Novell Identity Manager 役割ベースプロビジョニングモジュール

3.6

2008 年 1 月 18 日

www.novell.com

ユーザアプリケーション：インストールガイド

Novell®

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、いかなる黙示の保証も否認し、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、いかなる黙示の保証も否認し、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ついては、「Novell International Trade Services (http://www.novell.com/info/exports/)」の Web ページをご参照ください。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。

米国 Novell, Inc., およびノベル株式会社は、本書に記載されている製品内で実地されている技術に関連する知的所有権を有しています。具体的には、これらの知的所有権には、Novell Legal Web サイト (http://www.novell.com/company/legal/patents/) に記載されている 1 つまたは複数の米国特許、米国および他の国における 1 つまたは複数のその他の特許、または申請中の特許が含まれますが、これらに限定されるものではありません。

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 Documentation (http://www.novell.com/documentation)」の Web ページ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属します。

目次

このガイドについて

Novell® Identity Manager 役割ベースプロビジョニングモジュール 3.6 は、Identity Manager ユーザアプリケーションと役割ベースプロビジョニングで構成されています。このガイドでは、Novell Identity Manager 役割ベースプロビジョニングモジュール 3.6 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 役割ベースプロビジョニングモジュール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。オンラインヘルプ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、または www.novell.com/documentation/feedback.html にアクセスして、ご意見をお寄せください。

追加のマニュアル

Identity Manager 役割ベースプロビジョニングモジュール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。

概要

1

このセクションでは、インストールの概要およびシステム要件について説明します。主なトピックは次のとおりです。

- 9 ページのセクション 1.1「インストールの概要」
- 10 ページのセクション 1.2「インストーラプログラムの概要」
- 10 ページのセクション 1.3「システム要件」

1.1 インストールの概要

Novell® Identity Manager 役割ベースプロビジョニングモジュール 3.6 のインストール手順では、役割および役割ベースプロビジョニングモジュールの両方をサポートするユーザアプリケーションをインストールします。インストールは、次の手順で行います。

1. Identity Manager 役割ベースプロビジョニングモジュールへ移行する場合は、『*Identity Manager 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/idmrbpm36/pdfdoc/migration/migration.pdf)』を参照してください。
2. システム要件を満たしていることを確認します。詳細については、10 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。
3. Identity Manager のメタディレクトリをインストールします。手順については、『*Identity Manager 3.5.1 インストールガイド* (http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf)』を参照してください。必要なドライバを作成し、ユーザアプリケーションおよび役割ベースプロビジョニングモジュールをインストールするには、Identity Manager メタディレクトリサーバをインストールしておく必要があります。
4. インストールのために必要な準備をすべて実行します。詳細については、19 ページの第 2 章「インストールの必要条件」を参照してください。
5. ダウンロードディレクトリ内で、prerequisitefiles.zip ファイルを見つけ、圧縮解除します。圧縮解除したファイルを手動でインストールまたは適用します。
6. Designer を使用してドライバを作成および設定する場合は、Designer 2.1.1 をインストールします。「Designer のインストール (http://www.novell.com/documentation/designer21/admin_guide/index.html?page=/documentation/designer21/admin_guide/data/gsinstall.html)」を参照してください。
7. iManager または Designer 2.1.1 でユーザアプリケーションドライバを作成します。iManager でドライバを作成する方法についての説明は、33 ページのセクション 3.1「iManager でのユーザアプリケーションドライバの作成」にあります。

   Novell Identity Manager ユーザアプリケーションおよび役割ベースプロビジョニングモジュールをインストールするには、ユーザアプリケーションドライバがすでに存在している (ただし、有効にはなっていない) 必要があります。
8. iManager または Designer 2.1.1 でロールサービスドライバを作成します。iManager でドライバを作成する方法についての説明は、37 ページのセクション 3.2「iManager での役割サービスドライバの作成」にあります。

Novell Identity Manager ユーザアプリケーションおよび役割ベースプロビジョニングモジュールをインストールするには、ロールサービスドライバがすでに存在している (ただし、有効にはなっていない) 必要があります。

9 Novell Identity Manager ユーザアプリケーションおよび役割ベースプロビジョニングモジュールをインストールおよび設定します。次の章を参照してください。

- 39 ページの第 4 章「GUI を使用した JBoss へのインストール」
- 71 ページの第 5 章「コンソールまたは単一コマンドによるインストール」
- 81 ページの第 6 章「WebSphere Application Server へのインストール」

注 : WebSphere* を使用している場合は、手動で WAR ファイルを展開する必要があります。

10 インストール後に必要なタスクを実行します。

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*、または Microsoft* SQL Server* 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 では、WAR を手動で展開する必要があります。
- Novell Audit のログを有効にするよう選択した場合、ログを有効にする。
- 既存のマスタキーをインポートして、特定の役割ベースプロビジョニングモジュールインストールを復元したり、クラスタをサポートできるようにする。

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 39ページの第4章「GUIを使用したJBossへのインストール」または 81 ページの第 6 章「WebSphere Application Server へのインストール」を参照してください。
- 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、71 ページのセクション 5.1「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、71 ページのセクション 5.2「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。

1.3 システム要件

Novell Identity Manager 役割ベースプロビジョニングモジュール 3.6 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	メモ
メタディレクトリシステム (Identity Manager 3.5.1) ◆ メタディレクトリエンジン ◆ Novell Audit エージェント ◆ サービスドライバ ◆ Identity Manager ドライバ ◆ ユーティリティ (アプリケーションツール、および Novell Audit Setup ツールを含む)	次のいずれかのオペレーティングシステムが必要です。 ◆ Netware® 6.5 SP6 ◆ 最新のサポートパックを適用した Novell Open Enterprise Server (OES) 1.0 ◆ Novell Open Enterprise Server (OES) 2.0 ◆ 最新のサービスパックを適用した Windows* 2000 Server (32 ビット) ◆ 最新のサービスパックを適用した Windows Server 2003 (32 ビット) ◆ Red Hat Linux 3.0、4.0、5.0 ES および AS (32 ビットと 64 ビットの両方がサポートされています) ◆ 最新のサポートパックを適用した SUSE Linux Enterprise Server 9 および 10 (32 ビットと 64 ビットの両方がサポートされています) ◆ Solaris* 9 または 10 ◆ AIX* 5.2L、バージョン 5.2 または 5.3 次のいずれかのバージョンの eDirectory™ が必要です。 ◆ eDirectory 8.7.3.10 ◆ eDirectory 8.8.1 または 8.8.2 2.0.5 (NMAS™ 3.1.3)	メタディレクトリシステムプラットフォームを使用している場合は、お使いの実装において VMware* を使用できます。 このリリースの Identity Manager ソフトウェアコンポーネントはすべて、64 ビットプロセッサまたは 64 ビットオペレーティングシステムで動作していても、32 ビットです。別途指定されている場合以外は、OES、NetWare、Windows、および Linux プラットフォーム (Red Hat* および SUSE®) では、次のプロセッサはすべて 32 ビットモードでサポートされます。 ◆ Intel* x86-32 ◆ AMD* x86-32 ◆ Intel EM64T ◆ AMD Athlon64*およびOpteron* Identity Manager は eDirectory 8.8 の次の機能をサポートしています。 ◆ 同じサーバ上にある eDirectory の複数のインスタンス ◆ 暗号化属性 eDirectory 8.8 は 64 ビット Red Hat Linux 4.0 をサポートしています。 Windows Server 2003 では 64 ビットバージョンのパスワード同期を利用できます。 eDirectory 8.8 をインストールする前に、必ず eDirectory データベースを完全にバックアップしてください。eDirectory 8.8 はデータベース構造の一部をアップグレードし、その後でロールバックはできません。 Xen Virtual Machine (VM) で SLES 10 を並行仮想化モードでゲストオペレーティングシステムとして実行している場合、SUSE Linux Enterprise Server 10 において Xen* の視覚化機能がサポートされるようになりました。SLES 10 用の Xen パッチが必要です (TID 番号 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=52670386&stateId=1%200%204926187) を参照)。

必須システムコンポーネント	システム要件	メモ
Web ベースの管理サーバ ◆ パスワード ◆ iManager 2.6 およびプラグイン ◆ iManager 2.7 およびプラグイン ◆ ドライバ環境設定	次のいずれかのオペレーティングシステムが必要です。 ◆ 最新のサポートパックを適用した、NetWare 上の Novell Open Enterprise Server (OES) 1.0 ◆ Novell Open Enterprise Server (OES) 2.0 ◆ 最新のサポートパックを適用した NetWare 6.5 ◆ 最新のサービスパックを適用した Windows 2000 Server (32 ビット) ◆ 最新のサービスパックを適用した Windows Server 2003 (32 ビット) ◆ Microsoft Windows Vista* ◆ Red Hat Linux 3.0、4.0、5.0 ES および AS (32 ビットと 64 ビットの両方がサポートされています) ◆ 最新のサポートパックを適用した Solaris* 9 または 10 ◆ 最新のサポートパックを適用した SUSE Linux Enterprise Server 9 または 10 (32 ビットと 64 ビットの両方がサポートされています) iManager Workstation を使用してサポートされるオペレーティングシステムは次のとおりです。 ◆ 最新のサービスパックを適用した Windows 2000 Professional ◆ Windows XP SP2 ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 次のソフトウェアが必要です。 ◆ 最新のサポートパックとプラグインを適用した Novell iManager 2.6 または 2.7	このリリースの Identity Manager ソフトウェアコンポーネントはすべて、64 ビットプロセッサまたは 64 ビットオペレーティングシステムで動作していても、32 ビットです。 別途示されている場合以外は、OES、NetWare、Windows、および Linux プラットフォーム (Red Hat および SUSE) では次のプロセッサのすべてが 32 ビットモードでサポートされます。 ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 および Opteron ◆ サポートされるブラウザは、iManager 2.6 により決まります。このリストには現在、次のブラウザが含まれています。 ◆ Internet Explorer* 6、SP1 以降 ◆ Internet Explorer 7 ◆ Firefox* 2.0 以降 ◆ iManager 設定ウィザードまたは Designer ユーティリティを実行して、ポータルコンテンツを eDirectory にインストールまたは展開する必要があります。 ◆ (Windows の場合) Novell Client™ 4.9 は、ノベル用ダウンロードの Web サイト (http://download.novell.com/index.jsp) から入手できます。 ◆ iManager によって他のツリーにログインしてリモート Identity Manager サーバを管理すると、リモートサーバの IP アドレスの代わりにサーバ名を使用している場合はエラーが発生することがあります。 ◆ パスワード同期エージェントは 64 ビット版の Windows 2003 上でのみサポートされます。

必須システムコンポーネント	システム要件	メモ
セキュアログサービス ◆ セキュアログサーバ ◆ プラットフォームエージェント (クライアントコンポーネント) ◆ Novell Audit 2.0.2 または Sentinel™ 5.1.3	セキュアログサーバでは、次のオペレーティングシステムのいずれかがサポートされます。 ◆ 最新のサポートパックを適用した Novell Open Enterprise Server (OES) 1.0 または 2.0 ◆ 最新のサポートパックを適用した NetWare 6.5 ◆ 最新のサービスパックを適用した Windows 2000 Server (32 ビット) ◆ 最新のサービスパックを適用した Windows Server 2003 (32 ビット) ◆ Linux Red Hat Linux 3.0、4.0、5.0 ES または AS (32 ビットおよび 64 ビット。ただし、Novell Audit は 32 ビットモードでのみ動作します) ◆ 最新のサポートパックを適用した Solaris 9 または 10 ◆ 最新のサポートパックを適用した SUSE Linux Enterprise Server 9 または 10 (32 ビットおよび 64 ビット。ただし、Novell Audit は 32 ビットモードでのみ動作します) ◆ 最新のサポートパックを適用した Novell eDirectory 8.7.3.6 または 8.8 (セキュアログサーバにインストールする必要があります) プラットフォームエージェントでは、次のオペレーティングシステムのいずれかがサポートされます。 ◆ Novell Open Enterprise Server (OES) 1.0 SP1 または最新のサポートパック ◆ 最新のサポートパックを適用した NetWare 6.5 ◆ 最新のサービスパックを適用した Windows 2000 または 2000 Server、XP、あるいは Windows Server 2003 (32 ビット) ◆ Red Hat Linux 3、4 AS または ES (32 ビットおよび 64 ビット。ただし、Novell Audit は 32 ビットモードのみ動作します) ◆ Solaris 8、9、または 10 ◆ SUSE Linux Enterprise Server 9 または 10 (32 ビットおよび 64 ビット。ただし、Novell Audit は 32 ビットモードでのみ動作します) 最新のサポートパックとプラグインを適用した iManager 2.6 または 2.7	OES、NetWare、Windows、および Linux プラットフォーム (Red Hat および SUSE) では次のプロセッサのすべてが 32 ビットモードでサポートされます。 ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 および Opteron セキュアサーバの最小要件は次のとおりです。 ◆ Pentium II 400 MHz を搭載したシングルプロセッサのサーバクラス PC ◆ 最低 40MB のディスク容量 ◆ 512 MB RAM eDirectory イベントのログ記録を可能にする eDirectory Instrumentation では、次のバージョンの eDirectory がサポートされます。 ◆ eDirectory 8.7.3 (NetWare、Windows、Linux、および Solaris) ◆ 最新のサポートパックを適用した eDirectory 8.8 NetWare イベントのログ記録を可能にする NetWare Instrumentation では、次のバージョンの NetWare がサポートされます。 ◆ 最新のサポートパックを適用した NetWare 5.1 ◆ 最新のサポートパックを適用した NetWare 6.0 ◆ 最新のサポートパックを適用した NetWare 6.5 または NetWare 6.5 ◆ 最新のサポートパックを適用した Novell Open Enterprise Server (OES)

必須システムコンポーネント	システム要件	メモ
ユーザアプリケーションのアプリケーションサーバ	次に説明するように、ユーザアプリケーションは JBoss* および WebSphere 上で動作します。 JBoss 4.0.5 GA は次のサーバでサポートされています。 ◆ Novell Open Enterprise Server (OES) 1.0 SP2 または最新のサポートパック -- Linux のみ ◆ SUSE Linux Enterprise Server 9 SP2 (OES 1.0 SP2 に付属) または 10.1.x (64 ビット JVM*) ◆ Windows 2000 Server SP4 (32 ビット) ◆ Windows 2003 Server SP1 (32 ビット) ◆ Solaris 10 サポートパック (日付が 6/06 のもの) WebSphere 6.1 は次のプラットフォームでサポートされています。 ◆ Solaris 10 (64 ビット) ◆ Windows 2003 SP1 ユーザアプリケーションには JRE* 1.5.0_14 が必要です。	SUSE Linux Enterprise Server では、次のプロセッサが 32 ビットモードでサポートされます。 ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 および Opteron SUSE Linux Enterprise Server は次のプロセッサでは 64 ビットモードで動作します。 ◆ Intel EM64T ◆ AMD Athlon64 ◆ AMD Opteron ◆ Sun* SPARC* Xen Virtual Machine (VM) で SLES 10 を並行仮想化モードでゲストオペレーティングシステムとして実行している場合、SUSE Linux Enterprise Server 10 において Xen* の視覚化機能がサポートされるようになりました。SLES 10 用の Xen パッチが必要です (TID 番号 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=52670386&stateId=1%200%204926187) を参照)。

必須システムコンポーネント	システム要件	メモ
ユーザアプリケーションのブラウザ	次に説明するように、ユーザアプリケーションは Firefox と Internet Explorer の両方をサポートしています。 Firefox 2 は次のプラットフォームでサポートされています。 ◆ Windows 2000 Professional SP4 ◆ Windows XP SP2 ◆ Red Hat Enterprise Linux WS 4.0 ◆ Novell Linux Desktop 9 ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 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 2000 Professional SP4 ◆ Windows XP SP2 ◆ Windows Vista Enterprise バージョン 6 Internet Explorer 6 SP1 は次のプラットフォームでサポートされています。 ◆ Windows 2000 Professional SP4 ◆ Windows XP SP2	
ユーザアプリケーション用のデータベースサーバ ◆ MySQL ◆ Oracle ◆ MS SQL ◆ DB2	JBoss では次のデータベースがサポートされています。 ◆ MySQL バージョン 5.0.27 ◆ Oracle 9i (9.2.0.1.4) ◆ Oracle 10g リリース 2 (10.2.0.1.0) ◆ MS SQL 2005 SP1 WebSphere では次のデータベースがサポートされています。 ◆ Oracle 10g リリース 2 (10.2.0) ◆ MS SQL 2005 SP1 ◆ DB2 DV2 v9.1.0.0	ユーザアプリケーションは、環境設定データの保存や、処理中の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。 セキュアログサービスと、ユーザアプリケーションおよびワークフローのプロビジョニングには、どちらもデータベースが必要です。1 つのデータベースを設定して両方のアプリケーションにサービスを提供するか、それぞれに独立したデータベースを設定することができます。セキュアログサービスには、特定のデータベースは含まれていません。 Oracle はシンクライアントドライバおよび OCI クライアントドライバの両方でサポートされています。

必須システムコンポーネント	システム要件	メモ
ワークステーション ◆ Designer 2.1.1 for Identity Manager 3.5.1 ◆ iManager による Web アクセス	Designer は、次のプラットフォームでテストされています。 Windows: ◆ 最新のサービスパックを適用した Windows 2000 Professional ◆ Windows XP SP2 ◆ Microsoft Windows Vista Linux: ◆ SUSE Linux Enterprise Server 10 (Designer の場合のみ) ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ Red Hat Enterprise Linux WS 4.0 (Designer のみ)、デフォルトは Gnome* ◆ Red Hat Fedora Core 5 (Designer のみ)、デフォルトは Gnome ◆ Novell Linux Desktop 9、デフォルトは KDE	Designer は、Eclipse を開発プラットフォームとして使用します。プラットフォーム固有の情報については、Eclipse の Web サイト (http://www.eclipse.org) を参照してください。 Designer のハードウェアの最小および推奨要件は次のとおりです。 ◆ プロセッサ : 最低 1 GHz、2 GHz 以上を推奨 ◆ RAM: 最低 512 MB、1 GB 以上を推奨 ◆ 解像度 : 最低 1024 x 768、1280 x 1024 を推奨 ソフトウェアの前提条件は次のとおりです。 ◆ Microsoft Internet Explorer 6.0 SP1 ◆ Microsoft Internet Explorer 7 ◆ または Mozilla* Firefox 2.0

必須システムコンポーネント	システム要件	メモ
接続されたシステムサーバ (リモートローダが実行されるサーバとは別のサーバでホストされます) ◆ リモートローダ ◆ リモートローダ設定ツール (Windows のみ) ◆ Novell Audit エージェント ◆ パスワード同期エージェント ◆ 接続されたシステムのドライバシム ◆ 接続されたシステムのツール	ドライバでは、接続されたシステムが使用可能であること、関連する API が提供されていることが必要です。 各システムに固有のオペレーティングシステムおよび接続システムの要件については、Identity Manager ドライバのマニュアル (http://www.novell.com/documentation/idm35drivers) を参照してください。	接続されたアプリケーションの場合は、アプリケーション固有の知識と責任を持つユーザが必要です。 リモートローダシステム : ◆ 最新のサポートパックを適用した Windows NT* 4.0、Windows 2000 Server、または Windows Server 2003 ◆ 最新のサービスパックを適用した Windows Server* 2003 (64 ビット) ◆ パスワード同期エージェントは Windows Server 2003 (64 ビット) でサポートされています ◆ Red Hat Linux 3.0、4.0、5.0 ES または AS ◆ SUSE Linux Enterprise Server 9 または 10 ◆ AIX 5.2L、バージョン 5.2 または 5.3 Java リモートローダシステム : ◆ HP-UX* 11i ◆ OS/400 ◆ xOS* ◆ JVM 1.4.2 以降がインストールされているシステムで使用できる必要があります
Audit	Novell Audit 2.0.2	
ユーザアプリケーションの SSO 統合	Novell Access Manager 3.0.1 が必要です。	JDK*1.5 で作成された saslsaml.jar のバージョンを含みます。

インストールの必要条件

2

このセクションでは、Identity Manager 役割ベースプロビジョニングモジュールをインストールするための前提条件について説明します。主なトピックは次のとおりです。

2.1 Java Development Kit

JBoss、WebSphere、および識別ボールトには、それぞれ独自の Java Development Kit の要件があります。

JBoss アプリケーションサーバ : JBoss アプリケーションサーバでは、Java 2 Platform Standard Edition Development Kit バージョン 1.5.0_14 を使用します。

次のように、このバージョンの Sun JDK を使用して、役割ベースプロビジョニングモジュールのインストーラを起動します。

Linux または Solaris:

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

Windows:

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

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/jdk1.5.0_10
```

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ありません。

WebSphere アプリケーションサーバ : WebSphere* アプリケーションサーバでは、WebSphere Application Server 6.1.0.9 以降に付属する IBM JDK を使用し、無制限ポリシーファイルを適用してください。6.1.0.9 用の WAS JDK FixPack を適用します。

識別ボールト (メタディレクトリ) インストーラ : 識別ボールト (メタディレクトリ) インストーラは、NetWare® を除くすべてのプラットフォームに専用の JVM のコピーをイン

ストールします。NetWare では、識別ボールトはシステムにインストールされているどのバージョンの Java でも使用します。

2.2 Identity Manager メタディレクトリのインストール

Identity Manager 3.5.1 のメタディレクトリをインストールします。手順については、『*Novell Identity Manager 3.5.1 インストールガイド* (http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf)』に記載されています。

Identity Manager 役割ベースプロビジョニングモジュール管理者に識別ボールトへのアクセスを付与します。このためには、iManager で、Identity Manager 役割ベースプロビジョニングモジュールのユーザが存在するコンテキストに管理者アクセスを割り当てます。

2.3 JBoss アプリケーションサーバのインストール

JBoss* アプリケーションサーバを使用する予定の場合、次のいずれかを実行します。

- 製造元の指示に従って、JBoss 4.2.0 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。
- 役割ベースプロビジョニングモジュール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 ページのセクション 2.3.1 「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。

JBoss サーバは、Identity Manager 役割ベースプロビジョニングモジュールのインストールが終了するまで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。

RAM: Identity Manager 役割ベースプロビジョニングモジュールを実行するための推奨 RAM 容量は、最低 512MB です。

ポート : 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。役割ベースプロビジョニングモジュールのインストール時に、このポートを入力する必要があります。(アプリケーションサーバのデフォルトは 8080 です)。

SSL: 外部のパスワード管理機能を使用する場合は、Identity Manager 役割ベースプロビジョニングモジュールおよび IDMPwdMgt.war ファイルの展開先の JBoss サーバで、SSL を有効にします。SSL を有効にする手順については、JBoss のマニュアルを参照してください。また、ファイアウォールの SSL ポートが開いていることも確認してください。IDMPwdMgt.war ファイルの詳細については、112 ページのセクション 7.5「外部パスワード WAR へのアクセス」を参照してください。また、『*IDM ユーザアプリケーション : 管理ガイド* (http://www.novell.com/documentation/idmrbpm36/index.html)』も参照してください。

2.3.1 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 ユーティリティを使用して、JBoss アプリケーションサーバと MySQL をシステムにインストールできます。

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。JBoss アプリケーションサーバを Windows システムにサービスとしてインストールするには、24 ページのセクション 2.3.2「JBoss アプリケーションサーバのサービスとしての インストール」を参照してください。

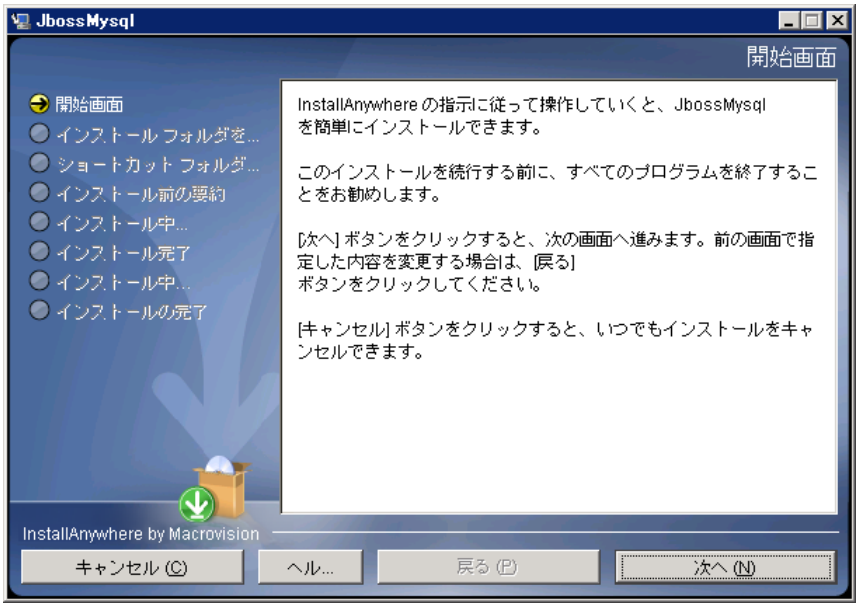
1 JbossMysql.bin または JbossMysql.exe を参照して実行します。このユーティリティは、次の場所にあるユーザアプリケーションインストーラにバンドルされています。

/linux/user_application (Linux の場合)
/nt/user_application (Windows の場合)

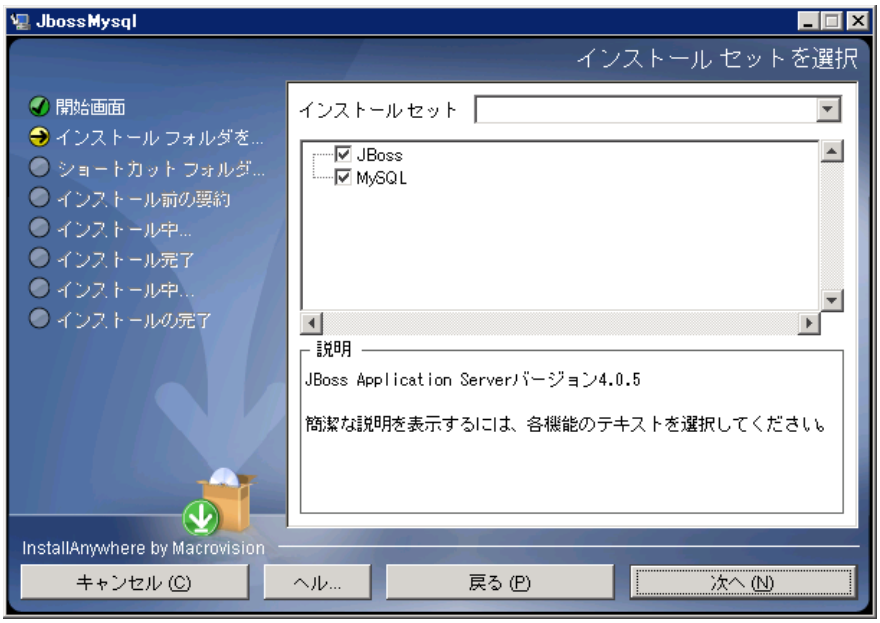
Solaris 用のユーティリティはありません。

2 ロケールを選択します。

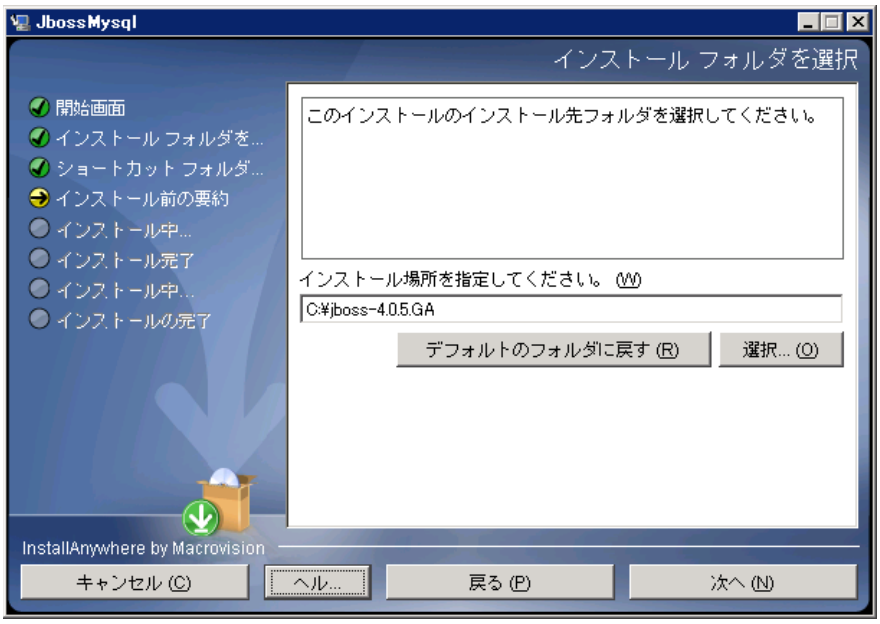
3 導入ページを読み、［次へ］をクリックします。



4 インストールする製品を選択し、［次へ］をクリックします。

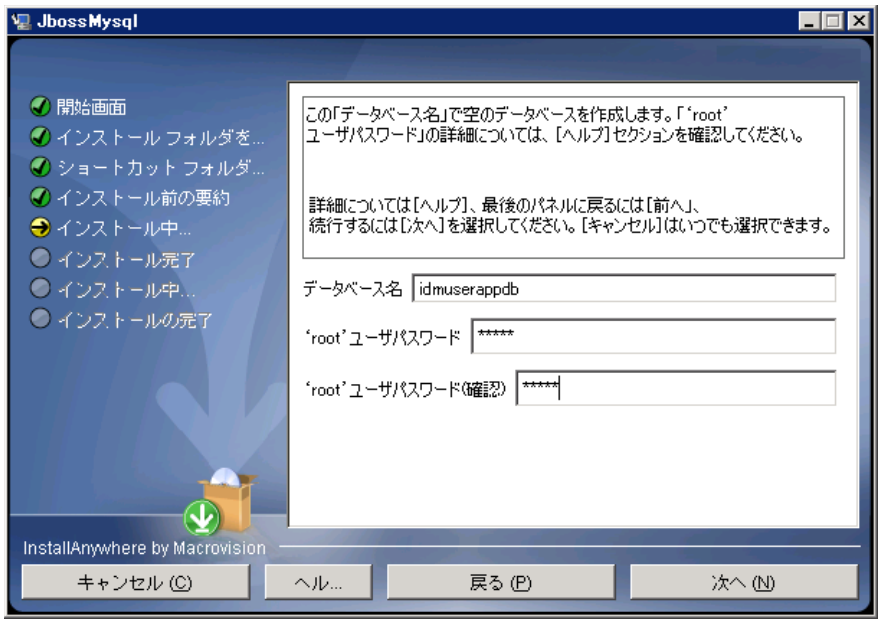


5 ［*選択*］をクリックして、選択した製品をインストールする基本フォルダを選択し、［*次へ*］をクリックします。



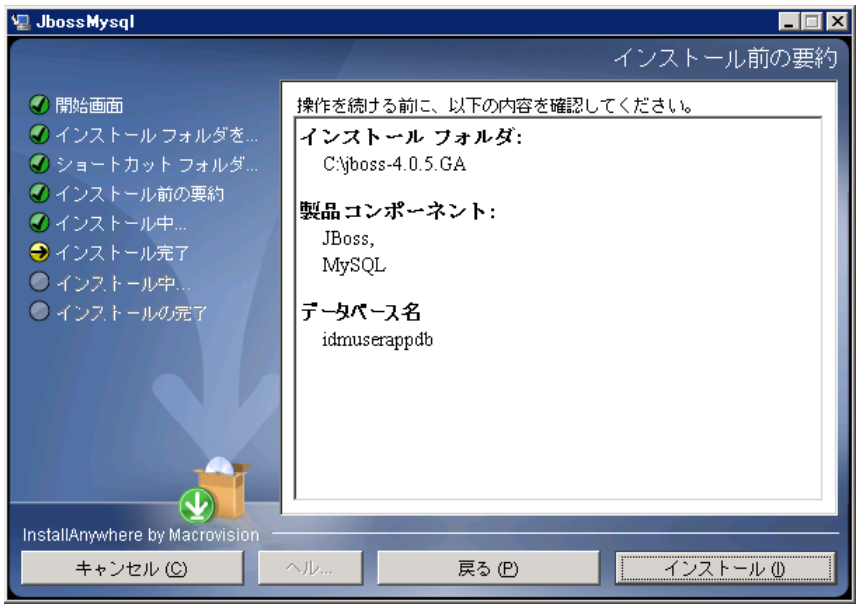
6 データベースの名前を指定します。この名前はユーザアプリケーションをインストールするために必要です。

7 データベースの root ユーザのパスワードを指定します。



8 ［次へ］をクリックします。

9 ［インストール前の概要］で指定した内容を確認し、［インストール］をクリックします。



選択した製品がインストールされると、正常に完了したことを示すメッセージが表示されます。MySQL データベースをインストールした場合は、25 ページのセクション 2.5.2「MySQL データベースの環境設定」に進みます。

2.3.2 JBoss アプリケーションサーバのサービスとしてのインストール

JBoss アプリケーションサーバをサービスとして実行するには、Java Service Wrapper またはサードパーティのユーティリティを使用します。http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows (http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows) に掲載されている JBoss の指示を参照してください。

このセクションは次のトピックで構成されています。

- 24 ページの 「Java Service Wrapper の使用」
- 24 ページの 「サードパーティのユーティリティの使用」

Java Service Wrapper の使用

Java Service Wrapper を使用すると、JBoss アプリケーションサーバを Windows サービス、あるいは Linux または UNIX のデーモンとしてインストール、起動、および停止できます。使用できるユーティリティとダウンロードサイトについては、インターネットで確認してください。

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。次に、サンプル環境設定ファイルをいくつか示します。

wrapper.conf :

wrapper.java.command=%JAVA_HOME%/bin/java

wrapper.java.mainclass=org.tanukisoftware.wrapper.WrapperSimpleApp

wrapper.java.classpath.1=%JBOSS_HOME%/server/default/lib/wrapper.jar

wrapper.java.classpath.2=%JAVA_HOME%/lib/tools.jar wrapper.java.classpath.3=./run.jar

wrapper.java.library.path.1=%JBOSS_HOME%/server/default/lib wrapper.java.additional.1=-server wrapper.app.parameter.1=org.jboss.Main wrapper.logfile=%JBOSS_HOME%/server/default/log/wrapper.log wrapper.ntservice.name=JBoss wrapper.ntservice.displayname=JBoss Server

---

重要 : JBOSS_HOME 環境変数を正しく設定する必要があります。ラッパ自体はこの環境変数を設定しません。

---

java-service-wrapper-service.xml : <Xxml version="1.0" encoding="UTF-8"?><!DOCTYPE server><server> <mbean code="org.tanukisoftware.wrapper.jmx.WrapperManager" name="JavaServiceWrapper:service=WrapperManager"/> <mbean code="org.tanukisoftware.wrapper.jmx.WrapperManagerTesting" name="JavaServiceWrapper:service=WrapperManagerTesting"/></server

サードパーティのユーティリティの使用

以前のバージョンでは、JavaService といったサードパーティのユーティリティを使用して、JBoss アプリケーションサーバを Windows サービ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したが、

重要 : 現在では、JBoss は JavaService の使用を推奨していません。詳細については、http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService (http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService) を参照してください。

2.4 WebSphere Application Server のインストール

WebSphere Application Server を使用する場合、WebSphere 6.1.0.9 をダウンロードしてインストールします。6.1.0.9 用の WAS JDK FixPack を適用します。

2.5 データベース

データベースとデータベースドライバをインストールして、データベースまたはデータベースインスタンスを作成します。Identity Manager 役割ベースプロビジョニングモジュールのインストール手順で使用するために、次のデータベースパラメータを記録しておきます。

- 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

データソースファイルがこのデータベースを指している必要があります。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、Identity Manager 役割ベースプロビジョニングモジュールの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 役割ベースプロビジョニングモジュール 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 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。

データベースでは UTF-8 を有効にする必要があります。

- 25 ページのセクション 2.5.1「MySQL のインストール」
- 25 ページのセクション 2.5.2「MySQL データベースの環境設定」

2.5.1 MySQL のインストール

IDM ユーザアプリケーションユーティリティを使用して MySQL* をインストールするか、MySQL を自分でインストールする場合は、25 ページのセクション 2.5.2「MySQL データベースの環境設定」を参照してください。

注 : データベースを移行する場合は、インストールプログラムで移行オプションを選択する前にデータベースを起動しておきます。データベースを移行しない場合は、Identity Manager 役割ベースプロビジョニングモジュールのインストール時にデータベースが実行されていなくてもかまいません。この場合、アプリケーションサーバを起動する前にデータベースを起動してください。

2.5.2 MySQL データベースの環境設定

MySQL と Identity Manager 3.5.1 が連携動作するように、MySQL の環境設定を行う必要があります。MySQL を自分でインストールした場合は、設定も自分で行う必要がありま

す。JbossMysql を使用して MySQL をインストールした場合は、このユーティリティが正しい値を設定してくれますが、次のために維持する値を知っておく必要があります。

- 26 ページの 「INNODB ストレージエンジンとテーブルタイプ」
- 26 ページの 「文字セット」
- 26 ページの 「大文字と小文字の区別」

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。

文字セット

サーバ全体またはデータベース単体に対し、文字セットとして UTF8 を指定します。サーバ全体に UTF8 を指定するには、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;

データベースの文字セットを指定した場合は、次に示すように、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&characterEncoding

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。

2.6 セキュリティ上の前提条件

Novell Access Manager™ または iChain® の［Cookie Forward］オプションをオンにすると、Identity Manager 役割ベースプロビジョニングモジュールの［同時ログアウト］を有効にできます。手順については、『*Novell Access Manager 3.0 SP1 管理ガイド*』の「Cookie ヘッダへの差し込み (http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b5pqck8.html)」を参照してください。

2.7 製品のダウンロード

Novell ダウンロード (http://download.novell.com/index.jsp) から、Identity Manager 役割ベースプロビジョニングモジュール 3.6 の製品を入手します。

正しいユーザアプリケーションの .iso イメージファイルをダウンロードします。正しいイメージファイルは、Identity_Manager_3_6_0_User_Application_Provisioning.iso です。

この .iso ファイルには次の配信ディレクトリが含まれています。

/linux/user_application (Linux 用)
/nt/user_application (Windows 用)
/solaris/user_application (Solaris 用)
/36MetaDirSupport (IDM 3.6 ユーザアプリケーションをサポートするように IDM 3.5.1 メタディレクトリを更新するために必要なファイルを含む)

表 2-1 は、Identity Manager 役割ベースプロビジョニングモジュール 3.6 をインストールするのに必要なファイルおよびスクリプトの一覧を示しています。

表 2-1 *Identity Manager 3.6 ユーザアプリケーションのインストールに必要なファイルとスクリプト*

ファイル	説明
IDMProv.war	これは、役割ベースプロビジョニングモジュールの WAR です。Identity Manager 3.6 ユーザアプリケーションと、Identity セルフサービス機能および役割ベースプロビジョニングモジュールが含まれています。
IDMUserApp.jar	これは、役割ベースプロビジョニングモジュールのインストールプログラムです。
silent.properties	このファイルには、サイレントインストールに必要なインストールパラメータが含まれています。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。
prerequisitefiles.zip	この ZIP ファイルには、手動でのインストールが必要なその他のファイルが含まれます。
UserApplication_3_6_0-IDM3_5_1-V1.xml	これは、ユーザアプリケーションドライバ用の設定ファイルです。

ファイル	説明
iManager_icons_for_roles.zip	これには、eDirectory の役割オブジェクト用の iManager アイコンが含まれます。

ヒント：iManager_icons_for_roles.zip および prerequisites.zip は、/36MetaDirSupport ディレクトリ内にあります。その他のファイルは、<*operating_system*> /user_application ディレクトリ内にあります。

Identity Manager 役割ベースプロビジョニングモジュールをインストールするシステムには、少なくとも 320 MB の空き容量が必要です。

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)。

2.8 prerequisitefiles.zip ファイルの内容のインストール

ダウンロードした .iso イメージで prerequisitefiles.zip ファイルを探し、そのファイルを圧縮解除します。この中には、表 2-2 に示されている、手動でインストールする必要があるファイルが含まれています。

表 2-2 手動でのインストールが必要なファイル

ファイル名	説明	説明
nrf-extensions.sch	eDirectory™ スキーマファイル	29 ページのセクション 2.8.1「役割ベースプロビジョニングモジュールバージョン 3.6 用の eDirectory スキーマの拡張」
nrfdriver.jar	役割サービスドライバの JAR	30 ページのセクション 2.8.2「役割サービスドライバ用の JAR ファイルのコピー」
RoleService-IDM3_5_1-V1.xml	役割サービスドライバの設定ファイル	31 ページのセクション 2.8.3「役割サービスドライバの設定ファイルのコピー」
UserApplicationn_3_6_0-IDM3_5_1-V1.xml	役割ベースプロビジョニングモジュールをサポートするユーザアプリケーションドライバの設定ファイル	31 ページのセクション 2.8.4「ユーザアプリケーションドライバの設定ファイルのコピー」
dirxml.lsc	ロギングアプリケーションのログスキーマファイル	31 ページのセクション 2.8.5「dirxml.lsc ファイルのコピー」

- 29 ページのセクション 2.8.1「役割ベースプロビジョニングモジュールバージョン 3.6 用の eDirectory スキーマの拡張」
- 30 ページのセクション 2.8.2「役割サービスドライバ用の JAR ファイルのコピー」
- 31 ページのセクション 2.8.3「役割サービスドライバの設定ファイルのコピー」
- 31 ページのセクション 2.8.4「ユーザアプリケーションドライバの設定ファイルのコピー」
- 31 ページのセクション 2.8.5「dirxml.lsc ファイルのコピー」

2.8.1 役割ベースプロビジョニングモジュールバージョン 3.6 用の eDirectory スキーマの拡張

次の各セクションの説明に従って、役割ベースプロビジョニングモジュール用に eDirectory スキーマを拡張します。

- 29 ページの 「Windows でスキーマを拡張する」
- 30 ページの 「UNIX/Linux でスキーマを拡張する」
- 30 ページの 「NetWare でスキーマを拡張する」

Windows でスキーマを拡張する

Windows サーバのスキーマを拡張するには、NDSCons.exe を使用します。eDirectory に付属しているスキーマファイル (*.sch) は、デフォルトで C:\Novell\NDS ディレクトリにインストールされます。

1. *[スタート] > [設定] > [コントロールパネル] > [Novell eDirectory サービス]* の順にクリックします。
2. *install.dlm* をクリックし、*[開始]* をクリックします。

3 *［Install Additional Schema Files (追加のスキーマファイルのインストール)］*をクリックし、*［次へ］*をクリックします。

4 管理権を持つユーザとしてログインし、*［OK］*をクリックします。

5 スキーマファイルのパスおよび名前 (たとえば、c:\Novell\NDS\nrf-extensions.sch など) を指定します。

6 ［*完了*］をクリックします。

UNIX/Linux でスキーマを拡張する

UNIX/Linux プラットフォームで役割ベースプロビジョニングモジュール用に eDirectory スキーマを拡張するには、次の手順を実行します。

1 役割ベースプロビジョニングモジュールスキーマファイルである nrf-extensions.sch を追加します。追加するには、コマンドラインから次のように ndssch コマンドを入力します。

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

NetWare でスキーマを拡張する

NetWare サーバのスキーマを拡張するには、NWConfig.nlm を使用します。eDirectory に付属しているスキーマファイル (*.sch) は、sys:\system\schema ディレクトリにインストールされます。

1 サーバコンソールで、「nwconfig」と入力します。

2 *［ディレクトリオプション］*>*［スキーマの拡張］*の順に選択します。

3 管理権を持つユーザとしてログインします。

4 <F3> を押して異なるパスを指定し、sys:\system\schema (または *.sch ファイルのパス) および nrf-extensions.sch スキーマファイルを入力します。

5 <Enter> を押します。

2.8.2 役割サービスドライバ用の JAR ファイルのコピー

メタディレクトリサーバに手動で役割サービスドライバをインストールします。インストールするには、実行可能な役割サービス JAR ファイル nrfdriver.jar を、圧縮解除した prerequisitefiles.zip アーカイブから、システムの正しいディレクトリにコピーします。

表 2-3 *役割サービスドライバの JAR ファイルの場所*

オペレーティングシステム	ディレクトリ
UNIX (eDirectory 8.7.x)	/usr/lib/dirxml/classes
UNIX (eDirector 8.8.x)	/opt/novell/eDirectory/lib/dirxml/classes
Windows	<drive>:\novell\nds\lib
NetWare	SYS:SYSTEM\LIB

2.8.3 役割サービスドライバの設定ファイルのコピー

役割サービスドライバの設定ファイル RoleService_IDM3_5_1-V1.xml を、システムの正しいディレクトリに手動でインストールします。

表 2-4 役割サービスドライバの設定ファイルの場所

オペレーティングシステム	ディレクトリ
Linux (eDirectory 8.7.x)	/usr/lib/dirxml/classes
Linux (eDirectory 8.8)	/var/opt/novell/iManager/nps/DirXML.Drivers
Windows	C:\Program Files\Novell\tomcat\webapps\nps\Dirxml.Drivers
NetWare	SYS:\tomcat\4\webapps\nps\Dirxml.Drivers

2.8.4 ユーザアプリケーションドライバの設定ファイルのコピー

ユーザアプリケーションドライバの設定ファイル UserApplication_3_6_0-IDM3_5_1-V1.xml を、システムの正しいディレクトリに手動でインストールします。

表 2-5 ユーザアプリケーションドライバの設定ファイルの場所

オペレーティングシステム	ディレクトリ
Linux (eDir 8.7.x)	/usr/lib/dirxml/classes
Linux (eDir 8.8)	/var/opt/novell/iManager/nps/DirXML.Drivers
Windows	C:\Program Files\Novell\tomcat\webapps\nps\Dirxml.Drivers
NetWare	SYS:\tomcat\4\webapps\nps\Dirxml.Drivers

2.8.5 dirxml.lsc ファイルのコピー

『Identity Manager Y ユーザアプリケーション : 管理ガイド (http://www.novell.com/documentation/idmrbpm36/pdfdoc/agpro/agpro.pdf)』の「ログの設定」セクションでの説明に従って、dirxml.lsc ファイルを Audit サーバにコピーします。

2.9 役割用の iManager アイコンのインストール

ダウンロードした .iso イメージで、iManager_icons_for_roles.zip ファイルを探し、そファイルを圧縮解除します。圧縮解除したアイコンファイルを nps/portal/modules/dev/images/dir ディレクトリにコピーします。iManager を再起動し、新しいアイコンが使用されるようにします。

ドライバの作成

3

このセクションでは、役割ベースプロビジョニングモジュールを使用するために必要なドライバの作成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。

利用可能なドライバ設定は次のとおりです。

- iManager で、ドライバセットごとに役割サービスドライバを 1 つ追加できます。
- 1 つのユーザアプリケーションドライバは、1 つの役割サービスドライバに関連付けることができます。
- 1 つのユーザアプリケーションは、1 つのユーザアプリケーションドライバに関連付けることができます。

3.1 iManager でのユーザアプリケーションドライバの作成

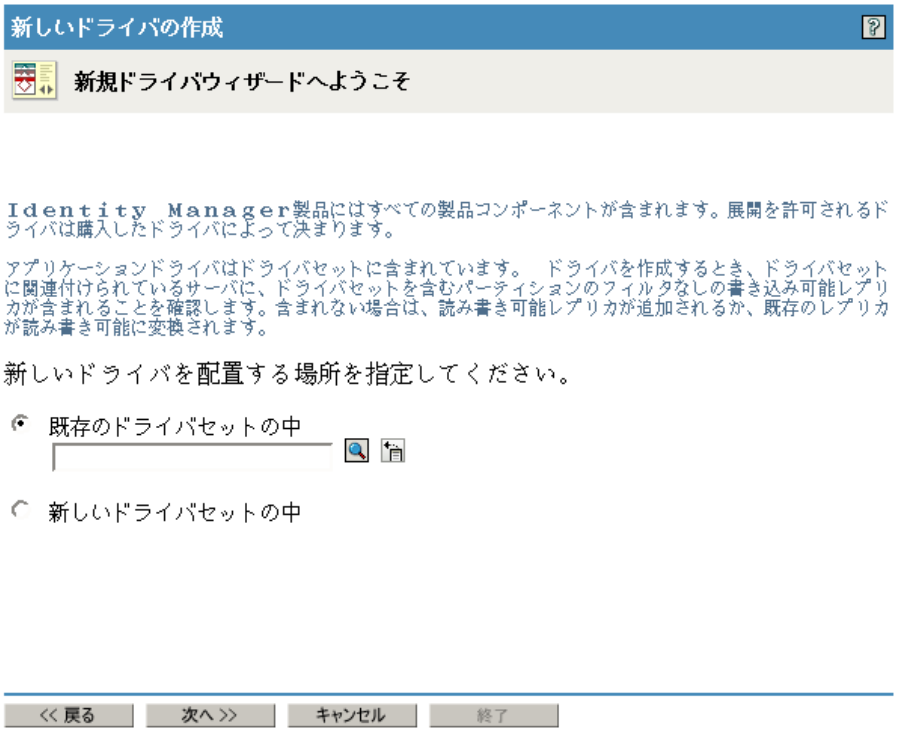
クラスタのメンバーである役割ベースプロビジョニングモジュールを除き、Identity Manager 役割ベースプロビジョニングモジュールごとに個別のユーザアプリケーションドライバを作成する必要があります。同じクラスタに属する役割ベースプロビジョニングモジュールは、単一のユーザアプリケーションドライバを共有する必要があります。クラスタで役割ベースプロビジョニングモジュールを実行する場合は、『*Identity Manager ユーザアプリケーション管理ガイド* (http://www.novell.com/documentation/idmrbpm36/index.html)』を参照してください。

役割ベースプロビジョニングモジュールは、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。

重要 : クラスタ以外の役割ベースプロビジョニングモジュール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ドライバセットに関連付ける

1. iManager 2.6 以降を Web ブラウザで開きます。
2. *［役割とタスク］* > *［Identity Manager ユーティリティ］* の順に選択し、［*新規ドライバ*］を選択してドライバ作成ウィザードを起動します。

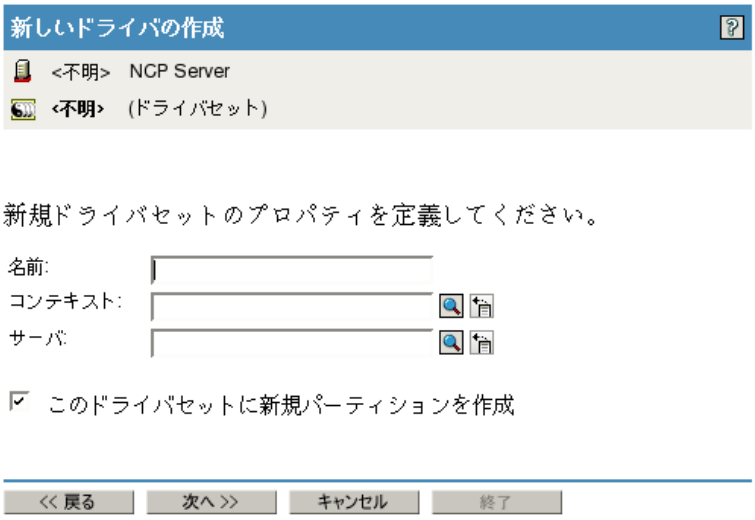


3 既存のドライバセット内にドライバを作成するには、［*既存のドライバセットの中*］を選択して、オブジェクトセレクタアイコンをクリックします。続いて、［*次へ*］をクリックしてステップ 4 に進みます。

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 ［*サーバからのドライバ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 *［UserApplication_3_6_0-IDM3_5_1-V1.xml］* を選択します。これは、役割ベースプロビジョニングモジュールをサポートするユーザアプリケーションドライバの設定ファイルです。

［UserApplication_3_6_0-IDM3_5_1-V1.xml］ がこのドロップダウンリストにない場合、ファイルが正しい場所にコピーされていません。31 ページのセクション 2.8.4「ユーザアプリケーションドライバの設定ファイルのコピー」を参照してください。

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役割ベースプロビジョニングモジュール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。

フィールド	説明
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: (値は［はい］/［いいえ］です)	［*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。

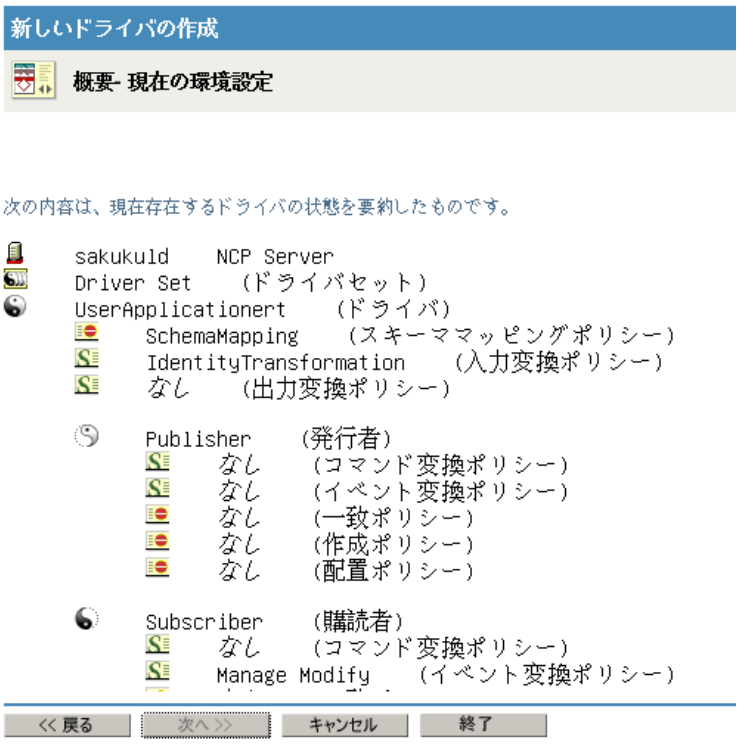
9 ［*同等セキュリティの定義*］をクリックして、［同等セキュリティ］ウィンドウを表示します。管理者または他のスーパバイザオブジェクトを参照して選択し、［*追加*］をクリックします。

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)［*Exclude Administrative Roles (管理者の役割を除外する)*］をクリックします。

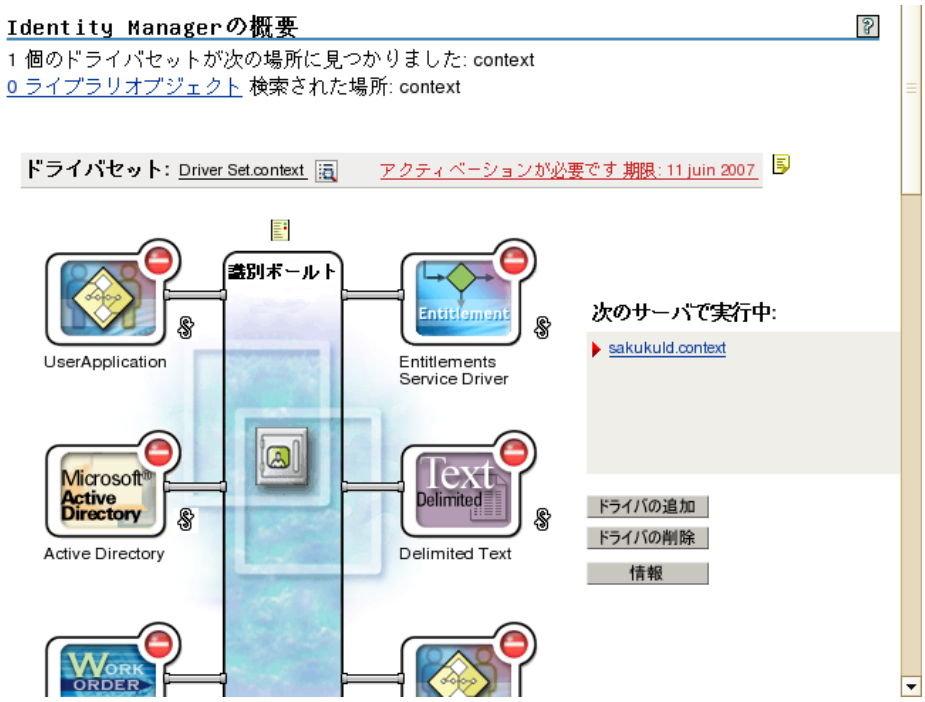
11 *［追加］*をクリックし、ドライバアクションに対して除外するユーザ (管理者の役割など) を選択します。続いて、*［OK］*を 2 回クリックして、*［次へ］*をクリックします。

12 ［*OK*］をクリックして、［同等セキュリティ］ウィンドウを閉じ、概要ページを表示します。



13 表示されている情報が正しければ、［*終了*］または［*概要の終了*］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。ドライバは、役割ベースプロビジョニングモジュールをインストールするまでオフのままにしてください。



3.2 iManager での役割サービスドライバの作成

iManager で役割サービスドライバを作成する

1. iManager 2.6 以降を Web ブラウザで開きます。
2. *［Identity Manager］* > *［Identity Manager の概要］* で、役割サービスドライバをインストールするドライバセットを選択します。

   役割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には、ユーザアプリケーションドライバのバージョン 3.6(UserApplication_3_6_0-IDM3_5_1-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、役割カタログは利用できません。

   ドライバセットごとに 1 つの役割サービスドライバのみ利用できます。
3. *［ドライバの追加］* をクリックします。
4. 新規ドライバウィザードで、デフォルトである *［既存のドライバセットの中］* をそのままにします。［*次へ*］をクリックします。
5. ドロップダウンリストから *［RoleService-IDM3_5_1-V1.xml］* を選択します。これは、役割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の設定ファイルです。

   ［RoleService-IDM3_5_1-V1.xml］ がこのドロップダウンリストにない場合、ファイルが正しい場所にコピーされていません。31 ページのセクション 2.8.3「役割サービスドライバの設定ファイルのコピー」を参照してください。

   ［*次へ*］をクリックします。

   ドライバの作成時に次のエラーが表示される場合があります。

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

エラーが表示される場合は、iManager が新しい役割スキーマをまだ取得していない可能性があります。役割サービスドライバには新しいスキーマが必要です。iManager セッションを再起動してください (すべてのブラウザを閉じ、iManager に再度ログインします)。または、サーバを再起動してください。

6 ［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のドライバ名を指定するか、デフォルト名 Role 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。
User Application Driver DN (ユーザアプリケーションドライバ DN)	役割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。
User Application Identity (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。
User Application Password (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。

7 情報を入力したら、*［完了］* をクリックします。

GUI を使用した JBoss へのインストール

4

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に Identity Manager 役割ベースプロビジョニングモジュールをインストールする方法について説明します。コンソールや単一のコマンドを使用して JBoss にモジュールをインストールする方法については、71 ページの第 5 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。

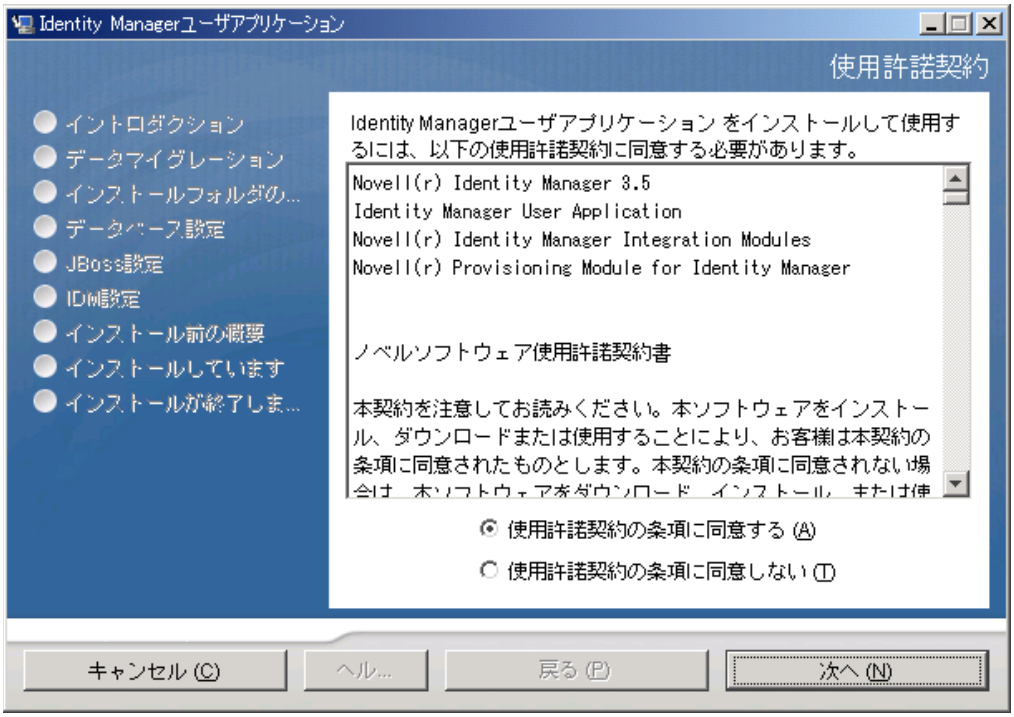
コマンドラインを使用してインストールする場合は、71 ページの第 5 章「コンソールまたは単一コマンドによるインストール」を参照してください。

4.1 インストーラ GUI の起動

1. 27 ページの 表 2-1 で説明されている手順に従って、インストールファイルを含むディレクトリへの移動します。
2. 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。

   java -jar IdmUserApp.jar
3. ドロップダウンメニューから言語を選択してから、［*OK*］をクリックします。

4 使用許諾契約を読み、[*使用許諾契約の条項に同意する*]、[*次へ*] の順に選択します。



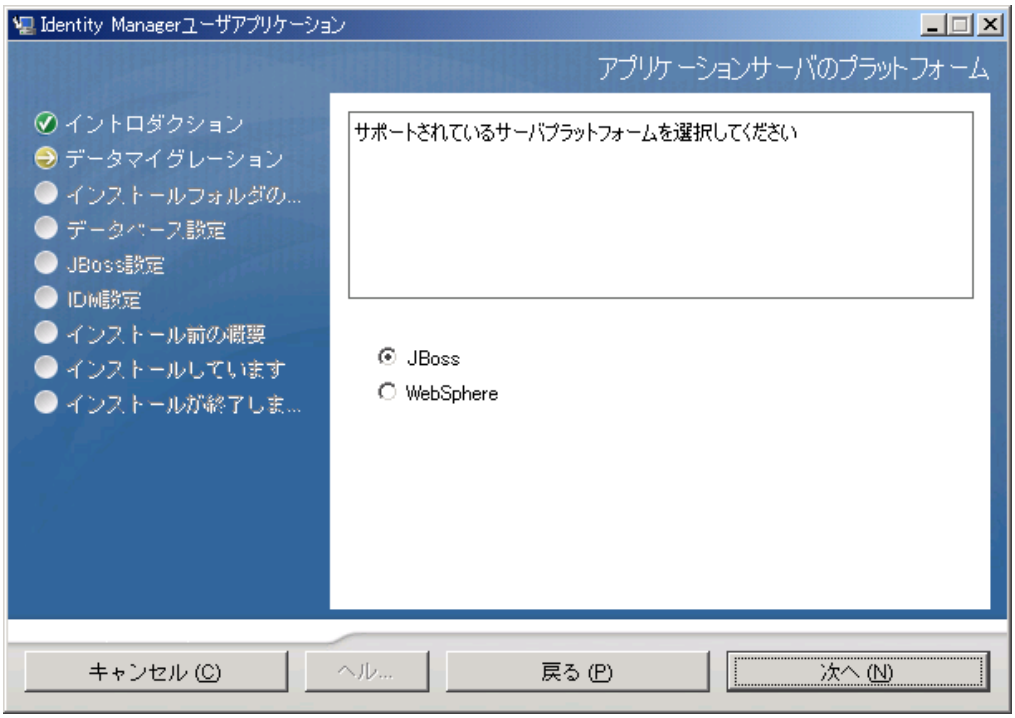
5 インストールウィザードの [イントロダクション] ページを読み、[*次へ*] をクリックします。

6 40 ページのセクション 4.2「アプリケーションサーバプラットフォームの選択」に進みます。

4.2 アプリケーションサーバプラットフォームの選択

39 ページのセクション 4.1「インストーラ GUI の起動」の手順を完了し、次の手順に進みます。

1 JBoss アプリケーションサーバのプラットフォームを選択して、［*次へ*］をクリックします。



4.3 データベースの移行

1 データベースを移行する場合は、［*次へ*］をクリックして、43 ページのセクション 4.4「WAR の場所の指定」に進みます。

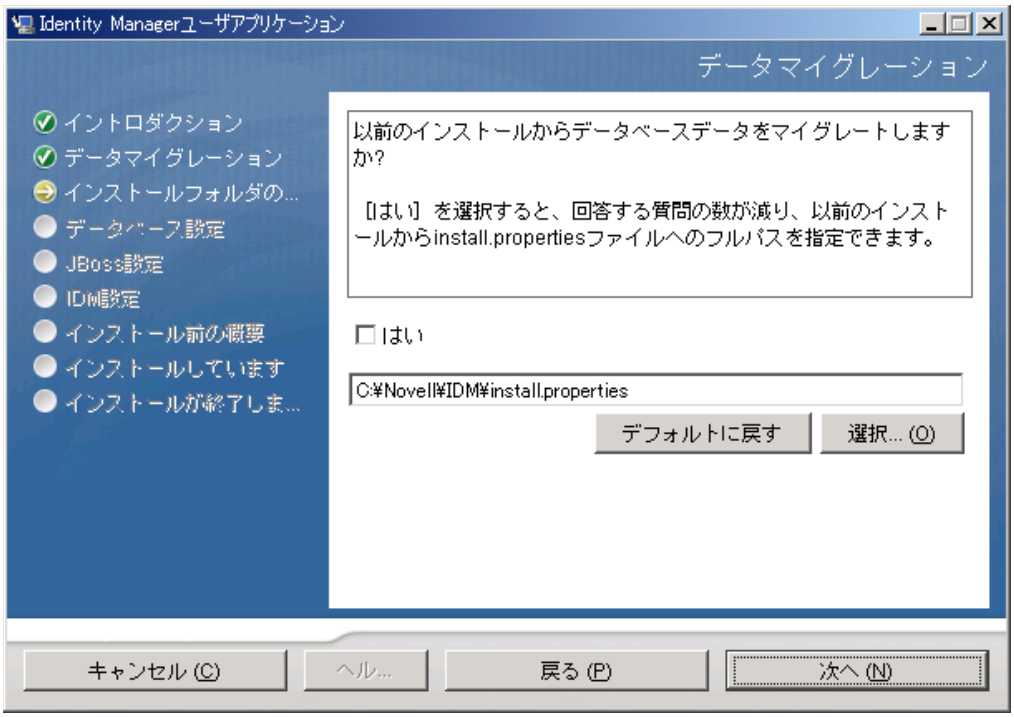
バージョン 3.0 またはバージョン 3.01 のユーザアプリケーションから既存のデータベースを使用する場合は、データベースを移行する必要があります。次の手順に進んでください。

2 移行するデータベースが開始されたことを確認します。

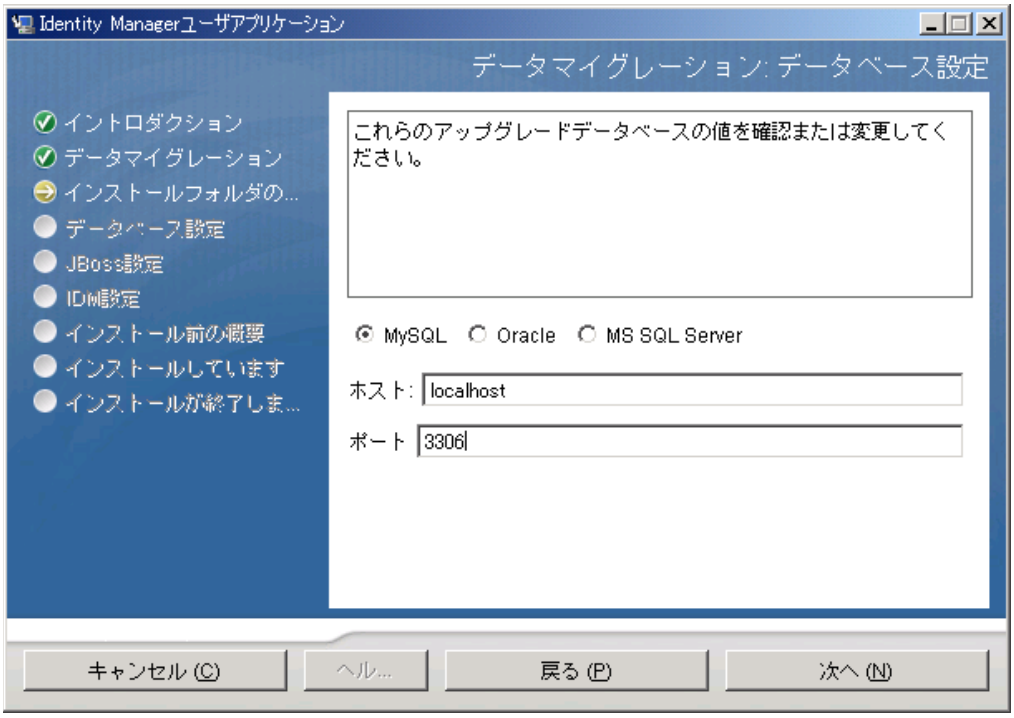
3 インストールプログラムの［データマイグレーション］ページで［*はい*］をクリックします。

4 ［*選択*］をクリックして、Identity Manager 3.0 または 3.01 の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 install.properties ファイルに移動します。

以前のインストールの install.properties ファイルの場所を指定すると、以降のページで指定する項目数を減らすことができます。



5 データベースのタイプ、ホスト名、およびポートを確認するようメッセージが表示されます。確認して *[次へ]* をクリックします。



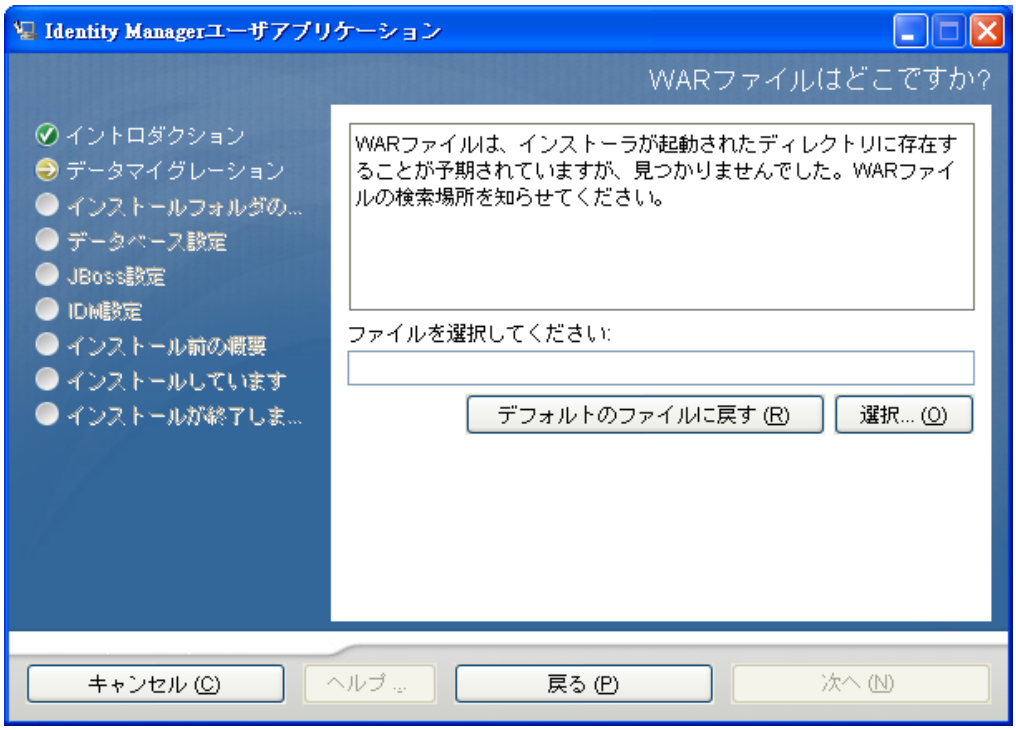
6 *[次へ]* をクリックして、43 ページのセクション 4.4「WAR の場所の指定」または 43 ページのセクション 4.5「インストールフォルダの選択」に進みます。

ユーザアプリケーションのインストーラによって、ユーザアプリケーションが更新され、データがバージョン 3.0 または 3.0.1 データベースからバージョン 3.5.1 で使用するデータベースに移行されます。データベースの移行に関する詳細と補足ステップについては、『*Identity Manager 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/idmrbpm36/index.html)』を参照してください。

4.4 WAR の場所の指定

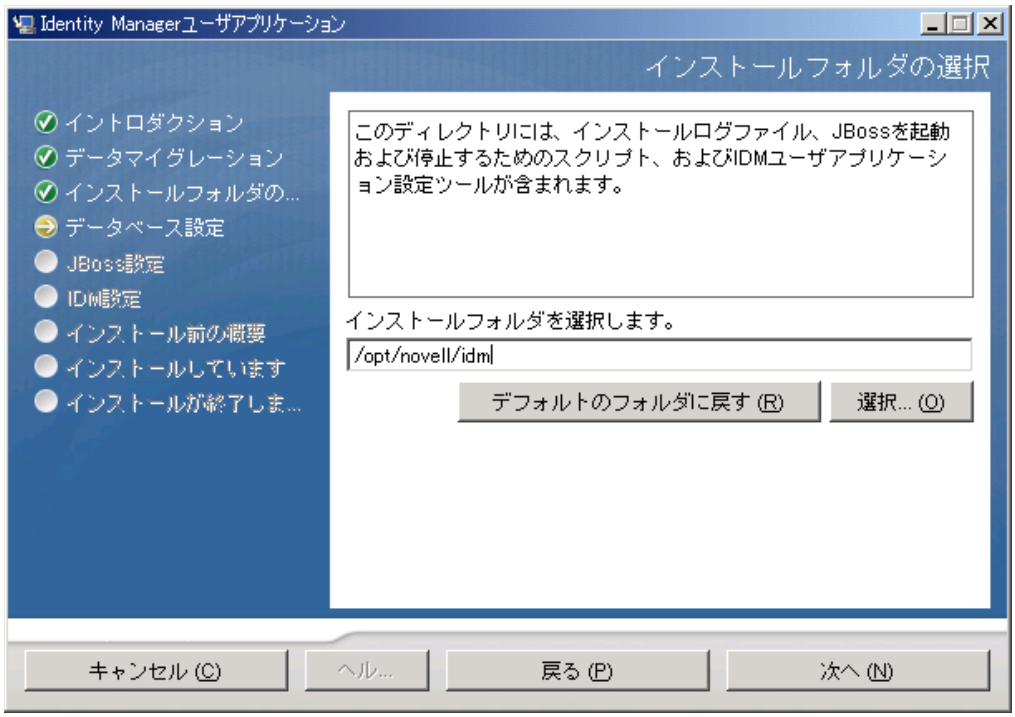
Identity Manager ユーザアプリケーションの WAR ファイルがインストーラとは別のディレクトリにある場合は、インストーラによって WAR へのパスを入力するようメッセージが表示されます。

1. 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]* をクリックします。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。
2. *[次へ]* をクリックして、43 ページのセクション 4.5「インストールフォルダの選択」に進みます。



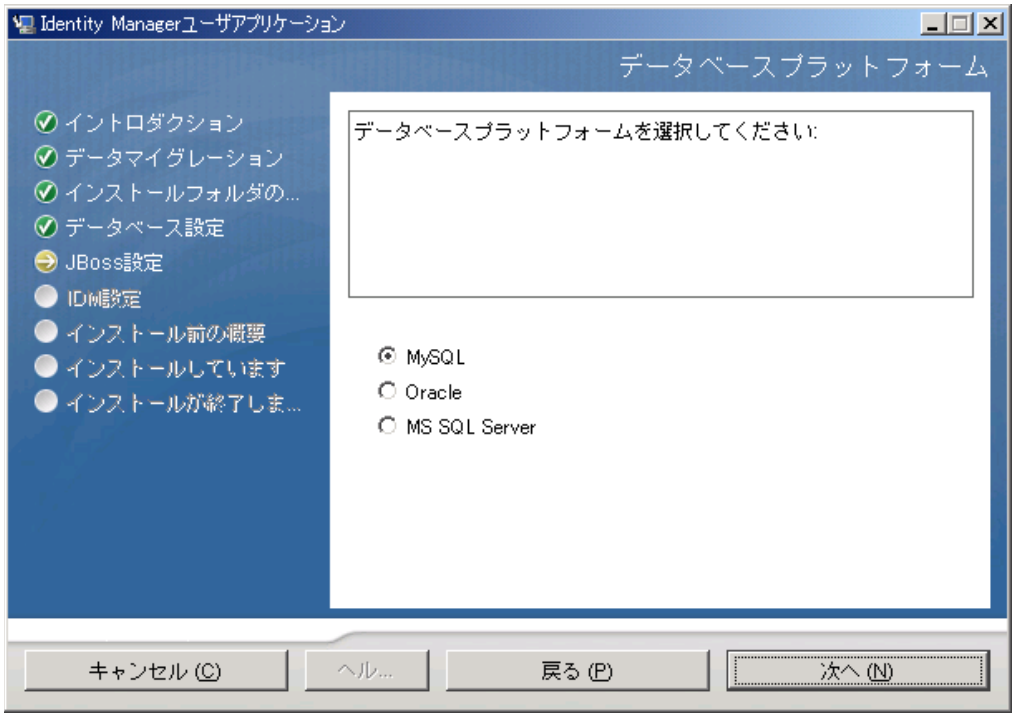
4.5 インストールフォルダの選択

1. [インストールフォルダ] ページで、ユーザアプリケーションをインストールする場所を選択します。デフォルトの場所を記憶して使用する必要がある場合は、[*デフォルトのファイルに戻す*] をクリックします。または、インストールファイルに別の場所を選択する場合は、[*選択*] をクリックして場所を参照します。
2. *[次へ]* をクリックして、44 ページのセクション 4.6「データベースプラットフォームの選択」に進みます。



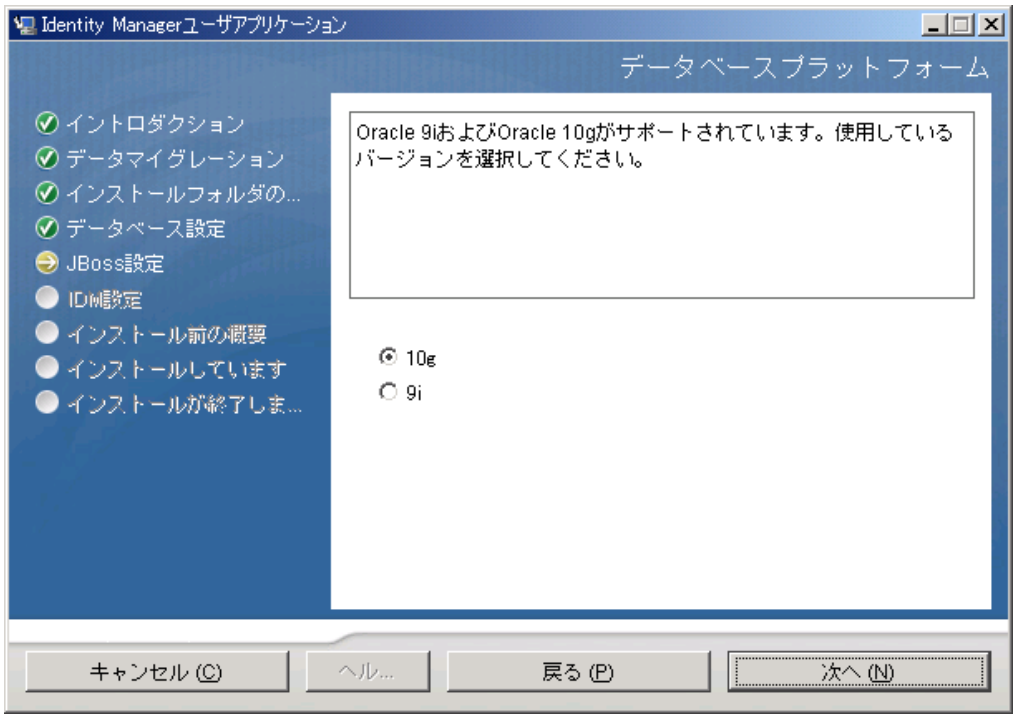
4.6 データベースプラットフォームの選択

1 使用するデータベースプラットフォームを選択します。



2 Oracle データベースを使用している場合は、ステップ 3 に進みます。それ以外の場合は、スキップしてステップ 4 に進みます。

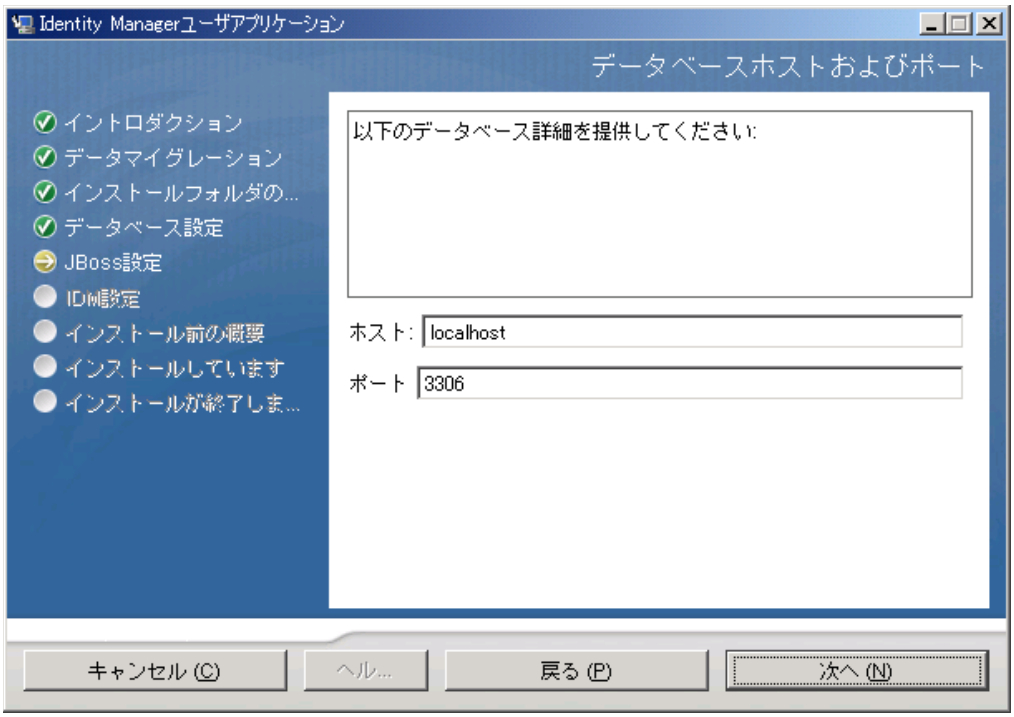
3 Oracle データベースを使用している場合は、インスト × ラによって、使用しているバージョンの入力が要求されます。バージョンを選択します。



4 ［次へ］をクリックして、45 ページのセクション 4.7「データベースのホストとポートの指定」に進みます。

4.7 データベースのホストとポートの指定

1 次のフィールドに入力します。

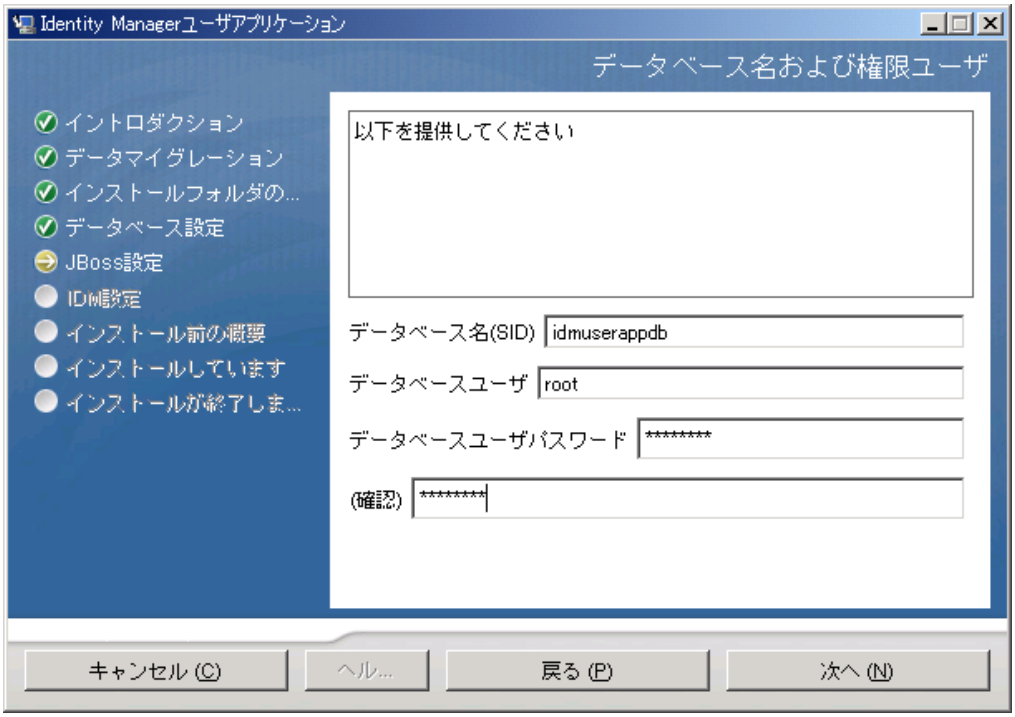


フィールド	説明
ホスト	データベースサーバのホスト名または IP アドレスを指定します。 クラスタでは、クラスタの各メンバーには同じホスト名または IP アドレスを指定します。
ポート	データベースの待ち受けポート番号を指定します。 クラスタでは、クラスタの各メンバーには同じポートを指定します。

2 [*次へ*] をクリックして、46 ページのセクション 4.8「データベース名および権限を持つユーザの指定」に進みます。

4.8 データベース名および権限を持つユーザの指定

1 次のフィールドに入力します。

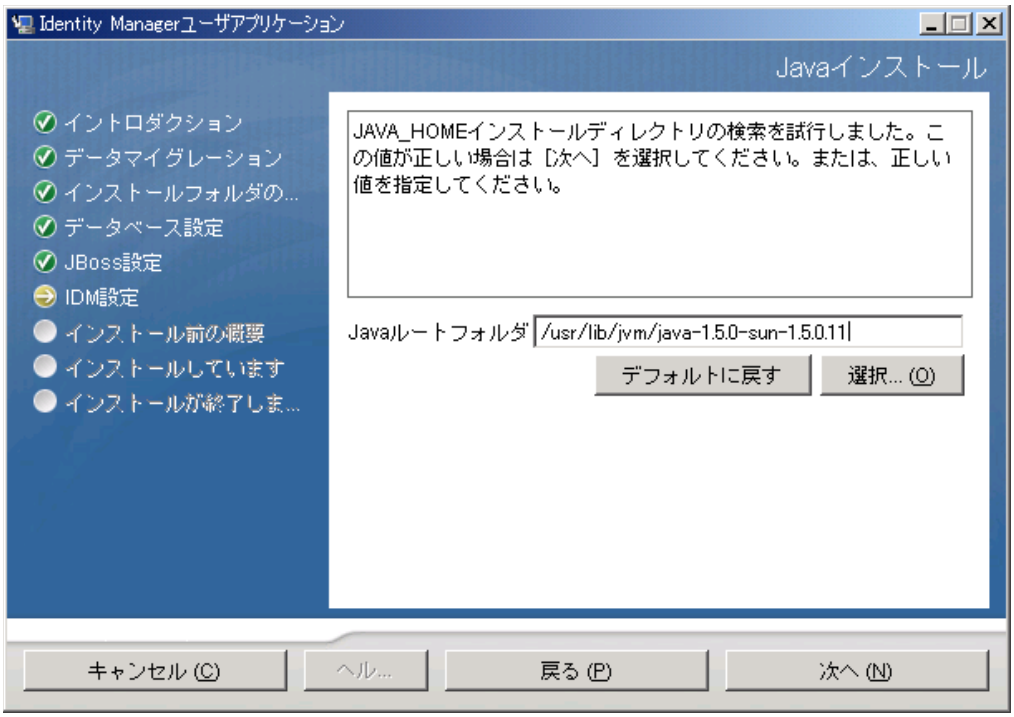


フィールド	説明
データベース名 (または sid)	MySQL または MS SQL Server では、設定済みデータベースの名前を指定します。Oracle では、前に作成した Oracle システム ID(SID) を指定します。 クラスタでは、クラスタの各メンバーには同じデータベース名または SID を指定します。
データベースユーザ	データベースのユーザを指定します。 クラスタでは、クラスタの各メンバーには同じデータベースユーザを指定します。
データベースのパスワード/*パスワードの確認*	データベースのパスワードを指定します。 クラスタでは、クラスタの各メンバーには同じデータベースパスワードを指定します。

2 ［*次へ*］をクリックして、47 ページのセクション 4.9「Java のルートディレクトリの指定」に進みます。

4.9 Java のルートディレクトリの指定

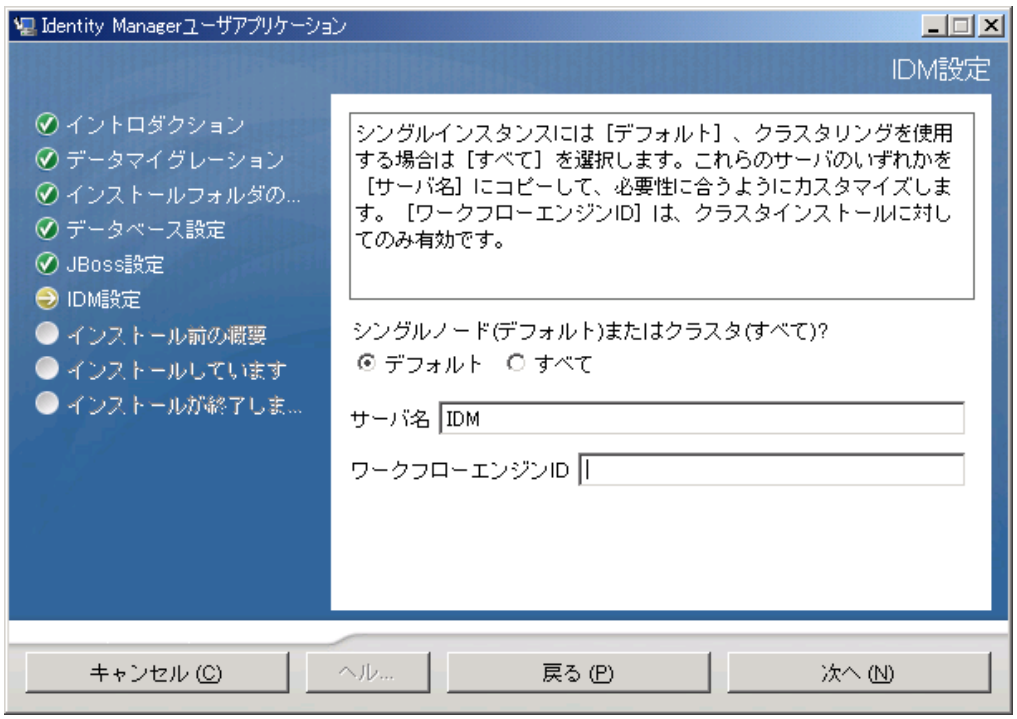
1 ［*選択*］をクリックして、Java のルートフォルダをブラウズします。デフォルトの場所を使用するには、［*デフォルトの復元*］をクリックします。



2 ［次へ］をクリックして、50 ページのセクション 4.11「Jboss アプリケーションサーバ設定の指定」に進みます。

4.10 アプリケーションサーバ環境設定タイプの選択

1 次のフィールドに入力します。



オプション	説明
［*単一*］（デフォルト）または［*クラスタリング*］（すべて）	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の場合は、［*すべて*］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。
サーバ名	サーバ名を指定します。 サーバ名は、アプリケーションサーバ設定の名前、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*］に基づいた設定が作成されます。 Identity Manager 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に注意して、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。『*Identity Manager ユーザアプリケーション：管理ガイド*』のセクション 3.5.4「クラスタ化のワークフローの設定」で説明されています。

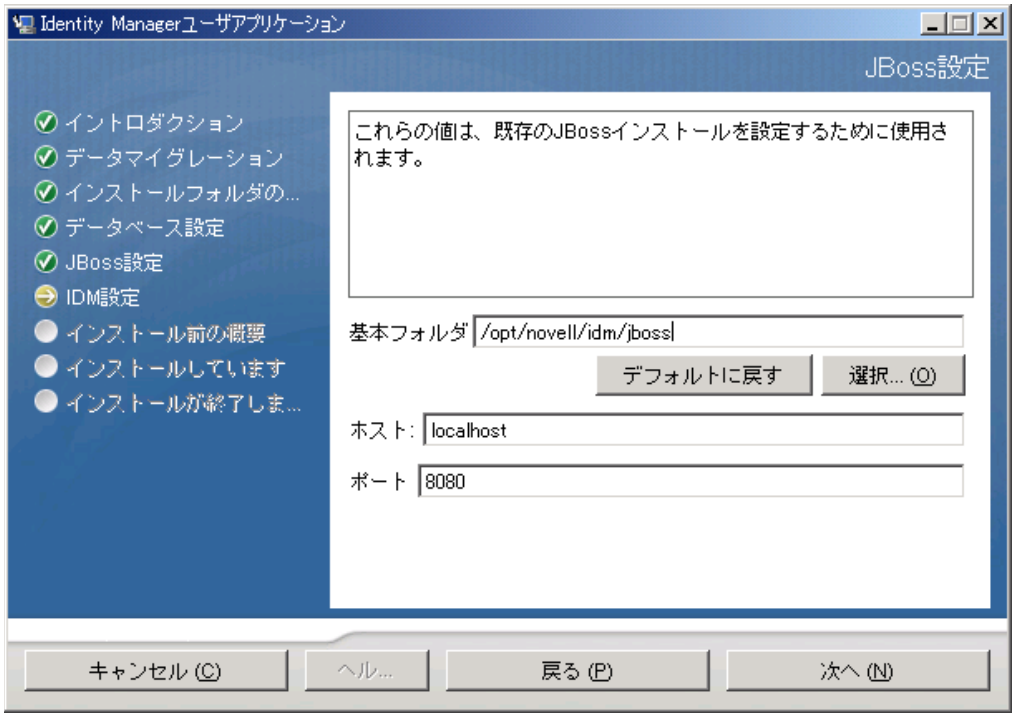
2 ［*次へ*］をクリックして、50 ページのセクション 4.12「Novell Audit のログの有効化」に進みます。

4.11 Jboss アプリケーションサーバ設定の指定

このページで、ユーザアプリケーションに JBoss アプリケーションサーバの位置を指定します。

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方法については、20 ページのセクション 2.3.1「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。

1 基本フォルダ、ホスト、およびポートを指定します。



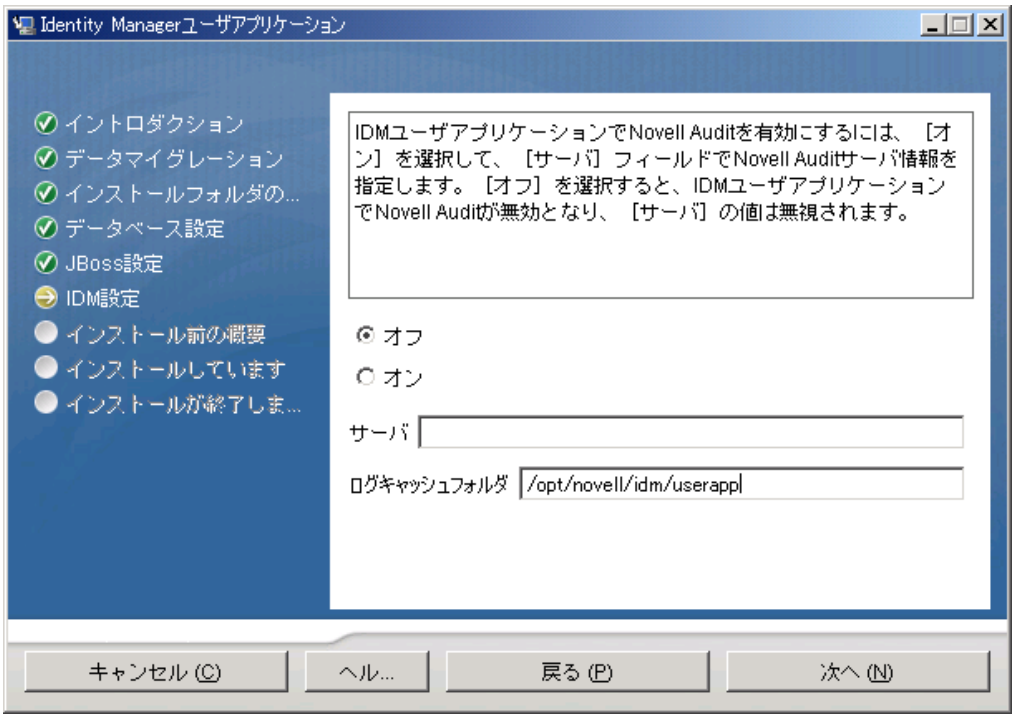
フィールド	説明
基本フォルダ	アプリケーションサーバの場所を指定します。
ホスト	アプリケーションサーバのホスト名または IP アドレスを指定します。
ポート	アプリケーションサーバの待ち受けポート番号を指定します。JBoss デフォルトポートは 8080 です。

2 [次へ] をクリックして、48 ページのセクション 4.10「アプリケーションサーバ環境設定タイプの選択」に進みます。

4.12 Novell Audit のログの有効化

(オプション) ユーザアプリケーションの Novell Audit のログを有効にするには、次の操作を行います。

1 次のフィールドに入力します。



オプション	説明
オン	ユーザアプリケーションで Novell Audit のログが有効になります。 Novell Audit のログの設定の詳細については、『Identity Manager 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。*
オフ	ユーザアプリケーションで Novell Audit のログが無効になります。ユーザアプリケーションの［*管理*］タブを使用すると、後で有効にできます。 Novell Audit のログを有効にする方法については、『*Identity Manager 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。
サーバ	Novell Audit ログをオンにする場合は、Novell Audit 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。

2 ［*次へ*］をクリックして、53 ページのセクション 4.14「ユーザアプリケーションの設定」に進みます。

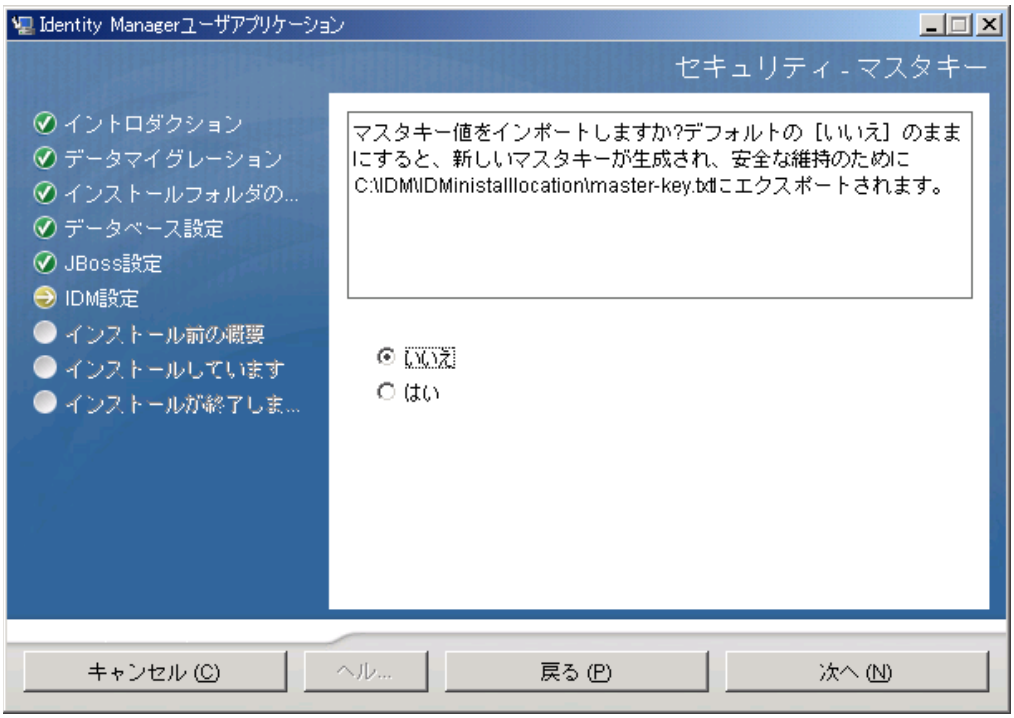
4.13 マスタキーの指定

既存のマスタキーをインポートするか、新しいマスタキーを作成するかを指定します。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。

1 *[はい]* クリックして既存のマスタキーをインポートするか、または *[いいえ]* をクリックして新しいマスタキーを作成します。



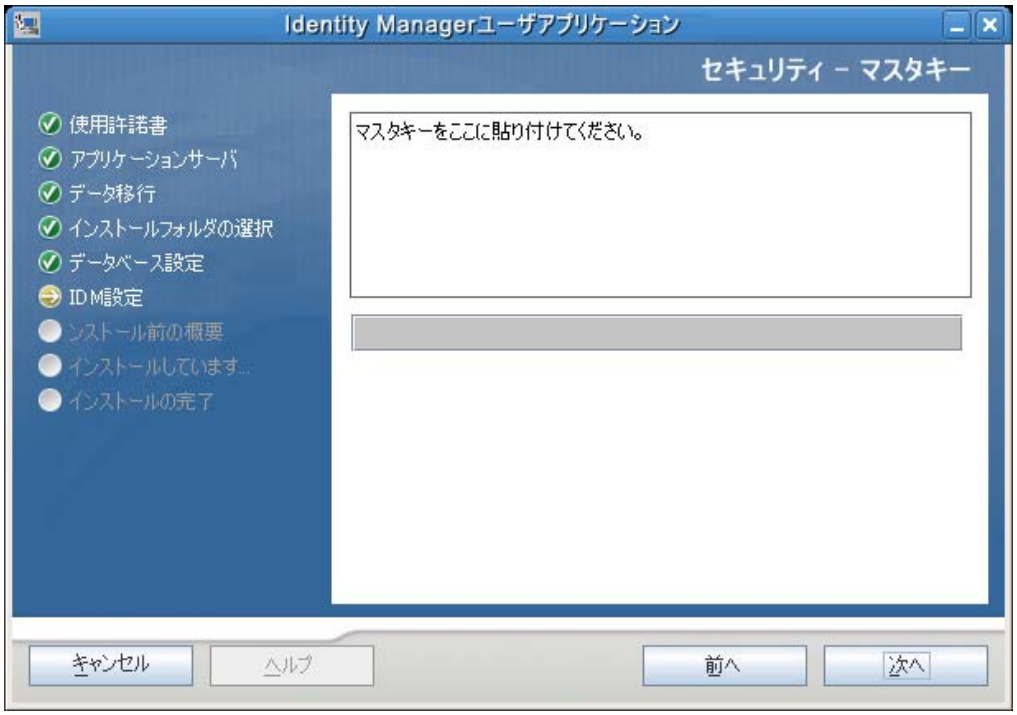
2 ［*次へ*］をクリックします。

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。

［*いいえ*］を選択する場合は、53 ページのセクション 4.14「ユーザアプリケーションの設定」までスキップされます。インストール終了後、111 ページのセクション 7.1「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。

［*はい*］を選択して、ステップ 3 に進みます。

3 既存の暗号化マスタキーのインポートを選択する場合は、該当するキーをインストール手順ウィンドウに切り取りおよび貼り付けします。



4 ［次へ］をクリックします。

4.14 ユーザアプリケーションの設定

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。

1 表 4-1 で説明されている、基本のユーザアプリケーション環境設定パラメータを設定してから、ステップ 2 に進みます。

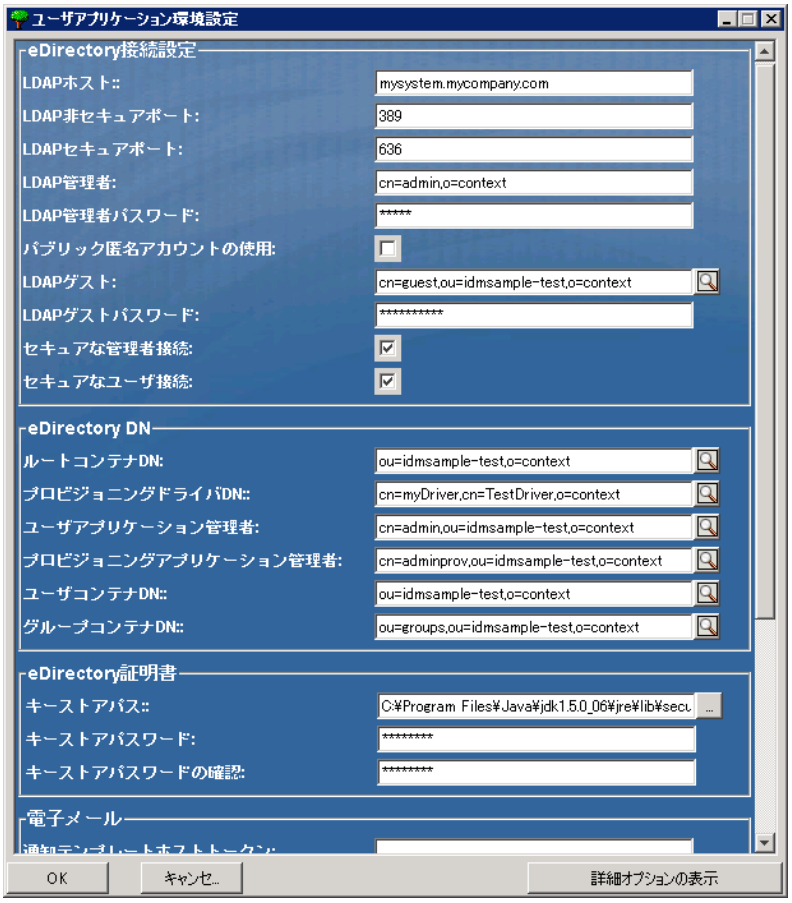

ユーザアプリケーション環境設定
eDirectory接続設定
LDAPホスト:
mysystem.mycompany.com
LDAP非セキュアポート:
389
LDAPセキュアポート:
636
LDAP管理者:
cn=admin,o=context
LDAP管理者パスワード:
*****
パブリック匿名アカウントの使用:
LDAPゲスト:
cn=guest,ou=idmsample-test,o=context
LDAPゲストパスワード:
****
セキュアな管理者接続:
セキュアなユーザ接続:
eDirectory DN
ルートコンテナDN:
ou=idmsample-test,o=context
プロビジョニングドライバDN:
cn=myDriver,cn=TestDriver,o=context
ユーザアプリケーション管理者:
cn=admin,ou=idmsample-test,o=context
プロビジョニングアプリケーション管理者:
cn=adminprov,ou=idmsample-test,o=context
ユーザコンテナDN:
ou=idmsample-test,o=context
グループコンテナDN:
ou=groups,ou=idmsample-test,o=context
eDirectory証明書
キーストアパス:
C:¥Program Files¥Java¥jdk1.5.0_06¥jre¥lib¥secu
キーストアパスワード:
****
キーストアパスワードの確認:
****
電子メール
OK
キャンセ...
詳細オプションの表示

表 4-1 *ユーザアプリケーション環境設定 : 基本パラメータ*

設定のタイプ	フィールド	説明
eDirectory 接続設定	*LDAP ホスト*	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`
	LDAP 非セキュアポート	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。
	LDAP セキュアポート	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。
	LDAP 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。
	LDAP 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。
	セキュアな管理者接続	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	フィールド	説明
eDirectory 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。
	プロビジョニングドライバ DN	必須。前述の 33 ページのセクション 3.1「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`
	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、*IDM 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。
	プロビジョニングアプリケーション管理者	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。

設定のタイプ	フィールド	説明
eDirectory DN(続き)	*役割管理者*	この役割は、Novell Identity Manager 役割ベースプロビジョニングモジュールで利用可能です。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。
	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 :** ユーザがワークフローを実行できるようにする場合は、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は、このコンテナ内に存在する点に注意してください。
	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。
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実行に使用しているの JDK 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。 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 / キーストアパスワードの確認	必須。cacerts のパスワードを指定します。デフォルトは、「changeit」です。

設定のタイプ	フィールド	説明
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。
	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。
	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。
	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電子メールが送信されるように指定します。
	通知 SMTP 電子メールホスト:	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。
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］*を選択する場合は、*［パスワードを忘れた場合のリンク］*および *［パスワードを忘れた場合の返信リンク］*に値を指定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.jsf(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.jsf ファイルを指定します。詳細については、68 ページの「パスワード WAR の使用」を参照してください。

設定のタイプ	フィールド	説明
	パスワードを忘れた場合の返信リンク	外部のパスワード管理 WAR を使用している場合は、外部の［パスワード管理 WAR］が Web サービス、たとえば https:// *idmhost:sslport*/idm 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パスを指定します。

2 追加ユーザアプリケーション環境設定パラメータに設定する場合は、［*詳細オプションの表示*］をクリックします。(スクロールしてパネル全体を表示します。) 表 4-2 は、詳細オプションのパラメータについて説明します。

このステップで説明した追加パラメータを設定しない場合は、スキップしてステップ 3 に進みます。

表 4-2 *ユーザアプリケーション環境設定 : すべてのパラメータ*

設定のタイプ	フィールド	説明
eDirectory 接続設定	*LDAP ホスト*	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 非セキュアポート	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。
	LDAP セキュアポート	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。
	LDAP 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。
	LDAP 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。
	セキュアな管理者接続	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	フィールド	説明
eDirectory 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。
	プロビジョニングドライバDN	必須。前述の 33 ページのセクション 3.1「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`
	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、*IDM 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。
	プロビジョニングアプリケーション管理者	プロビジョニングアプリケーション管理者は、ユーザアプリケーションの*［要求と承認］*タブを使用して利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。

設定のタイプ	フィールド	説明
メタディレクトリユーザ 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 :** ユーザがワークフローを実行できるようにする場合は、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は、このコンテナ内に存在する点に注意してください。
	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。
	役割管理者	この役割は、Novell Identity Manager 役割ベースプロビジョニングモジュールで利用可能です。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。

設定のタイプ	フィールド	説明
メタディレクトリユーザグループ	*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。
	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)。
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 *キーストアパスワードの確認*	必須。cacerts のパスワードを指定します。デフォルトは、「changeit」です。
プライベートキーストア	*プライベートキーストアパス*	プライベートキーストアには、ユーザアプリケーションのプライベートキーおよび証明書が含まれます。予約済み。入力しない場合は、このパスはデフォルトで /jre/lib/security/cacerts になります。
	プライベートキーストアパスワード	このパスワードは、別のパスワードを指定するまでは changeit です。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。
	プライベートキーの別名	この別名は、別の別名を指定するまでは novelIIDMUserApp です。
	プライベートキーパスワード	このパスワードは、別のパスワードを指定するまでは nove1IIDM です。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。

設定のタイプ	フィールド	説明
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。
Novell Audit デジタル署名および証明書キー		Novell Audit デジタル署名キーおよび証明書が含まれます。
	Novell Audit デジタル署名証明書	デジタル署名証明書が表示されます。
	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 および iChain 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［同時ログアウト］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。同時ログアウトが有効な場合は、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に再ルーティングされます。ご使用の環境に応じて、次の 2 つの URL のいずれかにより、同時ログアウト機能が正しいページに移動します。 Access Manager: https://yourAccessGatewayServer/AGLogout iChain: https://youriChainServer/cmd/ICSLogout

設定のタイプ	フィールド	説明
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。
	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。
	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。
	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。
	通知テンプレートセキュアプロトコルトークン	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。
	通知 SMTP 電子メールホスト :	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	フィールド	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］*を選択する場合は、*［パスワードを忘れた場合のリンク］*および *［パスワードを忘れた場合の返信リンク］*に値を指定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.jsf(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.jsf ファイルを指定します。詳細については、68 ページの「パスワード WAR の使用」を参照してください。
	パスワードを忘れた場合の返信リンク	外部のパスワード管理 WAR を使用している場合は、外部の［パスワード管理 WAR］が Web サービス、たとえば https:// *idmhost:sslport*/idm 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パスを指定します。
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	フィールド	説明
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の LDAP 名を指定します。 コンテナの詳細については、『*Novell iManager 2.6 管理ガイド (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*』を参照してください。
	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。

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。

3 設定で環境設定を完了したら、［*OK*］をクリックして、69 ページのセクション 4.16「選択を確認してインストール」に進みます。

4.15 パスワード WAR の使用

［*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。

- 68 ページのセクション 4.15.1「外部パスワード管理 WAR の指定」
- 69 ページのセクション 4.15.2「内部パスワード WAR の指定」

4.15.1 外部パスワード管理 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/ 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］* には、外部の［パスワード管理 WAR］が Web サービス、たとえば https://*idmhost:sslport*/idm 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外部パスワード管理 WAR パスを指定します。

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。112 ページのセクション 7.4「JBoss サーバ間の SSL 通信の設定」も参照してください。

5 次のいずれかの操作を行います。

- インストーラを使用している場合は、このステップで情報を読み、69 ページのステップ 6 に進みます。
- configupdate ユーティリティを使用して、インストールのルートディレクトリ内の外部パスワード WAR を使用している場合は、このステップを読み、手動で WAR の名前を［*パスワードを忘れた場合のリンク*］で指定した最初のディレクトリに名前変更します。そのあと、69 ページのステップ 6 に進みます。

インストールの終了前に、インストーラによって IDMPwdMgt.war(インストーラにバンドルされています) は指定する最初のディレクトリの名前に名前変更されます。名前変更された IDMPwdMgt.war は外部パスワード WAR になります。たとえば、http://www.idmpwdmgthost.com/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf を指定する場合は、インストーラによって IDMPwdMgt.war は ExternalPwd.war に名前変更されます。インストーラによって、名前変更された WAR はインストールルートディレクトリに移動されます。

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。

4.15.2 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。

4.16 選択を確認してインストール

1 ［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。

2 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ませんので、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値を再入力する必要があります。

3 インストールおよび環境設定パラメータで満足したら、［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。

4.17 ログファイルの表示

1. インストールがエラーなしで完了した場合は、111 ページの第 7 章「インストール後のタスク」に移動します。
2. 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。

   問題を解決するヘルプについては、115 ページのセクション 7.12「トラブルシューティング」を参照してください。

コンソールまたは単一コマンドによるインストール

5

このセクションでは、39 ページの第 4 章「GUI を使用した JBoss へのインストール」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。

- 71 ページのセクション 5.1「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」
- 71 ページのセクション 5.2「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」

5.1 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。

1. 27 ページの 表 2-1 で説明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. 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
4. 39 ページの第 4 章「GUI を使用した JBoss へのインストール」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。
5. 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、53 ページのセクション 4.14「ユーザアプリケーションの設定」で説明されている値を入力します。
6. 外部パスワード管理 WAR を使用している場合は、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コピーします。
7. 111 ページの第 7 章「インストール後のタスク」に進みます。

5.2 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. 27 ページの 表 2-1 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 5-1 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 5-1 *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。 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。
NOVL_CONFIG_LDAPADMIN=	eDirectory 接続設定 : LDAP 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。
NOVL_CONFIG_LDAPADMINPASS=	eDirectory 接続設定 : LDAP 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。

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。 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。
NOVL_CONFIG_PROVISIONROOT=	eDirectory DN: プロビジョニングドライバ DN。 必須。前述の 33 ページのセクション 3.1「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。 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、*IDM 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 役割ベースプロビジョニングモジュールで利用可能です。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_USERCONTAINERDN=	メタディレクトリユーザ 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 :** ユーザがワークフローを実行できるようにする場合は、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は、このコンテナ内に存在する点に注意してください。
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。 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。

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_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。 必須。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。 ［*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。 ［*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。 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。 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。
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory 接続設定 : LDAP セキュアポート。 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。

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_ANONYMOUS=	eDirectory 接続設定 : 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。 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。
NOVL_CONFIG_NOTFSMTPEMAILHOST=	電子メール : 通知 SMTP 電子メールホスト。 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。

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_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.jsf(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.jsf 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、68 ページの「パスワード WAR の使用」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。 外部のパスワード管理 WAR を使用している場合は、外部の［パスワード管理 WAR］が Web サービス、たとえば https:// *idmhost:sslport*/idm 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パスを指定します。
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。 LDAP ユーザオブジェクトクラス (通常は inetOrgPerson)。
NOVL_CONFIG_LOGINATTRIBUTE=	メタディレクトリユーザ ID: 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)。
NOVL_CONFIG_NAMINGATTRIBUTE=	メタディレクトリユーザ ID : 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。
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。 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。

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_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。 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。 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。 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。 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_PRIVATESTOREPATH=	プライベートキーストア : プライベートキーストアパス。 ユーザアプリケーションのプライベートキーと証明書を含むプライベートキーストアへのパスを指定します。予約済み。入力しない場合は、このパスはデフォルトで /jre/lib/security/cacerts になります。
NOVL_CONFIG_PRIVATESTOREPASSWORD=	プライベートキーストア : プライベートキーストアパスワード。
NOVL_CONFIG_PRIVATEKEYALIAS=	プライベートキーストア : プライベートキーの別名。 この別名は、別の別名を指定するまでは novellIDMUserApp です。
NOVL_CONFIG_PRIVATEKEYPASSWORD=	プライベートキーストア : プライベートキーパスワード。
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。

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_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。
NOVL_CONFIG_AUDITCERT=	Novell Audit デジタル署名証明書
NOVL_CONFIG_AUDITKEYFILEPATH=	Novell Audit 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。

WebSphere Application Server へのインストール

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版のインストーラを使用して、WebSphere Application Server に 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。

6.1 インストーラ GUI の起動

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。

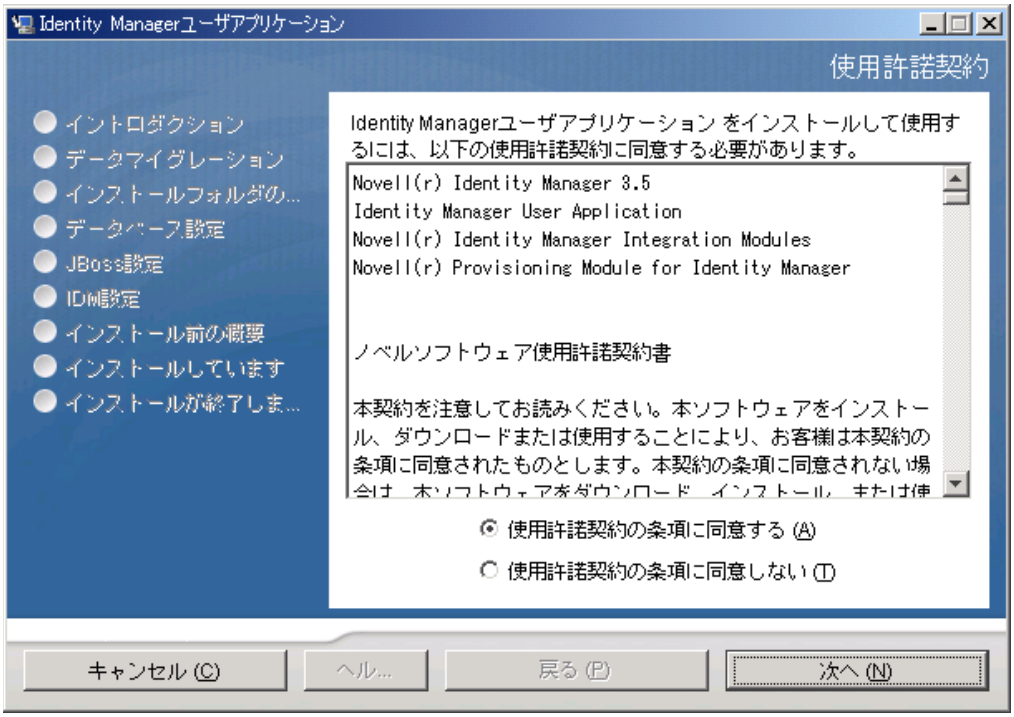
2 次のコマンドを入力して、インストーラを起動します。

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

注 : 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。

3 ドロップダウンメニューから言語を選択してから、［OK］をクリックします。

4 使用許諾契約を読み、*[使用許諾契約の条項に同意する]*、*[次へ]* の順にクリックします。

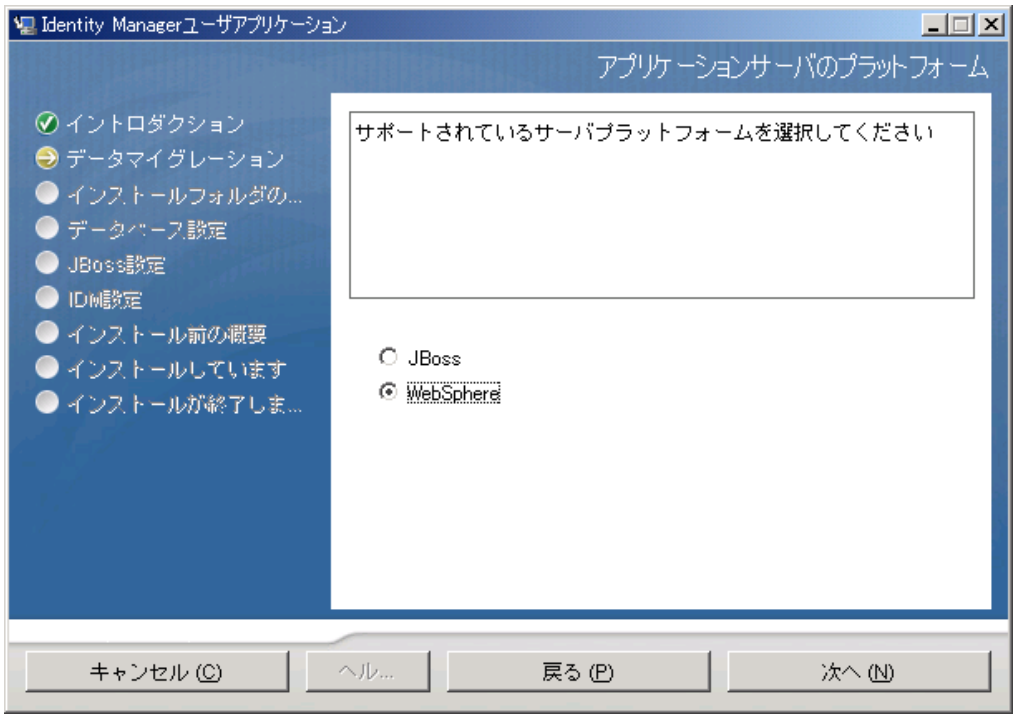


5 インストールウィザードの［イントロダクション］ページを読み、*[次へ]* をクリックします。

6.2 アプリケーションサーバプラットフォームの選択

1 ［アプリケーションサーバのプラットフォーム］ウィンドウで、WebSphere 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。

2 *[次へ]* を選択します。それが終了したら 83 ページのセクション 6.3「WAR の場所の指定」に進みます。

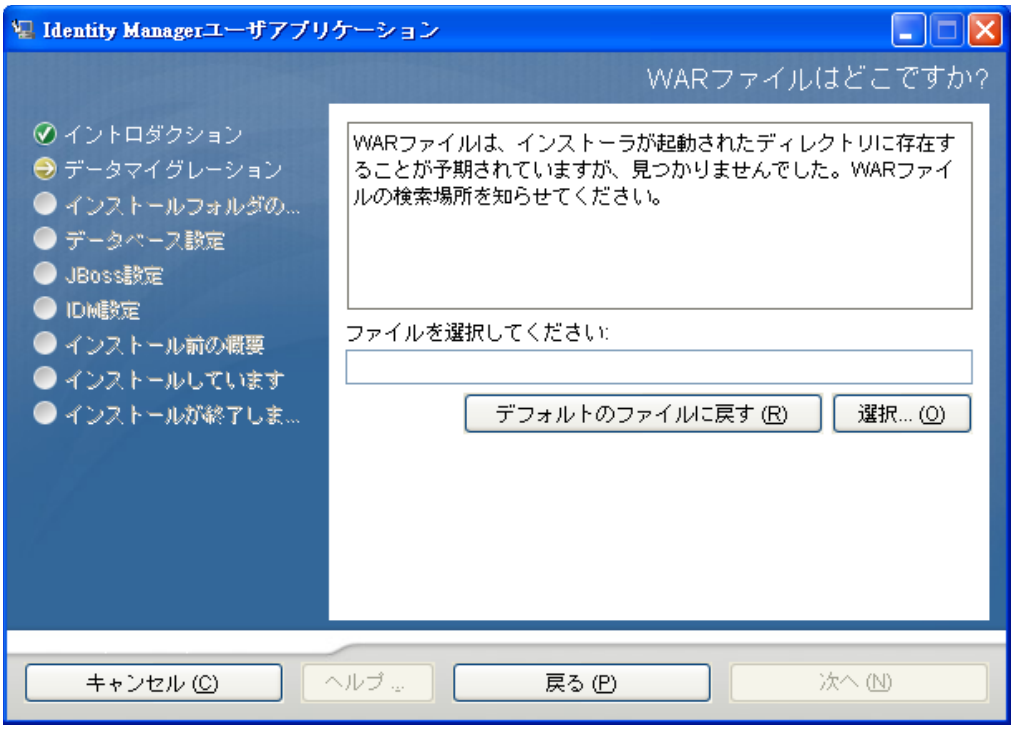


6.3 WAR の場所の指定

81 ページのセクション 6.1「インストーラ GUI の起動」の手順を完了し、次の手順に進みます。

Identity Manager 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。

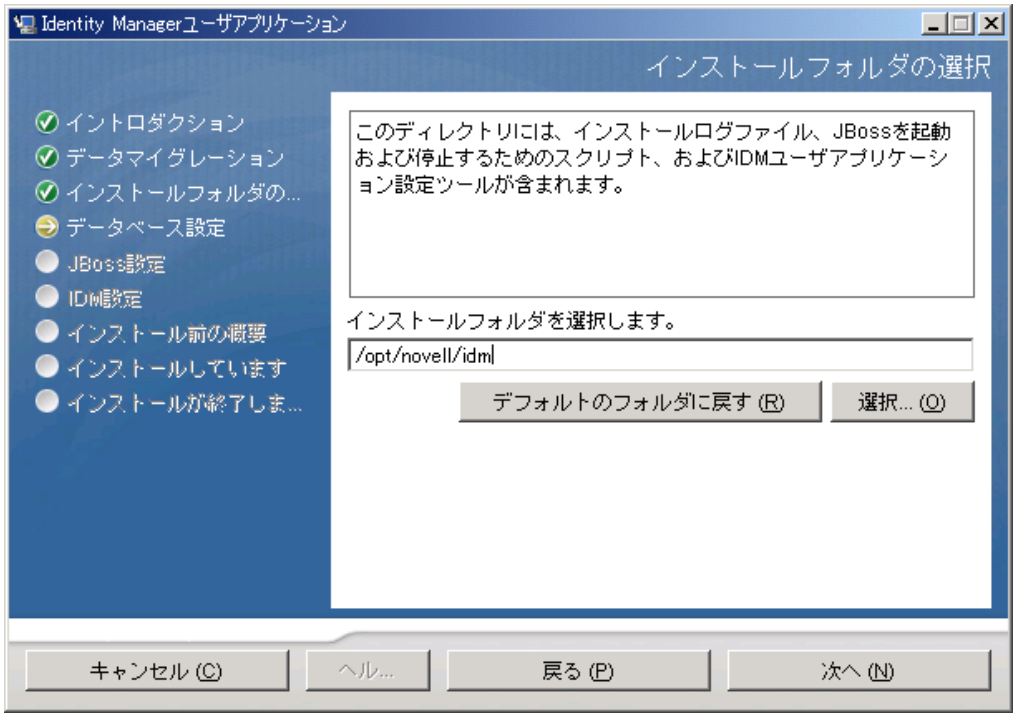
1 WAR がデフォルトの場所にある場合は、*[デフォルトのファイルに戻す]* をクリックできます。または、WAR ファイルの場所を指定する場合は、*[選択]* をクリックして場所を選択します。



2 *[次へ]* をクリックして、84 ページのセクション 6.4「インストールフォルダの選択」に進みます。

6.4 インストールフォルダの選択

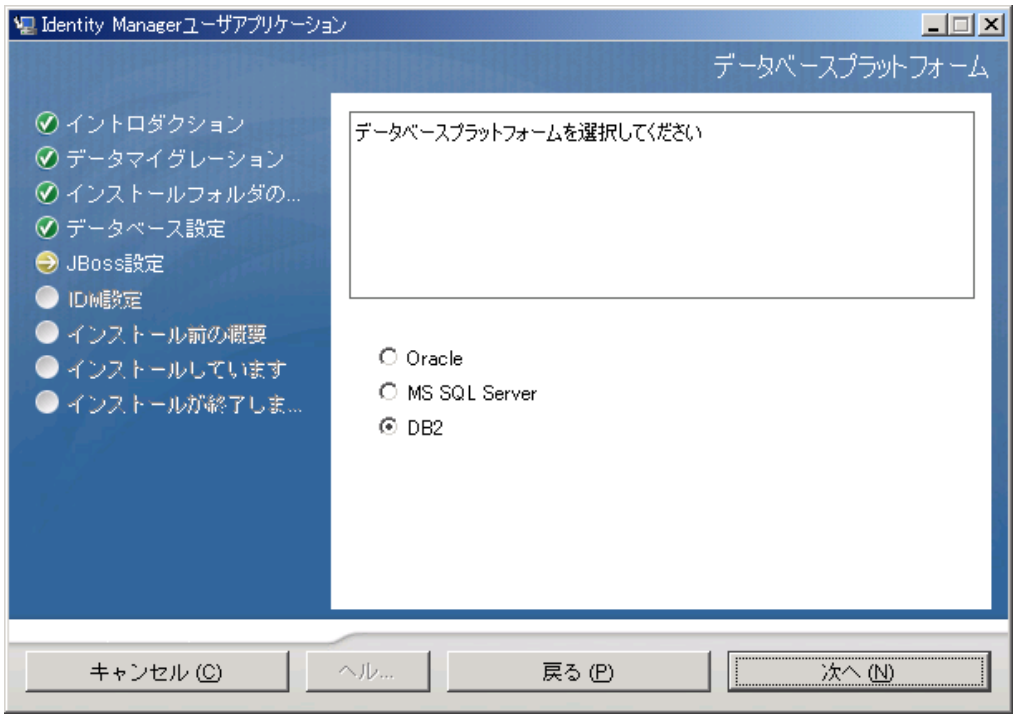
1 [インストールフォルダ] ページで、ユーザアプリケーションをインストールする場所を選択します。デフォルトの場所を使用する場合は、*[デフォルトのファイルに戻す]* をクリックします。または、インストールファイルに別の場所を選択する場合は、*[選択]* をクリックして場所を参照します。



2 *[次へ]* をクリックして、85 ページのセクション 6.5「データベースプラットフォームの選択」に進みます。

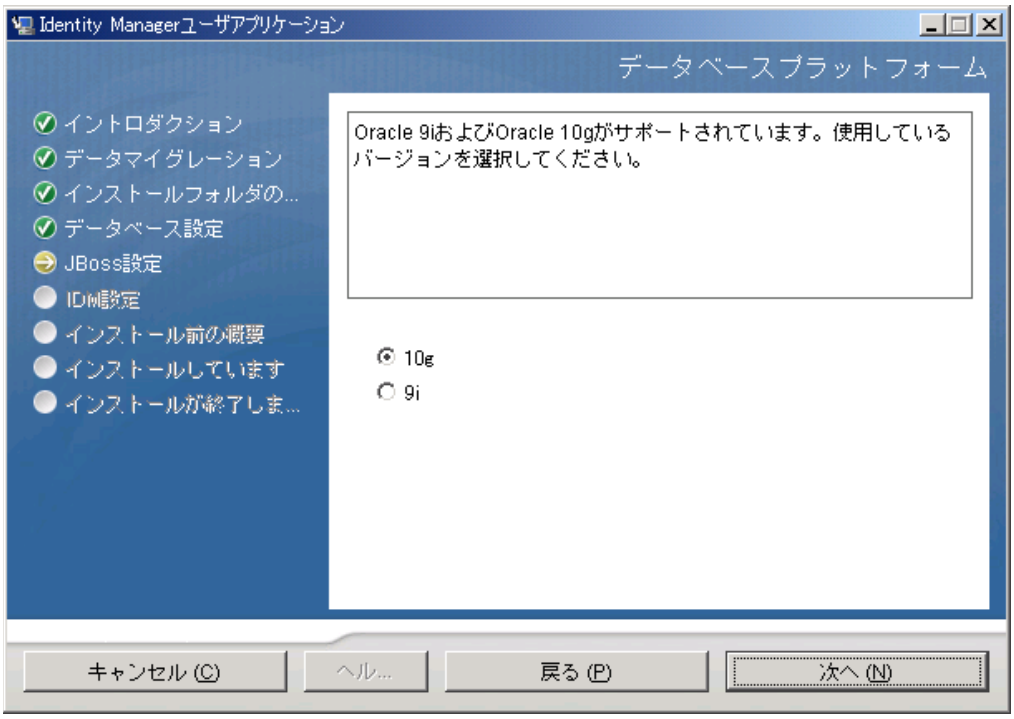
6.5 データベースプラットフォームの選択

1 使用するデータベースプラットフォームを選択します。



2 Oracle データベースを使用している場合は、ステップ 3 に進みます。それ以外の場合は、スキップしてステップ 4 に進みます。

3 Oracle データベースを使用している場合は、インスト × ラによって、使用しているバージョンの入力が要求されます。バージョンを選択します。

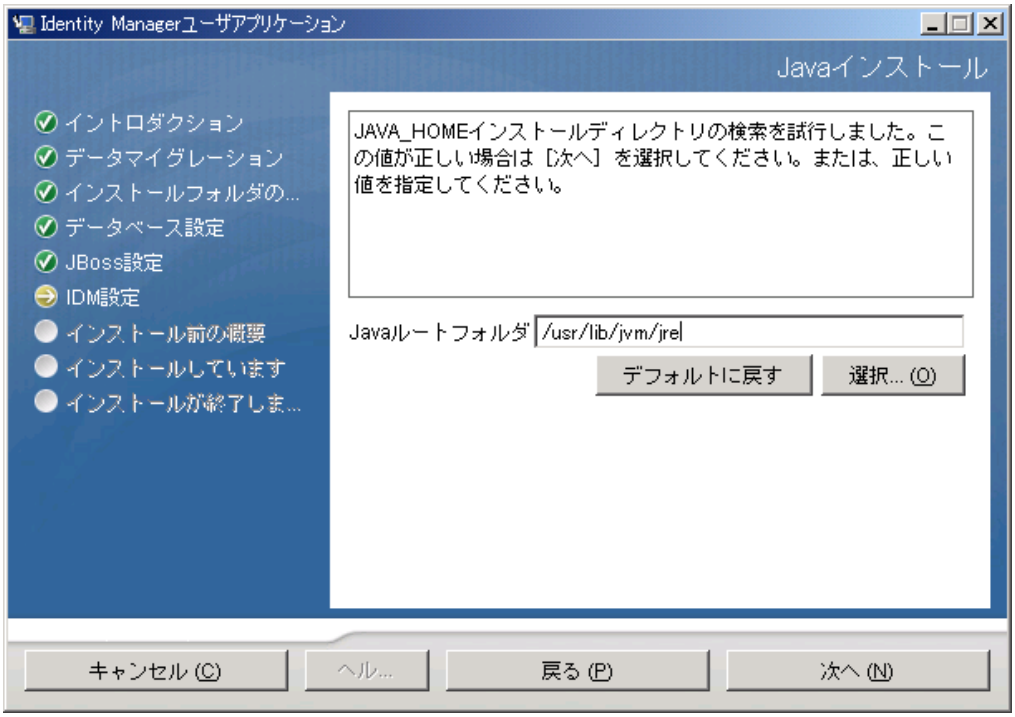


4 *[次へ]* をクリックして、86 ページのセクション 6.6「Java のルートディレクトリの指定」に進みます。

6.6 Java のルートディレクトリの指定

注 : 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。

1 *[選択]* をクリックして、Java のルートフォルダを参照します。または、デフォルトの場所を使用するには、*[デフォルトの復元]* をクリックします。

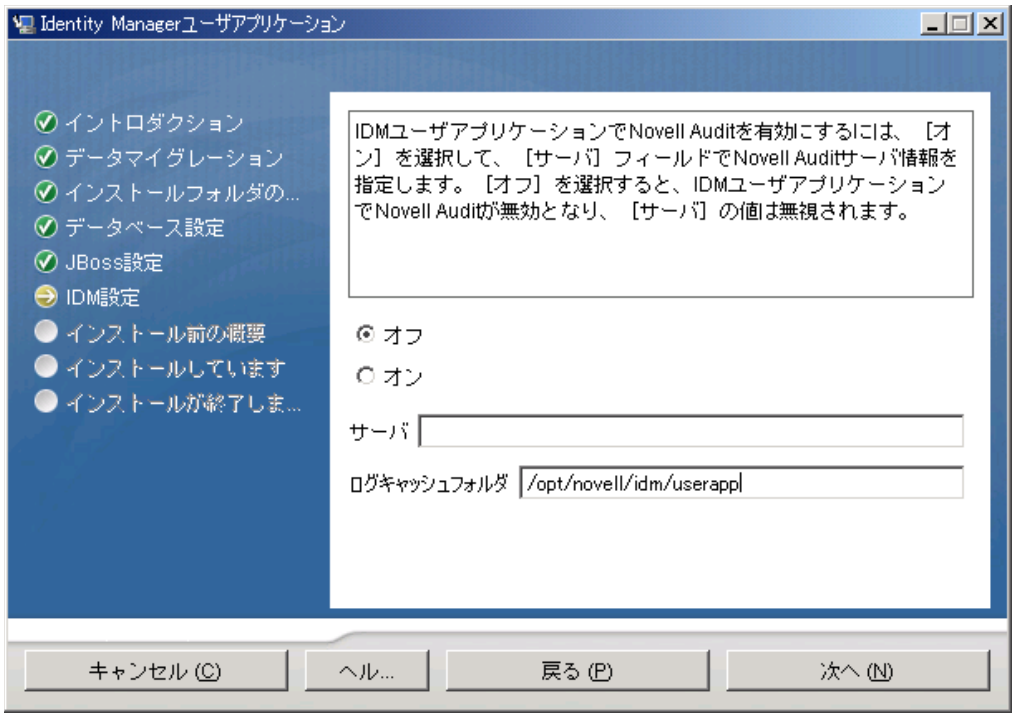


2 ［次へ］をクリックして、87 ページのセクション 6.7「Novell Audit のログの有効化」に進みます。

6.7 Novell Audit のログの有効化

ユーザアプリケーションの Novell® Audit のログ (オプション) を有効にする

1 次のフィールドに入力します。



オプション	説明
オフ	ユーザアプリケーションで Novell Audit のログが無効になります。ユーザアプリケーションの *［管理］* タブを使用すると、後でログを有効にできます。 Novell Audit のログの有効化の詳細については、*『Identity Manager 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。
オン	ユーザアプリケーションで Novell Audit のログが有効になります。 Novell Audit のログの設定の詳細については、*『Identity Manager 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。*
サーバ	Novell Audit ログをオンにする場合は、Novell Audit 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	ログキャッシュ用のディレクトリを指定します。

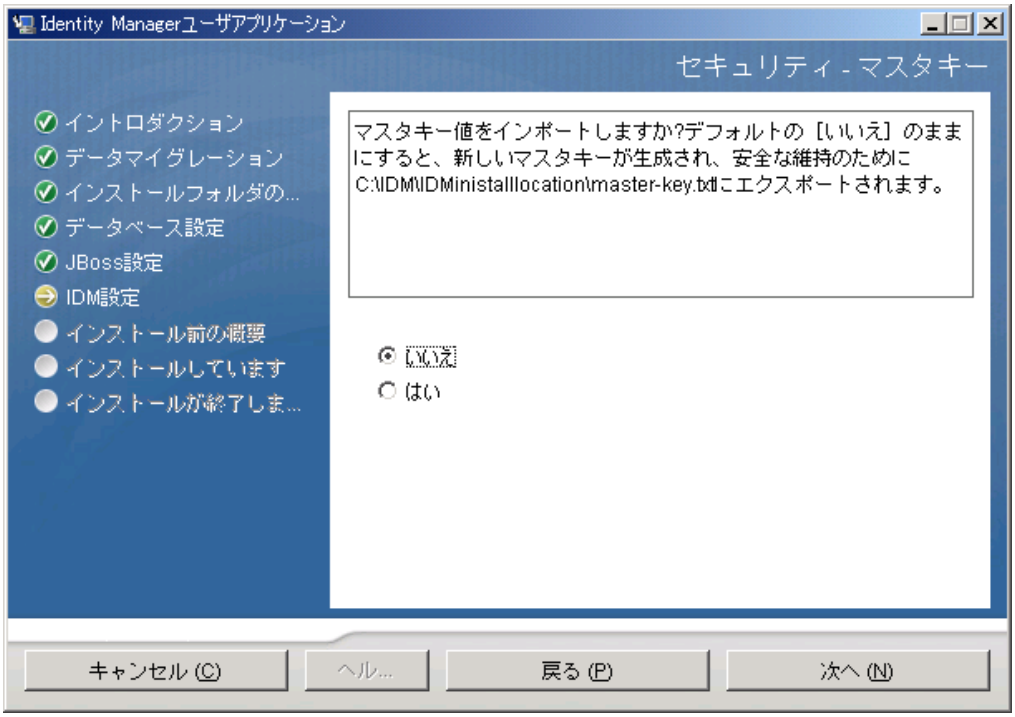
2 *［次へ］* をクリックして、89 ページのセクション 6.8「マスタキーの指定」に進みます。

6.8 マスタキーの指定

既存のマスタキーをインポートするか、新しいマスタキーを作成するかを指定します。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。

1 *[はい]* クリックして既存のマスタキーをインポートするか、または *[いいえ]* をクリックして新しいマスタキーを作成します。

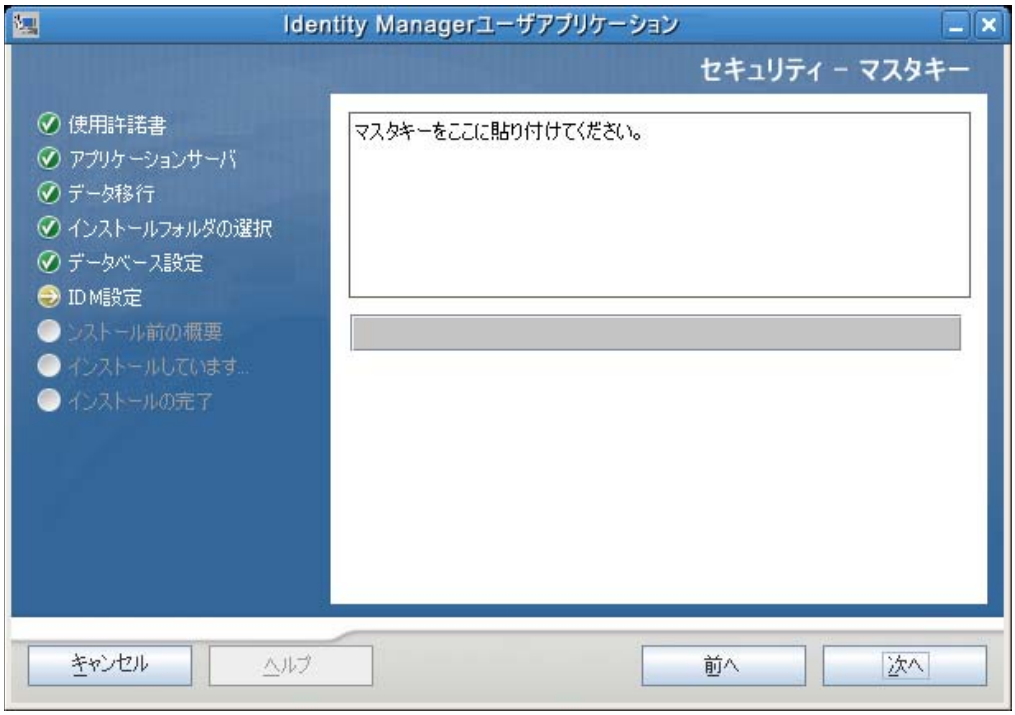


2 ［*次へ*］をクリックします。

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。

［*いいえ*］を選択する場合は、90 ページのセクション 6.9「ユーザアプリケーションの設定」までスキップされます。インストールが完了したら、マスタキーを手動で記録する必要があります。*[はい]* を選択した場合は、89 ページのステップ 3 に進みます。

3 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。



4 *[次へ]* をクリックして、90 ページのセクション 6.9「ユーザアプリケーションの設定」に進みます。

6.9 ユーザアプリケーションの設定

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。

1 *[次へ]* をクリックして、［ユーザアプリケーション環境設定］ページの 1 ページ目に移動します。

2 93 ページの 表 6-1 で説明されている基本のユーザアプリケーション環境設定パラメータを設定してから、ステップ 3 に進みます。

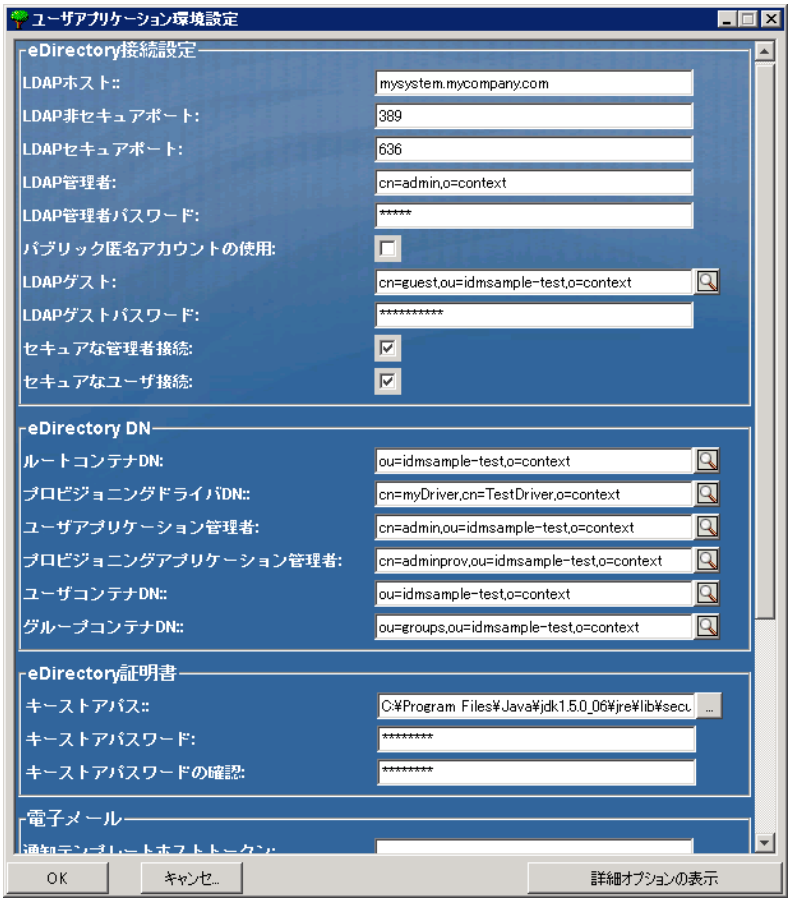

ユーザアプリケーション環境設定
eDirectory接続設定
LDAPホスト:
mysystem.mycompany.com
LDAP非セキュアポート:
389
LDAPセキュアポート:
636
LDAP管理者:
cn=admin,o=context
LDAP管理者パスワード:
*****
パブリック匿名アカウントの使用:
LDAPゲスト:
cn=guest,ou=idmsample-test,o=context
LDAPゲストパスワード:
****
セキュアな管理者接続:
セキュアなユーザ接続:
eDirectory DN
ルートコンテナDN:
ou=idmsample-test,o=context
プロビジョニングドライバDN:
cn=myDriver,cn=TestDriver,o=context
ユーザアプリケーション管理者:
cn=admin,ou=idmsample-test,o=context
プロビジョニングアプリケーション管理者:
cn=adminprov,ou=idmsample-test,o=context
ユーザコンテナDN:
ou=idmsample-test,o=context
グループコンテナDN:
ou=groups,ou=idmsample-test,o=context
eDirectory証明書
キーストアパス:
C:¥Program Files¥Java¥jdk1.5.0_06¥jre¥lib¥secu
キーストアパスワード:
****
キーストアパスワードの確認:
****
電子メール
OK
キャンセ...
詳細オプションの表示

表 6-1 *ユーザアプリケーション環境設定 : 基本パラメータ*

設定のタイプ	フィールド	説明
eDirectory 接続設定	*LDAP ホスト*	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`
	LDAP 非セキュアポート	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。
	LDAP セキュアポート	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。
	LDAP 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。
	LDAP 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。
	セキュアな管理者接続	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	フィールド	説明
eDirectory 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。
	プロビジョニングドライバ 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。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、*IDM 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。
	プロビジョニングアプリケーション管理者	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。

設定のタイプ	フィールド	説明
eDirectory DN(続き)	*役割管理者*	この役割は、Novell Identity Manager 役割ベースプロビジョニングモジュールで利用可能です。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。
	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 :** ユーザがワークフローを実行できるようにする場合は、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は、このコンテナ内に存在する点に注意してください。
	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。
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実行に使用しているの JDK 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。 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 / キーストアパスワードの確認	必須。cacerts のパスワードを指定します。デフォルトは、「changeit」です。

設定のタイプ	フィールド	説明
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。
	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。
	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。
	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電子メールが送信されるように指定します。
	通知 SMTP 電子メールホスト:	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。
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］*を選択する場合は、*［パスワードを忘れた場合のリンク］*および *［パスワードを忘れた場合の返信リンク］*に値を指定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.jsf(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.jsf 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	外部のパスワード管理 WAR を使用している場合は、外部の［パスワード管理 WAR］が Web サービス、たとえば https:// *idmhost:sslport*/idm 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パスを指定します。

3 追加ユーザアプリケーション環境設定パラメータに設定する場合は、［*詳細オプションの表示*］をクリックします。(スクロールしてパネル全体を表示します。) 表 98 ページの 表 6-2 は、詳細オプションのパラメータについて説明しています。このステップで説明した追加パラメータを設定しない場合は、スキップしてステップ 4 に進みます。

表 6-2 *ユーザアプリケーション環境設定 : すべてのパラメータ*

設定のタイプ	フィールド	説明
eDirectory 接続設定	*LDAP ホスト*	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 非セキュアポート	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。
	LDAP セキュアポート	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。
	LDAP 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。
	LDAP 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。
	セキュアな管理者接続	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	フィールド	説明
eDirectory 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。
	プロビジョニングドライバ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。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、*IDM 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。
	プロビジョニングアプリケーション管理者	プロビジョニングアプリケーション管理者は、ユーザアプリケーションの*［要求と承認］*タブを使用して利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。

設定のタイプ	フィールド	説明
メタディレクトリユーザ 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 :** ユーザがワークフローを実行できるようにする場合は、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は、このコンテナ内に存在する点に注意してください。
	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。
	役割管理者	この役割は、Novell Identity Manager 役割ベースプロビジョニングモジュールで利用可能です。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。

設定のタイプ	フィールド	説明
メタディレクトリユーザグループ	*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。
	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)。
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 *キーストアパスワードの確認*	必須。cacerts のパスワードを指定します。デフォルトは、「changeit」です。
プライベートキーストア	*プライベートキーストアパス*	プライベートキーストアには、ユーザアプリケーションのプライベートキーおよび証明書が含まれます。予約済み。入力しない場合は、このパスはデフォルトで /jre/lib/security/cacerts になります。
	プライベートキーストアパスワード	このパスワードは、別のパスワードを指定するまでは changeit です。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。
	プライベートキーの別名	この別名は、別の別名を指定するまでは novellIDMUserApp です。
	プライベートキーパスワード	このパスワードは、別のパスワードを指定するまでは nove1IIDM です。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。

設定のタイプ	フィールド	説明
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。
Novell Audit デジタル署名および証明書キー		Novell Audit デジタル署名キーおよび証明書が含まれます。
	Novell Audit デジタル署名証明書	デジタル署名証明書が表示されます。
	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 および iChain 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。

設定のタイプ	フィールド	説明
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。
	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。
	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。
	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。
	通知テンプレートセキュアプロトコルトークン	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。
	通知 SMTP 電子メールホスト :	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	フィールド	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］*を選択する場合は、*［パスワードを忘れた場合のリンク］*および *［パスワードを忘れた場合の返信リンク］*に値を指定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.jsf(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.jsf 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	外部のパスワード管理 WAR を使用している場合は、外部の［パスワード管理 WAR］が Web サービス、たとえば https:// *idmhost:sslport*/idm 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パスを指定します。
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。
	eDirectory インデックスの作成	
	サーバ DN	

設定のタイプ	フィールド	説明
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の LDAP 名を指定します。 コンテナの詳細については、『*Novell iManager 2.6 管理ガイド (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*』を参照してください。
	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。

4 環境設定が完了したら、*［OK］*をクリックして、106 ページのセクション 6.10「選択を確認してインストール」に進みます。

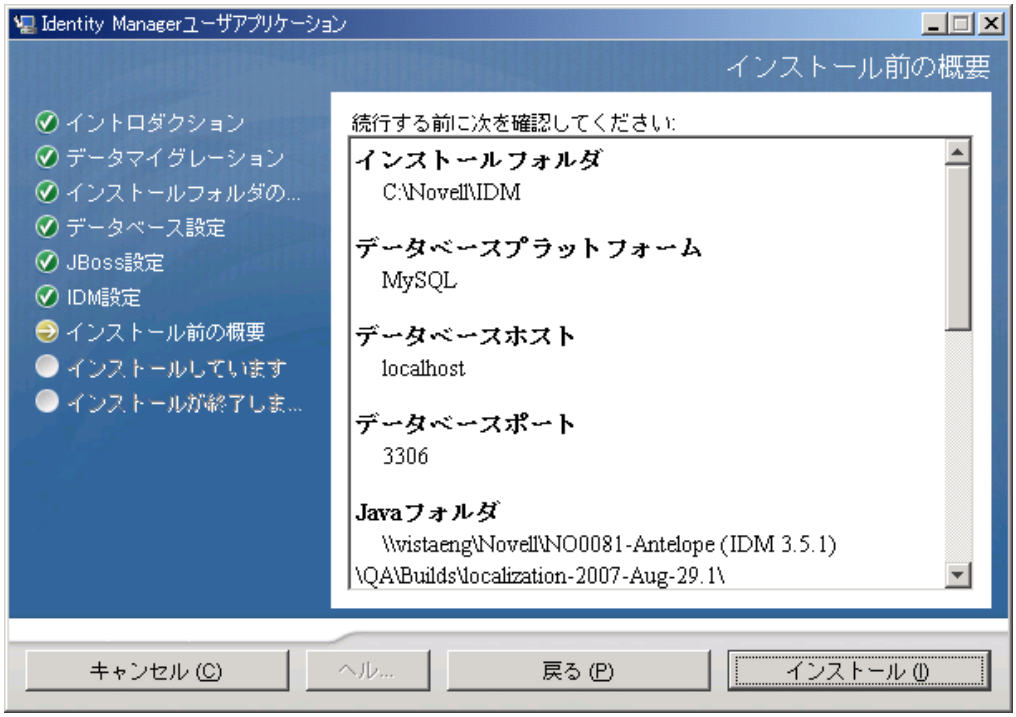
6.10 選択を確認してインストール

1 ［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。

2 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ませんので、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値を再入力する必要があります。

3 インストールおよび環境設定パラメータで満足したら、［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。



6.11 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、107 ページのセクション 6.12「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。

6.12 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。

注 : 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。

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

1 ユーザアプリケーションのインストール中に、eDirectory™ ルート認証局の証明書が、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エクスポートされます。これらの証明書を、WebSphere サーバをホストするマシンにコピーします。

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 (109 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 (109 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、109 ページのセクション 6.14「IDM WAR ファイルの展開」に進みます。

6.13.1 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 (バイナリ DER データ)*］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。

6.13.2 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。

6.14 IDM WAR ファイルの展開

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、*［アプリケーション］> ［新規アプリケーションのインストール］* の順に移動します。

3 IDM War ファイルの場所を参照します。

IDM WAR ファイルはユーザアプリケーションのインストール中に設定されます。このファイルは、ユーザアプリケーションのインストール時に指定した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ります。

4 アプリケーションのコンテキストルートを入力します (例 : IDMProv)。これが URL のパスになります。

5 *[Prompt me only when additional information is required.]* のラジオボタンはオンのままにします。その後、*[次へ]* をクリックし、[Select installation options] ページに移動します。

6 このページのデフォルト値をそのまま使用し、*[Next]* をクリックして [Map modules to servers] ページに移動します。

7 このページのデフォルト値をそのまま使用し、*[Next]* をクリックして [Map resource references to resources] ページに移動します。

8 認証方法では、*[Use default method]* チェックボックスをオンにします。続いて、*[Authentication data entry]* ドロップダウンで、先に作成したエイリアス (MyServerNode01/MyAlias など) を選択します。

9 認証設定の下の表で、展開するモジュールを検索します。[Target Resource JNDI Name] というタイトルのカラムの下で、参照ボタンをクリックして JNDI 名を指定します。これによりリソースのリストが表示されます。先に作成したデータソースを選択して [*Apply*] ボタンをクリックし、[Map resource references to resources] ページに戻ります (例 : MyDataSource)。

10 *[Next]* を選択して、[*Map virtual hosts for Web modules*] ページに移動します。

11 このページのデフォルト値をそのまま使用し、*[次へ]* を選択して [概要] ページへ移動します。

12 *[完了]* をクリックして展開を完了します。

13 展開が完了したら、[*保存*] をクリックして変更内容を保存します。

14 110 ページのセクション 6.15「アプリケーションの起動」に進みます。

6.15 アプリケーションの起動

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。

6.16 ユーザアプリケーションポータルへのアクセス

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

インストール後のタスク 7

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。

7.1 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。

7.2 インストール後の設定

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 役割ベースプロビジョニングモジュール 3.6 管理ガイド*』の「ユーザアプリケーション環境の設定」セクション
- 『*Novell IDM 役割ベースプロビジョニングモジュール 3.6 設計ガイド*』

7.3 クラスタインストールのチェック

JBoss クラスタでは、クラスタ内のアプリケーションサーバごとに次の項目が設定されていることを確認します。

- 固有のパーティション名 (パーティション名)
- 固有のパーティション UDP(partition.udpGroup)
- 固有のワークフローエンジン ID
- 同じ (同一の)WAR ファイル。WAR は、デフォルトで jboss\server\IDM\deploy ディレクトリにインストールによって書き込まれます。

アプリケーションサーバ クラスタ

詳細については、『*Identity Manager ユーザアプリケーション : 管理ガイド* (http://www.novell.com/documentation/idmrbpm36/index.html)』の第 4 章のクラスタについてのセクションを参照してください。

7.4 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 IDMPwdMgt.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。

7.5 外部パスワード WAR へのアクセス

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.jsf。
- 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。

7.6 ［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］* および *［パスワードを忘れた場合の返信リンク］* 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.jsf)
- ［*パスワードを忘れた場合の返信リンク*］(たとえば https://idmhost:sslport/idm)

7.7 電子メール通知の設定

［パスワードを忘れた場合］およびワークフロー電子メール通知機能を実装するには、次のようにします。

1. iManager の［役割とタスク］の下で、*［ワークフロー管理］*、*［電子メールサーバオプション］* の順に選択します。
2. ［*ホスト名*］の下で SMTP サーバ名を指定します。
3. ［*送信者*］の隣で、電子メールアドレス (たとえば *noreply@novell.com*) を指定してから、［*OK*］をクリックします。

7.8 インストールのテスト JBoss アプリケーションサーバの場合

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必要がある場合は、stop-jboss.sh または stop-jboss.bat、または 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［］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*

このアドレスでは、*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設定情報を指定した場合は、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表示ページが表示されるはずです。

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、115 ページのセクション 7.12「トラブルシューティング」を参照します。

7.9 プロビジョニングチームと要求の設定

プロビジョニングチームとプロビジョニングチーム要求を設定して、ワークフロータスクを有効にします。手順については、『*Identity Manager ユーザアプリケーション : 管理ガイド*(http://www.novell.com/documentation/idmrbpm36/index.html)』を参照してください。

7.10 eDirectory でのインデックスの作成

IDM ユーザアプリケーションのパフォーマンスを改善するには、eDirectory 管理者で、manager、ismanager、および srvprvUUID の属性についての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くても、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のユーザアプリケーションのパフォーマンス向上を経験できます。Index Manager を使用したインデックスの作成手順については、『*Novell eDirectory 管理ガイド*(http://www.novell.com/documentation)』を参照してください。

7.11 インストール後の IDM WAR ファイルの再設定

IDM WAR ファイルを更新する

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、60 ページの 表 4-2、72 ページの 表 5-1、または 98 ページの 表 6-2 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。

7.12 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)。
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 (ただし、Identity Manager に付属するバージョンの MySQL 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。

項目	推奨されるアクション
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)。

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`