどありません)。 MySQL が実行されていること (および正しいコピーが実行されていること) を確認してください。MySQL の他のすべてのインスタンスを強制終了します。/idm/mysql/start-mysql.sh を実行してから、/idm/start-jboss.sh を実行します。 テキストエディタで /idm/mysql/setup-mysql.sh を調べ、疑わしい値をすべて修正してください。次に、スクリプトを実行し、/idm/start-jboss.sh を実行します。
アプリケーションサーバの起動時に、キーストアエラーが発生する。	アプリケーションサーバで、ユーザアプリケーションのインストール時に指定した JDK を使用されていません。 次のように keytool コマンドを使用して、証明書ファイルをインポートします。 `keytool -import -trustcacerts -alias` *`aliasName`* `-file` *`certFile`* `-keystore ..\lib\security\cacerts -storepass changeit` ◆ *aliasName* は、この証明書に選択した一意の名前に置き換えます。 ◆ *certFile* は、証明書ファイルのフルパスおよび名前に置き換えます。 ◆ デフォルトのキーストアパスワードは、changeit です (別のパスワードがある場合は、それを指定します)。

項目	推奨されるアクション
電子メール通知が送信されない。	configupdate ユーティリティを実行して、電子メール送信者および電信メールホストのユーザアプリケーション環境設定パラメータに値を指定したかどうかを確認します。 Linux および Solaris では、インストールディレクトリ (デフォルトでは、/opt/novell/idm) から次のコマンドを実行します。 `configupdate.sh` Windows では、インストールディレクトリ (デフォルトでは c:\opt\novell\idm) から次のコマンドを実行します。 `configupdate.bat`

IDM ユーザアプリケーション環境設定の参照

A

このセクションでは、ユーザアプリケーションのインストール、または環境設定更新中に、値を提供するオプションについて説明します。

A.1 ユーザアプリケーション環境設定 : 基本パラメータ

図 A-1 ユーザアプリケーション環境設定の基本オプション

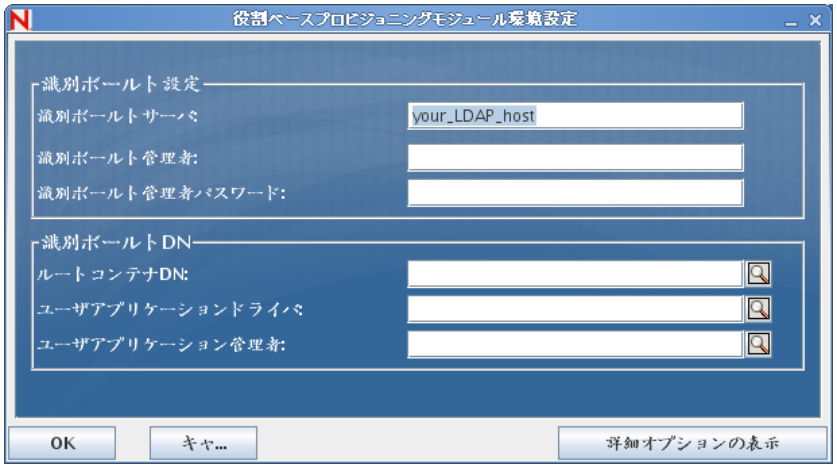


表 A-1 ユーザアプリケーション環境設定の基本オプション

設定のタイプ	オプション	説明
識別ボールト設定	*識別ボールトサーバ*	必須。LDAP サーバのホスト名または IP アドレスと、そのセキュアポートを指定します。たとえば、次のようにします。 `myLDAPhost`
	識別ボールト管理者	必須。LDAP 管理者の資格情報を指定します。このユーザは既に存在している必要があります。ユーザアプリケーションは、このアカウントを使用して識別ボールドへの管理接続を行います。この値は、マスタキーに基づいて暗号化されます。 ユーザアプリケーションの［管理］タブを使用してこの設定を修正しない限り、configupdate ユーティリティを使用してこの設定を修正できます。
	識別ボールト管理者パスワード	必須。LDAP 管理者パスワードを指定します。このパスワードは、マスタキーに基づいて暗号化されます。 ユーザアプリケーションの［管理］タブを使用してこの設定を修正しない限り、configupdate ユーティリティを使用してこの設定を修正できます。

設定のタイプ	オプション	説明
識別ボールト DN	*ルートコンテナ DN*	必須。ルートコンテナの LDAP 識別名を指定します。これは、ディレクトリ抽象化層で検索ルートが指定されない場合に、デフォルトのエンティティ定義検索ルートとして使用されます。
	ユーザアプリケーションドライバ DN	必須。ユーザアプリケーションドライバの識別名を指定します (45 ページのセクション 4.1「iManager でのユーザアプリケーションドライバの作成」で説明)。たとえば、ドライバが UserApplicationDriver でドライバセットの名前が myDriverSet であり、ドライバセットが o=myCompany のコンテキストにある場合は、次の値を入力します。 `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	ユーザアプリケーション管理者	必須。指定されたユーザアプリケーションのユーザコンテナについての管理タスクを実行する権限のある、識別ボールト内の既存のユーザ。このユーザは、ユーザアプリケーションの［*管理者*］タブを使用してポータルを管理できます。 ユーザアプリケーション管理者が、iManager、Novell Designer for identity Manager、またはユーザアプリケーション (*［要求と承認］* タブ) に公開されているワークフロー管理タスクに参加する場合は、この管理者に、ユーザアプリケーションドライバに含まれるオブジェクトインスタンスに対する適切なトラスティ権限を与える必要があります。詳細は、『*ユーザアプリケーション : 管理ガイド*』を参照してください。 ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［セキュリティ］* ページを使用する必要があります。 ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。

注 : インストール後には、このファイルでほとんどの設定を編集できます。編集するには、インストールサブディレクトリにある configupdate.sh スクリプトまたは Windows configupdate.bat ファイルを実行します。クラスタ内でこれを記憶します。このファイルの設定はクラスタのすべてのメンバーで同じである必要があります。

A.2 ユーザアプリケーション環境設定 : すべてのパラメータ

この表には、［*詳細オプションの表示*］をクリック時に利用可能な環境設定パラメータが含まれています。

表 A-2 *ユーザアプリケーション環境設定 : すべてのオプション*

設定のタイプ	オプション	説明
識別ボールト設定	*識別ボールトサーバ*	必須。LDAP サーバのホスト名または IP アドレスを指定します。たとえば、次のようにします。 myLDAPhost
	LDAP ポート	LDAP サーバの非セキュアポートを指定します。たとえば、「389」のように指定してください。
	セキュア LDAP ポート	LDAP サーバのセキュアポートを指定します。たとえば、「636」のように指定してください。
	識別ボールト管理者	必須。LDAP 管理者の資格情報を指定します。このユーザは既に存在している必要があります。ユーザアプリケーションは、このアカウントを使用して識別ボールドへの管理接続を行います。この値は、マスタキーに基づいて暗号化されます。
	識別ボールト管理者パスワード	必須。LDAP 管理者パスワードを指定します。このパスワードは、マスタキーに基づいて暗号化されます。
	パブリック匿名アカウントの使用	ログインしていないユーザに、LDAP パブリック匿名アカウントへのアクセスを許可します。
	LDAP ゲスト	ログインしていないユーザに、許可されたポートレットへのアクセスを許可します。このユーザアカウントは、識別ボールトにすでに存在している必要があります。［LDAP ゲスト］を有効にするには、［*パブリック匿名アカウントの使用*］の選択を解除する必要があります。［ゲストユーザ］を無効にするには、［*パブリック匿名アカウントの使用*］を選択します。
	LDAP ゲストパスワード	LDAP ゲストパスワードを指定します。
	セキュア管理者接続	このオプションを選択すると、管理者アカウントを使用したすべての通信でセキュアソケットを使用する必要があります (このオプションを使用すると、パフォーマンスに悪影響を及ぼすことがあります)。この設定を行うと、SSL を必要としない他の処理では SSL を使用せずに処理を実行できるようになります。
	セキュアなユーザ接続	このオプションを選択すると、ログインユーザのアカウントを使用したすべての通信でセキュアソケットを使用する必要があります (このオプションを使用すると、パフォーマンスに深刻な悪影響を及ぼすことがあります)。この設定を行うと、SSL を必要としない他の処理では SSL を使用せずに処理を実行できるようになります。

設定のタイプ	オプション	説明
識別ボールト DN	*ルートコンテナ DN*	必須。ルートコンテナの LDAP 識別名を指定します。これは、ディレクトリ抽象化層で検索ルートが指定されない場合に、デフォルトのエンティティ定義検索ルートとして使用されます。
	ユーザアプリケーションドライバ DN	必須。ユーザアプリケーションドライバの識別名を指定します (45 ページのセクション 4.1「iManager でのユーザアプリケーションドライバの作成」で説明)。たとえば、ドライバが UserApplicationDriver でドライバセットの名前が myDriverSet であり、ドライバセットが o=myCompany のコンテキストにある場合は、次の値を入力します。 `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	ユーザアプリケーション管理者	必須。指定されたユーザアプリケーションのユーザコンテナについての管理タスクを実行する権限のある、識別ボールト内の既存のユーザ。このユーザは、ユーザアプリケーションの［*管理者*］タブを使用してポータルを管理できます。 ユーザアプリケーション管理者が、iManager、Novell Designer for identity Manager、またはユーザアプリケーション (*［要求と承認］* タブ) に公開されているワークフロー管理タスクに参加する場合は、この管理者に、ユーザアプリケーションドライバに含まれるオブジェクトインスタンスに対する適切なトラスティ権限を与える必要があります。詳細は、*ユーザアプリケーション : 管理ガイド*を参照してください。 ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［セキュリティ］* ページを使用する必要があります。 ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。
	プロビジョニング管理者	プロビジョニング管理者は、ユーザアプリケーション全体を通して使用可能なプロビジョニングワークフロー機能を管理します。このユーザは、プロビジョニン管理者に指定される前に、識別ボールトに存在する必要があります。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［管理者の割り当て］* ページを使用します。

設定のタイプ	オプション	説明
	コンプライアンス管理者	コンプライアンス管理者はシステムの役割であり、メンバーはこの *［コンプライアンス］* タブのすべての機能が実行可能です。このユーザは、コンプライアンスモジュール管理者として指定される前に、識別ボールトに存在している必要があります。 configupdate の間、この値への変更は、有効なコンプライアンス管理者が割り当てられていない場合のみ反映されます。有効なコンプライアンス管理者が存在する場合は、変更は保存されません。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［管理者の割り当て］* ページを使用します。
	役割管理者	この役割を使用すると、そのメンバーはすべての役割の作成、削除、変更、およびユーザ、グループ、またはコンテナへの役割の付与または取り消しを行うことができます。さらに役割のメンバーは、任意のユーザに対してレポートを実行できます。デフォルトでは、この役割にはユーザアプリケーション管理者が割り当てられています。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［管理者の割り当て］* ページを使用します。 configupdate の間、この値への変更は、有効な役割管理者が割り当てられていない場合のみ反映されます。有効な役割管理者が存在する場合は、変更は保存されません。
	セキュリティ管理者	この役割により、メンバーはセキュリティドメイン内のすべての機能を付与されます。 セキュリティ管理者は、セキュリティドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。セキュリティドメインを使用すると、セキュリティ管理者は Roles Based Provisioning Module 内のすべてのドメインへのアクセス許可を設定できます。セキュリティ管理者はチームを構成でき、またドメイン管理者、委任管理者、およびその他のセキュリティ管理者も割り当てることができます。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［管理者の割り当て］* ページを使用します。
	リソース管理者	この役割により、メンバーはリソースドメイン内のすべての機能を付与されます。リソース管理者はリソースドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［管理者の割り当て］* ページを使用します。

設定のタイプ	オプション	説明
	RBPM 設定管理者	この役割により、メンバーは構成ドメイン内のすべての機能を付与されます。RBPM 設定管理者は、構成ドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。RBPM 設定管理者は、Roles Based Provisioning Module 内のナビゲーションアイテムへのアクセスを制御します。また、RBPM 設定管理者は委任と代理サービス、デジタル署名サービス、ユーザインタフェースのプロビジョニング、およびワークフローエンジンを設定します。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの *［管理］*>*［管理者の割り当て］* ページを使用します。
識別ボールトユーザ ID	*ユーザ コンテナ DN*	必須。ユーザコンテナの LDAP 識別名 (DN) または完全修飾 LDAP 名を指定します。 このコンテナ内 (およびその下) のユーザが、ユーザアプリケーションにログインできます。 ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。 **重要 :** ユーザによるワークフローの実行を可能とさせる場合は、ユーザアプリケーションドライバの設定中に指定したユーザアプリケーション管理者が、確実にこのコンテナに存在するようにしてください。
	ユーザコンテナのスコープ	これにより、ユーザの検索スコープが定義されます。
	ユーザオブジェクトクラス	LDAP ユーザオブジェクトクラス (通常は inetOrgPerson)。
	ログイン属性	ユーザのログイン名を表す LDAP 属性 (たとえば CN)。
	名前付け属性	ユーザまたはグループをルックアップする際に ID として使用する LDAP 属性これはログイン属性と同じではありません。ログイン属性はログイン中にのみ使用し、ユーザおよびグループの検索中には使用しません。
	ユーザメンバーシップ属性	オプション。ユーザのグループメンバーシップを表す LDAP 属性です。この名前にはスペースを使用しないでください。

設定のタイプ	オプション	説明
識別ボールトユーザグループ	*グループコンテナDN*	必須。グループコンテナの LDAP 識別名 (DN) または完全修飾 LDAP 名を指定します。ディレクトリ抽象化レイヤ内のエンティティ定義で使用します。
		ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。
	グループコンテナのスコープ	これにより、グループの検索スコープが定義されます。
	グループオブジェクトクラス	LDAP オブジェクトクラス (通常は groupofNames)。
	グループメンバーシップ属性	ユーザのグループメンバーシップを表す属性です。この名前にはスペースを使用しないでください。
	ダイナミックグループの使用	ダイナミックグループを使用する場合は、このオプションを選択します。
	ダイナミックグループオブジェクトクラス	LDAP ダイナミックグループオブジェクトクラス (通常は dynamicGroup)。
識別ボールト証明書	*キーストアパス*	必須。アプリケーションサーバが実行に使用しているの JRE のキーストア (cacerts) ファイルへのフルパスを指定するか、小さな参照ボタンをクリックして cacerts ファイルに移動します。
		ユーザアプリケーションのインストールによって、キーストアファイルが変更されます。Linux または Solaris では、ユーザにはこのファイルへの書き込み許可が必要です。
	キーストアパスワード	必須。cacerts のパスワードを指定します。デフォルトは、「changeit」です。
	キーストアパスワードの確認	
トラステッドキーストア	*トラステッドストアパス*	トラステッドキーストアには、有効なデジタル署名に使用するすべてのトラステッド署名者の証明書が含まれます。入力しない場合は、ユーザアプリケーションはシステムプロパティ javax.net.ssl.trustStore からパスを取得します。パスがそこではない場合は、jre/lib/security/cacerts だと推測されます。
	トラステッドストアパスワード	このフィールドを入力しない場合は、ユーザアプリケーションはシステムプロパティ javax.net.ssl.trustStorePassword からパスワードを取得します。値がそこではない場合は、changeit が使用されます。このパスワードは、マスタキーに基づいて暗号化されます。
	キーストアタイプJKS	使用するデジタル署名のタイプを示します。このフィールドがチェックされている場合、トラステッドストアパスはタイプ JKS です。
	キーストアタイプPKCS12	使用するデジタル署名のタイプを示します。このフィールドがチェックされている場合、トラステッドストアパスはタイプ PKCS12 です。

設定のタイプ	オプション	説明
Novell Audit デジタル署名および証明書キー		監査サービスのためのデジタル署名キーおよび証明書を含みます。
	Novell Audit デジタル署名証明書	監査サービスのためのデジタル署名証明書を表示します。
	Novell Audit デジタル署名秘密鍵	デジタル署名秘密鍵が表示されます。このキーは、マスタキーに基づいて暗号化されます。
Access Manager の設定	*同時ログアウト有効*	このオプションが選択されている場合は、ユーザアプリケーションによってユーザアプリケーションおよび Novell Access Manager または iChain の同時ログアウトがサポートされます。Novell Access Manager または iChain はログアウト時に Cookie をチェックし、Cookie が存在する場合は、ユーザを ICS ログアウトページに再ルーティングします。
	［同時ログアウト］ページ	Novell Access Manager または iChain ログアウトページへの URL。URL は Novell Access Manager または iChain が期待するホスト名です。ICS ログが有効な場合は、ユーザはユーザアプリケーションからログアウトし、ユーザはこのページを再ルーティングします。
電子メール サーバの設定	*NotificationTemplate ホスト*	Identity Manager ユーザアプリケーションをホストしているアプリケーションサーバを指定します。たとえば、次のようにします。 `myapplication serverServer` この値は、電子メールテンプレートの $HOST$ トークンと置き換えられます。作成される url は、プロビジョニング要求タスクと承認通知へのリンクです。
	通知テンプレート PORT	プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $PORT$ トークンの置き換えに使用されます。
	通知テンプレート SECURE PORT	プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $SECURE_PORT$ トークンの置き換えに使用します。
	通知テンプレート PROTOCOL	非セキュアプロトコル、HTTP を参照してください。プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $PROTOCOL$ トークンの置き換えに使用します。
	通知テンプレート SECURE PROTOCOL	セキュアプロトコル、HTTP を参照してください。プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $SECURE_PROTOCOL$ トークンの置き換えに使用されます。
	通知 SMTP 電子メール送信者:	プロビジョニング電子メール内のユーザからの電子メールを指定します。
	SMTP サーバ名:	プロビジョニング電子メールを使用している SMTP 電子メールホストを指定します。これは、IP アドレスまたは DNS 名が可能です。

設定のタイプ	オプション	説明
パスワード管理		
	外部パスワード WAR の使用	この機能によって、外部の［パスワードを忘れた場合］の War にある［パスワードを忘れた場合］ページと、外部の［パスワードを忘れた場合］の WAR が Web サービスを経由してユーザアプリケーションを呼び戻すのに使用する URL を指定できます。 *［外部パスワード WAR の使用］*を選択した場合、*［パスワードを忘れた場合のリンク］*、*［パスワードを忘れた場合の返信リンク］*、および *［パスワードを忘れた場合の Web サービス URL］*に値を入力する必要があります。. *［外部パスワード War の使用］*を選択しない場合は、デフォルトの内部パスワード管理機能が使用されます。/jsps/pwdmgt/ForgotPassword.jsp(最初は http(s) プロトコルなし)。これは、ユーザを、外部 WAR ではなく、ユーザアプリケーションに組み込まれた［パスワードを忘れた場合］機能にリダイレクトします。
	パスワードを忘れた場合のリンク	この URL は［パスワードを忘れた場合］機能ページを指します。外部または内部のパスワード管理 WAR にある ForgotPassword.jsp ファイルを指定します。
	パスワードを忘れた場合の返信リンク	ユーザがパスワードを忘れた場合の操作を実行した後でクリックできるように、*［パスワードを忘れた場合の返信リンク］*を指定します。
	［パスワードを忘れた場合の Web サービス URL］	これは、外部の［パスワードを忘れた場合］の War がコアのパスワードを忘れた場合の機能を実行するユーザアプリケーションを呼び戻すために使用する URL です。URL のフォーマットは次のとおりです。 `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
その他	*セッションのタイムアウト*	アプリケーションセッションのタイムアウト。
	OCSP URI	クライアントインストールが On-Line Certificate Status Protocol (OCSP) を使用する場合は、Uniform Resource Identifier (URI) を指定します。たとえば、フォーマットは http://host:port/ocspLocal です。OCSP URI によって、トラステッド証明書オンラインの状態は更新されます。
	許可設定パス	許可環境設定ファイルの完全修飾名。

設定のタイプ	オプション	説明
	識別ボールトインデックスの作成	インストールユーティリティでマネージャ、ismanager、および srvprvUUID の属性のインデックスを作成する場合、このチェックボックスを選択します。これらの属性にインデックスがない場合、ユーザアプリケーションのユーザは、特にクラスタ化された環境ではユーザアプリケーションが低いパフォーマンスの状態にあります。ユーザアプリケーションをインストール後、iManager を使用して、手動でこれらのインデックスを作成できます。詳細については、116 ページのセクション 9.3.1「eDirectory でのインデックスの作成」を参照してください。 最良のパフォーマンスを得るには、インデックス作成が完了している必要があります。ユーザアプリケーションを利用可能な状態にする前にインデックスをオンラインモードにする必要があります。
	識別ボールトインデックスの削除	マネージャ、ismanager、および srvprvUUID の属性のインデックスを削除します。
	サーバDN	インデックスを作成または削除する必要のある eDirectory サーバを選択します。 **注 :** 複数の eDirectory サーバでインデックスの環境設定を行うには、configupdate ユーティリティを複数回実行する必要があります。一度に指定できるのは 1 つのサーバのみです。
コンテナオブジェクト	*選択済み*	使用する各コンテナオブジェクトタイプを選択します。
	コンテナオブジェクトタイプ	地域、国、部門、組織、およびドメインの規格コンテナから選択します。iManager 内で自分のコンテナを定義でき、これを［*新規コンテナオブジェクトの追加*］の下に追加できます。
	コンテナ属性名	コンテナオブジェクトタイプに関連する属性タイプ名をリストします。
	新規コンテナオブジェクトの追加 : コンテナオブジェクトタイプ	コンテナとして使用できる識別ボールトからオブジェクトクラス名、LDAP を指定します。
	新規コンテナオブジェクトの追加 : コンテナ属性名	コンテナオブジェクトの属性名を指定します。