ユーザアプリケーション：インストールガイド

Novell®
Identity Manager Roles Based Provisioning Module

3.6.1

2008 年 7 月 23 日

www.novell.com

保証と著作権

米国 Novell, Inc., およびノベル株式会社は、本書の内容または本書を使用した結果について、いかなる保証、表明または約束も行っていません。また、本書の商品性、および特定の目的への適合性について、いかなる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て、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。これらの知的所有権は、「Novell Legal Patents (http://www.novell.com/company/legal/patents/)」の Web ページに記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります。

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

オンラインマニュアル: 本製品とその他の Novell 製品の最新のオンラインマニュアルにアクセスするには、「Novell 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

このガイドでは、Novell® Identity Manager Roles Based Provisioning Module 3.6.1 のインストール方法について説明します。主なセクションは次のとおりです。

対象読者

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

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンライン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 Roles Based Provisioning Module に関する追加のマニュアルについては、Identity Manager マニュアルの Web サイト (http://www.novell.com/documentation/lg/dirxmldrivers/index.html) を参照してください。

マニュアルの表記規則

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

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

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

Roles Based Provisioning Module インストール概要

1

このセクションでは、Roles Based Provisioning Module をインストールするステップの概要を説明します。また、メタディレクトリサーバのインストールで必要となるユーザアプリケーション標準エディションの追加のインストールおよび環境設定にも役立ちます。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「インストールのチェックリスト」
- 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」
- 11 ページのセクション 1.3「システム要件」

ユーザアプリケーションまたは Roles Based Provisioning Module の以前のバージョンからマイグレートする場合、『*ユーザアプリケーション：マイグレーションガイド*(http://www.novell.com/documentation/idmrbpm361/index.html)』を参照してください。

1.1 インストールのチェックリスト

Novell® Identity Manager Roles Based Provisioning Module またはユーザアプリケーション標準エディションをインストールするには、以下のタスクを実行する必要があります。

- ❑ ソフトウェアがシステム要件を満たしているかどうかを確認します。詳細については、11 ページのセクション 1.3「システム要件」を参照してください。
- ❑ Identity Manager 3.6.1Roles Based Provisioning Module をダウンロードします。詳細については、17 ページのセクション 2.2「Roles Based Provisioning Module のダウンロード」を参照してください。
- ❑ 以下のサポートコンポーネントを設定します。
  - ❑ サポートされているIdentity Managerのメタディレクトリがインストールされていることを確認します。詳細については、17 ページのセクション 2.1「Identity Manager メタディレクトリのインストール」を参照してください。
  - ❑ アプリケーションサーバをインストールおよび設定します。詳細については、19 ページのセクション 2.3「アプリケーションサーバのインストール」を参照してください。
  - ❑ データベースをインストールおよび設定します。詳細については、22 ページのセクション 2.4「データベースのインストール」を参照してください。
  - ❑ ユーザアプリケーションの以前のバージョンから移行し、引き続き Identity Manager 3.5.1 メタディレクトリを使用する場合、以下のタスクを実行します。
    - ❑ 役割サービスおよびユーザアプリケーションドライバのインストールユーティリティを実行して識別ボールトスキーマを拡張し、必要な役割サービスおよびユーザアプリケーションドライバの環境設定ファイルをインストールして、必要に応じて追加ファイルをコピーします。詳細については、24 ページのセクション 2.6「メタディレクトリ 3.5.1 用追加ファイルのインストール」を参照してください。

注 : Identity Manager 3.6 メタディレクトリは、役割サービスおよびユーザアプリケーションドライバのインストールユーティリティをサイレントに実行します。これで、必要なファイルはすべて揃ったことになります。

- ❑ 正しいiManagerの場所にiManager_icons_for_roles.zipのコンテンツをコピーします。詳細については、26 ページのセクション 2.6.3「iManager アイコンのコピー」を参照してください。
- ❑ afadmin.jar ファイルを正しい場所にコピーします。詳細については、26 ページの 「afadmin.jar のコピー」を参照してください。

❑ iManager for Identity Manager 3.0 または Designer for Identity Manager 3.0 でユーザアプリケーションドライバを作成します。

- iManager の場合 : 27 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」
- Designer の場合 : ユーザアプリケーション : 設計ガイド (http://www.novell.com/documentation/idmrbpm361/index.html)

❑ iManager for Identity Manager 3.0 または Designer for Identity Manager 3.0 で役割サービスドライバを作成します。

- iManager の場合 : 29 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」
- Designer の場合 : ユーザアプリケーション : 設計ガイド (http://www.novell.com/documentation/idmrbpm361)

❑ Novell Identity Manager ユーザアプリケーションまたは Roles Based Provisioning Module をインストールおよび設定します (インストールプログラムを開始する前に、正しい JDK* がインストールされている必要があります。詳細については、23 ページのセクション 2.5「Java Development Kit のインストール」を参照してください)。

インストールプログラムは、次の 3 つのモードのいずれかで起動できます。

- グラフィカルユーザインタフェース 以下のいずれかを参照してください。
  - 33 ページの第 4 章「GUI インストーラを使用した JBoss へのインストール」
  - 41 ページの第 5 章「GUI インストーラを使用した WebSphere アプリケーションサーバのインストール」
  - 49 ページの第 6 章「GUI インストーラを使用した WebLogic アプリケーションサーバのインストール」
- コンソール (コマンドライン) インタフェース詳細については、57 ページのセクション 7.1「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、58 ページのセクション 7.2「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。

❑ 67 ページの第 8 章「インストール後のタスク」で説明されているインストール後のタスクを実行します。

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* および WebLogic* では、WAR を手動で展開する必要があります。
- そのように選択した場合は、Novell Audit のログまたは OpenXDAS のログを有効にします。
- 既存のマスタキーをインポートして、特定の Roles Based Provisioning Module のインストールを復元し、クラスタをサポートできるようにします。
- 3.5.1 Provisioning Moduleまたは3.6 Roles Based Provisioning Moduleから既存のデータを 3.6.2 の必要なデータ形式に移行します。

1.3 システム要件

Novell Identity Manager Roles Based Provisioning Module 3.6.1 を使用するには、表 1-1 に記述されている必要な各コンポーネントの 1 つが存在している必要があります。

表 1-1 *システム要件*

必須システムコンポーネント	システム要件
Identity Manager 3.5.1 (メタディレクトリシステム)	最新のサポートパックを適用した SUSE® Linux Enterprise Server (SLES) 10 (32 ビットと 64 ビットの両方がサポートされます) eDirectory™: 8.8.2 セキュリティサービス 2.0.5 (NMAS™ 3.1.3)
Identity Manager 3.6 (メタディレクトリシステム)	次のいずれかのオペレーティングシステムが必要です。 ◆ Windows Server* 2003 SP2 (32 ビット) ◆ 最新のサポートパックを持つ Linux Red Hat 5.0 (32 ビット) ◆ 最新のサポートパックを持つ SLES* 10 SP2 (32 ビット) ◆ Solaris* 10 (32 ビット) ◆ AIX* 5L v5.3 (32 ビット) eDirectory: 8.8.3

必須システムコンポーネント	システム要件
Web ベースの管理サーバ ◆ iManager 2.6 およびプラグイン (メタディレクトリ 3.5.1 のみ) ◆ iManager 2.7 およびプラグイン	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 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、または 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持つ 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 ◆ Windows Vista UltimateおよびBusinessエディション(iManager 2.7のみ) ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 ◆ openSUSE® 10.3 (iManager 2.7 のみ) 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持つ Novell iManager 2.6 または 2.7

必須システムコンポーネント	システム要件
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 または Sentinel 6.1(メタディレクトリ 3.6 のみ)	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持つ Novell Open Enterprise Server 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 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

必須システムコンポーネント	システム要件
ユーザアプリケーションのアプリケーションサーバ	ユーザアプリケーションは、以下に説明するように JBoss*、WebSphere*、および WebLogic* 上で動作します。 JBoss 4.2.2 GA 付属のユーザアプリケーションでは、JRE* 1.5.0_15 が必要とされ、以下のプラットフォーム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 2003 Server SP1 (64 ビット) ◆ Solaris 10 サポートパック (日付が 6/06 のもの) ◆ Red Hat Linux 5 (32 ビット) WebSphere 6.1 のユーザアプリケーションには IBM JDK が必要です。フィックスパックの最低レベルは、制限なしのポリシーファイルが適用された状態の 6.1.0.9 です。これら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 (64 ビット) WebLogic 10 のユーザアプリケーションは JRockit* 1.5.0_06 を必要とし、以下のプラットフォームでサポートされています。 ◆ Solaris 10 (32 ビットまたは 64 ビット) ◆ Windows 2003 SP1
ユーザアプリケーションのブラウザ	ユーザアプリケーションは、以下に説明するように Firefox* および Internet Explorer* の両方をサポートしています。 Firefox 2* は以下でサポートされています。 ◆ Windows XP SP2 ◆ Windows Vista ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ openSUSE 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 XP SP2 ◆ Windows Vista Enterprise 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 XP SP2

必須システムコンポーネント	システム要件
ユーザアプリケーション用のデータベースサーバ	JBoss では次のデータベースがサポートされています。 ◆ MySQL バージョン 5.0.51 ◆ 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 WebLogic では以下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 以下の JDBC ドライバがサポートされています。 MS SQL Server バージョン 1.2.2828.100 Oracle シンドライバ : Oracle JDBC ドライババージョン 10.2.0.1.0 Oracle OCI ドライバ : Oracle JDBC ドライババージョン 10.2.0.2.0 MySQL コネクタ /J 5.0.8 DB2 ドライババージョン 1.4.2
ワークステーション ◆ Designer 3.0 for Identity Manager 3.6 ◆ 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: ◆ Windows XP SP2 ◆ Microsoft Windows Vista Linux: ◆ SUSE Linux Enterprise Server 10 (Designer の場合のみ) ◆ SUSE Linux Enterprise Desktop 10 ◆ openSUSE 10
Audit	Novell Audit 2.0.2
OpenXDAS	OpenXDAS バージョン 0.5.257
ユーザアプリケーションの SSO 統合	Novell Access Manager 3.0.1 を必要とします。

前提条件

2

このセクションでは、Identity Manager Roles Based Provisioning Module またはユーザアプリケーション標準エディションをインストールする前にインストールまたは設定する必要があるソフトウェアおよびコンポーネントを説明します。主なトピックは次のとおりです。

2.1 Identity Manager メタディレクトリのインストール

Roles Based Provisioning Module 3.6.1 は、Identity Manager 3.5.1 または 3.6 のメタディレクトリと共に使用できます。

Identity Manager 3.6 メタディレクトリのインストール手順については、『*Novell Identity Manager 3.6 インストールガイド*(http://www.novell.com/documentation/idm36/)』を参照してください。

Identity Manager 3.5.1 メタディレクトリがある場合、Roles Based Provisioning Module 3.6.1 が動作する前に複数のファイルを更新する必要があります。詳細については、24 ページのセクション 2.6「メタディレクトリ 3.5.1 用追加ファイルのインストール」を参照してください。Identity Manager 3.6 メタディレクトリの場合は、インストールの一環としてこれらのファイルが自動的にインストールされるため、この処理は Identity Manager 3.6 メタディレクトリでは必要ありません。

2.2 Roles Based Provisioning Module のダウンロード

Novell ダウンロード (http://download.novell.com/index.jsp) から Identity Manager Roles Based Provisioning Module3.6.1 を取得します。表 2-1 に表示されている製品の .iso イメージファイルをダウンロードします。

表 2-1 *.iso ダウンロードファイル*

本製品について	この .iso をダウンロード
Roles Based Provisioning Module	Identity_Manager_3_6_1_User_Application_ Provisioning.iso

本製品について	この .iso をダウンロード
ユーザアプリケーション標準エディション	Identity_Manager_3_6_1_User_Application_NON_Provisioning.iso

Identity Manager 3.5.1 メタディレクトリがある場合、Roles_Driver_Install_Utility.iso もダウンロードする必要があります。この .iso に含まれるファイルがすでに Identity Manager 3.6 メタディレクトリのインストールの一部であるために、Identity Manager 3.6 メタディレクトリユーザである場合、Roles_Driver_Install_Utility.iso をダウンロードする必要はありません。

表 2-2 では、Roles Based Provisioning Module またはユーザアプリケーション標準エディションの .iso ファイルからのインストールファイルについて説明します。

***表 2-2** iso で送信されるファイルおよびスクリプト*

ファイル	説明
IDMProv.war	Roles Based Provisioning Module WARIdentity セルフサービス機能および Roles Based Provisioning Module を持つ Identity Manager 3.6.1 ユーザアプリケーションが含まれています。
IDM.war	ユーザアプリケーション標準エディション WAR。Identity セルフサービス機能をサポートする Identity Manager 3.6.1 ユーザアプリケーションが含まれています。
IDMUserApp.jar	Roles Based Provisioning Module およびユーザアプリケーションインストールプログラム
silent.properties	サイレントインストールに必要なパラメータに含まれるファイルこれらのパラメータは、GUI またはコンソールインストール手順で設定するインストールパラメータに対応します。このファイルをコピーしてから、コンテンツを修正してインストール環境に適合させる必要があります。
JBossMySQL.bin または JBossMySQL.exe	JBoss アプリケーションサーバおよび MySQL データベースをインストールする便利なユーティリティ
nmassaml.zip	SAML をサポートするための eDirectory メソッドが含まれます。Access Manager を使用していない場合のみ必要となります。
afadmin.jar	Identity Manager 3.5.1 メタディレクトリにのみ必要です。
prerequisitefiles.zip	Identity Manager 3.5.1 メタディレクトリにのみ必要です。 正しい場所に手動でコピーされる必要のあるその他のファイルが含まれます。

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

デフォルトのインストール場所は次のとおりです。

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

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

2.3 アプリケーションサーバのインストール

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

2.3.1 JBoss アプリケーションサーバのインストール

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

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

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

表 2-3 *JBoss アプリケーションサーバの最少推奨要件*

コンポーネント	推奨
RAM	Identity Manager Roles Based Provisioning Module を実行する場合、JBoss アプリケーションサーバの最少推奨 RAM は 512MB です。
ポート	8080 は、アプリケーションサーバのデフォルトです。アプリケーションサーバが使用するポートを記録します。

コンポーネント	推奨
SSL	外部のパスワード管理を使用する予定がある場合、SSL を有効にします。 ◆ Identity Manager Roles Based Provisioning Module および IDMPwdMgt.war ファイルを展開する JBoss サーバの SSL を有効にします。 ◆ SSL ポートがファイアウォール上で開いていることを確認します。 SSL の有効化の詳細については、JBoss の文書を参照してください。 IDMPwdMgt.war ファイルの詳細については、70 ページのセクション 8.5「外部パスワード管理の環境設定」を参照してください。また、『*ユーザアプリケーション : 管理ガイド* (http://www.novell.com/documentation/idmrbpm361/index.html)』も参照してください。

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

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

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

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

Solaris 用のユーティリティは利用できません。

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

インストール画面	説明
インストールセットの選択	インストールする製品を選択します。 ◆ *JBoss*: 指定するディレクトリに、起動と停止を行うスクリプトと共に JBoss アプリケーションサーバをインストールします。 **注 :** このユーティリティでは、JBoss アプリケーションサーバは Windows サービスとしてインストールされません。手順については、21 ページの 「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またはデーモン」を参照してください。 ◆ *MySQL*: 指定するディレクトリに、起動と停止を行うスクリプトと一緒に MySQL をインストールし、MySQL データベースを作成します。
JBoss 親フォルダの選択	[*選択*] をクリックし、デフォルト以外のインストールフォルダを選択します。
MySQL 親フォルダの選択	[*選択*] をクリックし、デフォルト以外のインストールフォルダを選択します。

インストール画面	説明
MySQL 情報	以下の内容を指定します。 ◆ *データベース名*: 作成するインストーラのデータベース名を指定します。ユーザアプリケーションインストールユーティリティによりこの名前を入力するようメッセージが表示されるので、名前と場所を書き留めます。 ◆ *「ルート」ユーザパスワード*(および確認パスワード): このデータベースに対してルートパスワードを指定します (また、ルートパスワードを確認します)。
インストール前の概要	概要ページを確認します。仕様が正しい場合、［*インストール*］をクリックします。

選択した製品がインストールされると、ユーティリティでは正常に完了したことを示す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、22 ページのセクション 2.4.1「MySQL データベースの設定」に進みます。

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またはデーモン

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

JavaServiceWrapper の使用 JavaServiceWrapper を使用して、JBoss アプリケーションサーバを Windows サービス、Linux、または UNIX のデーモンプロセスとしてインストール、開始、および停止することができます。JBoss による手順については、http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows (http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows) を参照してください。ラッパーは 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 によって管理します (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss) を参照してください)。

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

2.3.2 WebLogic アプリケーションサーバのインストール

WebLogic アプリケーションサーバ 10 の使用を計画している場合、これをダウンロードおよびインストールします。サポートされているバージョンの情報については、11 ページのセクション 1.3「システム要件」を参照してください。

2.3.3 WebSphere アプリケーションサーバのインストール

WebSphere アプリケーションサーバ 6.1 の使用を予定している場合、これをダウンロードおよびインストールします。サポートされているバージョンの情報については、11 ページのセクション 1.3「システム要件」を参照してください。

2.4 データベースのインストール

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

- データベースおよびデータベースドライバのインストール
- データベースまたはデータベースインスタンスの作成
- Identity Manager Roles Based Provisioning Module のインストール手順で使用するための以下のデータベースパラメータの記録
  - ホストおよびポート
  - データベース名、ユーザ名、およびユーザパスワード
- データベースをポイントするデータソースファイルの作成

  方法はアプリケーションサーバに応じて変わります。JBoss の場合は、Identity Manager Roles Based Provisioning Module 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 Roles Based Provisioning ModuleWAR ファイルの名前に基づいてファイルに名前を付けます。WebSphere および WebLogic の場合は、インストール前に手動でデータソースを設定します。
- データベースでは UTF-8 を有効にする必要があります。

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

2.4.1 MySQL データベースの設定

ユーザアプリケーションには、MySQL の特定の設定オプションが必要です。MySQL を自分でインストールする場合、これらを設定します。JBossMySQL ユーティリティを使用して MySQL をインストールすると、ユーティリティによって正しい値が設定されますが、以下を維持するための値は把握しておく必要があります。

- 22 ページの 「INNODB ストレージエンジンとテーブルタイプ」
- 23 ページの 「文字セット」
- 23 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のみに対し、文字セットとして UTF-8 を指定します。サーバ全体に UTF-8 を指定するには、my.cnf (Linux または Solaris) または my.ini (Windows) に以下のオプションを含めます。

character_set_server=utf8

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

create database databasename character set utf8 collate utf8_bin;

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

```
<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&amp;characterEncoding=utf8&amp;connectionCollation=ut
f8_bin</connection-url>
```

大文字と小文字の区別

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

lower_case_table_names=1

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

2.5 Java Development Kit のインストール

Roles Based Provisioning Module およびユーザアプリケーション標準エディションのインストールプログラムでは、少なくとも Java 2 プラットフォーム標準エディション Development Kit バージョン 1.5 を使用する必要があります。

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

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

2.6 メタディレクトリ 3.5.1 用追加ファイルのインストール

Identity Manager メタディレクトリ 3.5.1 を使用する場合、これらのセクションで説明されている追加ステップを実行する必要があります。

- 24 ページのセクション 2.6.1「GUI を使用した役割サービスドライバのインストール」
- 25 ページのセクション 2.6.2「コンソールからの役割サービスドライバのインストール」
- 26 ページのセクション 2.6.3「iManager アイコンのコピー」
- 26 ページのセクション 2.6.4「afadmin.jar のコピー」

Linux/Unix ユーザの場合、これをルートユーザとしてインストールします。

2.6.1 GUI を使用した役割サービスドライバのインストール

Identity Manager 3.5.1 メタディレクトリを使用する場合のみ必要となります。Identity Manager 3.6 メタディレクトリをインストールした場合、これらのファイルはすでにインストールされています。

役割サービス、およびユーザアプリケーションドライバのインストールユーティリティには、次の処理を行うオプションがあります。

- Identity 識別ボールトスキーマを拡張して、ユーザアプリケーション、および Roles Based Provisioning Module をサポートする。
- 役割サービスドライバ、およびユーザアプリケーションドライバの環境設定ファイルをメタディレクトリサーバにインストールする。
- 役割サービス、およびユーザアプリケーションドライバの環境設定ファイルを iManager にインストールする。

メタディレクトリ、および iManager マシンの両方にこのインストーラを実行する必要があります。

注 : メタディレクトリは、このインストーラを使用するデフォルトのロケーションにインストールされる必要があります。

Roles_Driver_Install_Utility.iso へのアクセス

1 自分のオペレーティングシステム用のインストーラを見つけて実行します。

オペレーティングシステム	役割サービスドライバインストーラ
AIX	roles_driver_install.aix.bin
Linux	roles_driver_install.linux.bin
Solaris	roles_driver_install.solaris.bin
Windows	roles_dirver_install.exe

2 インストールを完了するには、次の情報を使用します。

インストール画面	説明
使用許諾契約	使用許諾契約を読み、［*使用許諾契約の条件に同意します*］を選択します。
コンポーネントの選択	*ドライバ*: メタディレクトリサーバに役割サービスドライバおよびユーザアプリケーションドライバをインストールし、サポートしているライブラリ JAR を更新します。 *スキーマ*: メタディレクトリスキーマを更新して、Roles Based Provisioning Module、およびユーザアプリケーション標準エディションに必要なオブジェクトを含めます。nrf-extensions.sch ファイルおよび srvprv.sch ファイルをインストールし、現在のプラットフォームに対してコマンド (Windows の場合は NdsCons.exe、UNIX/Linux の場合は ndssch) を実行します。 *ドライバ環境設定ファイル*: 役割サービスドライバおよびユーザアプリケーションドライバ環境設定ファイルをインストールします。これらのファイルは、iManager に新規のドライバを作成する際に使用されます。iManager をホストするマシンでこれを実行する必要があります。
認証	*スキーマ拡張子*を選択する場合、ユーザ名およびパスワードを指定する必要があります。このユーザは、識別ボールトへの管理権を持っている必要があります。例 : *cn=admin,o=novell*。
ドライバの場所の選択	役割サービスおよびユーザアプリケーションドライバのインストールを選択した場合、eDirectory サーバの場所を入力するよう促されます。これらは一般的に、メタディレクトリの /lib/dirxml/classes ディレクトリにインストールされます。
ドライバ環境設定ファイルの場所のインストール	iManager マシンでインストーラがドライバ環境設定ファイルを配置する必要のある場所を指定します。これらは、一般的には iManager の /nps/Dirxml.Drivers ディレクトリにインストールされます。
インストール前の概要	［インストール前の概要］ページを読んで、インストールパラメータの選択を確認し、インストールを完了します。

2.6.2 コンソールからの役割サービスドライバのインストール

コンソール (文字) モードでインストーラを実行するには、以下のコマンドを発行します。

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

24 ページのセクション 2.6.1「GUI を使用した役割サービスドライバのインストール」でグラフィカルユーザインタフェースで説明されているものと同じステップに従い、プロンプトを読み、コマンドラインで応答を入力します。

2.6.3 iManager アイコンのコピー

注 : この手順は、最新のプラグインと共に iManager 2.7 がインストールされている場合は必要ありません。

1. ダウンロードされた .iso イメージで、prerequisites.zip ファイルを見つけます。
2. ファイルを解凍してから、iManager_icons_for_roles.zip ファイルを配置します。
   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。
3. ファイルを解凍してから、nps/portal/modules/dev/images/dir ディレクトリに抽出したアイコンをコピーします。
4. 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。

2.6.4 afadmin.jar のコピー

注 : この手順は、最新のプラグインと共に iManager 2.7 がインストールされている場合は必要ありません。

1. ダウンロードされた .iso イメージで、prerequisites.zip を見つけます。
   このファイルは /36MetaDirSupport ディレクトリにあります。
2. ファイルを解凍してから、afadmin.jar ファイルを見つけます。
3. afadmin.jar ファイルを /iManager/nps/WEB-INF/lib ディレクトリにコピーします。

ドライバの作成

3

このセクションでは、Roles Based Provisioning Module を使用するための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。

ドライバ環境設定サポートでは、以下の処理を実行できます。

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

3.1 iManager でのユーザアプリケーションドライバの作成

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

クラスタのメンバーである Roles Based Provisioning Module を除き、Identity Manager Roles Based Provisioning Module 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 Roles Based Provisioning Module 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 Roles Based Provisoining Module を実行する場合は、『*ユーザアプリケーション : 管理ガイド*(http://www.novell.com/documentation/idmrbpm361/index.html)』を参照してください。

重要 : クラスタ以外の Roles Based Provisioning Module が単一のドライバを共有するように設定すると、Roles Based Provisioning Module 内で実行されている 1 つ以上のコンポーネントにおいてあいまいな状態が発生してしまいます。発生した問題の原因を突き止めるのは困難です。

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

1. Web ブラウザで iManager を開きます。

   iManager 2.6 (Identity Manager 3.5.1 用) または iManager 2.7 (Identity Manager 3.6 用) を使用します。

2. *［役割とタスク］> ［Identity Manager ユーティリティ］*に移動して、［*新規ドライバ*］または［*インポート環境設定*］を選択します (使用しているプラグインのバージョンによって異なります)。

Identity Manager 3.5.1 の場合は、［*新しいドライバ*］リンクを使用します。

Identity Manager 3.6 の場合は、［*インポート環境設定*］リンクを使用します。

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、ユーザアプリケーションドライバ環境設定ファイルを選択します。ファイル名 :

UserApplication_3_6_1-IDM3_5_1-V1.xml

このファイルがリストに存在しない場合、役割サービスドライバは正しくインストールされていない可能性があります。24 ページのセクション 2.6.1「GUI を使用した役割サービスドライバのインストール」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 Roles Based Provisioning Module をインストールする際に必要となります。

フィールド	説明
ドライバ名	作成するドライバの名前。
認証 ID	ユーザアプリケーション管理者の識別名。これは、ユーザアプリケーションポータルの管理権限を付与するユーザアプリケーション管理者になります。admin.orgunit.novell などの eDirectory™ 形式を使用するか、ユーザを参照して特定します。このフィールドは必須です。
パスワード	［認証 ID］で指定したユーザアプリケーション管理者のパスワード。
アプリケーションコンテキスト	ユーザアプリケーションのコンテキスト。これは、ユーザアプリケーション WAR ファイルのコンテキスト部分です。デフォルトは *IDM* です。
ホスト	Identity Manager ユーザアプリケーションが展開されたアプリケーションサーバのホスト名または IP アドレス。 ユーザアプリケーションがクラスタで実行されている場合は、ディスパッチャのホスト名または IP アドレスを入力します。
ポート	上でリストに表示されているホストのポート。

フィールド	説明
イニシエータの無効化を許可:	［*はい*］を選択すると、プロビジョニング管理者は、自分を代理として指定したユーザになりかわってワークフローを開始できます。

8 ［*次へ*］をクリックします。

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

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

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

11 *［追加］*をクリックし、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、［同等セキュリティ］ウィンドウを閉じてから、［*次へ*］をクリックして概要ページを表示します。

13 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、Roles Based Provisioning Module 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

注 : ユーザアプリケーション標準エディションを使用している場合、このセクションのステップを実行する必要はありません。

iManager で役割サービスドライバを作成して設定する

1 Web ブラウザで iManager を開きます。

2.6 (Identity Manager 3.5.1 用) または iManager 2.7 (Identity Manager 3.6 用) を使用します。

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 3.6.1(UserApplication_3_6_1-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。

3 *［ドライバの追加］*をクリックします。

4 ウィザードで、デフォルトの［*既存のドライバセット内*］を維持します。［*次へ*］をクリックします。

5 ドロップダウンリストから［*RoleService_3_6_1-IDM3_5_1-V1.xml*］を選択します。これは、Roles Based Provisioning Module をサポートする役割サービスドライバの環境設定ファイルです。

このファイル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。24 ページのセクション 2.6.1「GUI を使用した役割サービスドライバのインストール」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 および eDirectory を再起動して、新しく変更したスキーマがすべて正しくピックアップされるようにします。

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。
ユーザグループベースコンテナ DN	ドライバは、このベースコンテナのユーザ、コンテナ、およびグループでのみ動作します。グループの役割割り当てがある場合、役割ドライバは、コンテナのドメイン内のメンバーの役割のみを許可 / 無効にします。
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。
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。

オプション	説明
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、［*次へ*］をクリックします。

8 ［*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。

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

10 *［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。

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

12 情報が正しい場合、［*終了*］をクリックします。

GUI インストーラを使用した 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バージョン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 Roles Based Provisioning Module をインストールする方法について説明します。次のトピックについて説明します。

- 33 ページのセクション 4.1「ユーザアプリケーション WAR のインストールおよび環境設定」
- 39 ページのセクション 4.2「インストールのテスト」

コマンドラインを使用してインストールする場合は、57 ページの第 7 章「コンソールまたは単一コマンドによるインストール」を参照してください。

ルート以外のユーザとしてインストーラを実行します。

4.1 ユーザアプリケーション WAR のインストールおよび環境設定

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

1 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

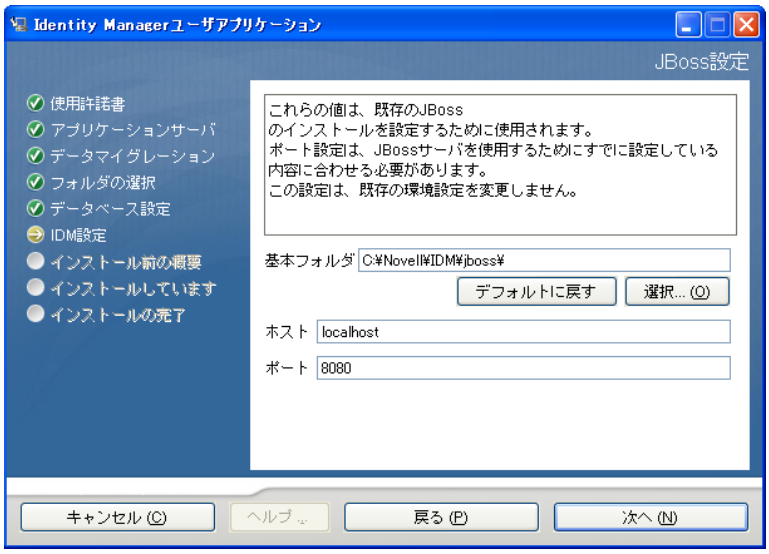
インストールプログラムを開始すると、言語を入力するよう促されます。

2 インストールを完了するには、各インストールパネルの指示に沿って、次の情報を使用します。

インストール画面	説明
Novell Identity Manager	インストールプログラムの言語を選択します。デフォルトでは、［英語］が選択されています。
使用許諾契約	使用許諾契約を読み、［*使用許諾契約の条件に同意します*］を選択します。
アプリケーションサーバプラットフォーム	［*JBoss*］を選択します。
標準またはプロビジョニング	*標準*: ユーザアプリケーション標準エディションをインストールする場合、このオプションを選択します。 *役割ベースプロビジョニング*: Roles Based Provisioning Module をインストールする場合、このオプションを選択します。
データマイグレーション	デフォルト値をそのまま使用します (［*はい*］が選択されていないことを確認してください)。 **警告 :** ［*はい*］を選択しないでください。［はい］を選択すると、ユーザアプリケーションの起動時に問題が発生します。 マイグレーションの詳細については、『*ユーザアプリケーション : マイグレーションガイド* (http://www.novell.com/documentation/idmrbpm361/index.html)』を参照してください。
WAR の場所	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。
インストールフォルダの選択	インストーラがファイルを配置する場所を指定します。
データベースプラットフォーム	データベースプラットフォームを選択します。データベースおよび JDBC ドライバはすでにインストールされている必要があります。含まれるオプション : ◆ MySQL ◆ Oracle (Oracle のバージョンの入力を促されます) ◆ MS SQL Server
データベースホストおよびポート	*ホスト*: データベースサーバのホスト名または IP アドレスを指定します。クラスタでは、クラスタの各メンバーには同じホスト名または IP アドレスを指定します。 *ポート*: データベースのリスナポート番号を指定します。クラスタの場合は、クラスタの各メンバーに同じポートを指定します。

インストール画面	説明
データベース名および権限付きユーザ	*データベース名* (または sid): MySQL または MMS SQL Server では、事前に設定したデータベース名を入力します。Oracle の場合は、前に作成した Oracle システム ID (SID) を指定します。クラスタでは、クラスタの各メンバーには同じデータベース名または SID を指定します。 *データベースユーザ*: 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。
Java のインストール	Java ルートのインストールフォルダを指定します。

JBoss アプリケーションサーバをインストールする場所の情報を入力するよう促されます。

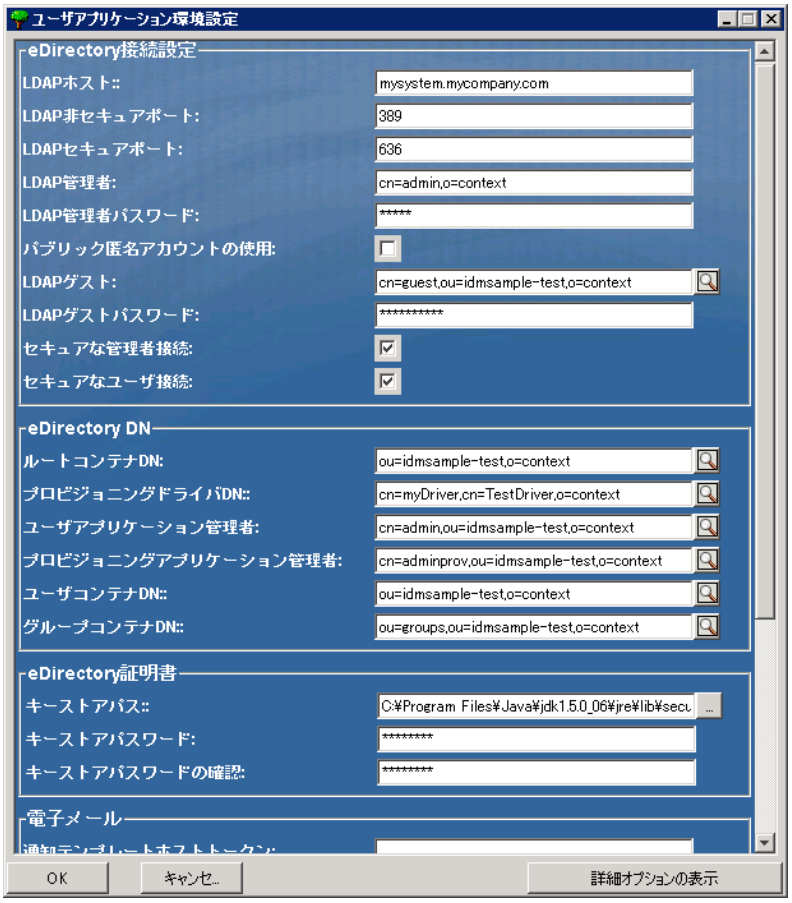


3 次の情報を使用して、このパネルを完了しインストールを続けます。

インストール画面	説明
JBoss 環境設定	JBoss アプリケーションサーバを見つける場所をユーザアプリケーションに伝えます。 このインストール手順では、JBoss アプリケーションサーバはインストールされません。JBoss アプリケーションサーバのインストール手順については、20 ページの 「JBoss アプリケーションサーバと MySQL データベースのインストール」を参照してください。 *ベースフォルダ*: アプリケーションサーバの場所を指定します。 *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リスナポート番号を指定します。JBoss デフォルトポートは 8080 です。
IDM 環境設定	アプリケーションサーバ設定のタイプを選択します。 ◆ このインストールがクラスタの一部の場合は、［*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。 ［*デフォルト*］を選択し、クラスタを後で必要とすると判断した場合は、ユーザアプリケーションを再インストールする必要があります。 *アプリケーション名*: アプリケーションサーバの環境設定の名前、アプリケーション WAR ファイルの名前、および URL コンテキストの名前です。インストールスクリプトによってサーバの環境設定が作成され、デフォルト名で*アプリケーション名*に基づく環境設定が作成されます。ユーザアプリケーションをブラウザから開始する場合は、アプリケーション名を書き留め、アプリケーション名を URL に含めてください。 *ワークフローエンジン ID*: クラスタ内の各サーバには、一意のワークフローエンジン ID を設定する必要があります。ワークフローエンジン ID については、『*ユーザアプリケーション: 管理ガイド*』の第 3.5.4 項「クラスタ化のワークフローの設定」で説明されています。
Audit のログ	ログを有効にするには、［*はい*］をクリックします。次のパネルでは、ログのタイプを指定するよう促されます。次のオプションから選択します。 ◆ *Novell Audit*: 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。 ◆ *OpenXDAS*: OpenXDAS ログサーバにイベントが記録されます。 Novell Audit のログ、または OpenXDAS のログ設定の詳細については、『*ユーザアプリケーション: 管理ガイド*』を参照してください。
Novell Audit	*サーバ*: Novell Audit のログを有効にする場合、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*: ログキャッシュのディレクトリを指定します。

インストール画面	説明
セキュリティ - マスタキー	*はい*: 既存のマスタキーをインポートできます。既存の暗号化マスタキーをインポートするよう選択した場合は、該当するキーを切り取ってインストール手順のウィンドウに貼り付けます。 *いいえ*: 新規のマスタキーを作成します。インストール終了後、67 ページのセクション 8.1「マスタキーの記録」で示すように、マスタキーを手動で記録します。 インストール手順で、インストールディレクトリにある master-key.txt ファイルに暗号化マスタキーが書き込まれます。 既存のマスタキーをインポートする理由には、次のようなものがあります。 ◆ インストールファイルをステージングシステムから運用システムに移動中で、ステージングシステムで使用したデータベースへのアクセスを保持する場合。 ◆ ユーザアプリケーションを最初の JBoss クラスタのメンバーにインストールしており、現在はクラスタの次のメンバーにインストールしている場合 (同じマスタキーが必要)。 ◆ ディスク故障のため、ユーザアプリケーションを復元する必要がある場合。ユーザアプリケーションを再インストールして、以前のインストールで使用したのと同じ暗号化マスタキーを指定する必要があります。これによって、前に保存した暗号化データにアクセスできます。

4 ユーザアプリケーション WAR ファイルを環境設定するために、インストールプログラムで使用される情報を入力するよう促されます。(この情報の入力を求められない場合、23 ページのセクション 2.5「Java Development Kit のインストール」で説明したステップを完了していない可能性があります。



5 次の情報を使用して、このパネルを完了しインストールを続けます。

インストール画面	説明
ユーザアプリケーション環境設定	ユーザアプリケーションをインストールすると、ユーザアプリケーション環境設定パラメータを設定できます。インストールすると、これらのパラメータの多くは configupdate.sh または configupdate.bat でも編集可能です。例外はパラメータ説明に記述されています。 クラスタの場合は、クラスタの各メンバーに同じユーザアプリケーション環境設定パラメータを指定します。 各オプションの詳細については、75 ページの付録 A「IDM ユーザアプリケーション環境設定の参照」を参照してください。

インストール画面	説明
インストール前の概要	［インストール前の概要］ページを読んで、インストールパラメータの選択を確認します。 必要に応じて、［*戻る*］を使用して前のインストールページに戻り、インストールパラメータを変更します。 ユーザアプリケーション環境設定ページでは値は保存されないため、インストールの前のページを再指定した後に、ユーザアプリケーション環境設定の値を再入力する必要があります。インストールおよび環境設定パラメータで納得いく設定ができたら、［インストール前の概要］ページに戻り、［*インストール*］をクリックします。
インストールの完了	インストールの終了が示されます。

4.1.1 インストールとログファイルの表示

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

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

4.2 インストールのテスト

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

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

start-jboss.sh(Linux および Solaris)

start-jboss.bat(Windows)

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

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

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

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

3a iManager にログインします。

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

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

3d ドライバで赤と白のアイコンをクリックします。

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

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

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

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

このアドレスでは、*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の環境設定情報を入力した場合、インストール中にアプリケーション名を指定しています。

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

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

このようなステップの完了後に、ブラウザに Identity Manager のユーザアプリケーションのページが表示されない場合は、エラーメッセージがないかどうか端末のコンソールを確認して、72 ページのセクション 8.7「トラブルシューティング」を参照します。

5 GUI インストーラを使用した WebSphere アプリケーションサーバのインストール

このセクションでは、グラフィカルユーザインタフェースバージョンのインストーラを使用して、WebSphere アプリケーションサーバに 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。

- 41 ページのセクション 5.1「ユーザアプリケーション WAR のインストールおよび環境設定」
- 45 ページのセクション 5.2「WebSphere 環境の環境設定」
- 47 ページのセクション 5.3「WAR ファイルの展開」
- 47 ページのセクション 5.4「ユーザアプリケーションの開始およびアクセス」

インストーラをルート以外のユーザとして実行します。

5.1 ユーザアプリケーション WAR のインストールおよび環境設定

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

1. 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

   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。

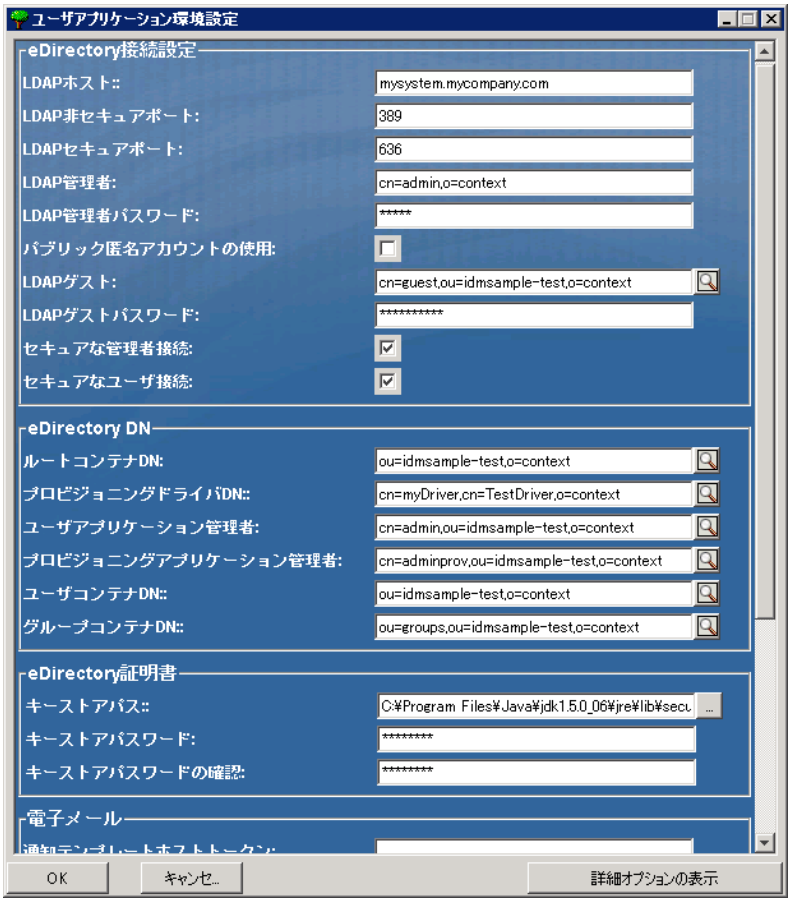
   インストールプログラムを開始すると、言語を入力するよう促されます。

3 インストールを完了するには、各インストールパネルの指示に沿って、次の情報を使用します。

インストール画面	説明
Novell Identity Manager	インストールプログラムの言語を選択します。デフォルトでは、［英語］が選択されています。
使用許諾契約	使用許諾契約を読み、［*使用許諾契約の条件に同意します*］を選択します。
アプリケーションサーバプラットフォーム	*WebSphere* を選択します。 ユーザアプリケーションの WAR ファイルがインストーラとは別のディレクトリにある場合は、インストーラによって WAR へのパスを入力するようメッセージが表示されます。 WAR がデフォルトの場所にある場合は、*［デフォルトのファイルに戻す］* をクリックできます。または、WAR ファイルの場所を指定する場合は、*［選択］* をクリックして場所を選択します。
標準またはプロビジョニング	*標準* : ユーザアプリケーション標準エディションをインストールする場合、このオプションを選択します。 *役割ベースプロビジョニング*: Roles Based Provisioning Module をインストールする場合、このオプションを選択します。
データマイグレーション	デフォルト値をそのまま使用します (［*はい*］が選択されていないことを確認してください)。 **警告 :** ［*はい*］を選択しないでください。［はい］を選択すると、ユーザアプリケーションの起動時に問題が発生します。 マイグレーションの詳細については、『*ユーザアプリケーション : マイグレーションガイド* (http://www.novell.com/documentation/idmrbpm361/index.html)』を参照してください。
WAR の場所	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。
インストールフォルダの選択	ファイルを配置するべきロケーションをインストーラに指定します。
データベースプラットフォーム	データベースプラットフォームを選択します。データベースおよび JDBC ドライバはすでにインストールされている必要があります。指定できる値は、次のとおりです。 ◆ Oracle (Oracle のバージョンの入力を促されます) ◆ MS SQL Server ◆ DB2
Java のインストール	Java ルートのインストールフォルダを指定します。 **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。

インストール画面	説明
IDM 環境設定	アプリケーションコンテキストの指定
Audit のログ	ログを有効にするには、[*はい*] をクリックします。次のパネルで、ログのタイプを指定するよう促されます。次のオプションから選択します。 ◆ *Novell Audit*: 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。* ◆ *OpenXDAS*: OpenXDAS ログサーバにイベントが記録されます。 Novell Audit のログ、または OpenXDAS のログ設定の詳細については、『*ユーザアプリケーション : 管理ガイド*』を参照してください。
Novell Audit	*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*: ログキャッシュのディレクトリを指定します。
セキュリティ - マスタキー	*はい*: 既存のマスタキーをインポートできます。既存の暗号化マスタキーをインポートするよう選択した場合は、該当するキーを切り取ってインストール手順のウィンドウに貼り付けます。 *いいえ*: 新規のマスタキーを作成します。インストール終了後、マスタキーを手動で記録します。 インストール手順で、インストールディレクトリにある master-key.txt ファイルに暗号化マスタキーが書き込まれます。 既存のマスタキーをインポートする理由には、次のようなものがあります。 ◆ インストールファイルをステージングシステムから運用システムに移動中で、ステージングシステムで使用したデータベースへのアクセスを保持する場合。 ◆ ユーザアプリケーションを最初のクラスタのメンバーにインストールしており、現在はクラスタの次のメンバーにインストールしている場合 (同じマスタキーが必要)。 ◆ ディスク故障のため、ユーザアプリケーションを復元する必要がある場合。ユーザアプリケーションを再インストールして、以前のインストールで使用したのと同じ暗号化マスタキーを指定する必要があります。これによって、前に保存した暗号化データにアクセスできます。

4 ユーザアプリケーション WAR ファイルを環境設定するために、インストールプログラムで使用される情報を入力するよう促されます。(この情報の入力を求められない場合、23 ページのセクション 2.5「Java Development Kit のインストール」で説明したステップを完了していない可能性があります。



5 次の情報を使用して、このパネルを完了しインストールを続けます。

インストール画面	説明
ユーザアプリケーション環境設定	ユーザアプリケーションをインストールすると、ユーザアプリケーション環境設定パラメータを設定できます。インストールすると、これらのパラメータの多くは configupdate.sh または configupdate.bat でも編集可能です。例外はパラメータ説明に記述されています。 詳細については、75 ページの付録 A「IDM ユーザアプリケーション環境設定の参照」を参照してください。
インストール前の概要	［インストール前の概要］ページを読んで、インストールパラメータの選択を確認します。 必要に応じて、［*戻る*］を使用して前のインストールページに戻り、インストールパラメータを変更します。 ユーザアプリケーション環境設定ページでは値は保存されないため、インストールの前のページを再指定した後に、ユーザアプリケーション環境設定の値を再入力する必要があります。インストールおよび環境設定パラメータで納得いく設定ができたら、［インストール前の概要］ページに戻り、［*インストール*］をクリックします。
インストールの完了	インストールが完了したことが示されます。

5.1.1 インストールログファイルの表示

エラーが発生せずにインストールが完了した場合は、45 ページのセクション 5.2.1「ユーザアプリケーション環境設定ファイルと JVM システムプロパティの追加」に進みます。

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

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

5.2 WebSphere 環境の環境設定

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

WebSphere を正常にインストールするには、次の手順が必要です。

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

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

インストーラはこのフォルダに sys-configuration-xmldata.xml ファイルを書き込みます。

9c *[説明]* には、プロパティの説明 (「sys-configuration-xmldata.xm へのパス」など) を指定します。

9d *[OK]* をクリックしてプロパティを保存します。

10 *[新規]* をクリックして、別の新しい JVM システムプロパティを追加します。

10a *[名前]* には、「idmuserapp.logging.config.dir」を指定します。

10b *[値]* には、インストール時に指定したインストールフォルダ (ディレクトリ) の名前を入力します。

10c *[説明]* には、プロパティの説明 (「idmuserapp_logging.xml へのパス」など) を指定します。

10d *[OK]* をクリックしてプロパティを保存します。

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

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

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

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

2 証明書を WebSphere のキーストアにインポートします。この作業は、WebSphere の管理者コンソール (46 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 (47 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、47 ページのセクション 5.3「WAR ファイルの展開」に進みます。

WebSphere 管理者コンソールを使用した証明書のインポート

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

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

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

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

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

6 [*追加*] をクリックします。

7 エイリアス名と証明書ファイルへのフルパスを入力します。

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

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

コマンドラインを使用した証明書のインポート

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

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

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

次に鍵ツールコマンドの例を示します。

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

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

5.3 WAR ファイルの展開

WebSphere 展開ツールを使用して、WAR ファイルを展開します。

5.4 ユーザアプリケーションの開始およびアクセス

ユーザアプリケーションを起動するには次の処理を行います。

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

   起動すると、［*アプリケーションステータス*］カラムに緑色の矢印が表示されます。

ユーザアプリケーションへのアクセス方法

1. 展開中に指定したコンテキストを使用してポータルにアクセスします。

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

GUI インストーラを使用した WebLogic アプリケーションサーバのインストール

6

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

ユーザグラフィカルインタフェース以外を使用したインストールの方法については、57 ページの第 7 章「コンソールまたは単一コマンドによるインストール」を参照してください。

ルート以外のユーザとしてインストーラを実行します。

6.1 WebLogic インストールチェックリスト

- ❑ WebLogic が有効な WAR を作成します。

  Identity Manager ユーザアプリケーションインストーラを使用してこのタスクを実行します。詳細については、50 ページのセクション 6.2「ユーザアプリケーション WAR のインストールおよび環境設定」を参照してください。

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

  詳細については、54 ページのセクション 6.3「WebLogic 環境の準備」を参照してください。

- ❑ WAR を展開します。

  詳細については、56 ページのセクション 6.4「ユーザアプリケーション WAR の展開」を参照してください。

6.2 ユーザアプリケーション WAR のインストールおよび環境設定

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

1. 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. 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.
   ```

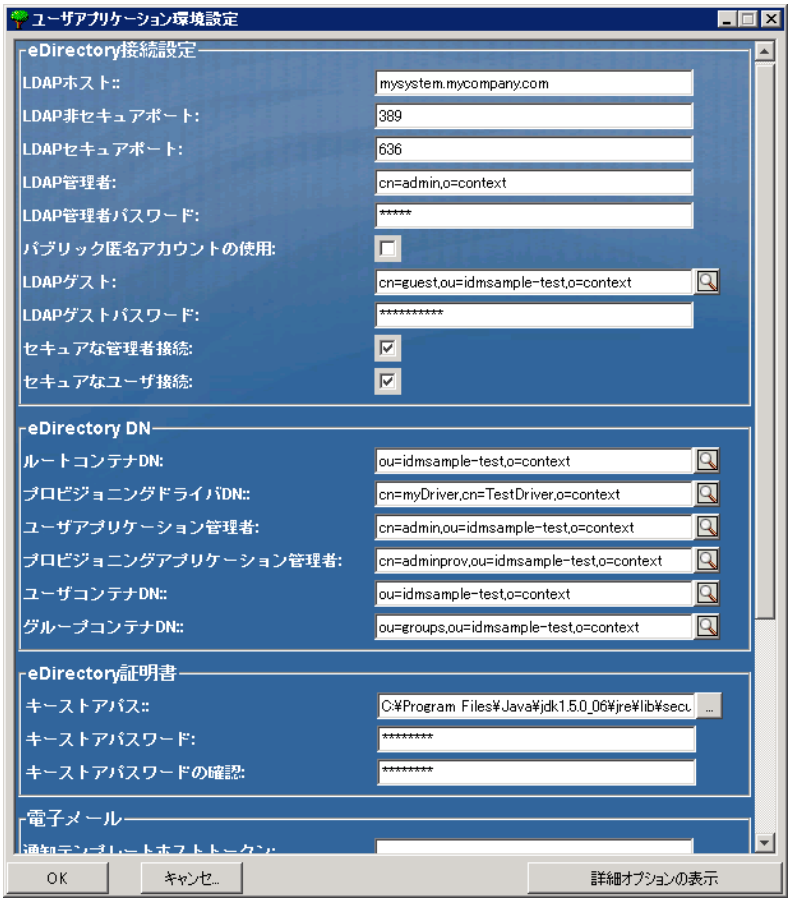
   インストールプログラムを開始すると、言語を入力するよう促されます。

3. インストールを完了するには、各インストールパネルの指示に沿って、次の情報を使用します。

インストール画面	説明
Novell Identity Manager	インストールプログラムの言語を選択します。デフォルトでは、［英語］が選択されています。
使用許諾契約	使用許諾契約を読み、［*使用許諾契約の条件に同意します*］を選択します。
アプリケーションサーバプラットフォーム	アプリケーションサーバでは、*WebLogic* を選択します。
標準またはプロビジョニング	*標準*: ユーザアプリケーション標準エディションをインストールする場合、このオプションを選択します。 *役割ベースプロビジョニング*: Roles Based Provisioning Module をインストールする場合、このオプションを選択します。
データマイグレーション	デフォルト値をそのまま使用します (［*はい*］が選択されていないことを確認してください)。 **警告 :** ［*はい*］を選択しないでください。［はい］を選択すると、ユーザアプリケーションの起動時に問題が発生します。 マイグレーションの詳細については、『*ユーザアプリケーション : マイグレーションガイド* (http://www.novell.com/documentation/idmrbpm361/index.html)』を参照してください。
WAR の場所	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。
インストールフォルダの選択	インストーラがファイルを配置する場所を指定します。
データベースプラットフォーム	データベースプラットフォームを選択します。データベースおよび JDBC ドライバはすでにインストールされている必要があります。指定できる値は、次のとおりです。 ◆ Oracle(バージョンの入力を促されます) ◆ MS SQL Server
Java のインストール	Java ルートのインストールフォルダを指定します。
IDM 環境設定	アプリケーションコンテキストを指定します。ブラウザからユーザアプリケーションを開始する場合、これは URL の一部となります。
Audit のログ	ログを有効にするには、［*はい*］をクリックします。次のパネルでは、ログのタイプを指定するよう促されます。次のオプションから選択します。 ◆ *Novell Audit*: 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。 ◆ *OpenXDAS*: OpenXDAS ログサーバにイベントが記録されます。 Novell Audit のログ、または OpenXDAS のログ設定の詳細については、『*ユーザアプリケーション : 管理ガイド*』を参照してください。

インストール画面	説明
Novell Audit	*サーバ*: Novell Audit のログを有効にする場合、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*: ログキャッシュのディレクトリを指定します。
セキュリティ - マスタキー	*はい*: 既存のマスタキーをインポートできます。既存の暗号化マスタキーをインポートするよう選択した場合は、該当するキーを切り取ってインストール手順のウィンドウに貼り付けます。 *いいえ*: 新規のマスタキーを作成します。インストール終了後、67 ページのセクション 8.1「マスタキーの記録」で示すように、マスタキーを手動で記録します。 インストール手順で、インストールディレクトリにある master-key.txt ファイルに暗号化マスタキーが書き込まれます。 既存のマスタキーをインポートする理由には、次のようなものがあります。 ◆ インストールファイルをステージングシステムから運用システムに移動中で、ステージングシステムで使用したデータベースへのアクセスを保持する場合。 ◆ ユーザアプリケーションを最初の JBoss クラスタのメンバーにインストールしており、現在はクラスタの次のメンバーにインストールしている場合 (同じマスタキーが必要)。 ◆ ディスク故障のため、ユーザアプリケーションを復元する必要がある場合。ユーザアプリケーションを再インストールして、以前のインストールで使用したのと同じ暗号化マスタキーを指定する必要があります。これによって、前に保存した暗号化データにアクセスできます。

4 ユーザアプリケーション WAR ファイルを環境設定するために、インストールプログラムで使用される情報を入力するよう促されます。(この情報の入力を求められない場合、23 ページのセクション 2.5「Java Development Kit のインストール」で説明したステップを完了していない可能性があります。



インストール画面	説明
ユーザアプリケーション環境設定	ユーザアプリケーションをインストールすると、ユーザアプリケーション環境設定パラメータを設定できます。インストールすると、これらのパラメータの多くは configupdate.sh または configupdate.bat でも編集可能です。例外はパラメータ説明に記述されています。 詳細については、75 ページの付録 A「IDM ユーザアプリケーション環境設定の参照」を参照してください。
インストール前の概要	［インストール前の概要］ページを読んで、インストールパラメータの選択を確認します。 必要に応じて、［*戻る*］を使用して前のインストールページに戻り、インストールパラメータを変更します。 ユーザアプリケーション環境設定ページでは値は保存されないため、インストールの前のページを再指定した後に、ユーザアプリケーション環境設定の値を再入力する必要があります。インストールおよび環境設定パラメータで納得いく設定ができたら、［インストール前の概要］ページに戻り、［*インストール*］をクリックします。
インストールの完了	インストールが完了したことが示されます。

6.2.1 インストールとログファイルの表示

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

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

6.3 WebLogic 環境の準備

- 54 ページのセクション 6.3.1「接続プールの環境設定」
- 54 ページのセクション 6.3.2「ユーザアプリケーション環境設定ファイルのロケーションの指定」
- 56 ページのセクション 6.3.3「ワークフロープラグインと WebLogic セットアップ」

6.3.1 接続プールの環境設定

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

  WebLogic 文書のデータソース作成の指示に従います。

  データソースの JNDI 名は、たとえば jdbc/IDMUADataSource のように、ユーザアプリケーション WAR を作成したときに指定したデータベースと同じ名前である必要があります。
- ❑ ユーザアプリケーションのインストールディレクトリから antlr-2.7.6.jar をドメインの lib フォルダにコピーします。

6.3.2 ユーザアプリケーション環境設定ファイルのロケーションの指定

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

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

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

```
set JAVA_PROPERTIES

export JAVA_PROPERTIES
```

3 JAVA_PROPERTIES のエントリの下に、次に対してエントリを追加します。

- -Dextend.local.config.dir: sys-configuration.xml ファイルを含むフォルダ (ファイル自体ではない) を指定します。
- -Didmuserapp.logging.config.dir: idmuserapp_logging.xml ファイルを含むフォルダ (ファイル自体ではない) を指定します。

Windows の場合の例 :

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

4 環境変数 EXT_PRE_CLASSPATH を設定し、antlr.jar を示します。

4a この行を見つけます。

```
ADD EXTENSIONS TO CLASSPATH
```

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

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

Linux の場合の例 :

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

5 ファイルを保存して終了します。

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

1 configupdate.bat または configupdate.sh を開きます。

2 次の行をファイル内で探します。

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

3 この下に次のエントリを追加します。

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

4 ファイルを保存して閉じます。

5 configupdate ユーティリティを実行し、証明書を BEA_HOME 下にある JDK のキーストアにインストールします。

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

6.3.3 ワークフロープラグインと WebLogic セットアップ

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

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

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

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

3. ファイルを保存して、サーバを再起動します。

この変更を行った後で、ワークフロー管理プラグインにログインできるはずです。

6.4 ユーザアプリケーション WAR の展開

- jsf-ri-1.1.1.war をライブラリとして展開します。
- インストールディレクトリ (一般に Novell\IDM) から、更新されているユーザアプリケーション WAR ファイルをアプリケーションドメインにコピーします。例を次に示します。

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

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

6.5 ユーザアプリケーションへのアクセス

- ユーザアプリケーション URL への移動 :

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

  例を次に示します。

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

コンソールまたは単一コマンドによるインストール

7

このセクションでは、33 ページの第 4 章「GUI インストーラを使用した 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。

- 57 ページのセクション 7.1「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」
- 58 ページのセクション 7.2「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」

7.1 コンソールからのユーザアプリケーションのインストール

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

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

---

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

   java -jar IdmUserApp.jar -i console
3. 33 ページの第 4 章「GUI インストーラを使用した 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。
4. ユーザアプリケーション環境設定パラメータを設定するには、手動で configupdate ユーティリティを起動します。コマンドラインで、configupdate.sh (Linux または Solaris) あるいは configupdate.bat (Windows) と入力して、75 ページのセクション A.1「ユーザアプリケーション環境設定 : 基本パラメータ」で説明されている値を入力します。
5. 外部パスワード管理 WAR を使用している場合、これをインストールディレクトリおよび、外部パスワード WAR 機能を実行するリモート JBoss サーバ展開ディレクトリに手動でコピーします。
6. 67 ページの第 8 章「インストール後のタスク」に進みます。

7.2 単一コマンドによるユーザアプリケーションのインストール

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

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

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

   ユーザアプリケーション環境設定パラメータの説明については、表 7-1 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 7-1 *サイレントインストール用のユーザアプリケーション環境設定パラメータ*

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

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory DN: ルートコンテナ DN。 ルートコンテナの LDAP 識別名を指定します。これは、ディレクトリ抽象化層で検索ルートが指定されない場合に、デフォルトのエントリティ定義検索ルートとして使用されます。
NOVL_CONFIG_PROVISIONROOT=	eDirectory DN: プロビジョニングドライバ DN。 前述の 27 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。 指定されたユーザアプリケーションのユーザコンテナについての管理タスクを実行する権限のある、識別ボールト内の既存のユーザ。このユーザは、ユーザアプリケーションの［*管理者*］タブを使用してポータルを管理できます。 ユーザアプリケーション管理者が、iManager、Novell Designer for identity Manager、またはユーザアプリケーション (*［要求と承認］*タブ) に公開されているワークフロー管理タスクに参加する場合は、この管理者に、ユーザアプリケーションドライバに含まれるオブジェクトインスタンスに対する適切なトラスティ権限を与える必要があります。詳細は、『*ユーザアプリケーション : 管理ガイド*』を参照してください。 ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［セキュリティ］* ページを使用する必要があります。

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

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

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

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_NOTFSMTPEMAILHOST=	電子メール : 通知 SMTP 電子メールホスト。 必須。プロビジョニング電子メールを使用している SMTP 電子メールホストを指定します。これは、IP アドレスまたは DNS 名が可能です。
NOVL_CONFIG_USEEXTPWDWAR=	パスワード管理 : 外部パスワード WAR の使用。 外部パスワード管理 WAR を使用している場合は、［*True*］を指定します。［*True*］を指定する場合は、*NOVL_CONFIG_EXTPWDWARPTH* および *NOVL_CONFIG_EXTPWDWARRTNPATH* の値も指定する必要があります。 デフォルトの内部パスワード管理機能を使用するには、［*False*］を指定します。/jsps/pwdmgt/ForgotPassword.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、70 ページの「外部パスワード管理の環境設定」を参照してください。
NOVL_CONFIG_EXTPWDWARRTNPATH=	パスワード管理 : パスワードを忘れた場合の返信リンク。 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。 必須。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。 必須。ユーザのログイン名を表す LDAP 属性 (たとえば CN)。
NOVL_CONFIG_NAMINGATTRIBUTE=	メタディレクトリユーザ ID : 名前付け属性。 必須。ユーザまたはグループをルックアップする際に ID として使用する LDAP 属性これはログイン属性と同じではありません。ログイン属性はログイン中にのみ使用し、ユーザおよびグループの検索中には使用しません。

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_USERMEMBERSHIPATTRIBUTE=	メタディレクトリユーザ ID: ユーザメンバーシップ属性。オプション。 必須。ユーザのグループメンバーシップを表す LDAP 属性です。この名前にはスペースを使用しないでください。
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	メタディレクトリユーザグループ : グループオブジェクトクラス。 必須。LDAP オブジェクトクラス (通常は groupofNames)。
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	メタディレクトリユーザグループ : グループメンバーシップ属性。 必須。ユーザのグループメンバーシップを表す属性を指定します。この名前にはスペースを使用しないでください。
NOVL_CONFIG_USEDYNAMICGROUPS=	メタディレクトリユーザグループ : ダイナミックグループ。 必須。ダイナミックグループを使用するには、［*True*］を指定します。使用しない場合は、［*False*］を指定します。
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	メタディレクトリユーザグループ : ダイナミックグループオブジェクトクラス。 必須。LDAP ダイナミックグループオブジェクトクラスを指定します (通常は dynamicGroup)。
NOVL_CONFIG_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。

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_TRUSTEDSTOREPATH=	トラステッドキーストア : トラステッドストアパス。 トラステッドキーストアには、有効なデジタル署名に使用するすべてのトラステッド署名者の証明書が含まれます。入力しない場合は、ユーザアプリケーションはシステムプロパティ javax.net.ssl.trustStore からパスを取得します。パスがそこではない場合は、jre/lib/security/cacerts と推測されます。
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	トラステッドキーストア : トラステッドストアパスワード。
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。

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_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。
NOVL_CONFIG_CREATEDIRECTORYINDEX	その他 : eDirectory インデックスの作成 サイレントインストーラで、NOVL_CONFIG_SERVERDN で指定した eDirectory サーバ上で manager、ismanager、および srvprvUUID の属性のインデックスが作成されるようにする場合、［true］を指定します。このパラメータが［true］に設定されている場合、NOVL_CONFIG_REMOVEEDIRECTORYINDEX は ［true］に設定できません。 最良のパフォーマンス結果を得るには、インデックス作成が完了している必要があります。ユーザアプリケーションを利用可能な状態にする前にインデックスをオンラインモードにする必要があります。
NOVL_CONFIG_REMOVEDIRECTORYINDEX	その他 : eDirectory インデックスの削除 サイレントインストーラで、NOVL_CONFIG_SERVERDN で指定したサーバのインデックスが削除されるようにする場合、［true］を指定します。このパラメータが ［true］に設定されている場合、NOVL_CONFIG_CREATEEDIRECTORYINDEX は［true］に設定できません。
NOVL_CONFIG_SERVERDN	その他 : サーバ DN インデックスを作成または削除する必要のある eDirectory サーバを指定します。

インストール後のタスク

8

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。

8.1 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。

8.2 ユーザアプリケーションの環境設定

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

- 『*Novell IDM Roles Based Provisioning Module 3.6.1 管理ガイド*』の「ユーザアプリケーション環境の設定」
- 『*Novell IDM Roles Based Provisioning Module 3.6.1 設計ガイド*』

8.2.1 Novell Audit の設定

『ユーザアプリケーション : 管理ガイド (http://www.novell.com/documentation/idmrbpm361/index.html)』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 (prerequisites.zip 内) を Audit サーバにコピーします。

8.3 eDirectory の設定

8.3.1 eDirectory でのインデックスの作成

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

これらのインデックスは、［*ユーザアプリケーション環境設定*］パネルの［*詳細*］タブの［eDirectory インデックスの作成］が選択されている場合、インストール中に自動的に作成できます (81 ページの 図 表 A-2 で説明されています)。インデックスを作成するためにインデックスマネージャを使用する手順については、『*Novell eDirectory 管理ガイド* (http://www.novell.com/documentation)』を参照してください。

8.3.2 SAML 認証メソッドのインストールおよび環境設定

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

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

eDirectory ツリーにおける SAML メソッドのインストール

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

     次の例で、Linux 上でこれを実行する方法を説明します。

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

     次の例で、Linux 上でこれを実行する方法を説明します。

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

eDirectory の属性の編集

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

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

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

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

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

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

6d［*OK*］をクリックします。

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

6f［*OK*］をクリックします。

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

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

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

8b［*すべてのオブジェクトクラスの表示*］を再び選択します。

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

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

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

9 オブジェクトビューアに戻ります。

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

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

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

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

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

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

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

   ConfigUpdate ユーティリティのパラメータの詳細については 75 ページのセクション A.1「ユーザアプリケーション環境設定 : 基本パラメータ」、58 ページの 図 表 7-1 を参照してください。

2. 新しい WAR ファイルをアプリケーションサーバに展開します。

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

8.5 外部パスワード管理の環境設定

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

- 70 ページのセクション 8.5.1「外部パスワード管理 WAR の指定」
- 71 ページのセクション 8.5.2「内部パスワード WAR の指定」
- 71 ページのセクション 8.5.3「外部パスワードの WAR 環境設定のテスト」
- 71 ページのセクション 8.5.4「JBoss サーバ間の SSL 通信の設定」

8.5.1 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。71 ページのセクション 8.5.4「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、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、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。

8.5.2 内部パスワード WAR の指定

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

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

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

8.5.3 外部パスワードの WAR 環境設定のテスト

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

- ブラウザ内で直接アクセスします。外部パスワード WAR で［パスワードを忘れた場合］ページに移動します。たとえば、http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.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。

8.5.4 JBoss サーバ間の SSL 通信の設定

インストール中にユーザアプリケーション環境設定ファイルで *［外部パスワード WAR の使用］*をオンにした場合は、ユーザアプリケーション WAR および 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。

8.6 ［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)

8.7 トラブルシューティング

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

項目	推奨されるアクション

インストール中に作成したユーザアプリケーションの環境設定を変更するとします。たとえば、次のような環境設定と仮定します。
◆ 識別ボールトの接続および証明書
◆ 電子メール設定
◆ メタディレクトリのユーザ識別情報、ユーザグループ
◆ Access Manager または iChain® の設定
	インストーラとは別に、環境設定ユーティリティを実行します。
	Linux および Solaris では、インストールディレクトリ (デフォルトでは、/opt/novell/idm) から次のコマンドを実行します。
	`configupdate.sh`
	Windows では、インストールディレクトリ (デフォルトでは、c:\opt\novell\idm) から次のコマンドを実行します。
	`configupdate.bat`

アプリケーションサーバのスタートアップ時に、ログメッセージ「ポート 8080 使用中、使用されている」とともに例外がスローされる。	すでに実行されている Tomcat (または他のサーバソフトウェア) のすべてのインスタンスをシャットダウンします。アプリケーションサーバを再設定して 8080 以外のポートを使用する場合は、必ず iManager のユーザアプリケーションドライバの config 環境設定を編集してください。
アプリケーションサーバの起動時に、トラステッド証明書が見つからないというメッセージが表示される。	ユーザアプリケーションのインストールで指定した JDK を使用して、アプリケーションサーバを起動するようにします。
ポータル管理ページにログインできない。	ユーザアプリケーションの管理者アカウントが存在することを確認します。これを、iManager の管理者アカウントと混同しないでください。2 つの別の管理者オブジェクトがあります (またはある必要があります)。

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

項目	推奨されるアクション

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

IDM ユーザアプリケーション環境設定の参照

A

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

A.1 ユーザアプリケーション環境設定 : 基本パラメータ

図 A-1 ユーザアプリケーション環境設定の基本オプション

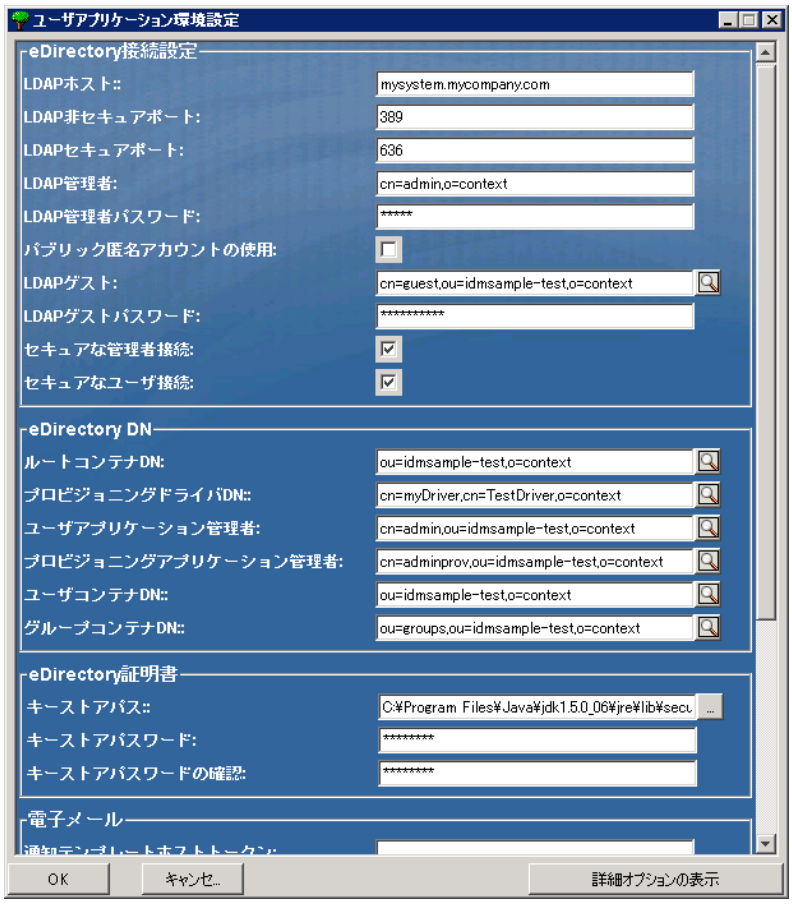


表 A-1 ユーザアプリケーション環境設定 : 基本オプション

設定のタイプ	オプション	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。 ユーザアプリケーションの［管理］タブを使用してこの設定を修正しない限り、configupdate ユーティリティを使用してこの設定を修正できます。
	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。 ユーザアプリケーションの［管理］タブを使用してこの設定を修正しない限り、configupdate ユーティリティを使用してこの設定を修正できます。
	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	オプション	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 (27 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」で説明)。たとえば、ドライバが UserApplicationDriver でドライバセットの名前が myDriverSet であり、ドライバセットが o=myCompany のコンテキストにある場合は、次の値を入力します。 `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	ユーザアプリケーション管理者	必須。指定されたユーザアプリケーションのユーザコンテナについての管理タスクを実行する権限のある、識別ボールト内の既存のユーザ。このユーザは、ユーザアプリケーションの［*管理者*］タブを使用してポータルを管理できます。 ユーザアプリケーション管理者が、iManager、Novell Designer for identity Manager、またはユーザアプリケーション (*［要求と承認］* タブ) に公開されているワークフロー管理タスクに参加する場合は、この管理者に、ユーザアプリケーションドライバに含まれるオブジェクトインスタンスに対する適切なトラスティ権限を与える必要があります。詳細は、『*ユーザアプリケーション : 管理ガイド*』を参照してください。 ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの *［管理］* > *［セキュリティ］* ページを使用する必要があります。 ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。
	プロビジョニング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	オプション	説明
	コンプライアンス管理者	コンプライアンスモジュール管理者はシステムの役割であり、メンバーはこの［*コンプライアンス*］タブのすべての機能が実行可能です。このユーザは、コンプライアンスモジュール管理者として指定される前に、識別ボールトに存在している必要があります。 configupdate の間、この値への変更は、有効なコンプライアンスモジュール管理者が割り当てられていない場合のみ反映されます。有効なコンプライアンスモジュール管理者が存在する場合は、変更は保存されません。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの *［役割］* > *［役割の割り当て］* ページを使用します。
eDirectory DN(続き)	*役割管理者*	この役割は、Novell Identity Manager Roles Based Provisioning Module で利用可能です。この役割を使用すると、そのメンバーはすべての役割の作成、削除、変更、およびユーザ、グループ、またはコンテナへの役割の付与または取り消しを行うことができます。さらに役割のメンバーは、任意のユーザに対してレポートを実行できます。デフォルトでは、この役割にはユーザアプリケーション管理者が割り当てられています。 ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの *［役割］* > *［役割の割り当て］* ページを使用します。 configupdate の間、この値への変更は、有効な役割管理者が割り当てられていない場合のみ反映されます。有効な役割管理者が存在する場合は、変更は保存されません。
	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 :** ユーザによるワークフローの実行を可能とさせる場合は、ユーザアプリケーションドライバの設定中に指定したユーザアプリケーション管理者が、確実にこのコンテナに存在するようにしてください。 ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。
	グループコンテナDN	必須。グループコンテナの LDAP 識別名 (DN) または完全修飾 LDAP 名を指定します。 ディレクトリ抽象化レイヤ内のエンティティ定義で使用します。 ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。

設定のタイプ	オプション	説明
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。
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、70 ページの 「外部パスワード管理の環境設定」を参照してください。

設定のタイプ	オプション	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*:*ssl*/*port*/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。

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

A.2 ユーザアプリケーション環境設定 : すべてのパラメータ

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

表 A-2 *ユーザアプリケーション環境設定：すべてのオプション*

設定のタイプ	オプション	説明
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	オプション	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 (27 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」で説明)。たとえば、ドライバが UserApplicationDriver でドライバセットの名前が myDriverSet であり、ドライバセットが o=myCompany のコンテキストにある場合は、次の値を入力します。 `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	ユーザアプリケーション管理者	必須。指定されたユーザアプリケーションのユーザコンテナについての管理タスクを実行する権限のある、識別ボールト内の既存のユーザ。このユーザは、ユーザアプリケーションの [*管理者*] タブを使用してポータルを管理できます。 ユーザアプリケーション管理者が、iManager、Novell Designer for identity Manager、またはユーザアプリケーション (*[要求と承認]* タブ) に公開されているワークフロー管理タスクに参加する場合は、この管理者に、ユーザアプリケーションドライバに含まれるオブジェクトインスタンスに対する適切なトラスティ権限を与える必要があります。詳細については、『*ユーザアプリケーション : 管理ガイド*』を参照してください。 ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの *[管理]* > *[セキュリティ]* ページを使用する必要があります。 ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。
	プロビジョニング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	オプション	説明
	コンプライアンス管理者	コンプライアンスモジュール管理者はシステムの役割であり、メンバーはこの［*コンプライアンス*］タブのすべての機能が実行可能です。このユーザは、コンプライアンスモジュール管理者として指定される前に、識別ボールトに存在している必要があります。 configupdate の間、この値への変更は、有効なコンプライアンスモジュール管理者が割り当てられていない場合のみ反映されます。有効なコンプライアンスモジュール管理者が存在する場合は、変更は保存されません。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの［*役割*］>［*役割の割り当て*］ページを使用します。
	役割管理者	この役割は、Novell Identity Manager Roles Based Provisioning Module で利用可能です。この役割を使用すると、そのメンバーはすべての役割の作成、削除、変更、およびユーザ、グループ、またはコンテナへの役割の付与または取り消しを行うことができます。さらに役割のメンバーは、任意のユーザに対してレポートを実行できます。デフォルトでは、この役割にはユーザアプリケーション管理者が割り当てられています。 ユーザアプリケーションの展開後にこの割り当てを変更するには、ユーザアプリケーションの［*役割*］>［*役割の割り当て*］ページを使用します。 configupdate の間、この値への変更は、有効な役割管理者が割り当てられていない場合のみ反映されます。有効な役割管理者が存在する場合は、変更は保存されません。

設定のタイプ	オプション	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。 このコンテナ内 (およびその下) のユーザが、ユーザアプリケーションにログインできます。 ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。 **重要 :** ユーザによるワークフローの実行を可能とさせる場合は、ユーザアプリケーションドライバの設定中に指定したユーザアプリケーション管理者が、確実にこのコンテナに存在するようにしてください。
	ユーザコンテナのスコープ	これにより、ユーザの検索スコープが定義されます。
	ユーザオブジェクトクラス	LDAP ユーザオブジェクトクラス (通常は inetOrgPerson)。
	ログイン属性	ユーザのログイン名を表す LDAP 属性 (たとえば CN)。
	名前付け属性	ユーザまたはグループをルックアップする際に ID として使用する LDAP 属性これはログイン属性と同じではありません。ログイン属性はログイン中にのみ使用し、ユーザおよびグループの検索中には使用しません。
	ユーザメンバーシップ属性	オプション。ユーザのグループメンバーシップを表す LDAP 属性です。この名前にはスペースを使用しないでください。
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。 ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。
	グループコンテナのスコープ	これにより、グループの検索スコープが定義されます。
	グループオブジェクトクラス	LDAP オブジェクトクラス (通常は groupofNames)。
	グループメンバーシップ属性	ユーザのグループメンバーシップを表す属性です。この名前にはスペースを使用しないでください。
	ダイナミックグループの使用	ダイナミックグループを使用する場合は、このオプションを選択します。
	ダイナミックグループオブジェクトクラス	LDAP ダイナミックグループオブジェクトクラス (通常は dynamicGroup)。

設定のタイプ	オプション	説明
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	必須。cacerts のパスワードを指定します。デフォルトは、「changeit」です。
	キーストアパスワードの確認	
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。
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。

設定のタイプ	オプション	説明
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。
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	オプション	説明
パスワード管理		
	外部パスワード WAR の使用	この機能によって、外部の［パスワードを忘れた場合］の War にある［パスワードを忘れた場合］ページと、外部の［パスワードを忘れた場合］の WAR が Web サービスを経由してユーザアプリケーションを呼び戻すのに使用する URL を指定できます。 *［外部パスワード WAR の使用］*を選択する場合は、*［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	インストールユーティリティでマネージャ、ismanager、および srvprvUUID の属性のインデックスを作成する場合、このチェックボックスを選択します。これらの属性にインデックスがない場合、ユーザアプリケーションのユーザは、特にクラスタ化された環境ではユーザアプリケーションが低いパフォーマンスの状態にあります。ユーザアプリケーションをインストール後、iManager を使用して、手動でこれらのインデックスを作成できます。詳細については、68 ページのセクション 8.3.1「eDirectory でのインデックスの作成」を参照してください。 最良のパフォーマンスを得るには、インデックス作成が完了している必要があります。ユーザアプリケーションを利用可能な状態にする前にインデックスをオンラインモードにする必要があります。
	eDirectory インデックスの削除	マネージャ、ismanager、および srvprvUUID の属性のインデックスを削除します。

設定のタイプ	オプション	説明
	サーバDN	インデックスを作成または削除する必要のある eDirectory サーバを選択します。 **注 :** 複数の eDirectory サーバでインデックスの環境設定を行うには、configupdate ユーティリティを複数回実行する必要があります。一度に指定できるのは 1 つのサーバのみです。
コンテナオブジェクト	*選択済み*	使用する各コンテナオブジェクトタイプを選択します。
	コンテナオブジェクトタイプ	地域、国、部門、組織、およびドメインの規格コンテナから選択します。iManager 内で自分のコンテナを定義でき、これを［*新規コンテナオブジェクトの追加*］の下に追加できます。
	コンテナ属性名	コンテナオブジェクトタイプに関連する属性タイプ名をリストします。
	新規コンテナオブジェクトの追加 : コンテナオブジェクトタイプ	コンテナとして使用できる識別ボールトからオブジェクトクラス名、LDAP を指定します。 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。