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

4.0.1

2011 年 04 月 15 日

www.novell.com

保証と著作権

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

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

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

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

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

Novell の商標

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

サードパーティ資料

サードパーティの商標は、それぞれの所有者に帰属します。

目次

このガイドについて

このガイドでは、Novell Identity Manager 役割ベースプロビジョニングモジュール 4.0.1 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。オンラインマニュアルの各ページの下部にあるユーザコメント機能を使用するか www.novell.com/documentation/feedback.html にアクセスしてコメントを記入してください。

追加のマニュアル

Identity Manager 4.0.1 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/idm401/index.html) を参照してください。

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。主なトピックは次のとおりです。

ユーザアプリケーションまたは Roles Based Provisioning Module の以前のバージョンから移行する場合、『*ユーザアプリケーション: マイグレーションガイド* (http://www.novell.com/documentation/idm40/index.html)』を参照してください。

1.1 インストールのチェックリスト

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

- ❑ ソフトウェアがシステム要件を満たしているかどうかを確認します。詳細については、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。
- ❑ Identity Manager Roles Based Provisioning Module をダウンロードします。詳細については、15 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、15 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、16 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、24 ページのセクション 2.4「データベースのインストール」を参照してください。
- ❑ Roles Based Provisioning Module Metadirectory コンポーネントをインストールします。詳細については、31 ページの第 3 章「役割ベースのプロビジョニングモジュールのインストール」を参照してください。
- ❑ Designer 4.0.1 for Identity Manager でユーザアプリケーションドライバを作成します。
  - 47 ページのセクション 4.1「Designer でのドライバの作成」を参照してください。
- ❑ Designer 4.0.1 for Identity Manager で役割とリソースサービスドライバを作成します。
  - 詳細については、47 ページのセクション 4.1「Designer でのドライバの作成」を参照してください。

- ❑ Novell Identity Manager ユーザアプリケーションをインストールし設定します。(インストールプログラムを開始する前に、正しい JDK がインストールされている必要があります。詳細については、30 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。
    - 57 ページの第 5 章「JBoss でのユーザアプリケーションのインストール」
    - 81 ページの第 6 章「WebSphere でのユーザアプリケーションのインストール」
    - 111 ページの第 7 章「WebLogic でのユーザアプリケーションのインストール」
  - コンソール (コマンドライン) インタフェース詳細については、131 ページのセクション 8.1「コンソールからのユーザアプリケーションのインストール」を参照してください。
  - サイレントインストール。詳細については、132 ページのセクション 8.2「単一コマンドによるユーザアプリケーションのインストール」を参照してください。
- ❑ 147 ページの第 9 章「インストール後のタスク」で説明されているインストール後のタスクを実行します。

重要 : 本書では、セキュリティ環境の設定手順は説明していません。セキュリティの詳細については、『ユーザアプリケーション : 管理ガイド (http://www.novell.com/documentation/idm40/index.html)』を参照してください。

1.2 インストーラプログラムの概要

ユーザアプリケーションのインストールプログラムは次の処理を実行します。

- ライセンスが Identity Manager 4.0.1 Advanced Edition 用か Standard Edition 用かを決定します。次に、ライセンスされたエディションの適切な画面が表示されます。
- 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 (PostgreSQL、Oracle, DB2、Microsoft SQL Server、または MySQL など)。データベースには、ユーザアプリケーションのデータとユーザアプリケーションの設定情報が保存されます。
- ユーザアプリケーション(アプリケーションサーバ上で実行されている)が識別ボールトおよびユーザアプリケーションドライバと安全に通信できるように、JDK の証明書ファイルを設定する。
- Novell Identity Managerユーザアプリケーション用の Java Web アプリケーションアーカイブ (WAR) ファイルを設定し、アプリケーションサーバに展開する。WebSphere および WebLogic では、WAR を手動で展開する必要があります。
- 必要な場合、Novell または OpenXDAS の監査クライアントを使用してログを有効にします。
- 既存のマスタキーをインポートして、特定の Roles Based Provisioning Module のインストールを復元し、クラスタをサポートできるようにします。

1.3 システム要件

Novell Identity Manager Roles Based Provisioning Module 4.0.1 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
メタディレクトリ	eDirectory 8.8.6 with Identity Manager 4.0.1 サポートされているオペレーティングシステムのリストは、Identity Manager および eDirectory のマニュアルを参照してください。
アプリケーションサーバ	ユーザアプリケーションは、以下で説明するように JBoss、WebSphere、および WebLogic 上で動作します。 JBoss 5.1 を持つユーザアプリケーションは Sun から提供されている JRE 1.6.0_20 を必要とし、次でサポートされます。 ◆ Windows Server 2003 SP2 (32 ビットのみ) ◆ Windows Server 2008 R2 (64 ビットのみ) ◆ Windows Server 2008 SP1 (32 ビットおよび 64 ビット) ◆ Open Enterprise Server 2 SP3 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 10 SP3 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 11 SP1 (32 ビットおよび 64 ビット) ◆ Red Hat Enterprise Linux 5.4 (32 ビットおよび 64 ビット) WebSphere 7.0 のユーザアプリケーションは、IBM J9 VM (build 2.4、J2RE 1.6.0) および Fix Pack 7 を必要とします。これらのプラットフォームでサポートされています。 ◆ Windows Server 2003 SP2 (32 ビットのみ) ◆ Windows Server 2008 R2 (64 ビットのみ) ◆ 最新のサポートパックを使用した Windows Server 2008 SP1 (32 ビットおよび 64 ビット) ◆ Open Enterprise Server 2 SP3 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 10 SP3 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 11 SP1 (32 ビットおよび 64 ビット) ◆ Red Hat Enterprise Linux 5.4 (32 ビットおよび 64 ビット) WebLogic 10.3 のユーザアプリケーションは JRockit JVM 1.6.0_17 を必要とし、次のプラットフォームでサポートされています。 ◆ Windows Server 2003 SP2 (32 ビットのみ) ◆ Windows Server 2008 R2 (64 ビットのみ) ◆ 最新のサポートパックを使用した Windows Server 2008 SP1 (32 ビットおよび 64 ビット) ◆ Open Enterprise Server 2 SP3 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 10 SP3 (32 ビットおよび 64 ビット) ◆ SUSE Linux Enterprise Server 11 SP1 (32 ビットおよび 64 ビット) ◆ Red Hat Enterprise Linux 5.4 (32 ビットおよび 64 ビット) **注 :** ゲストオペレーティングシステムがユーザアプリケーションによってサポートされているものである限り、ユーザアプリケーションは仮想化である Xen および VMW をサポートします。

必須システムコンポーネント	システム要件
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 3.6 は次のプラットフォームでサポートされています。 ◆ Windows XP SP3 ◆ Windows Vista ◆ Windows 7 ◆ SUSE Linux Enterprise Desktop 11 ◆ SUSE Linux Enterprise Server 11 ◆ Novell OpenSuSE 11.2 ◆ Apple Mac Internet Explorer 8 は次のプラットフォームでサポートされています。 ◆ Windows XP SP3 ◆ Windows Vista ◆ Windows 7 Internet Explorer 7 は次のプラットフォームでサポートされています。 ◆ Windows XP SP3
データベースサーバ	JBoss 5.1.0 では次のデータベースがサポートされています。 ◆ MS SQL 2008 ◆ MySQL バージョン 5.1 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 WebSphere 7.0 では次のデータベースがサポートされています。 ◆ DB2 9.5 ◆ MS SQL 2008 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 WebLogic 10.3 では次のデータベースがサポートされています。 ◆ MS SQL 2008 ◆ Oracle 11g ◆ PostgreSQL 8.4.3
Designer	Designer 4.0.1
OpenXDAS	OpenXDAS バージョン 0.8.345 SLES10 には次の OpenXDAS バージョンが必要です。 ◆ openxdas-0.8.351-1.1.i586.rpm ◆ openxdas-0.8.351-1.1.x86_64.rpm

必須システムコンポーネント	システム要件
ドメインサービス	Windows 用 OES 2 SP1 ドメインサービス
パスワード管理確認回答	パスワード管理確認回答機能には、NMAS Challenge Response Login Method バージョン : 2770 ビルド : 20080603 以降が必要です。

前提条件

2

このセクションでは、Identity Manager Roles Based Provisioning Module (RBPM) をインストールする前にインストールまたは設定する必要があるソフトウェアコンポーネント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 Identity Manager メタディレクトリのインストール

Roles Based Provisioning Module 4.0.1 は、Identity Manager 4.0.1 とともに使用する必要があります。

Identity Manager 4.0.1 のインストール方法については、Identity Manager のマニュアルの Web サイト (http://www.novell.com/documentation/idm40/index.html) を参照してください。

2.2 Roles Based Provisioning Module のダウンロード

Identity Manager Roles Based Provisioning Module 製品を入手するには、.iso イメージファイルの 1 つを Novell のダウンロード (http://download.novell.com/index.jsp) からダウンロードします。ダウンロードページでは、Identity Manager 4.0.1 Advanced Edition と Standard Edition とで異なる .iso イメージファイルが用意されています。ご使用のエディションに対して正しい .iso イメージファイルを選択します (たとえば、Identity_Manager_4.0.1_User_Application_Advanced.iso または Identity_Manager_4.0.1_User_Application_Standard.iso のいずれかを選択します)。

表 2-1 では、ユーザアプリケーションおよび Roles Based Provisioning Module に渡されるインストールファイルを説明しています。これらのファイルは、製品の /RBPM ディレクトリの .iso ファイルの中にあります。

表 2-1 *提供されるファイルおよびスクリプト*

ファイル	説明
IDMProv.war	Roles Based Provisioning Module WARIdentity Manager ユーザアプリケーションと、Identity セルフサービス、および役割ベースプロビジョニングモジュール機能が含まれています。
IDMUserApp.jar	ユーザアプリケーションのインストールプログラム。

ファイル	説明
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。
JBossPostgreSQL.bin or JBossPostgreSQL.exe	JBoss アプリケーションサーバおよび PostgreSQL データベースをインストールする便利なユーティリティ。
nmassaml.zip	SAML をサポートするための eDirectory メソッドが含まれます。Access Manager を使用していない場合のみ必要となります。
rbpm_driver_install.exe	役割ベースプロビジョニングモジュール (役割およびリソースサービスドライバ、ユーザアプリケーションドライバ、および eDirectory スキーマ) のメタディレクトリコンポーネント用 Windows インストールプログラム
rbpm_driver_install_linux.bin	役割ベースプロビジョニングモジュール (役割およびリソースサービスドライバ、ユーザアプリケーションドライバ、および eDirectory スキーマ) のメタディレクトリコンポーネント用 Linux インストールプログラム
rbpm_driver_install_solaris.bin	役割ベースプロビジョニングモジュール (役割およびリソースサービスドライバ、ユーザアプリケーションドライバ、および eDirectory スキーマ) のメタディレクトリコンポーネント用 Solaris インストールプログラム

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

デフォルトのインストール場所は次のとおりです。

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

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

2.3 アプリケーションサーバのインストール

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

2.3.1 JBoss アプリケーションサーバのインストール

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

- 製造元の指示に従って、JBoss アプリケーションサーバをダウンロードしてインストールします。サポートされているバージョンについては、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。
- Roles Based Provisioning Moduleのダウンロードに含まれるJBossPostgreSQL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 PostgreSQL) をインストールします。手順については、17 ページの 「JBoss アプリケーションサーバと PostgreSQL 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 2-2 *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	8180 は、アプリケーションサーバのデフォルトです。アプリケーションサーバが使用するポートを記録します。
SSL	外部のパスワード管理を使用する予定がある場合、SSL を有効にします。 ◆ Identity Manager Roles Based Provisioning Module および IDMPwdMgt.war ファイルを展開する JBoss サーバの SSL を有効にします。 ◆ SSL ポートがファイアウォール上で開いていることを確認します。 SSL の有効化の詳細については、JBoss の文書を参照してください。 IDMPwdMgt.war ファイルの詳細については、150 ページのセクション 9.5「外部パスワードを忘れた場合の管理の環境設定」を参照してください。また、『*ユーザアプリケーション: 管理ガイド* (http://www.novell.com/documentation/idm40/index.html)』も参照してください。

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

JBossPostgreSQL ユーティリティは、システムに JBoss アプリケーションサーバおよび PostgreSQL をインストールします。このユーティティはコンソールモードをサポートしないため、グラフィカルユーザインタフェースの環境が必要です。

注 : Windows 2008 で RBPM JBossPostgreSQL インストーラを実行する前に、Windows 管理者にシステムのパスワードポリシーは何かを確認する必要があります。Windows 2008 Server のパスワードポリシーでは、パスワードが特定のルールセットに適合する必要があります。たとえば、パスワードにアルファベット以外の文字に加え、大文字または小文字の文字が含まれていなければならない、または少なくとも 8 文字の長さでなければならない、などを要求するポリシーが考えられます。ポリシーは Windows 管理者が変更したり無効にしたりできます。

ルートとしてインストーラを実行します : ルートユーザでインストーラを実行する必要があります。

JBossPostgreSQL ユーティリティを実行するには

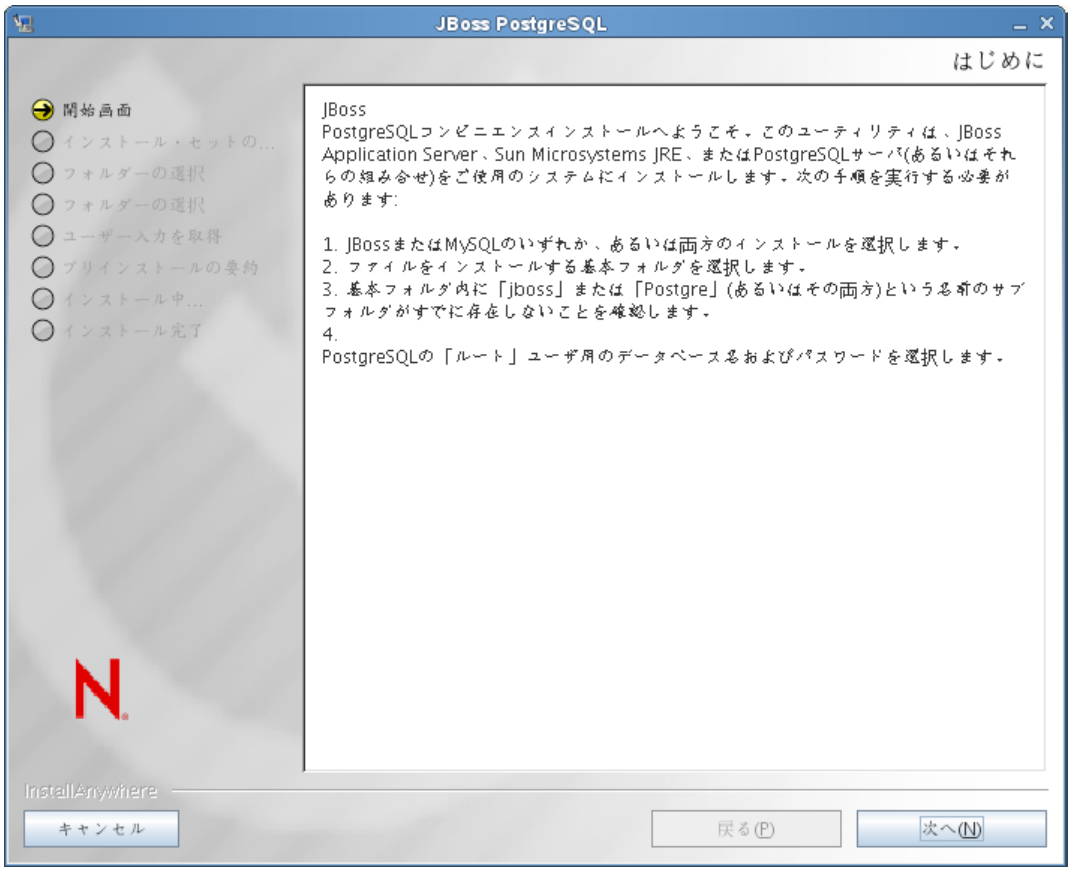
1 JBossPostgreSQL.bin または JBossPostgreSQL.exe を探して実行します。

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

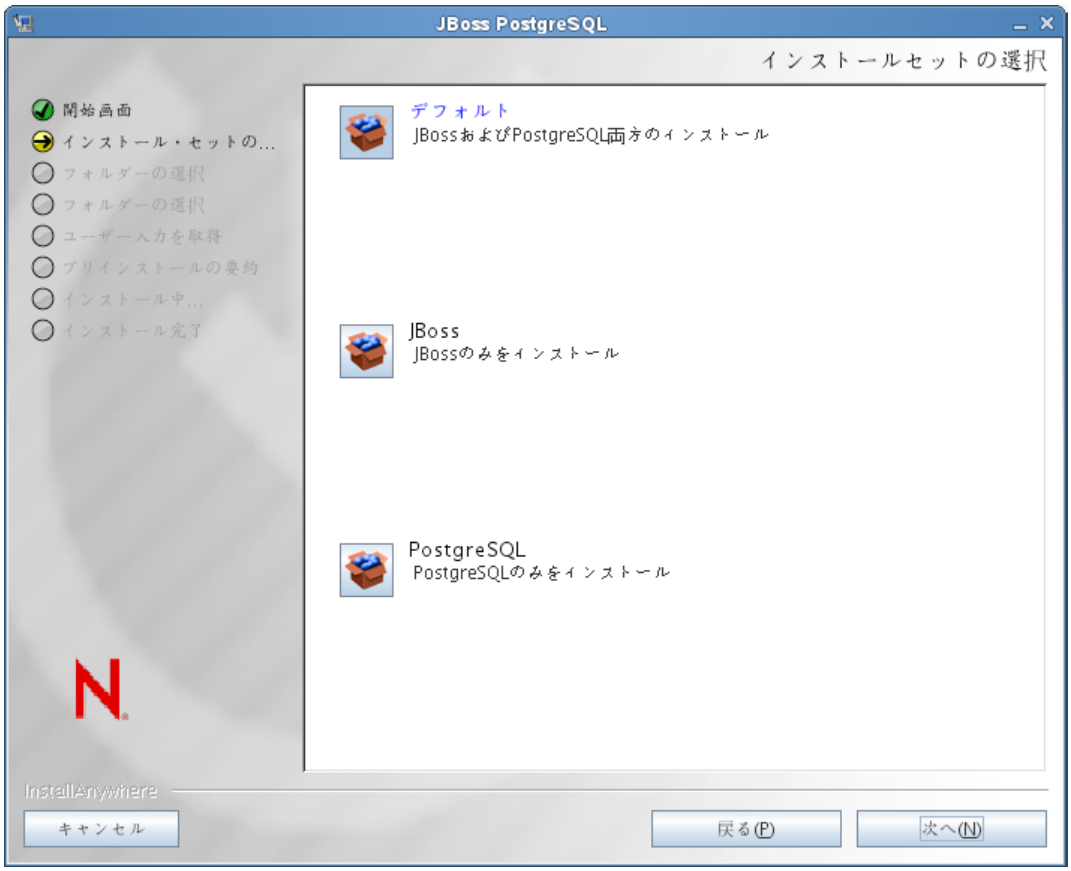
Solaris 用のユーティリティは利用できません。

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

その後、ユーティリティに導入画面が表示されます。

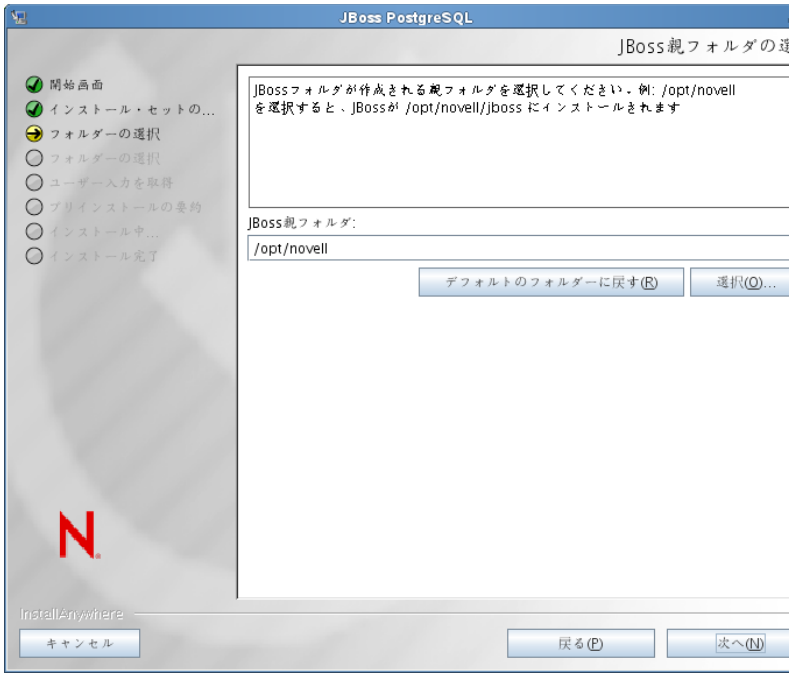
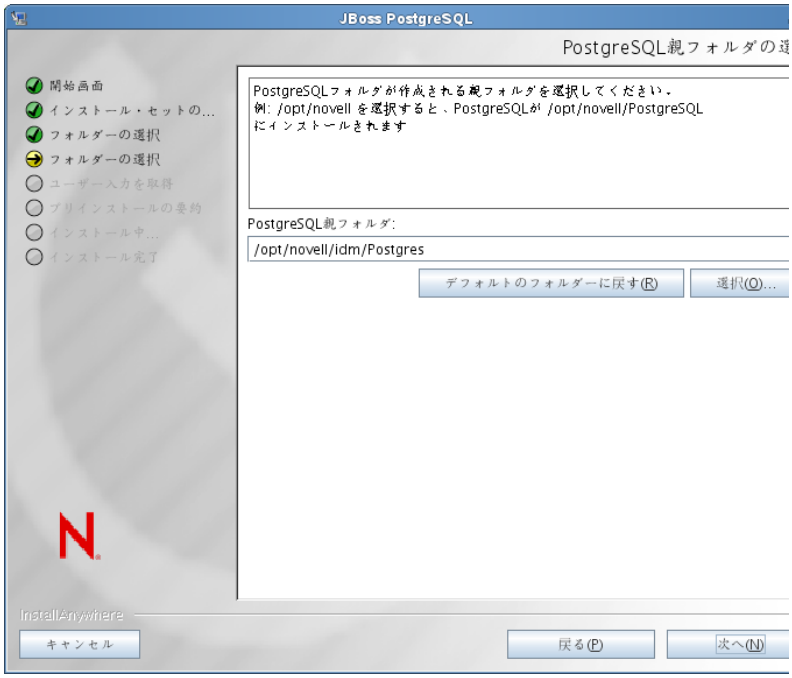


［次へ］をクリックすると、ユーティリティが *［Choose Install Set (インストールセットの選択)］* 画面を表示します。



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

インストール画面	説明
インストールセットの選択	インストールする製品を選択します。 ◆ *デフォルト*: 指定したディレクトリにJBossおよびPostgreSQLの両方を、それを起動および停止するスクリプトとともに、インストールします。 ◆ *JBoss*: 指定するディレクトリに、起動と停止を行うスクリプトと共に JBoss アプリケーションサーバをインストールします。 **注 :** このユーティリティでは、JBoss アプリケーションサーバは Windows サービスとしてインストールされません。手順については、23 ページの 「JBoss アプリケーションサーバのサーバデーモンとしてのインストール」を参照してください。 ◆ *PostgreSQL*: 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 PostgreSQL をインストールし、PostgreSQL データベースを作成します。

インストール画面	説明
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。 
PostgreSQL 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
PostgreSQL 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。デフォルトデータベースは idmadmin です。 ◆ *Database Admin (データベース管理者)*: ユーザはデータベースの管理者になります。デフォルトの管理者は idmuserappdb です。 ◆ *Password for Admin User (管理ユーザのパスワード)*: データベース管理者のパスワードです。 ◆ *Confirm Password Admin User (管理ユーザのパスワードの確認)*: パスワードを確認します。 ◆ *[PostgreSQL Port (PostgreSQL のポート)]* : PostgreSQL データベースがリスンするポートです。 
インストール前の概要	概要ページを確認します。仕様が正しい場合、*[インストール]* をクリックします。

インストール画面	説明
インストールの完了	選択した製品がインストールされると、ユーティリティでは正常に完了したことを示す次のメッセージが表示されます。 `The Installer has completed successfully.  Thank you for choosing Novell` **インストーラは novlua ユーザを作成します :** インストーラは novlua という名前で新しいユーザを作成します。jboss_init スクリプトは、JBoss をこのユーザで実行し、JBoss ファイルで定義されている権限がこのユーザに設定されます。 **重要 :** JBossPostgreSQL ユーティリティが JMX コンソールまたは JBoss Web コンソールを保護しないことに注意する必要があります。これにより、JBoss 環境は無防備なままになります。セキュリティ上の危険を排除するために、インストールを完了し時点で直ちに環境をロックダウンする必要があります。

JBoss アプリケーションサーバのサーバデーモンとしてのインストール

Linux 上では、JBoss はデフォルトでサービスとして開始します。システムの再起動時に JBoss を開始するように、/etc/init.d/jboss_init start/stop という名前のスクリプトがインストールされています。

JavaServiceWrapper の使用 : JavaServiceWrapper を使用して、JBoss アプリケーションサーバを Windows サービス、Linux、または UNIX のデーモンプロセスとしてインストール、開始、および停止することができます。http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows (http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows) で JBoss からの指示を参照してください。このようなラッパの 1 つは、http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html) にあります。これは、JMX (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss) を参照) で管理します。

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

2.3.2 WebLogic アプリケーションサーバのインストール

WebLogic アプリケーションサーバの使用を計画している場合、これをダウンロードおよびインストールします。サポートされているバージョンの情報については、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。

2.3.3 WebSphere アプリケーションサーバのインストール

WebSphere アプリケーションサーバの使用を予定している場合、これをダウンロードおよびインストールします。サポートされているバージョンの情報については、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。

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

2.4 データベースのインストール

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

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

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

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

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

2.4.1 MySQL データベース設定上の注意事項

ユーザアプリケーションには、次に説明するように MySQL 向けの特定の環境設定オプションが必要です。

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

INNODB ストレージエンジンとテーブルタイプ

ユーザアプリケーションは INNODB ストレージエンジンを使用します。これにより、MySQL の INNODB テーブルタイプを選択できます。テーブルタイプを指定せずに MySQL テーブルを作成した場合、テーブルはデフォルトで MyISAM テーブルタイプを受け付けます。MySQL サーバが確実に INNODB を使用するようにするには、my.cnf (Linux または Solaris の場合) または my.ini (Windows の場合) に次のオプションが含まれていることを確認します。

default-table-type=innodb

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

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

文字セット

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

character_set_server=utf8

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

create database databasename character set utf8 collate utf8_bin;

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

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

大文字と小文字の区別

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

lower_case_table_names=1

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

Ansi 設定

my.cnf ファイル (Linux の場合) または my.ini ファイル (Windows の場合) に、ansi エントリを追加する必要があります。このエントリを追加しないと、RBPM テーブルは作成されますがテーブルの初期データロードが実行されず、「ゲストコンテナページの定義が見つかりません」というエラーメッセージが表示されます。

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

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

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

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

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

ユーザアカウント要件

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

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

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

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

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

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

2.4.2 Oracle データベース設定上の注意事項

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

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

CREATE USER *idmuser* IDENTIFIED BY *password*

GRANT CONNECT, RESOURCE to *idmuser*

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

```
select * from nls_database_parameters;
```

UTF-8 が設定されていない場合、このデータが返されます。

```
NLS_CHARACTERSET
WE8MSWIN1252
```

UTF-8 が設定されている場合、このデータが返されます。

```
NLS_CHARACTERSET
AL32UTF8
```

2.4.3 MS SQL サーバデータベース設定の注意事項

MS SQL サーバデータベースを次のように設定します。

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

ユーザアプリケーションには、Microsoft SQL Server 2008 JDBC ドライバのバージョン 3.0.3.0.1119.0 が必要です。Sun Solaris、Red Hat Linux、および Windows 2000 以降のオペレーティングシステムのみが、この JDBC ドライバで公式にサポートされています。

2.4.4 DB2 データベース設定の注意事項

このセクションでは、DB2 設定についての注意事項について説明します。

データベースドライバ JAR の準備

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

- db2jcc.jar
- db2jcc_license_cu.jar

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

Windows の場合の例 :

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

Solaris および Linux の場合の例 :

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

デッドロックおよびタイムアウトを防ぐための DB2 データベースの調整

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

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

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

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

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

```
ALTER TABLE AFACTIVITY VOLATILE
ALTER TABLE AFACTIVITYTIMERTASKS VOLATILE
ALTER TABLE AFBRANCH VOLATILE
ALTER TABLE AFCOMMENT VOLATILE
ALTER TABLE AFDOCUMENT VOLATILE
ALTER TABLE AFENGINE VOLATILE
ALTER TABLE AFENGINESTATE VOLATILE
ALTER TABLE AFMODEL VOLATILE
ALTER TABLE AFPROCESS VOLATILE
ALTER TABLE AFPROVISIONINGSTATUS VOLATILE
ALTER TABLE AFQUORUM VOLATILE
ALTER TABLE AFRESOURCEREQUESTINFO VOLATILE
ALTER TABLE AFWORKTASK VOLATILE
ALTER TABLE AF_ROLE_REQUEST_STATUS VOLATILE
ALTER TABLE ATTESTATION_ATTESTER VOLATILE
ALTER TABLE ATTESTATION_ATTRIBUTE VOLATILE
ALTER TABLE ATTESTATION_QUESTION VOLATILE
ALTER TABLE ATTESTATION_REPORT VOLATILE
ALTER TABLE ATTESTATION_REQUEST VOLATILE
ALTER TABLE ATTESTATION_RESPONSE VOLATILE
ALTER TABLE ATTESTATION_SURVEY_QUESTION VOLATILE
ALTER TABLE ATTESTATION_TARGET VOLATILE
ALTER TABLE AUTHPROPS VOLATILE
ALTER TABLE DATABASECHANGELOG VOLATILE
ALTER TABLE DATABASECHANGELOGLOCK VOLATILE
ALTER TABLE DSS_APPLET_BROWSER_TYPES VOLATILE
ALTER TABLE DSS_APPLET_CFG VOLATILE
ALTER TABLE DSS_APPLET_CFG_MAP VOLATILE
ALTER TABLE DSS_BROWSER_TYPE VOLATILE
ALTER TABLE DSS_CONFIG VOLATILE
ALTER TABLE DSS_EXT_KEY_USAGE_RESTRICTION VOLATILE
ALTER TABLE DSS_USR_POLICY_SET VOLATILE
ALTER TABLE JBM_COUNTER VOLATILE
ALTER TABLE JBM_DUAL VOLATILE
ALTER TABLE JBM_ID_CACHE VOLATILE
ALTER TABLE JBM_MSG VOLATILE
ALTER TABLE JBM_MSG_REF VOLATILE
ALTER TABLE JBM_POSTOFFICE VOLATILE
ALTER TABLE JBM_ROLE VOLATILE
ALTER TABLE JBM_TX VOLATILE
ALTER TABLE JBM_USER VOLATILE
ALTER TABLE PORTALCATEGORY VOLATILE
ALTER TABLE PORTALPORTLETHANDLES VOLATILE
ALTER TABLE PORTALPORTLETSETTINGS VOLATILE
ALTER TABLE PORTALPRODUCERREGISTRY VOLATILE
ALTER TABLE PORTALPRODUCERS VOLATILE
ALTER TABLE PORTALREGISTRY VOLATILE
ALTER TABLE PROFILEGROUPPREFERENCES VOLATILE
ALTER TABLE PROFILEUSERPREFERENCES VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP_LABEL VOLATILE
ALTER TABLE PROVISIONING_VIEW_VALUE VOLATILE
```

```
ALTER TABLE PROVISIONING_VIEW_VALUE_LABEL VOLATILE
ALTER TABLE SECURITYACCESSRIGHTS VOLATILE
ALTER TABLE SECURITYPERMISSIONMETA VOLATILE
ALTER TABLE SECURITYPERMISSIONS VOLATILE
ALTER TABLE SEC_DELPROXY_CFG VOLATILE
ALTER TABLE SEC_DELPROXY_SRV_CFG VOLATILE
ALTER TABLE SEC_SYNC_CLEANUP_QUEUE VOLATILE
```

2.5 Java Development Kit のインストール

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

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

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

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

ユーザアプリケーションで使用するために、JAVA_HOME 環境変数が 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。

役割ベースのプロビジョニングモジュールのインストール

3

この項では、Roles Based Provisioning Module のインストールプログラムを使用して、Identity Manager に Roles Based Provisioning Module (RBPM) のランタイムコンポーネントをインストールする方法について説明します。主なトピックは次のとおりです。

重要 : このリリースでは、iManager を使用してユーザアプリケーションドライバおよび役割とリソースのサービスドライバを作成できなくなりました。ドライバのこの作成方法はサポートされなくなりました。これらのドライバを作成するには、47 ページの第 4 章「ドライバの作成」で説明されているように、Designer が提供する新しいパッケージ管理を使用する必要があります。

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

Identity Manager 4.0.1 は、自動的に RBPM のコアランタイムコンポーネントをインストールします。ただし、Roles Based Provisioning Module 用のインストールプログラムを個別に呼び出すこともできます。

RBPM インストールプログラムは Identity Manager メタディレクトリ環境がインストールされているマシン上で実行する必要があります。eDirectory がデフォルトの場所またはデフォルトの dib の場所にインストールされていない場合、インストールは失敗します。

注 : RBPM のインストールプログラムは、eDirectory がデフォルトの LDAP ポートである 389 および 636 で実行されていない場合も適切に実行されません。デフォルトの LDAP ポートで実行中でない場合は、スキーマが有効でなく、NrfCaseUpdate ユーティリティを実行する必要があると常に通知されます。この問題を修正するには、44 ページのセクション 3.4「スキーマの手動による拡張」で説明するように、手動でスキーマを拡張する必要があります。

これらの品目が Identity Manager にインストールされると、ユーザアプリケーションを実行するために必要なドライバを作成するために、47 ページの第 4 章「ドライバの作成」で説明されている手順に従う必要があります。

重要 : RBPM の 3.6.1 以前のリリースで作成された eDirectory ツリーにユーザアプリケーションドライバが含まれている場合、Roles Based Provisioning Module インストールプログラムを実行する前に NrfCaseUpdate ユーティリティを実行する必要があります。実行しないと、インストールが失敗します。バージョン 4.0.1 の新規インストールを実施する場合、または 3.7 からアップグレードする場合、この手順は必要はありません。

3.2 NrfCaseUpdate ユーティリティの実行

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

3.2.1 NrfCaseUpdate の概要

役割とリソースで大文字と小文字が混在する検索をサポートするには、NrfCaseUpdate プロシージャが必要です。このプロシージャは nrfLocalizedDescrs および nrfLocalizedNames 属性 (ユーザアプリケーションで使用される) を変更することによってスキーマを更新します。eDirectory のツリーが RBPM の 3.6.1 以前のリリースを使用して作成された場合、RBPM 4.0.1 をインストールする前、および Designer 4.0.1 で既存のドライバをマイグレートする前にこのプロシージャが必要になります。バージョン 4.0.1 の新規インストールを実施する場合、または 3.7 からアップグレードする場合、この手順は必要はありません。

3.2.2 インストールの概要

このセクションでは、既存の RBPM 環境を更新し移行するための手順の概要を説明します。この概要は、すべての更新を開始する前にユーザアプリケーションドライバのバックアップを作成する Designer 4.0.1 の使用法に重点を置きます。

1. Designer 4.0.1 のインストール
2. 識別ボールトのヘルスチェックを実行し、スキーマが適切に拡張されていることを確認します。TID 3564075 を使用してヘルスチェックを完了します。
3. 既存のユーザアプリケーションドライバを Designer 4.0.1 にインポートします。
4. Designer プロジェクトをアーカイブします。これは RBPM 4.0.1 以前のドライバの状態を表します。
5. NrfCaseUpdate プロセスを実行します。
6. 新しい Designer 4.0.1 プロジェクトを作成し、移行に備えてユーザアプリケーションドライバをインポートします。
7. RBPM 4.0.1 をインストールします。
8. Designer 4.0.1 を使用してドライバを移行します。
9. 移行したドライバを展開します。

3.2.3 NrfCaseUpdate のスキーマへの影響

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

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

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

3.2.4 ユーザアプリケーションドライバのバックアップの作成

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

1. Designer 4.0.1 をインストールします。これは RBPM 4.0.1 に同梱されています。
2. 識別ボールトを作成し、それをユーザアプリケーションドライバを含む Identity Manager ドライバにマップします。
3. *[ライブ] > [インポート]* コマンドの順に使用して、ドライバセットとユーザアプリケーションドライバをインポートします。
4. この Designer プロジェクトを保存しアーカイブします。

3.2.5 NrfCaseUpdate の使用

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

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

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

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

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

NrfCaseUpdate を実行するには、次の手順に従います。

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

   ```
   /root/idm/jre/bin/java -jar NrfCaseUpdate.jar -v
   ```
4. 既存のユーザアプリケーションドライバを持っているかどうか聞かれます。既存のユーザアプリケーションドライバを持っている場合は、［True］と答えます。そうでなければ、［False］と答えて 35 ページのステップ 15 にスキップします。

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

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

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

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

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

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

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

    ```
    Specify the fully qualified LDAP DN of the User Application driver located
    in the Identity Vault
    (e.g. cn=UserApplication,cn=driverset,o=acme):
    ```

DN にスペースが含まれる場合は、次に示すように一重引用符で囲む必要があります。

```
'cn=UserApplication driver,cn=driverset,o=acme'
```

12 ユーザアプリケーションをエクスポートする LDIF ファイルの名前を指定します。

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

19 すべてのドライバがインポートし直された後で、NrfCaseUpdate プロセスが正常であったことを確認します。詳細については、36 ページのセクション 3.2.6「NrfCaseUpdate プロセスの確認」を参照してください。

20 NrfCaseUpdate プロセスが正常であったことを確認した後に、RBPM 4.0.1 インストールを続行します。

3.2.6 NrfCaseUpdate プロセスの確認

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

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

確認が完了した後、RBPM 4.0.1 のインストールを続行し更新できます。

3.2.7 SSL 接続の JRE の有効化

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

まず、識別ボールトの認証局から自己署名証明書をエクスポートします。

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

次に、自己署名証明書を JRE のトラステッドストアにインポートします。

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

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

   次に例を示します。

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

3.2.8 無効にされたユーザアプリケーションドライバの復元

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

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

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

次のプロシージャは Designer 4.0.1 を使用してユーザアプリケーションドライババックアップを復元するプロセスを概説しています。

1. eDirectory を再起動して、有効にしたスキーマの変更を確認します。
2. ユーザアプリケーションドライバ、UserAppDriver のバックアップを含む、Designer 4.0.1 プロジェクトのコピーを開きます。このプロシージャはドライバ名を変更するので、プロジェクトのコピーを使用することが重要です。
3. ユーザアプリケーションドライバと識別ボールトの間の接続を選択し、右クリックしてから *［プロパティ］* を選択します。
4. 「UserAppDriver_restore」などの新しい名前を指定します。*［適用］* および *［OK］* を選択します。
5. *［保存］* をクリックしてプロジェクトを保存します。
6. 識別ボールトを選択することによって識別ボールト同期させ、*［ライブ］* > *［スキーマ］* > *［比較］* を選択し、*［元に戻すアクションのために Designer を更新］*。
7. プロジェクトを保存します。
8. ドライバを選択し、*［ドライバ］* > *［展開］* を選択することによって、名前変更したドライバを展開します。
9. NrfCaseUpdate を実行し、新しく名付けたドライバを LDIF ファイルにエクスポートします。
10. 編集用に LDIF ファイルのコピーを作成します。
11. 復元するユーザアプリケーションドライバを示すために参照する LDIF ファイルを編集し、すべてのドライバを名前変更します。たとえば、元のユーザアプリケーションドライバが「cn=UserAppDriver」の場合、「cn=UserAppDriver_restore」から「cn=UserAppDriver」へ名前変更します。この手順は、本物のユーザアプリケーションドライバを反映する LDIF ファイルを実質的に構築します。
12. ice を使用して、変更した LDIF ファイルをインポートします。

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

13. ice を使用したインポートが成功したことを確認するためには、そのステータスに注意してください。
14. ドライバの復元を確認するには、36 ページのセクション 3.2.6「NrfCaseUpdate プロセスの確認」の下の指示に従います。
15. 名前変更したドライバをドライバセットから削除します。

3.3 RBPM インストールプログラムの実行

1 次のプラットフォームのインストーラを起動します。

Linux:

`rbpm_driver_install_linux.bin`

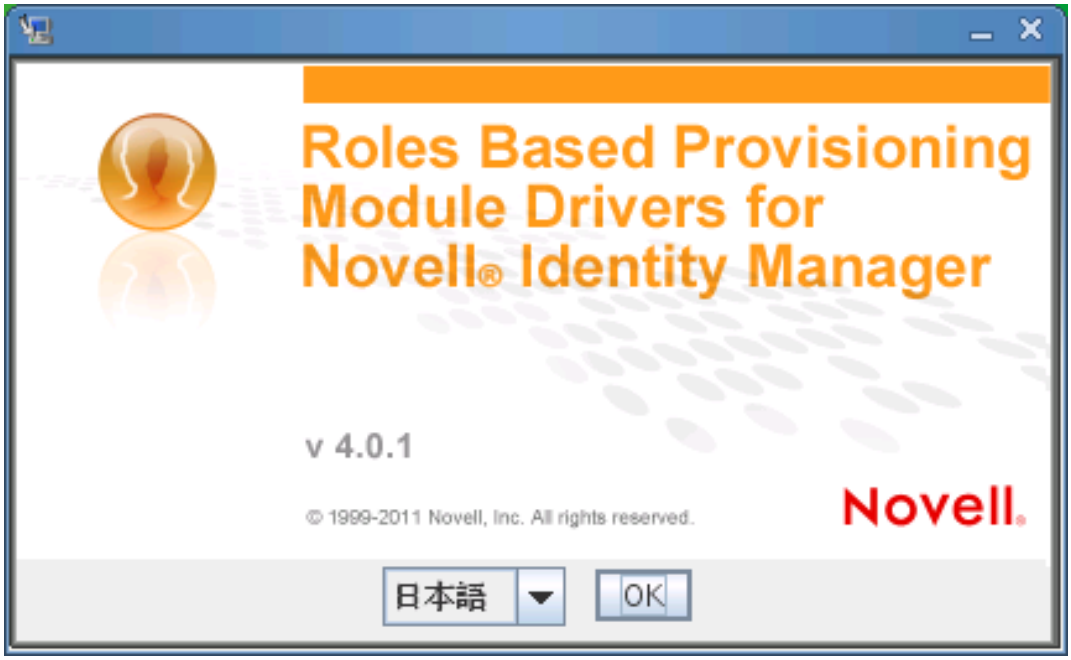
Solaris:

`rbpm_driver_install_solaris.bin`

Windows:

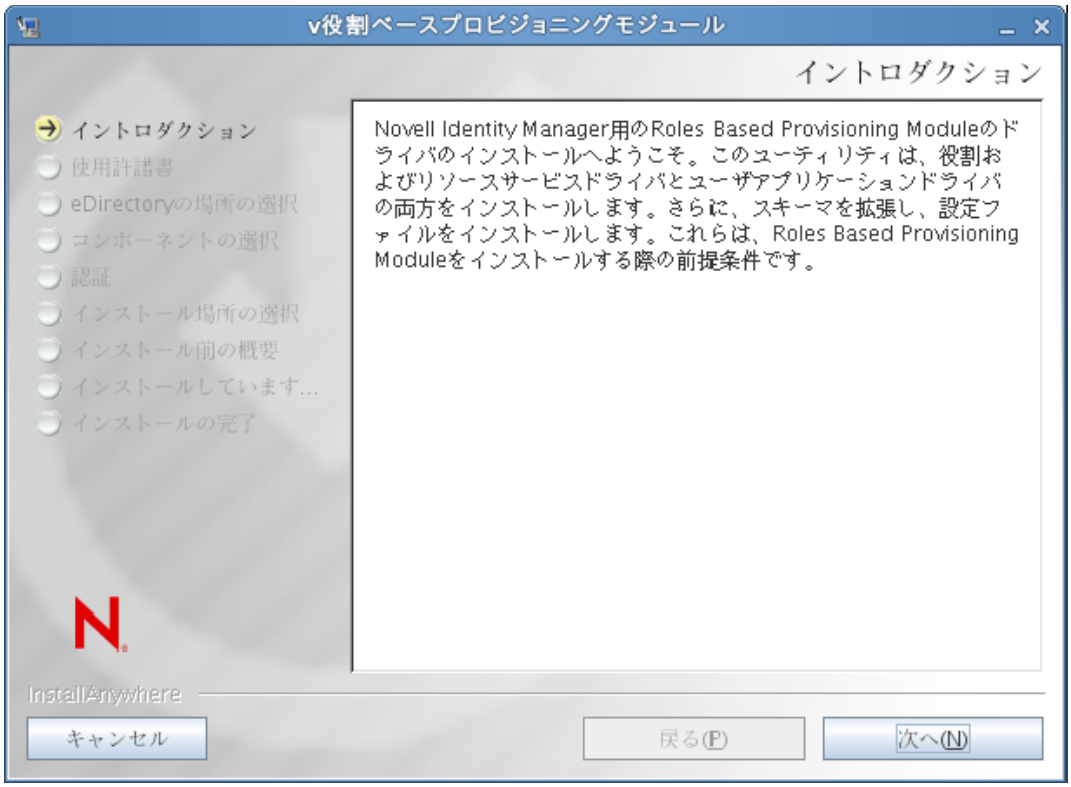
`rbpm_driver_install.exe`

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



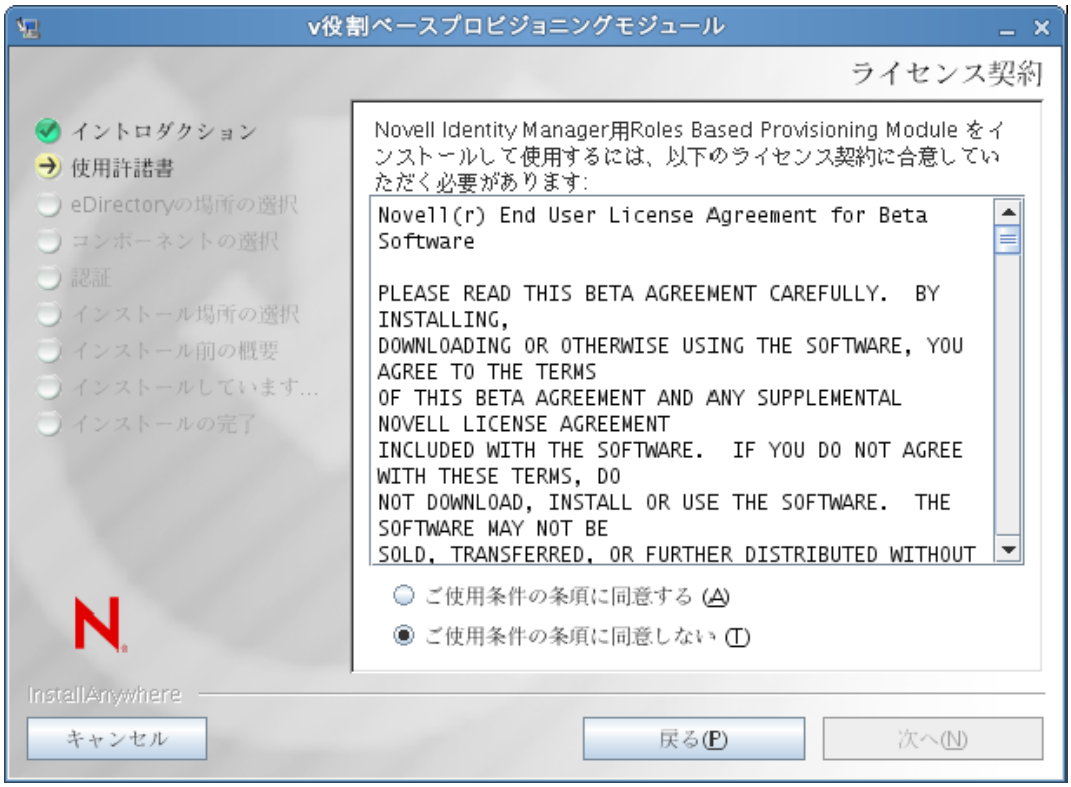
2 インストールする言語を選択して［OK］をクリックします。

インストーラにより、導入画面が表示されます。



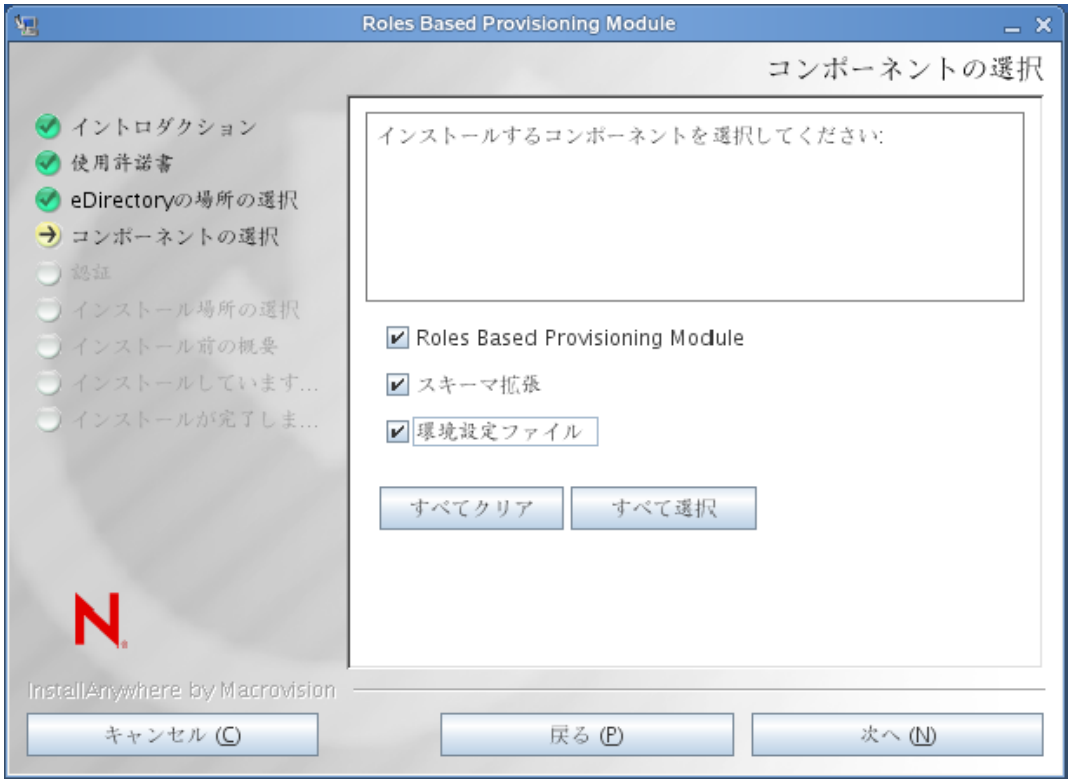
3 *[次へ]* をクリックします。

インストーラにより使用許諾契約画面が表示されます。



4 使用許諾契約に同意したら、*[次へ]* をクリックします。

インストールにより［コンポーネントの選択］画面が表示されます。

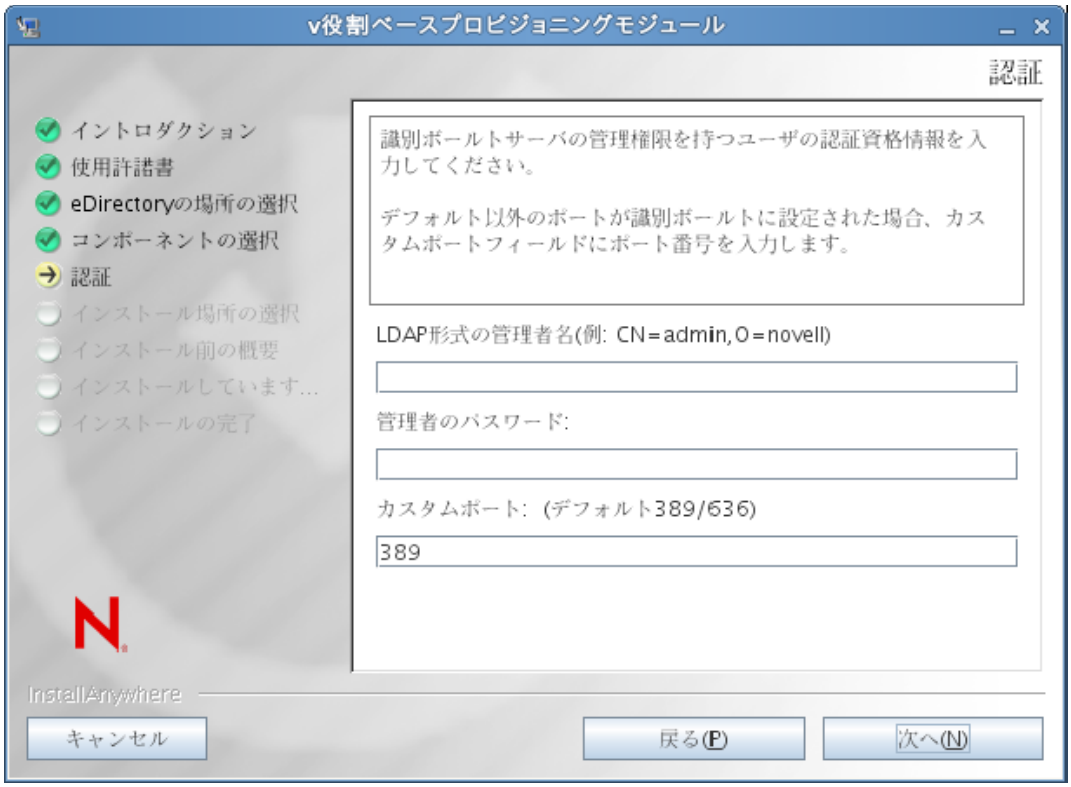


このコンポーネントを次に説明します。

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

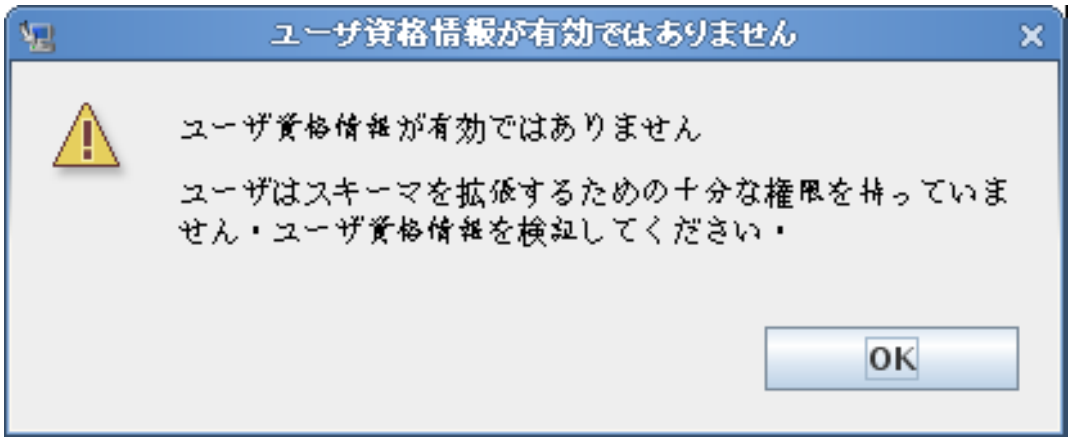
5 インストールするコンポーネントを選択し、*[次へ]* をクリックします。通常、すべてのコンポーネントをインストールします。

インストーラにより、認証画面が表示されます。



6 LDAP 形式で管理者名を指定し、パスワードを入力します。また、LDAP サーバのポートも指定します。

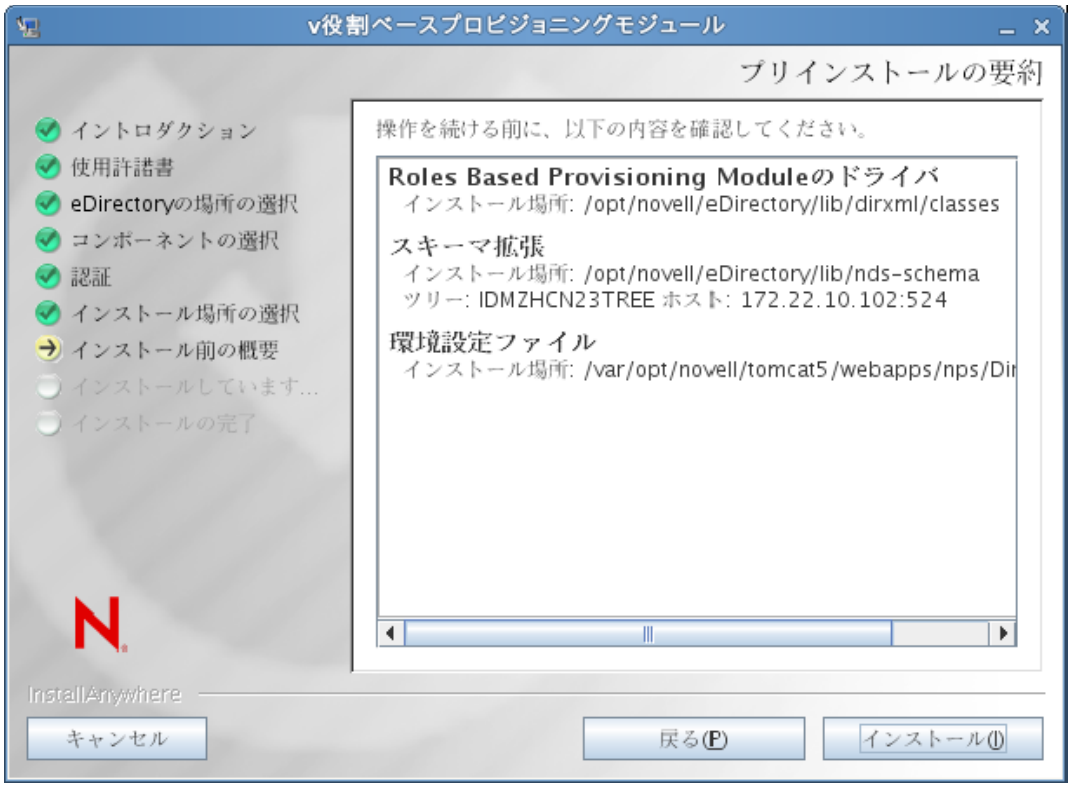
ユーザ資格情報が有効でない場合、またはユーザが必要な権限を持っていない場合、インストーラにより次のようなエラー画面が表示されます。



ユーザ資格情報が有効な場合、またはユーザが適切な権限を持っている場合、インストーラにより［Roles Based Provisioning Module のドライバライブラリのインストール場所］画面のインストール場所が表示されます。

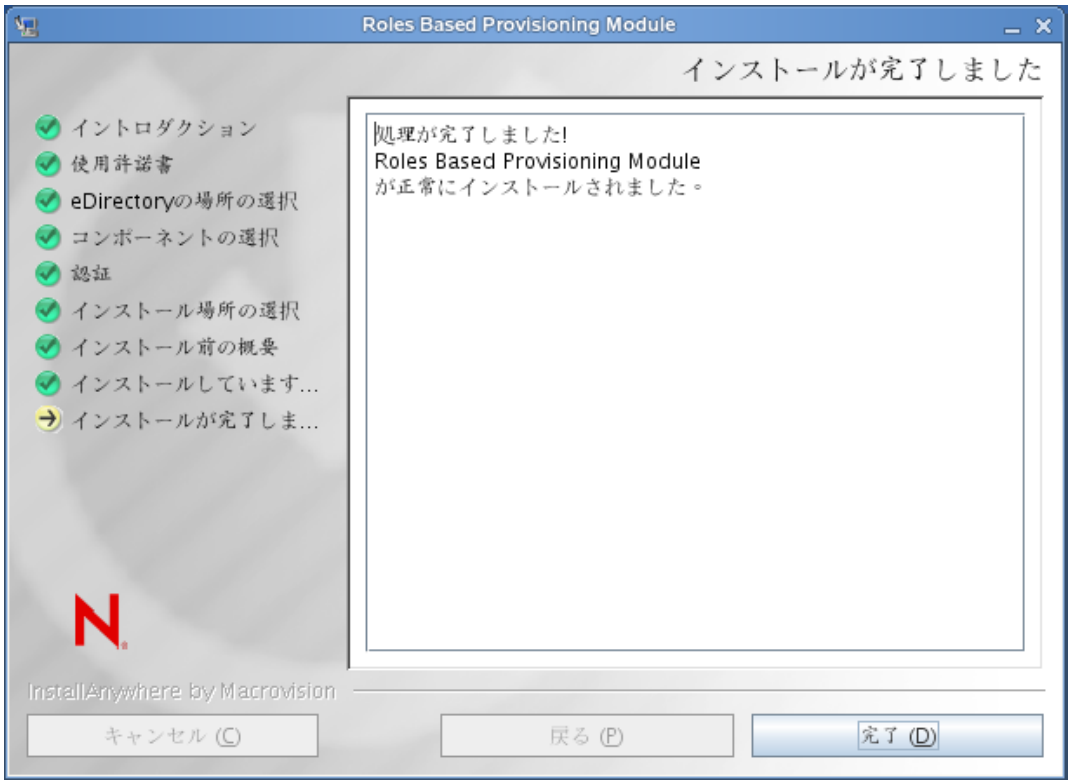
7 ドライバライブラリを保存するディスクの目的の場所を指定するには、*[次へ]* をクリックします。

インストーラにより［インストール前の概要］画面が表示されます。



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

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



注 : RBPM に関連付けられているランタイムコンポーネントをアンインストールする必要がある場合、Windows 上でアンインストールプログラムをサイレントモードで実行していない限り、アンインストールプログラムによって自動的にサーバマシンが再起動されます。この場合、手動で Windows マシンを再起動する必要があります。さらに、統合インストーラを使用せずに Identity Manager をアンインストールする必要がある場合、アンインストールプログラムを起動する前に、nds サービスを停止する必要があります。

3.4 スキーマの手動による拡張

この項では、スキーマを手動で拡張する方法について説明します。これらの手順は、eDirectory がデフォルトの場所にインストールされていない場合、または必要なデフォルトの LDAP ポートである 389 および 636 で実行されていない場合に発生する問題を修正するためにのみ必要です。

スキーマの手動で拡張するには (Windows)

1. Identity Manager をインストールした後で、eDirectory を停止します。
2. 次のコマンドを実行して、eDirectory のインストール場所にある sch_nt.cfg にリストされているスキーマを拡張します。

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

注 : <*dibPathLocation*> には DIBFiles フォルダが含まれる必要があります。

次にコマンドの例を示します。

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

注 : 上記のコマンドは、sch_nt.cfg を使用してすべてのスキーマファイルを拡張するのではなく、sch_nt.cfg に記載されている 1 つ 1 つのスキーマファイルを手動で拡張します。

3 *[Select Components (コンポーネントの選択)]* ウィンドウの中の *[スキーマ拡張]* オプションのチェックをオフにして、役割ドライバおよびリソースドライバをインストールします (38 ページのセクション 3.3「RBPM インストールプログラムの実行」で説明)。インストールを完了します。

4 役割ドライバおよびリソースドライバをインストールしたら、44 ページのステップ 2でリストされているコマンドを実行して役割ベースのスキーマファイル srvprv.sch および nrf-extensions.sch を拡張します。

注 : この手順では、schemaStart.bat を使用して必要なスキーマファイルを拡張します。

5 44 ページのステップ 2 にリストされているコマンドを使用して、NrfCaseupdate スキーマ (update-nrf-case.sch) を拡張します。

6 eDirectory を開始する .

スキーマの手動で拡張するには (SUSE)

1 *[Select Components (コンポーネントの選択)]* ウィンドウの中の *[スキーマ拡張]* オプションのチェックをオフにして、役割ドライバおよびリソースドライバをインストールします (38 ページのセクション 3.3「RBPM インストールプログラムの実行」で説明)。*[次へ]* をクリックします。

2 ドライバ用に適切なインストール場所を選択し、*[次へ]* をクリックします。

3 ドライバ環境設定ファイル用に適切なインストール場所を選択し、*[次へ]* をクリックします。インストールを完了します。

手順 1 ～ 3 によって、ドライバおよびドライバ環境設定ファイルが eDirectory のデフォルト以外の場所にコピーされます。

4 ndssch コマンド (すなわち、srvprv.sch、nrf-extensions.sch) を実行してスキーマを拡張します。

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

例 :

```
ndssch -h 172.16.1.137:524 -t TESTTREE -p 'PASSWORD'
.cn=admin.o=novell.T=TESTTREE.
/opt/novell/eDirectory/lib/nds-schema/srvprv.sch'
```

5 手順 4 を繰り返して nrf-extensions.sch を拡張します。

ドライバの作成

4

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

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

ドライバ環境設定サポートでは、次の処理を実行できます。

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

重要 : このリリースでは、iManager を使用してユーザアプリケーションドライバおよび役割とリソースのサービスドライバを作成できなくなりました。ドライバのこの作成方法はサポートされなくなりました。これらのドライバを作成するには、以下で説明されているように、Designer が提供する新しいパッケージ管理を使用する必要があります。

4.1 Designer でのドライバの作成

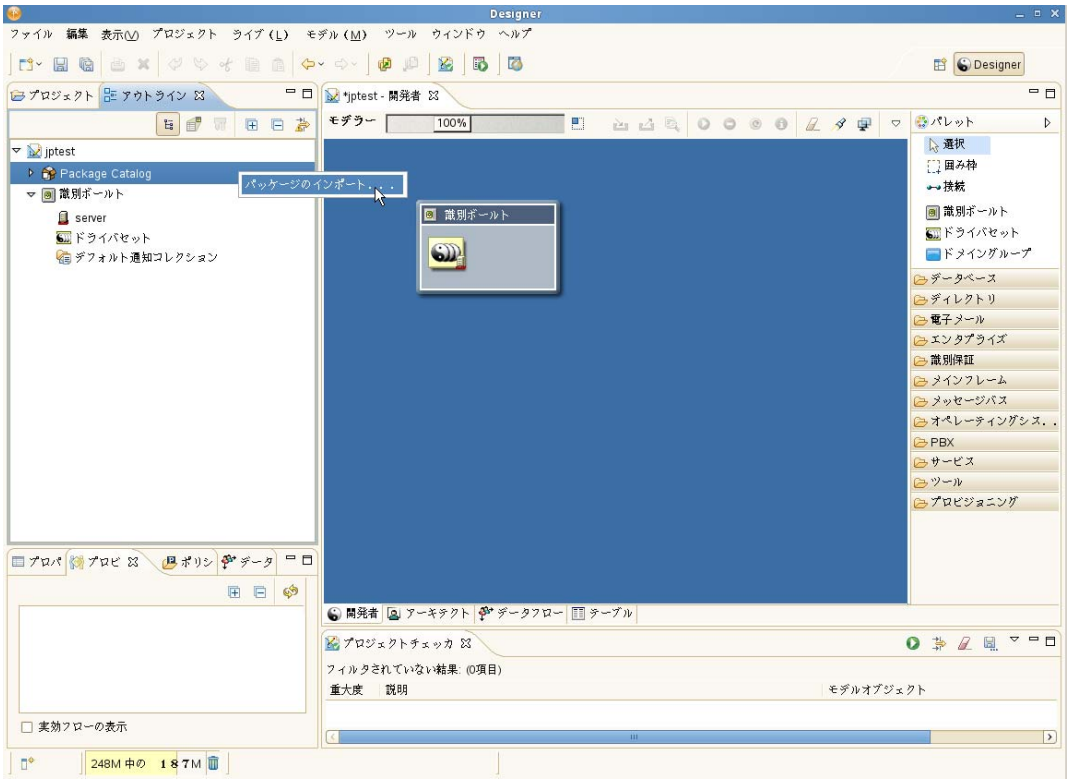
この項では、Designer でのドライバの作成方法について説明します。主なトピックは次のとおりです。

4.1.1 パッケージのインストール

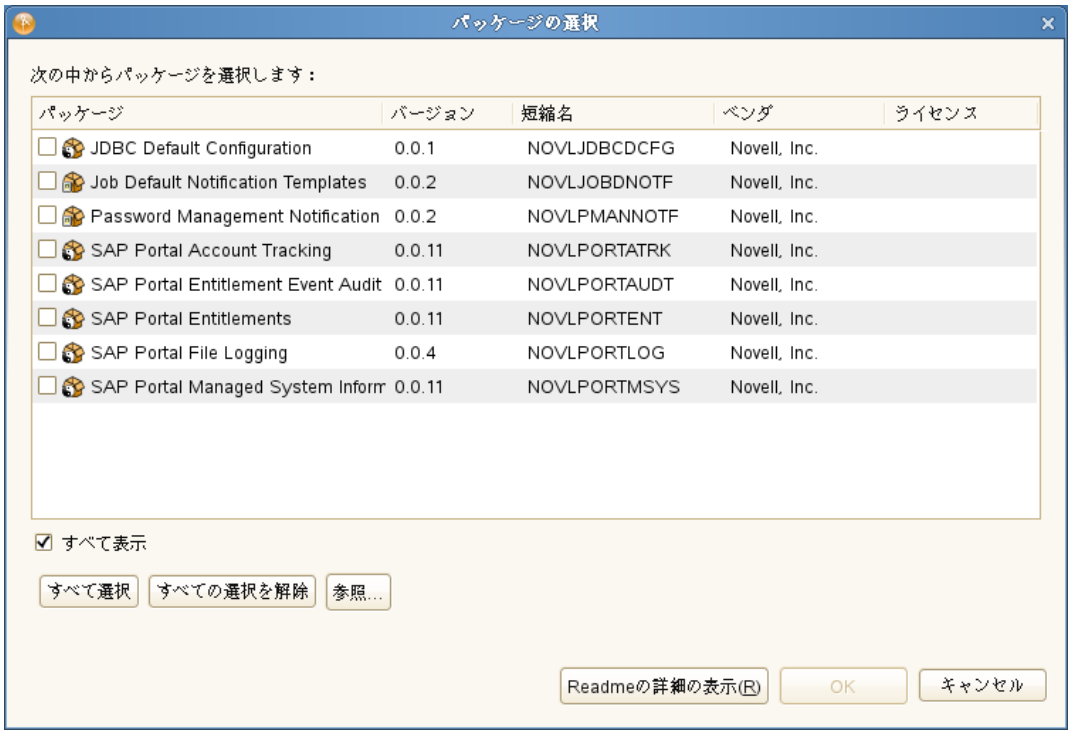
ドライバを設定する前に、パッケージカタログに必要なすべてのパッケージが含まれていることを確認する必要があります。新しい Identity Manager プロジェクトを作成すると、新しいプロジェクトにいくつかのパッケージをインポートするようにユーザインタフェースによって自動的に要求されます。プロジェクトの作成時にパッケージをインポートしない場合、下記のように、後でそれらをインストールする必要があります。

新しい Identity Manager プロジェクトを作成し、後からパッケージをインストールするには

1 Designer 内に新しい Identity Manager プロジェクトを作成したら、*[Package Catalog (パッケージカタログ)]* を選択し、*[パッケージのインポート]* をクリックします。



Designer に *［パッケージの選択］* ダイアログボックスが表示されます。



2 *［すべて選択］* をクリックし、*［OK］* をクリックします。

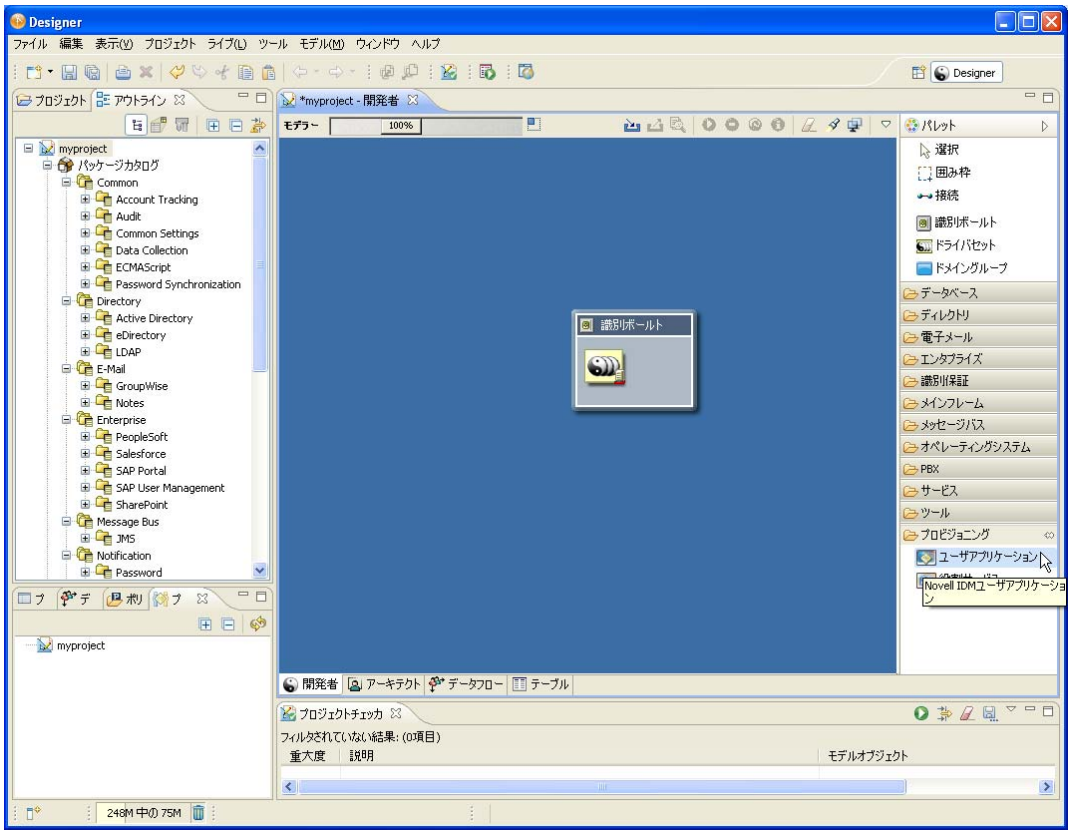
Designer によって、*[パッケージカタログ]* にいくつかの新しいパッケージフォルダが追加されます。これらのパッケージフォルダは、Designer 内の *[モデラー]* ビューの右側にあるパレットに含まれるオブジェクトに対応します。

3 *[保存]* をクリックしてプロジェクトを保存します。

4.1.2 Designer でのユーザアプリケーションドライバの作成

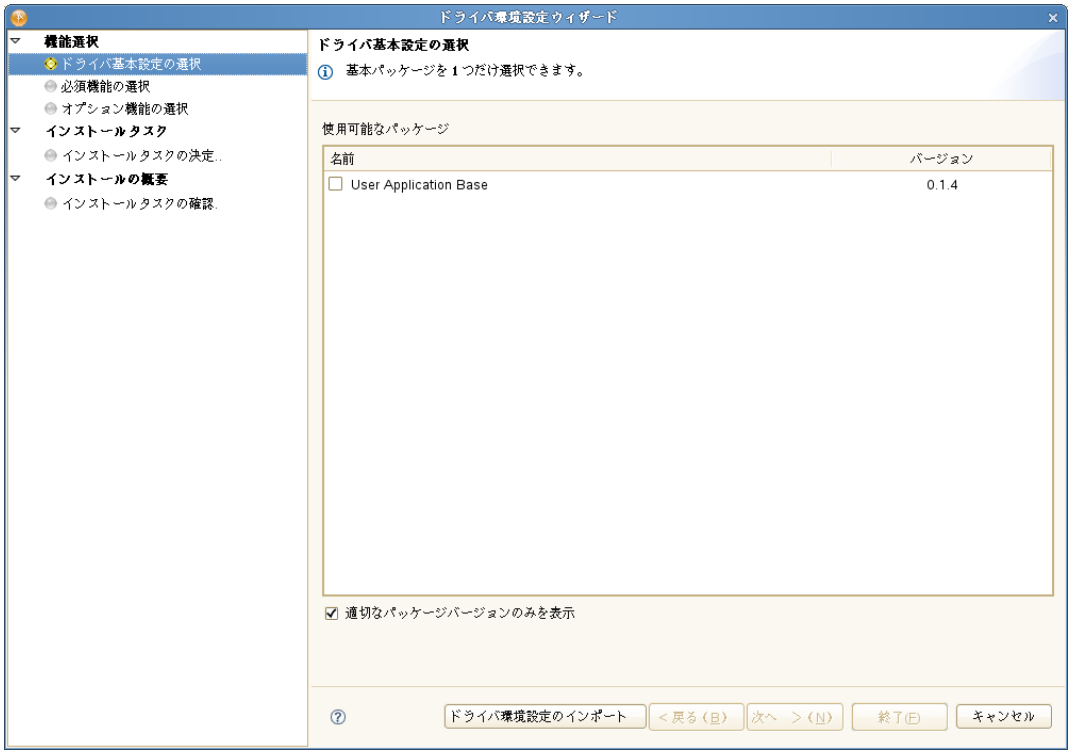
Designer でユーザアプリケーションドライバを作成するには

1 *[モデラー]* ビューのパレットの中から *[ユーザアプリケーション]* を選択します。

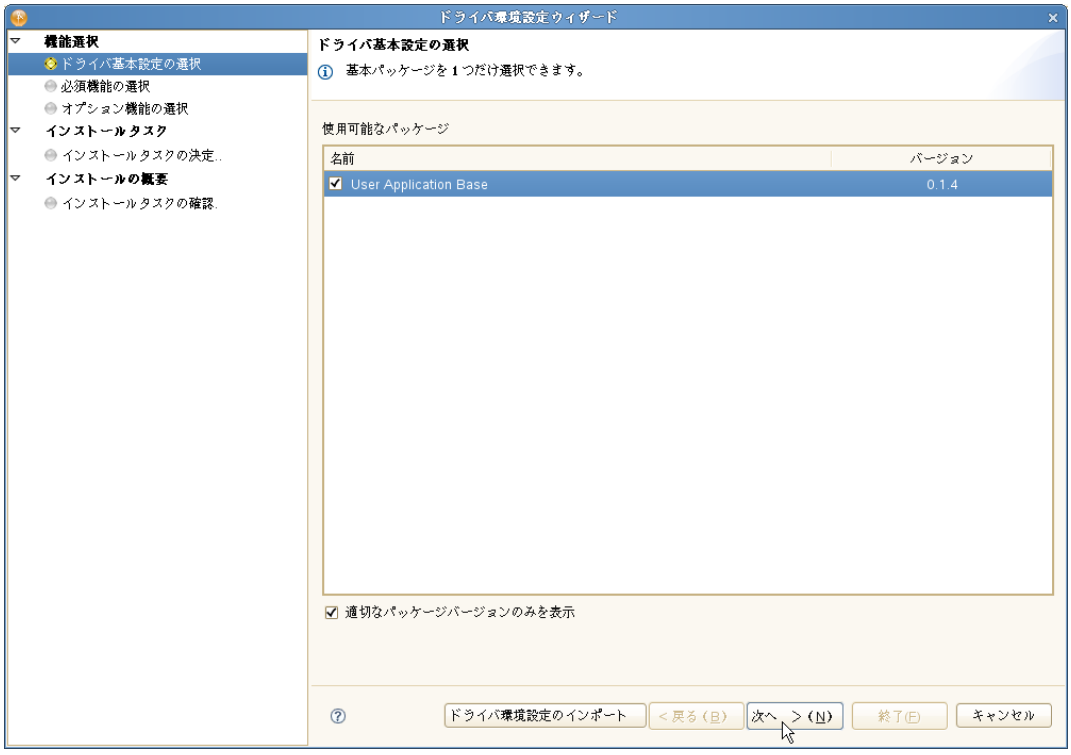


2 *[ユーザアプリケーション]* のアイコンを *[モデラー]* ビュー上にドラッグします。

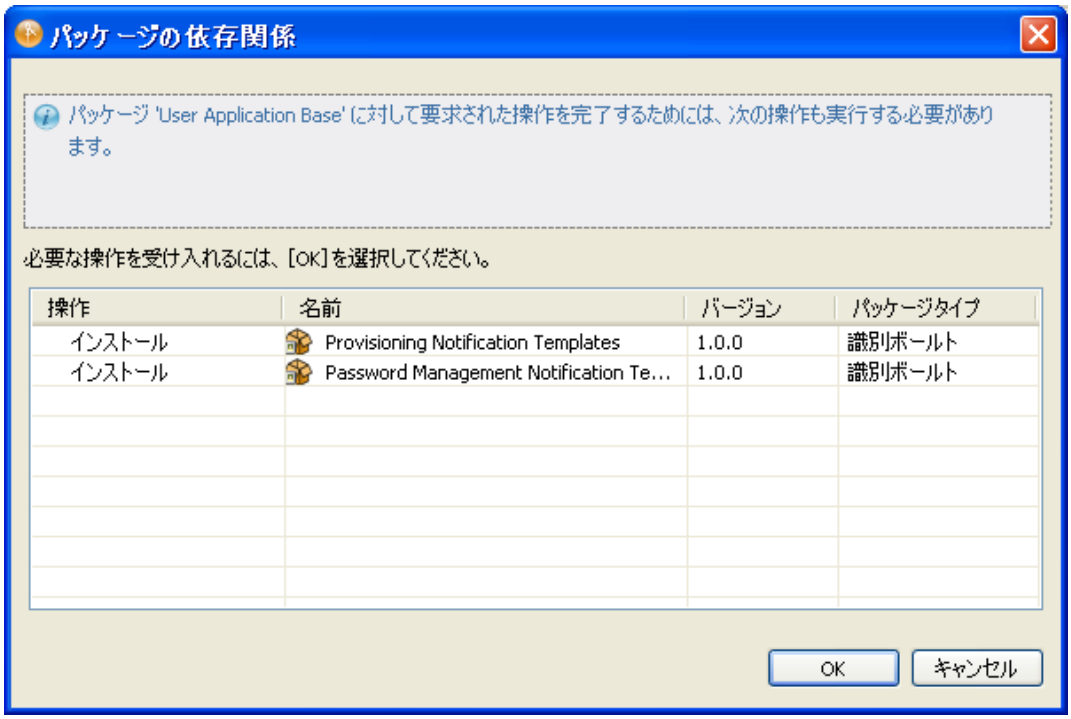
Designer によって、*ドライバ環境設定ウィザード*が表示されます。



3 *[User Application Base (ユーザアプリケーションベース)]* を選択し、*[次へ]* をクリックします。



いくつかの追加パッケージが必要であることを通知するダイアログがインタフェースに表示されます。



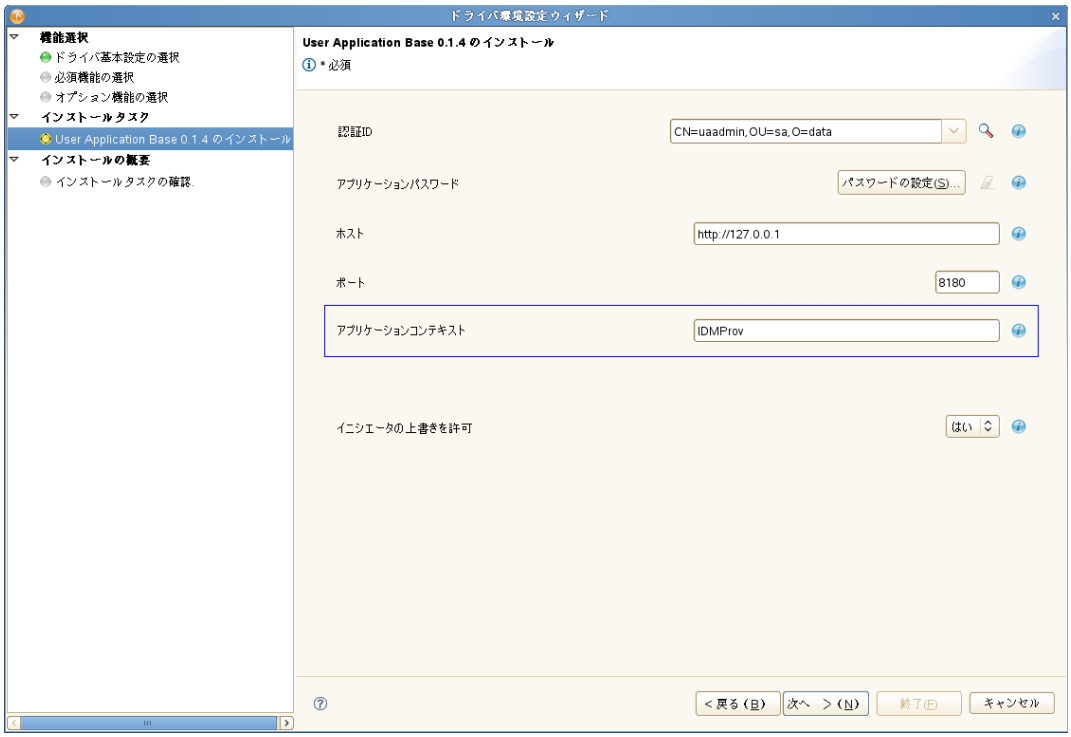
4 必要なパッケージをインストールするには *[OK]* をクリックします。

この時点で、ドライバの名前を付けることができる画面をウィザードが表示します。

5 デフォルトのドライバ名を受け入れるか、それをお好みで変更することができます。*[次へ]* をクリックします。

ウィザードがドライバの接続パラメータを指定できる画面を表示します。

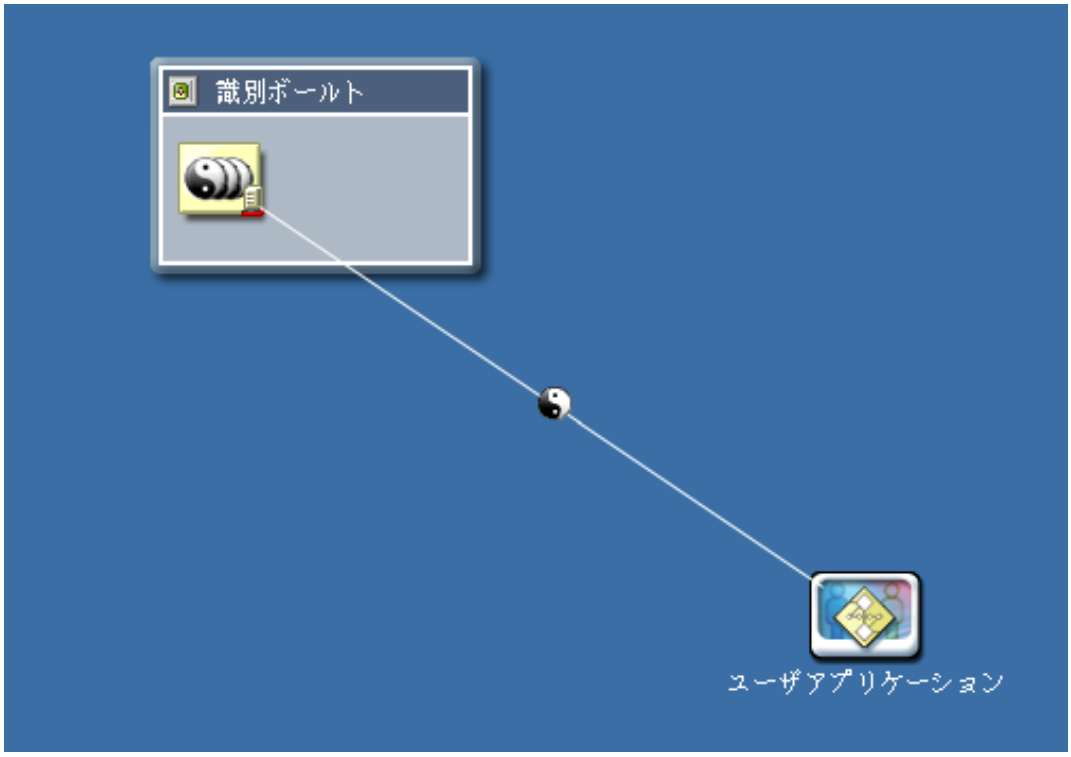
6 ユーザアプリケーション管理者用の ID およびパスワードに加え、ユーザアプリケーションサーバ用のホスト、ポート、およびアプリケーションコンテキストを指定します。プロビジョニング管理者が代理として指名されている別のユーザ名でワークフローを開始できるようにするには、*[イニシエータの無効化を許可]* に対して *[はい]* を選択します。



その後、ウィザードに *[インストールタスクの確認]* 画面が表示されます。

7 すべて正しいようであれば、*[完了]* をクリックします。

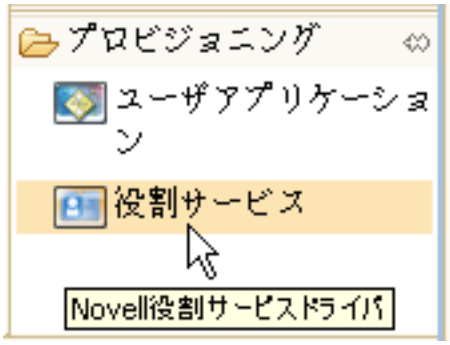
Designer が *[ユーザアプリケーション]* ドライバを *[モデラー]* ビューに追加します。



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

Designer で役割サービスドライバおよびリソースサービスドライバを作成するには

1 *［モデラー］*ビューのパレットの中から *［役割サービス］*を選択します。



2 *［役割サービス］*のアイコンを *［モデラー］*ビュー上にドラッグします。

Designer によって、*ドライバ環境設定ウィザード*が表示されます。

3 *［Role and Resource Service Base (役割とリソースのサービスベース)］*を選択し、*［次へ］*をクリックします。

ウィザードがドライバの名前を指定できる画面を表示します。

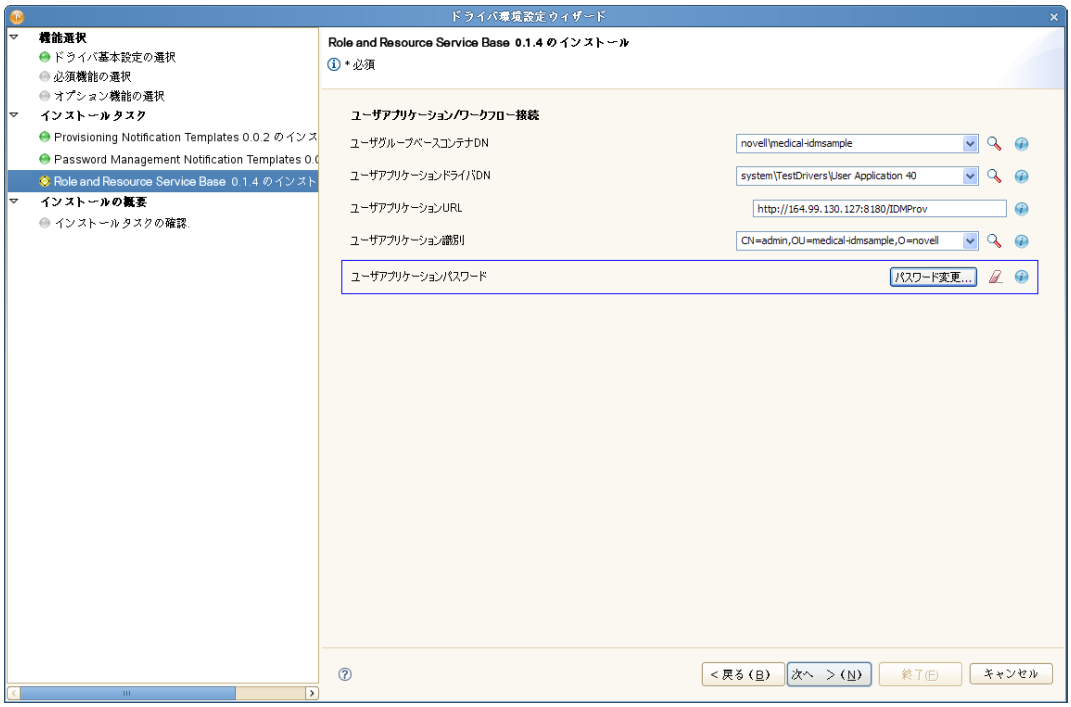
4 デフォルトのドライバ名を受け入れるか、それをお好みで変更することができます。

*［次へ］*をクリックします。

ウィザードがドライバの接続パラメータを指定できる画面を表示します。

5 ベースコンテナの DN と作成したユーザアプリケーションドライバを指定します。ドライバがまだ展開されていないので、ブラウズ機能では設定したばかりのユーザアプリケーションドライバは表示されません。したがって、ドライバの DN を入力する必要があります。

ユーザアプリケーション管理者用の ID およびパスワードとともに、ユーザアプリケーション用の URL を指定します。

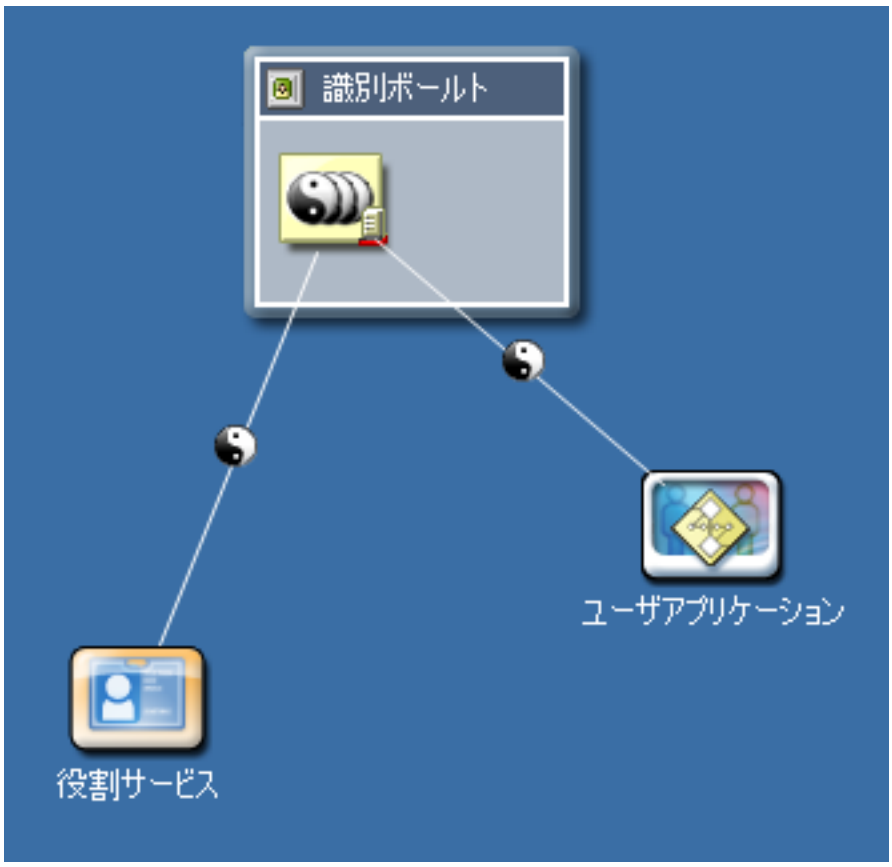


[次へ] をクリックします。

これにより、ウィザードに *[インストールタスクの確認]* 画面が表示されます。

6 すべて正しいようであれば、*[完了]* をクリックします。

Designer が *［役割サービス］*ドライバを *［モデラー］*ビューに追加します。



4.1.4 ドライバの展開

設定したドライバを展開するには

1. ドライバセットを選択します (*［モデラー］*ビューまたは *［アウトライン］*ビューのいずれかから)。
2. *［ライブ］* > *［展開］*を選択します。

   Designer は、どのオブジェクトが展開中かを示す進行状況ウィンドウを表示します。

注 : eDirectory の環境を複製するには、レプリカに Identity Manager の NCP サーバオブジェクトが含まれていることを確認する必要があります。Identity Manager は、サーバのローカルレプリカに制約されます。そのため、セカンダリサーバにサーバオブジェクトが含まれていない場合、役割およびリソースサービスドライバが正常に起動しないことがあります。

JBoss でのユーザアプリケーションのインストール

5

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

- 57 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」
- 78 ページのセクション 5.2「インストールのテスト」

コマンドラインを使用してインストールする場合は、131 ページの第 8 章「コンソールまたは単一コマンドによるインストール」を参照してください。

ルートとしてインストーラを実行します : ルートユーザでインストーラを実行する必要があります。

データマイグレーション : 移行の詳細については、『*ユーザアプリケーション : マイグレーションガイド* (http://www.novell.com/documentation/idm40/index.html)』を参照してください。

5.1 ユーザアプリケーション WAR のインストールおよび環境設定

注 : JBoss 5.1.0 の場合、インストールプログラムでは、Sun から提供されている Java 2 Platform Standard Edition Development Kit バージョン 1.6 (JRE または JDK) が必要です。別のバージョンを使用すると、インストールプロシージャはユーザアプリケーション WAR ファイルを正常に設定しません。インストールは成功したかのように見えますが、ユーザアプリケーションの起動を試みるとエラーが発生します。

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

ユーザアプリケーションインストーラを開始するには、Sun JRE の正しいバージョンを必ず使用します (10 ページのセクション 1.3「システム要件」の説明に従うこと)。Roles Based Provisioning Module とともに提供される JBossPostgreSQL ユーティリティを使用して JRE をインストールした場合、次のコマンドを使用してインストーラを開始できます。

Linux または Solaris:

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

Windows:

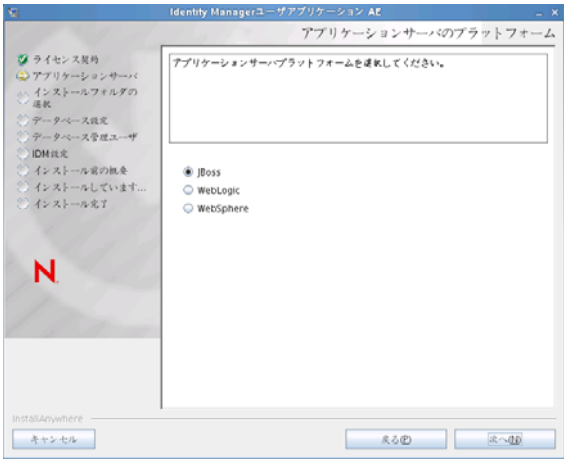
```
C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.6.0_14\bin\java.exe"
-jar IdmUserApp.jar
```

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

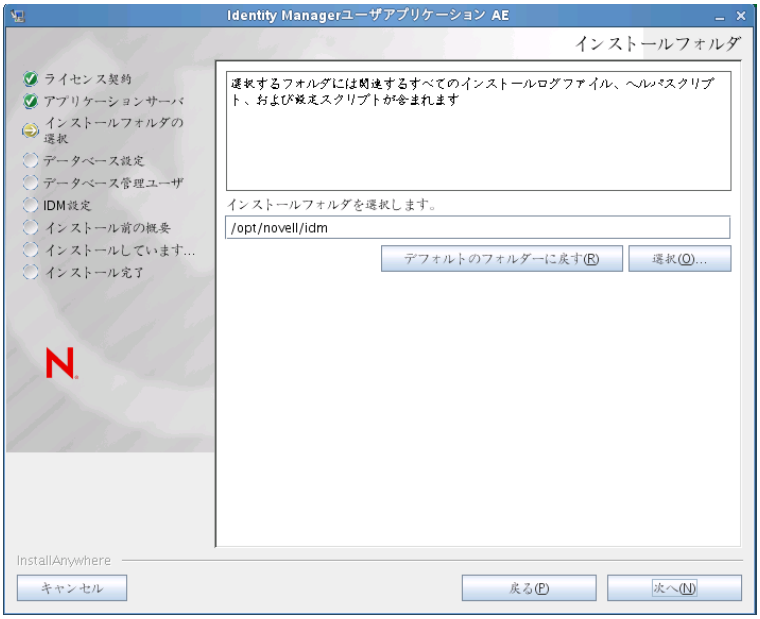
インストールプログラムを開始すると、言語を入力するよう次のように促されます。

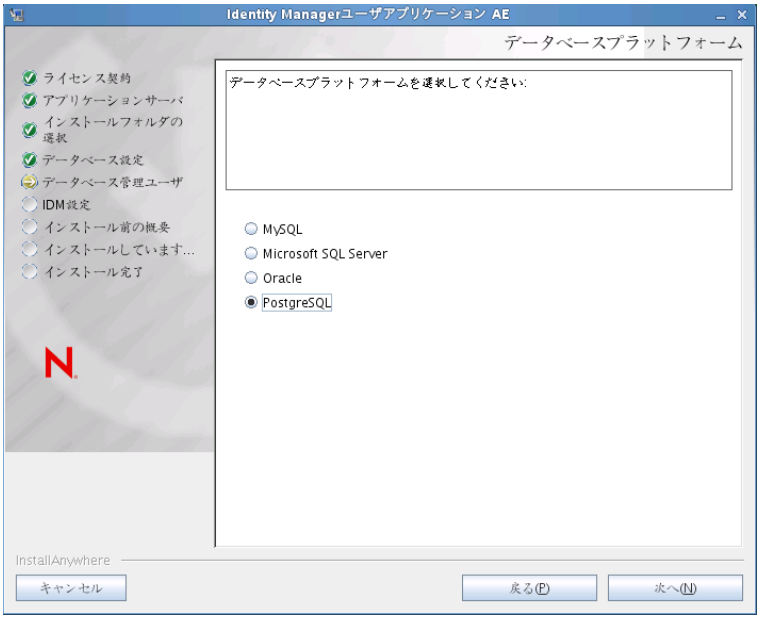
2 次の情報を使用して、言語を選択し、使用許諾契約を確認し、アプリケーションサーバプラットフォームを選択します。

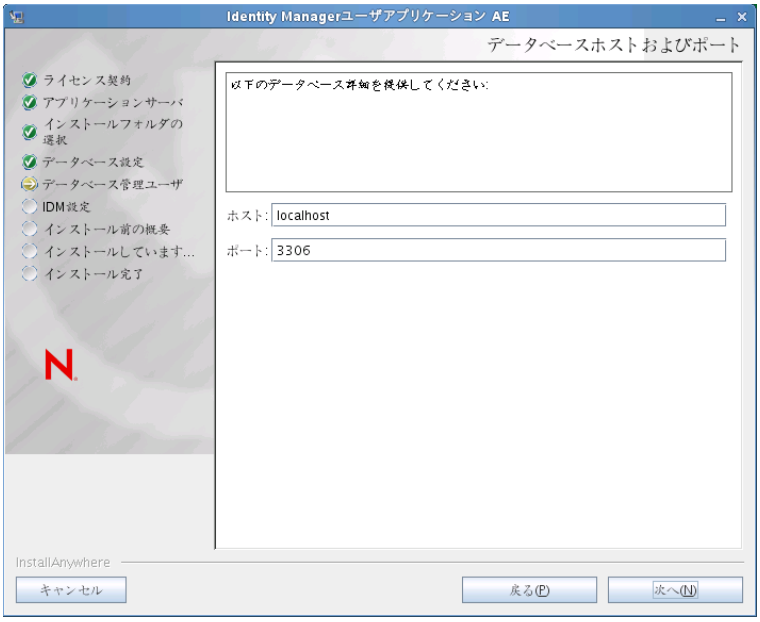
インストール画面	説明
ユーザアプリケーションインストール	インストールプログラムの言語を選択します。デフォルトでは、［英語］が選択されています。
使用許諾契約	使用許諾契約を読み、*［使用許諾契約の条件に同意します］*を選択します。

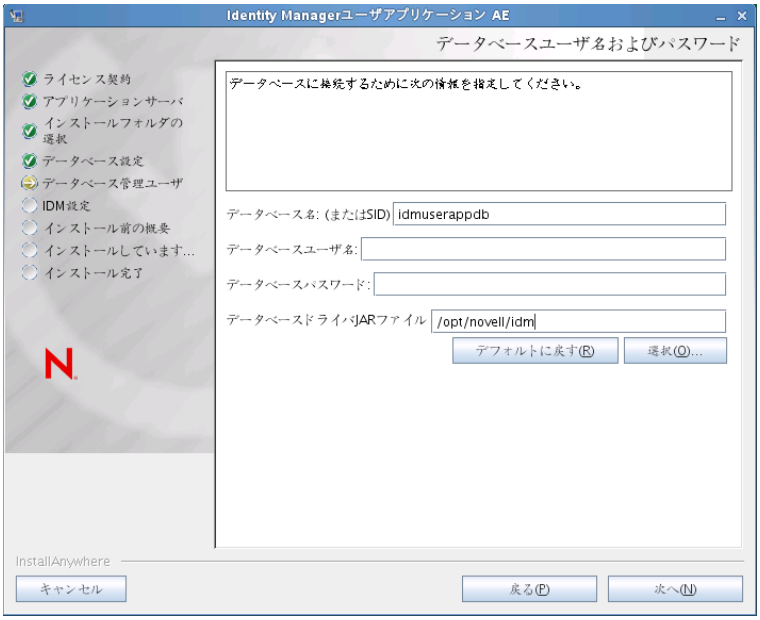
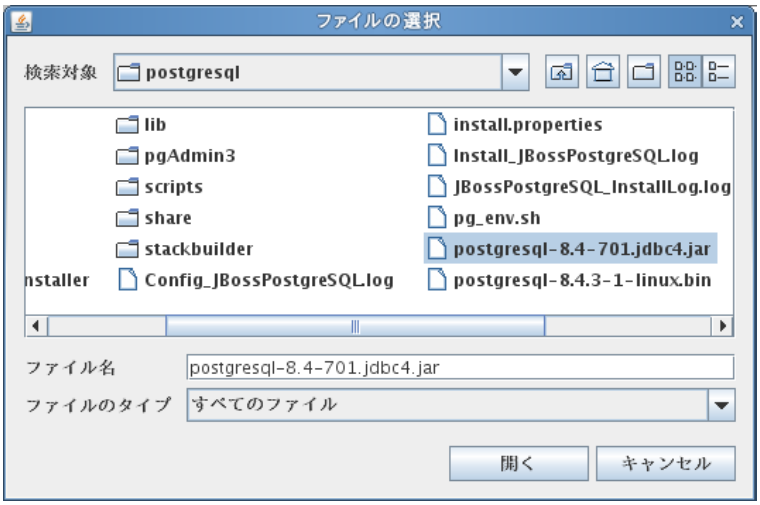
インストール画面	説明
アプリケーションサーバプラットフォーム	*[JBoss]* を選択します。  JBoss でインストールする場合、Sun の Java 環境を使用することによってインストールプログラムを開始する必要があります。アプリケーションサーバとして JBoss を選択し、インストールの開始に Sun の Java を使用しない場合、次のポップアップエラーメッセージが表示され、インストールは終了します。 

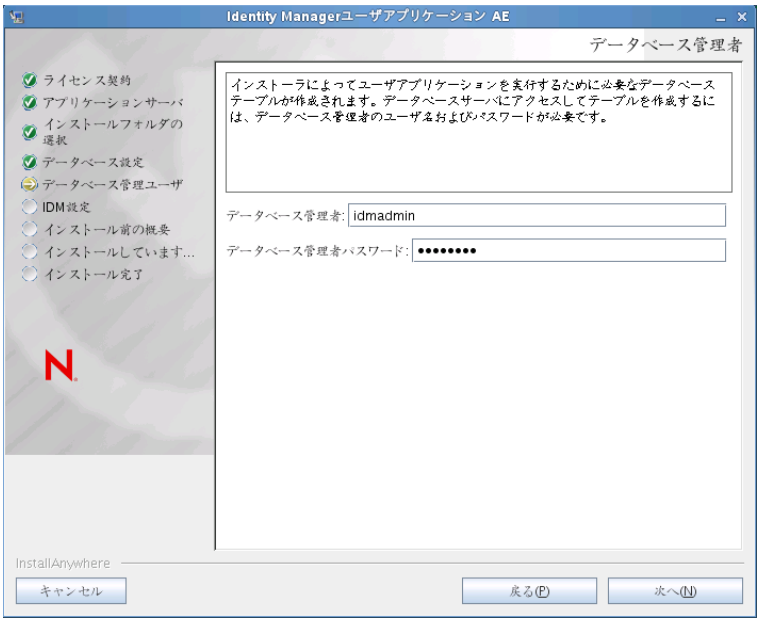
3 次の情報を使用して、インストールフォルダを選択し、データベースを設定します。

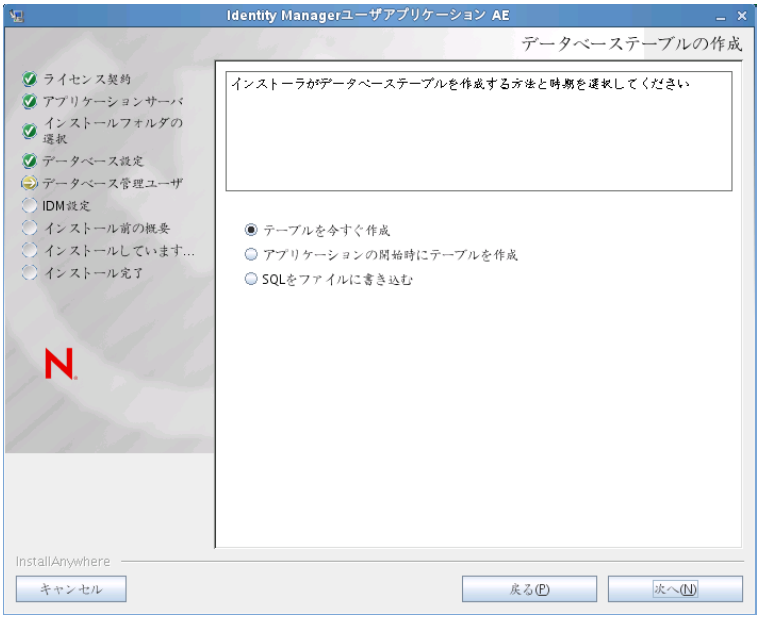
インストール画面	説明
インストールフォルダの選択	インストーラがファイルを配置する場所を指定します。 

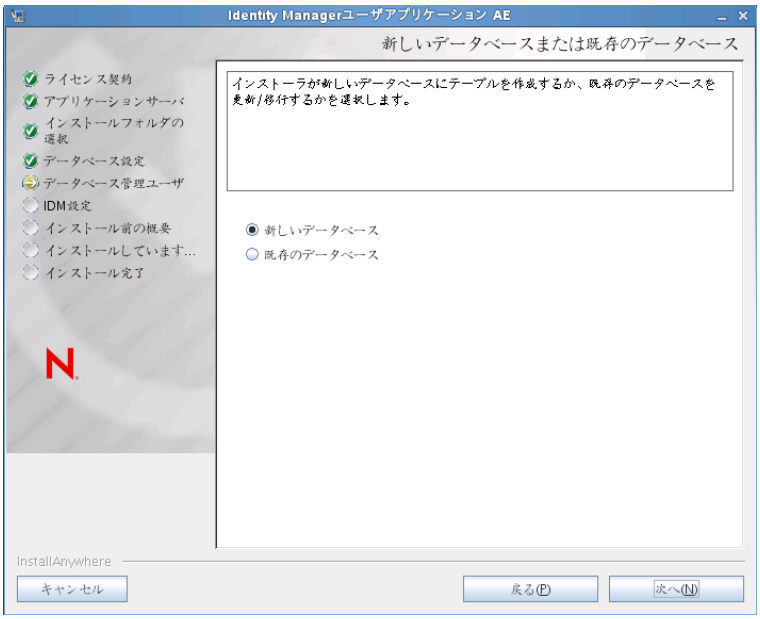
インストール画面	説明
データベースプラットフォーム	データベースプラットフォームの選択 :  データベースおよび JDBC ドライバはすでにインストールされている必要があります。JBoss の場合、オプションには次のプラットフォームが含まれます。 ◆ MySQL ◆ Microsoft SQL Server ◆ Oracle ◆ PostgreSQL

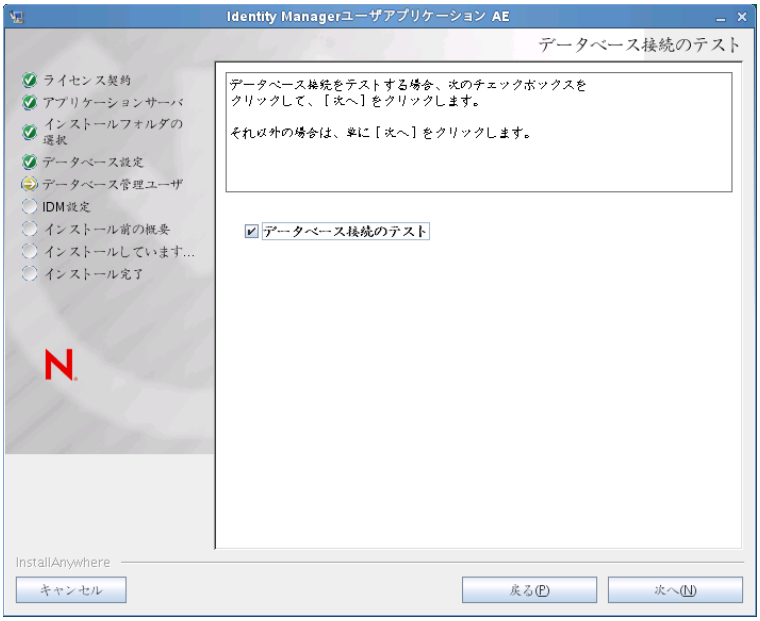
インストール画面	説明
データベースホストおよびポート	*ホスト*: データベースサーバのホスト名または IP アドレスを指定します。クラスタでは、クラスタの各メンバーには同じホスト名または IP アドレスを指定します。 *ポート*: データベースのリスナポート番号を指定します。クラスタの場合は、クラスタの各メンバーに同じポートを指定します。 

インストール画面	説明
データベースのユーザ名およびパスワード	*データベース名* (または SID): PostgreSQL、MySQL、または MS SQL Server の場合は、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。デフォルトのデータベース名は、idmuserappdb です。 *データベースユーザ名* : データベースユーザを指定します。クラスタでは、クラスタの各メンバーには同じデータベースユーザを指定します。 *データベースパスワード*: データベースパスワードを指定します。クラスタでは、クラスタの各メンバーには同じデータベースパスワードを指定します。 *データベース ドライバ JAR ファイル*: データベースサーバにシンクライアント JAR を指定します。これは必須です。  PostgreSQL の場合は、postgresql-8.4-701.jdbc4.jar ファイルを選択します。 

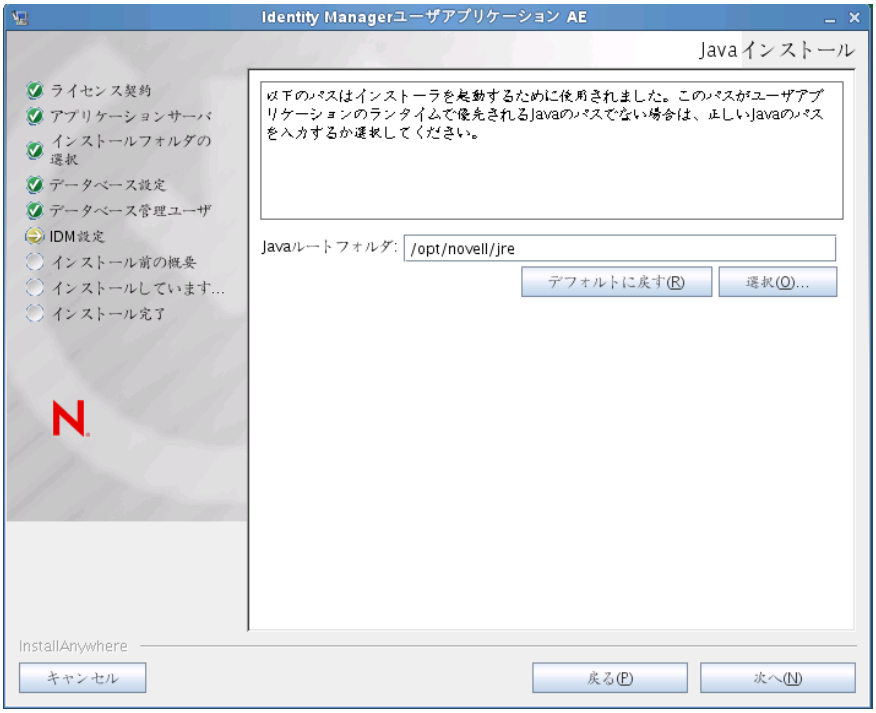
インストール画面	説明
データベース管理者	この画面には、［データベースユーザ名およびパスワード］ページから同じユーザ名とパスワードが事前に入力されています。以前に指定したデータベースユーザがデータベースサーバ内にテーブルを作成するための十分な許可を持っていない場合、必要な権限を持つ別のユーザ ID を入力する必要があります。 

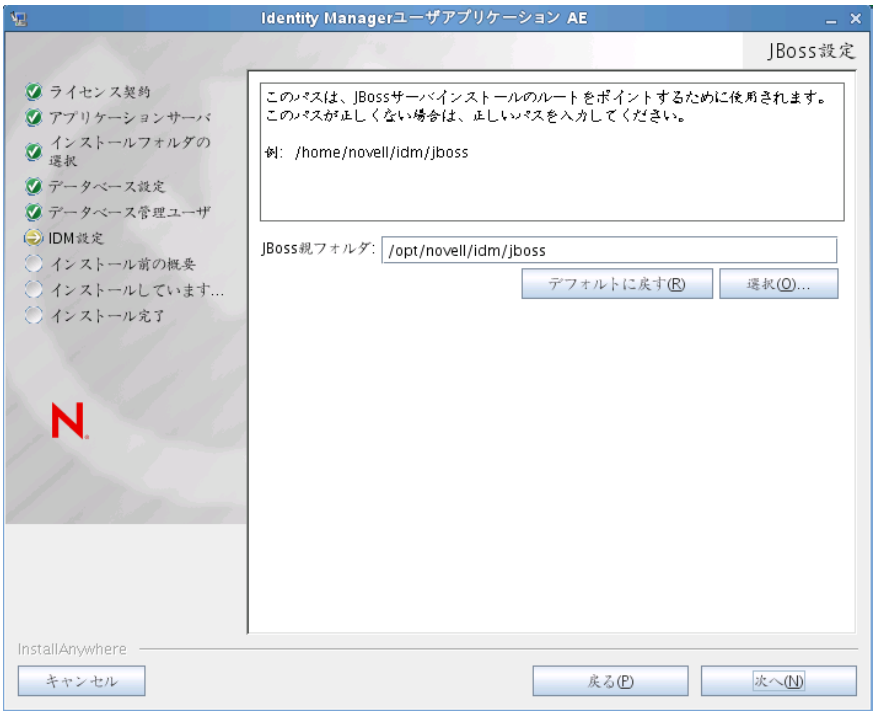
インストール画面	説明
データベーステーブルの作成	データベーステーブルを作成する必要がある場合に指定します。  [Create Database Tables (データベーステーブルの作成)] 画面では、インストール時、またはアプリケーションの起動時にテーブルを作成するオプションを選択できます。または、インストール時にスキーマファイルを作成することができます。このファイルを使用して、データベース管理者が後からテーブルを作成します。 スキーマファイルを生成する場合、*[SQL をファイルに書き込む]* チェックボックスをオンにし、*[スキーマ出力ファイル]* フィールドにファイルの名前を入力します。

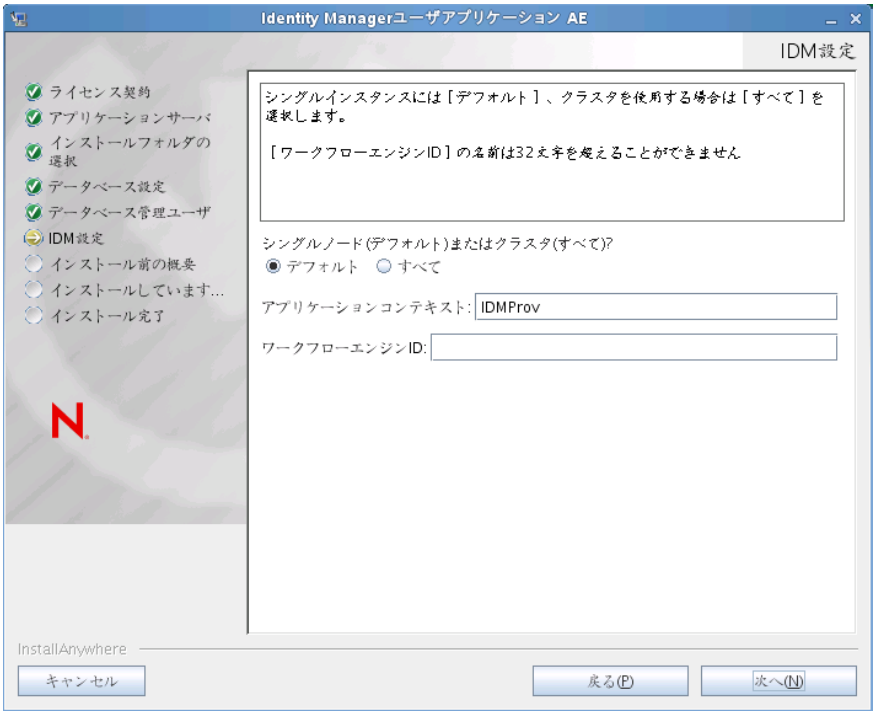
インストール画面	説明
新しいデータベースまたは既存のデータベース	使用するデータベースが新規または空の場合、*[新しいデータベース]* ボタンを選択します。データベースが以前のインストールに属する既存のものである場合、*[既存のデータベース]* ボタンを選択します。 

インストール画面	説明
データベース接続のテスト	前の画面で指定した情報が正しかったことを確認するには、*[データベース接続のテスト]* チェックボックスをオンにしてデータベース接続をテストします。  インストーラは、直接テーブルを作成するため、および .SQL ファイルを作成するための両方の場合にデータベースに接続する必要があります。データベース接続をテストして、それが失敗した場合でも、インストールを続行できます。その場合、『*ユーザアプリケーション：管理ガイド* (http://www.novell.com/documentation/idmrbpm40/agpro/?page=/documentation/idmrbpm40/agpro/data/bncf7rj.html)』で説明されるように、インストール後にテーブルを作成する必要があります。

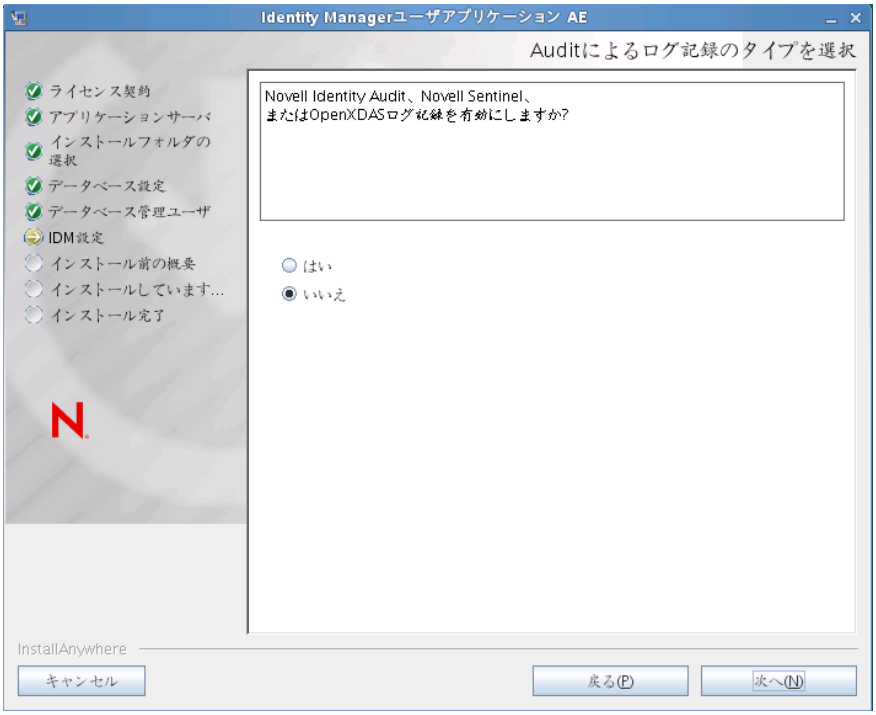
4 次の情報を使用して、Java、JBoss のインストール、および Identity Manager とともに監査設定とセキュリティを設定します。

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

インストール画面	説明
JBoss 環境設定	JBoss アプリケーションサーバを見つける場所をユーザアプリケーションに伝えます。 このインストール手順では、JBoss アプリケーションサーバはインストールされません。JBoss アプリケーションサーバのインストール手順については、17 ページの 「JBoss アプリケーションサーバと PostgreSQL データベースのインストール」を参照してください。 *JBoss Parent Folder (JBoss 親フォルダ)*: JBoss アプリケーションサーバの場所を指定します。 

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

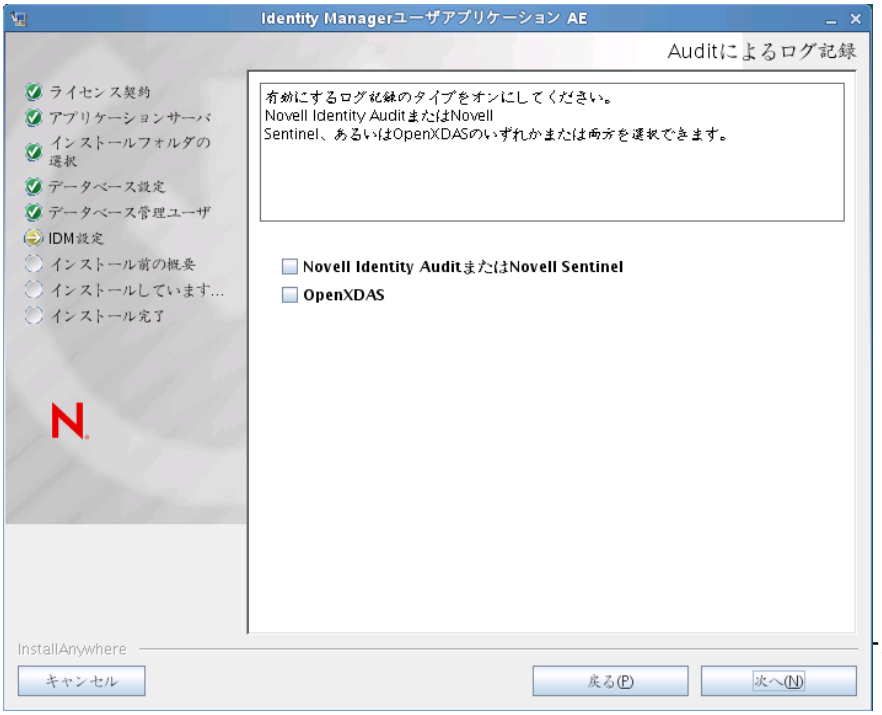
インストール画面	説明
Audit によるログ記録のタイプを選択	ログを有効にするには、*[はい]* をクリックします。ログを無効にするには、*[いいえ]* をクリックします。

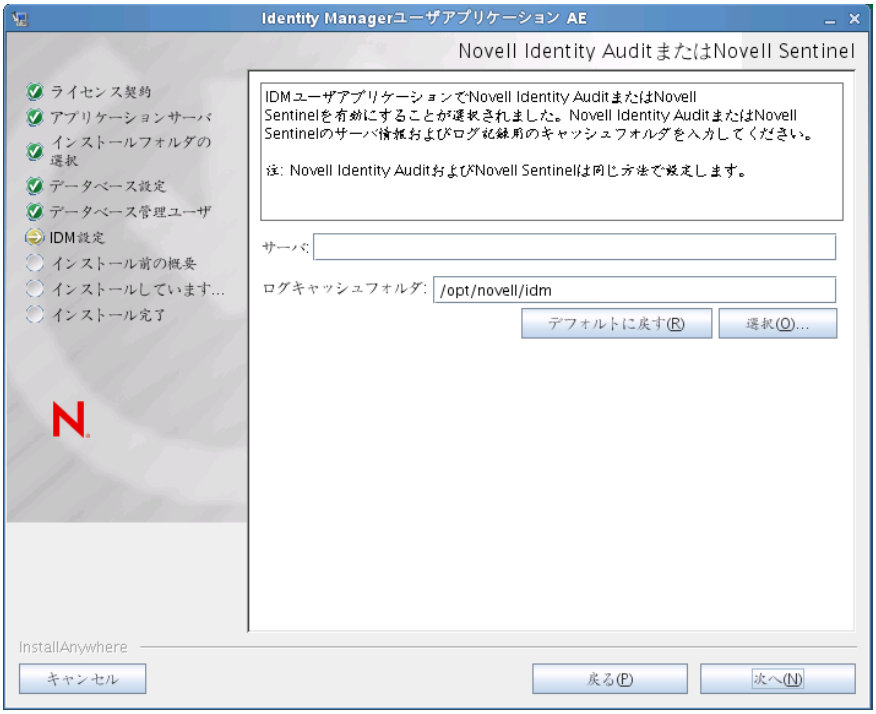


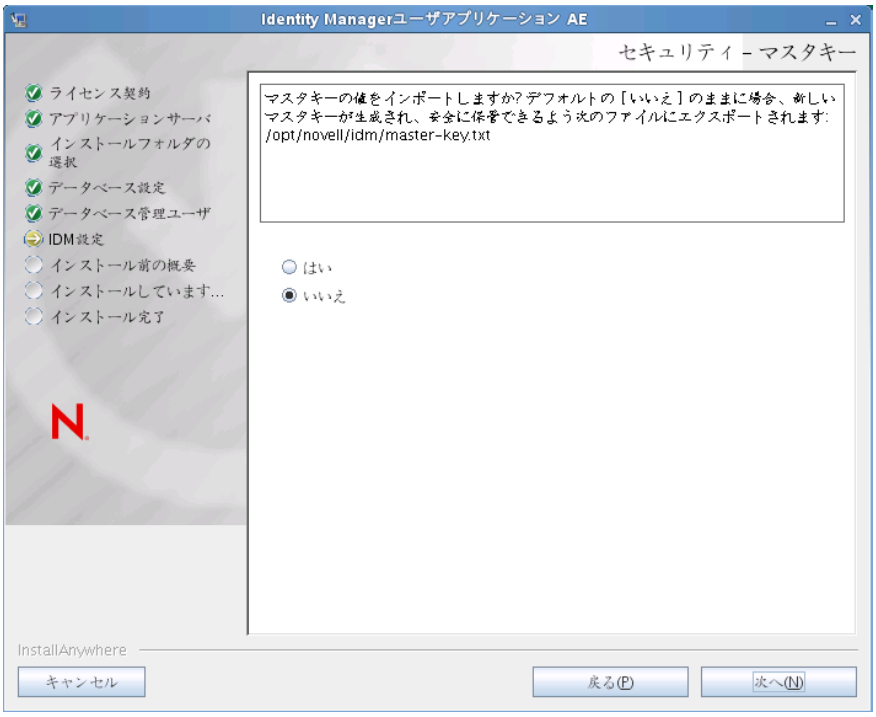
次のパネルでは、ログのタイプを指定するよう促されます。次のオプションから選択します。

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

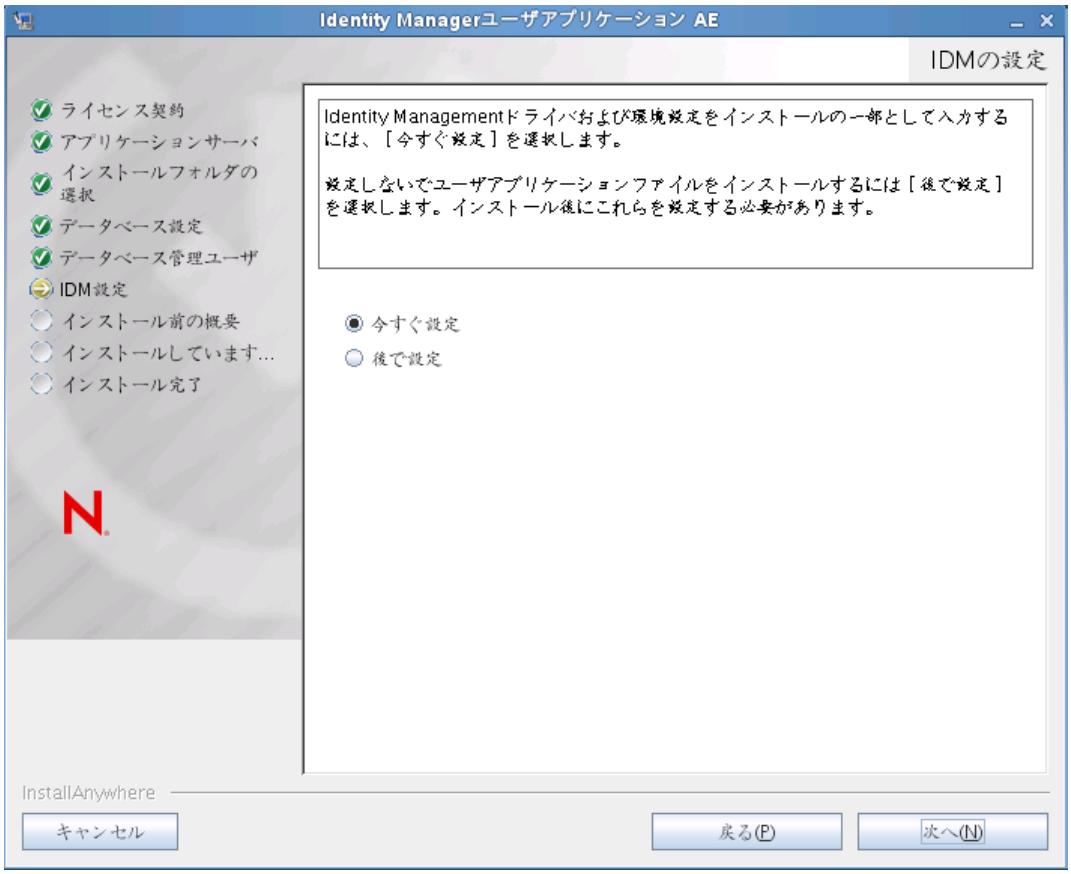
ログの設定の詳細については、『*ユーザアプリケーション: 管理ガイド*』を参照してください。



インストール画面	説明
Novell Identity Audit または Novell Sentinel	*サーバ*: ログを有効にする場合、サーバのホスト名または IP アドレスを指定します。ログをオフにする場合は、この値は無視されます。 *ログキャッシュフォルダ*: ログキャッシュのディレクトリを指定します。 

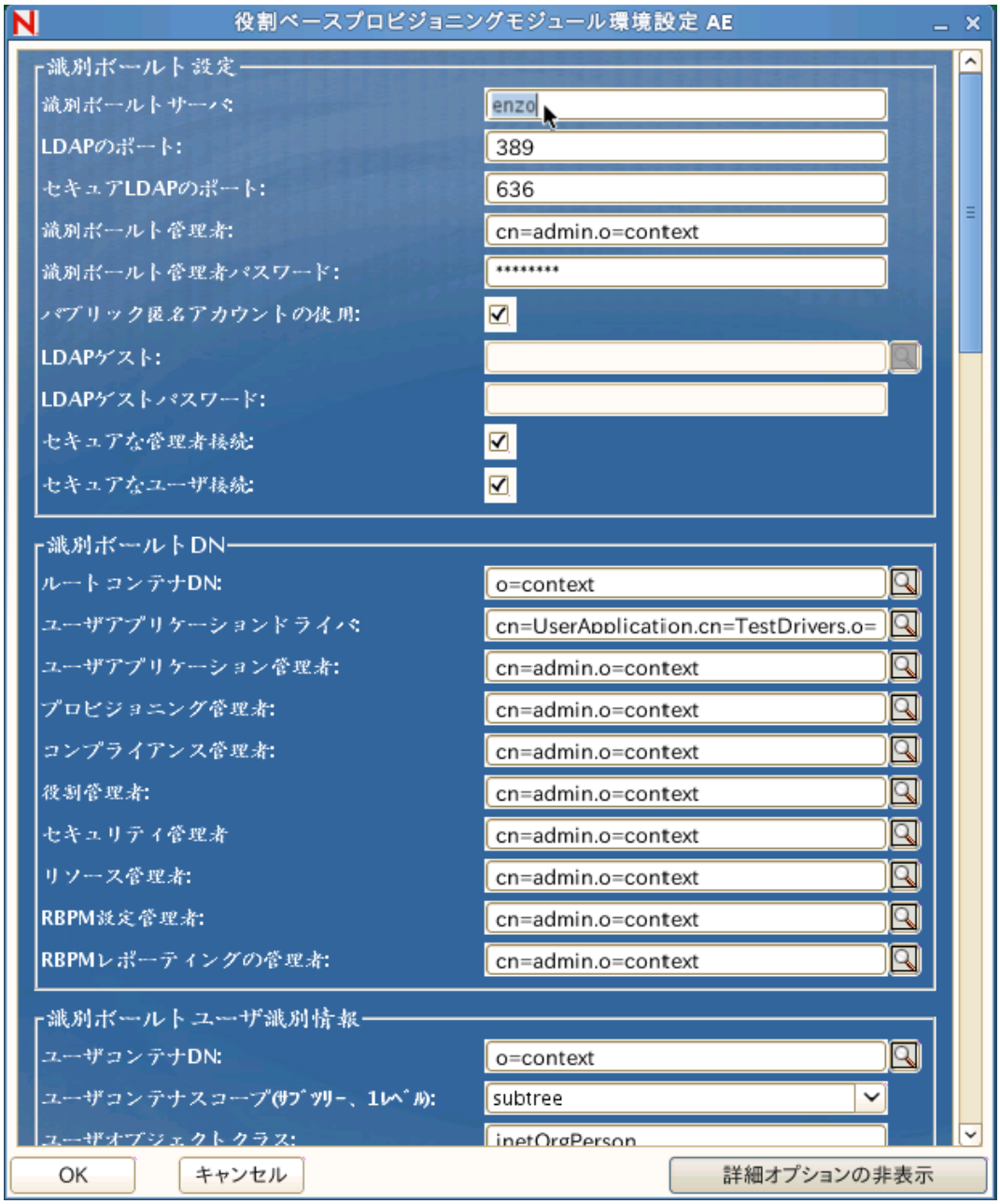
インストール画面	説明
セキュリティ - マスタキー	*はい*: 既存のマスタキーをインポートできます。既存の暗号化マスタキーをインポートするよう選択した場合は、該当するキーを切り取ってインストール手順のウィンドウに貼り付けます。 *いいえ*: 新規のマスタキーを作成します。インストール終了後、147 ページのセクション 9.1「マスタキーの記録」で示すように、マスタキーを手動で記録します。  インストール手順で、インストールディレクトリにある master-key.txt ファイルに暗号化マスタキーが書き込まれます。 既存のマスタキーをインポートする理由には、次のようなものがあります。 ◆ インストールファイルをステージングシステムから運用システムに移動中で、ステージングシステムで使用したデータベースへのアクセスを保持する場合。 ◆ ユーザアプリケーションを最初の JBoss クラスタのメンバーにインストールしており、現在はクラスタの次のメンバーにインストールしている場合 (同じマスタキーが必要)。 ◆ ディスク故障のため、ユーザアプリケーションを復元する必要がある場合。ユーザアプリケーションを再インストールして、以前のインストールで使用したのと同じ暗号化マスタキーを指定する必要があります。これによって、前に保存した暗号化データにアクセスできます。

5 この時点で RBPM を設定する場合は、*［Configure Now (今すぐ設定)］*を選択し、*［次へ］*をクリックします。



(この情報の入力を求められない場合、30 ページのセクション 2.5「Java Development Kit のインストール」で説明したステップを完了していない可能性があります。)

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



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

- ユーザコンテナ DN
- グループコンテナ DN

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

- プロビジョニング管理者
- コンプライアンス管理者
- 役割管理者

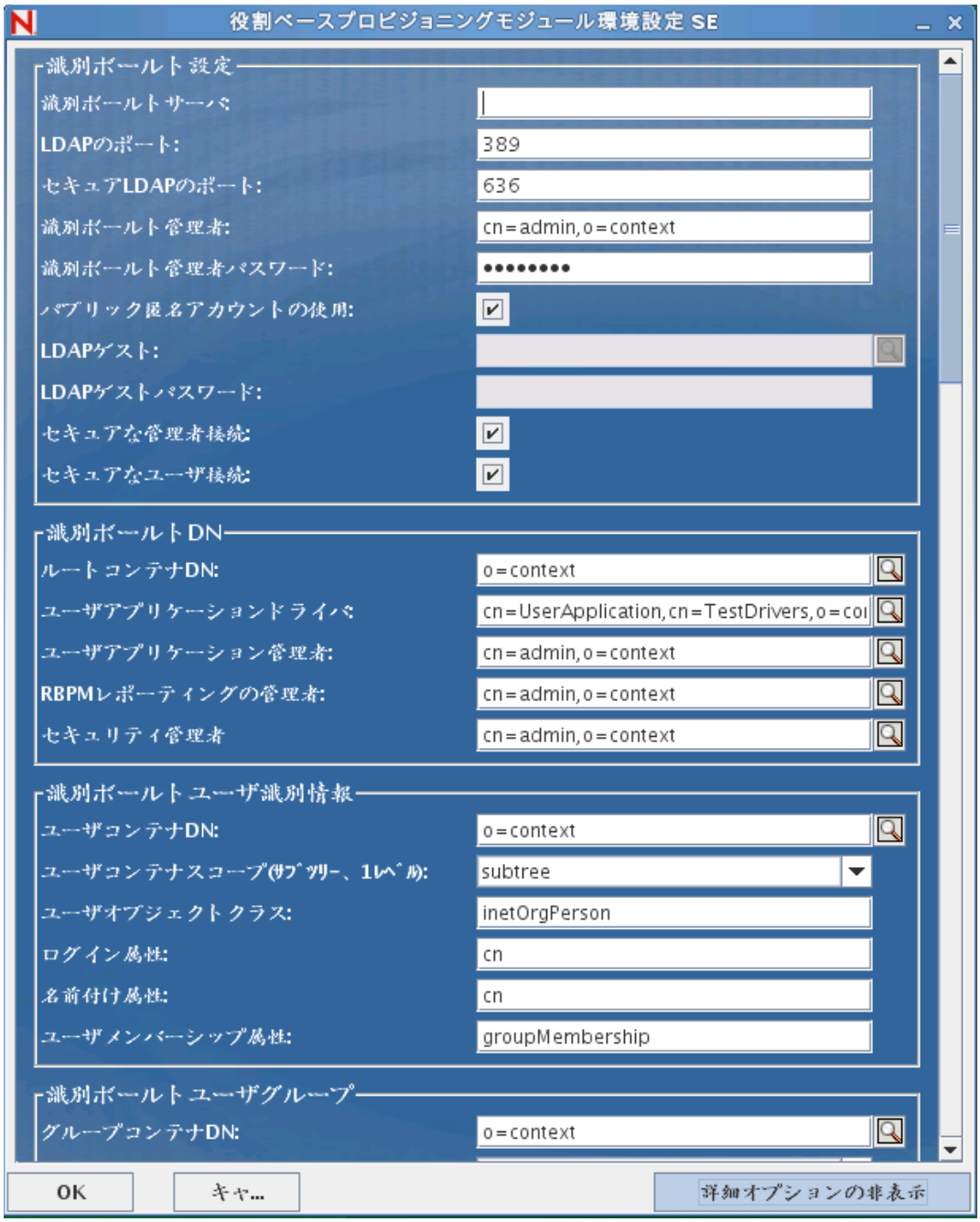
- セキュリティ管理者
- リソース管理者
- RBPM 設定管理者

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

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。

各オプションの詳細については、155 ページの付録 A「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。

Standard Edition のデフォルトビューには次のようなセキュリティフィールドのサブセットが表示されます。



Identity Manager 4.0.1 Standard Edition では、次の管理者のみ割り当てる必要があります。

- ユーザアプリケーション管理者
- RBPM レポーティング管理者
- セキュリティ管理者

注 : Standard Edition では、テストの目的の場合はセキュリティモデルがロックダウンされていません。したがって、セキュリティ管理者は、ドメイン管理者、委任された管理者、さらにはセキュリティ管理者などを割り当てることができます。ただし、こ

れらの高度な機能の使用は、運用環境ではサポートされません。運用環境では、すべての管理者の割り当てがライセンスによって制限されます。Novell は、運用環境が契約内容に必ず準拠するように、監査データベース内に監視データを収集します。その上、1 人のユーザのみにセキュリティ管理者としての許可を与えることを推奨します。

6 インストールを完了するには、次の情報を使用します。

インストール画面	説明
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。

インストーラは novlua ユーザを作成します : インストーラは novlua という名前で新しいユーザを作成します。jboss_init スクリプトは、JBoss をこのユーザで実行し、JBoss ファイルで定義されている権限がこのユーザに設定されます。

5.1.1 インストールとログファイルの表示

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

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

5.2 インストールのテスト

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

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

/etc/init.d/jboss_init start (Linux および Solaris)

start-jboss.bat (Windows)

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 -Dfile.encoding=UTF-8 -Dsun.jnu.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:MaxPermSize=512m

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ドライバの上に表示されている手順に従って、役割およびリソースのサービスドライバを開始します。

5 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 URL にアクセスします。

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

この URL では、*hostname*: *port* はアプリケーションサーバのホスト名で (たとえば、「myserver.domain.com」)、ポートはアプリケーションサーバのポートです (たとえば、JBoss のデフォルトは「8180」)。*ApplicationName* は、デフォルトで *IDMProv* 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。

6 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、152 ページのセクション 9.9「トラブルシューティング」を参照します。

WebSphere でのユーザアプリケーションのインストール

6

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

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

ルート以外のユーザとしてインストーラを実行します。

データマイグレーション : 移行の詳細については、『*ユーザアプリケーション : マイグレーションガイド* (http://www.novell.com/documentation/idm40/index.html)』を参照してください。

6.1 ユーザアプリケーション WAR のインストールおよび環境設定

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

1. インストールファイルが含まれるディレクトリに移動します。
2. IBM JDK に無制限のポリシーファイルを適用する必要があります。WebSphere のマニュアルを参照して、IBM が提供するこれらのファイルおよびそれらの適用方法の説明へのリンクを入手できます。インストールをこれ以上続行する前に、これらのファイルを IBM JDK 環境に適用します。無制限のポリシーファイル用の JAR ファイルは、JAVA_HOME\jre\lib\security に配置する必要があります。

   これらの制限なしポリシーファイルがないと、「無効なキーサイズ」というエラーが発生します。このプログラムの根本原因は制限なしポリシーファイル欠如です。したがって必ず正しい IBM JDK を使用してください。
3. IBM Java 環境を使用して、次に示すインストーラを開始します。

   Linux または Solaris:

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

   Windows:

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

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

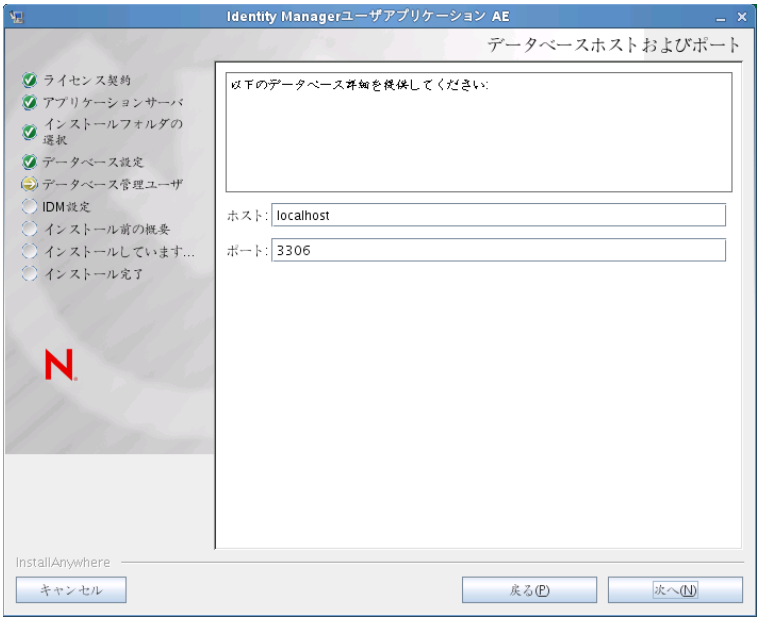
4 言語を選択し、使用許諾契約を確認し、アプリケーションサーバプラットフォームを選択するには、次の情報を使用します。

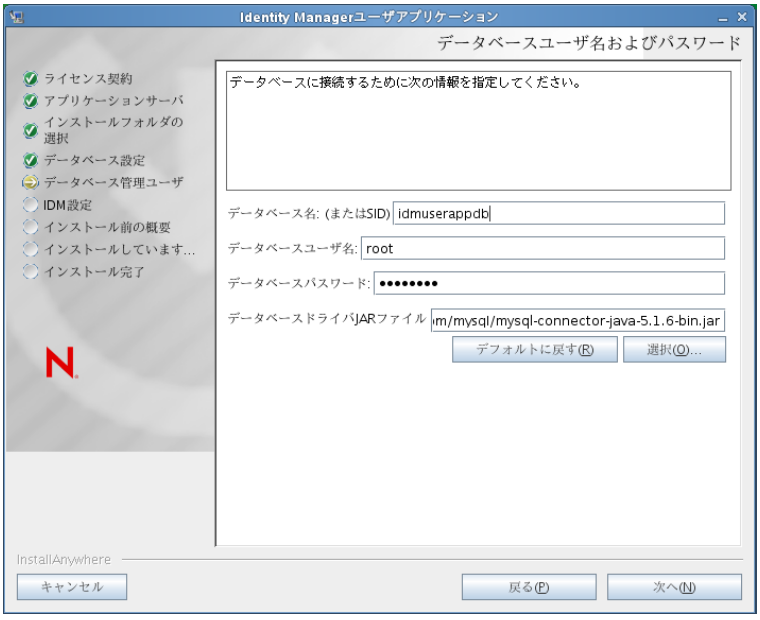
インストール画面	説明
ユーザアプリケーションインストール	インストールプログラムの言語を選択します。デフォルトでは、［英語］が選択されています。
使用許諾契約	使用許諾契約を読み、*［使用許諾契約の条件に同意します］*を選択します。

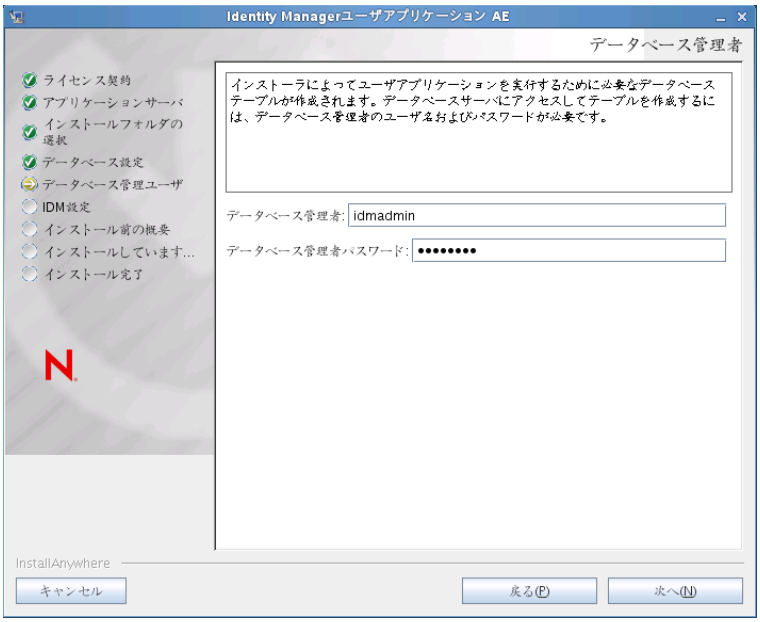
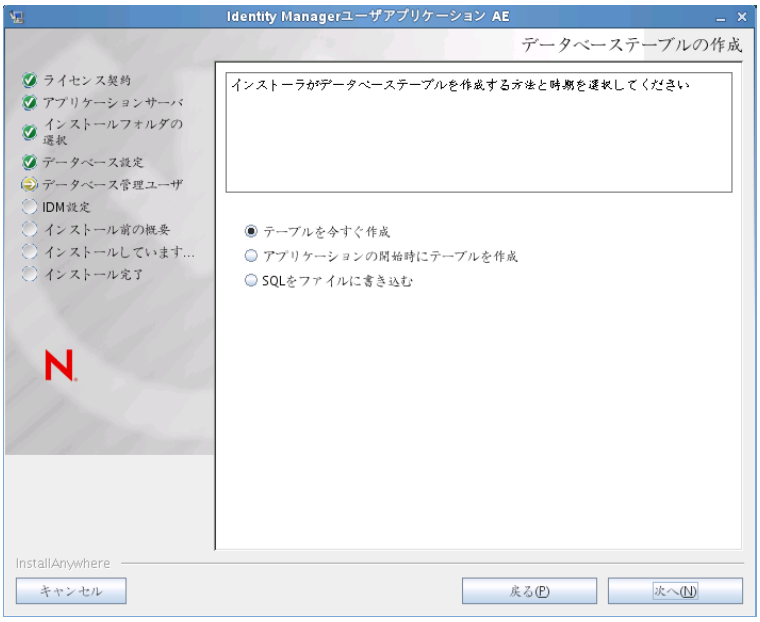
インストール画面	説明
アプリケーションサーバプラットフォーム	*WebSphere* を選択します。 ユーザアプリケーションの WAR ファイルがインストーラとは別のディレクトリにある場合は、インストーラによって WAR へのパスを入力するようメッセージが表示されます。 WAR がデフォルトの場所にある場合は、*[デフォルトのファイルに戻す]* をクリックできます。または、WAR ファイルの場所を指定する場合は、*[選択]* をクリックして場所を選択します。 WebSphere でインストールする場合、IBM Java 環境を使用することによってインストールプログラムを開始する必要があります。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

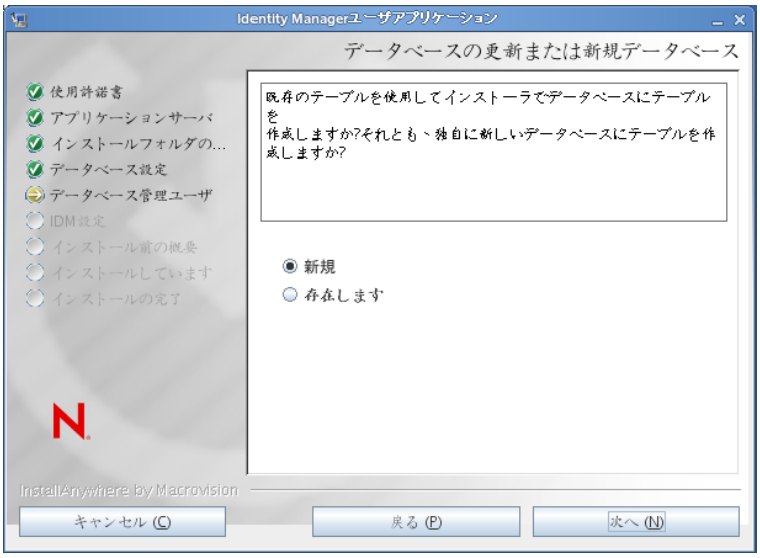
5 次の情報を使用して、インストールフォルダを選択し、データベースを設定します。

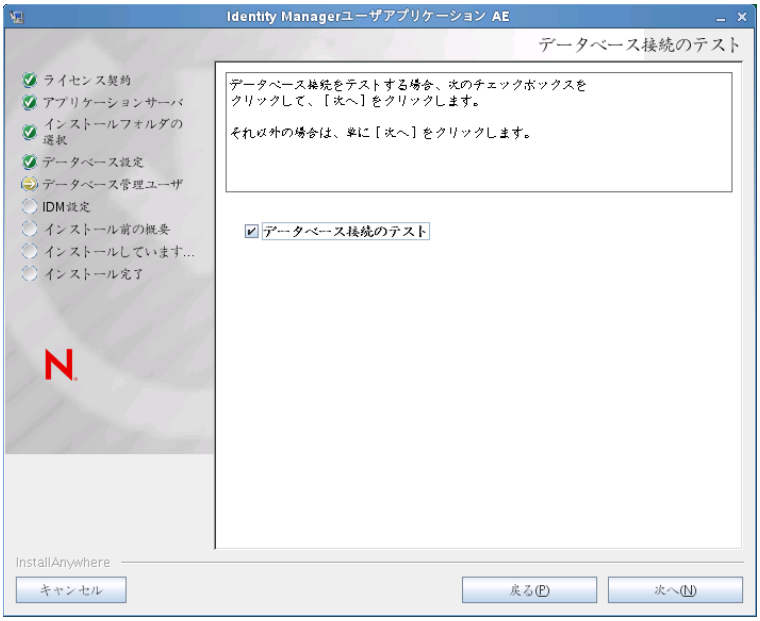
インストール画面	説明
インストールフォルダの選択	インストーラがファイルを配置する場所を指定します。
データベースプラットフォーム	データベースプラットフォームを選択します。データベースおよび JDBC ドライバはすでにインストールされている必要があります。WebSphere の場合、オプションには次のプラットフォームが含まれます。 ◆ Oracle ◆ Microsoft SQL Server ◆ IBM DB2 ◆ PostgreSQL

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

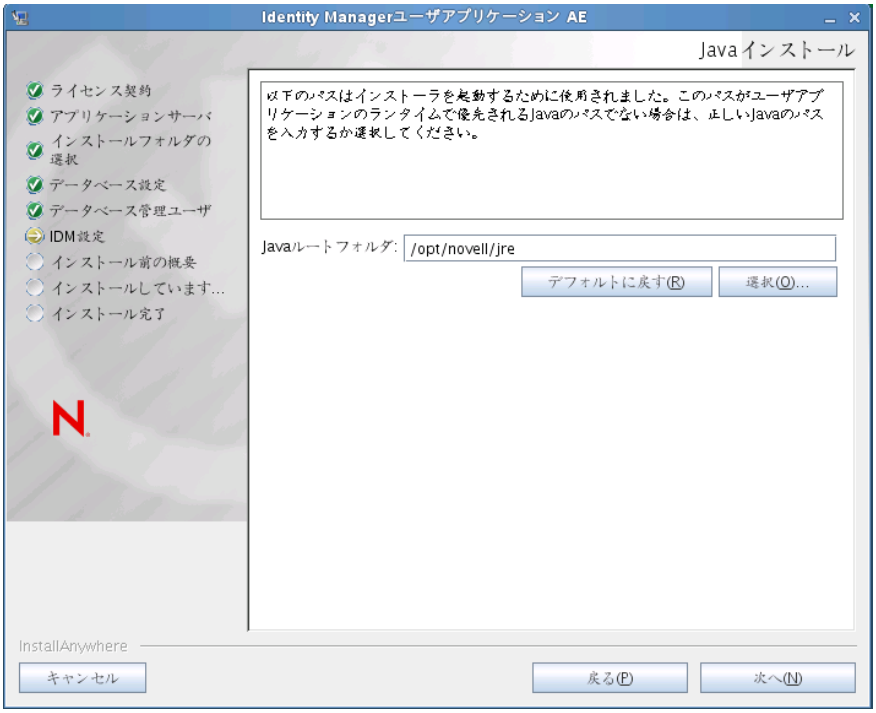
インストール画面	説明
データベースのユーザ名およびパスワード	*データベース名* (または SID): DB2、MS SQL Server、または PostgreSQL では、事前に設定したデータベース名を入力します。Oracle の場合は、前に作成した Oracle システム ID (SID) を指定します。クラスタでは、クラスタの各メンバーには同じデータベース名または SID を指定します。 *データベースユーザ名* : データベースユーザを指定します。クラスタでは、クラスタの各メンバーには同じデータベースユーザを指定します。 *データベースパスワード*: データベースパスワードを指定し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

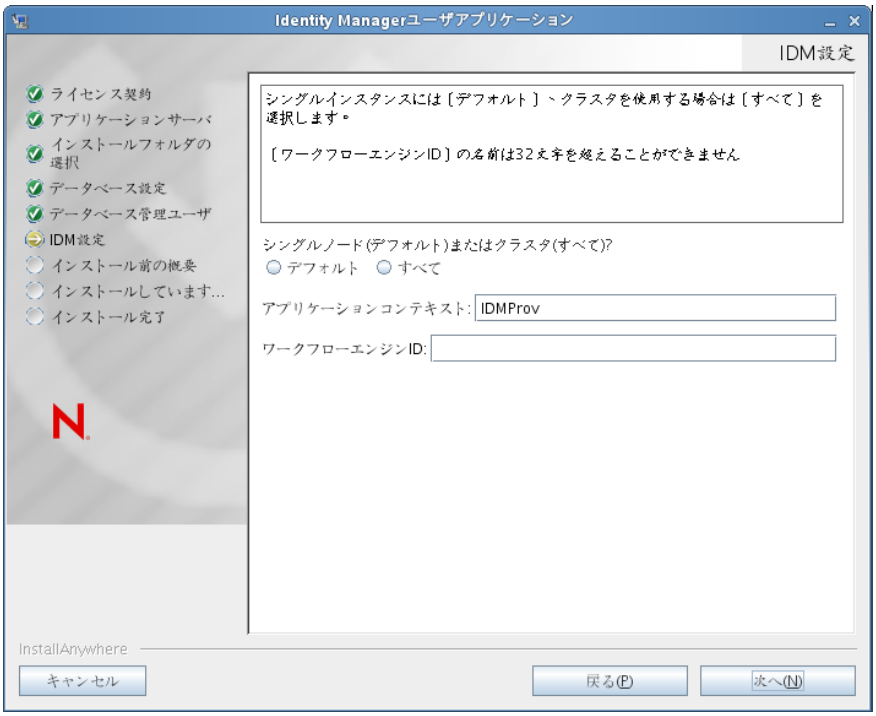
インストール画面	説明
データベース管理者	この画面には、［データベースユーザ名およびパスワード］ページから同じユーザ名とパスワードが事前に入力されています。以前に指定したデータベースユーザがデータベースサーバ内にテーブルを作成するための十分な許可を持っていない場合、必要な権限を持つ別のユーザ ID を入力する必要があります。 
データベーステーブルの作成	データベーステーブルを作成する必要がある場合に指定します。 

インストール画面	説明
新しいデータベースまたは既存のデータベース	使用するデータベースが新規または空の場合、*[新しいデータベース]* ボタンを選択します。データベースが以前のインストールに属する既存のものである場合、*[既存のデータベース]* ボタンを選択します。 

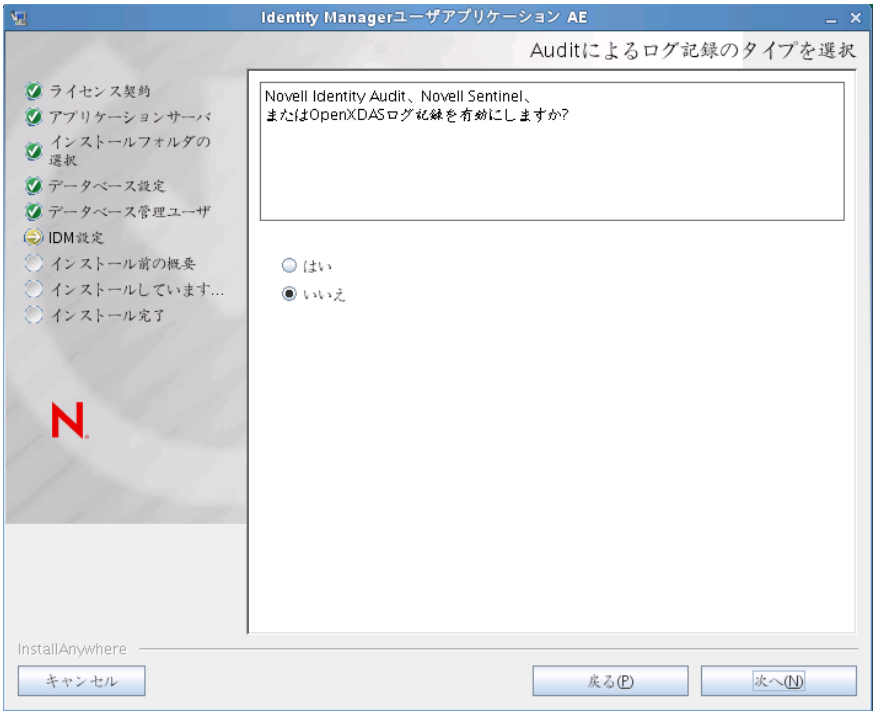
インストール画面	説明
データベース接続のテスト	前の画面で指定した情報が正しかったことを確認するには、*[データベース接続のテスト]* チェックボックスをオンにしてデータベース接続をテストします。  インストーラは、直接テーブルを作成するため、および .SQL ファイルを作成するための両方の場合にデータベースに接続する必要があります。データベース接続をテストして、それが失敗した場合でも、インストールを続行できます。その場合、『*ユーザアプリケーション：管理ガイド* (http://www.novell.com/documentation/idm40/agpro/?page=/documentation/idm40/agpro/data/bncf7rj.html)』で説明されるように、インストール後にテーブルを作成する必要があります。

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

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

インストール画面	説明
IDM 環境設定	*アプリケーションコンテキスト*: アプリケーションサーバの環境設定の名前、アプリケーション WAR ファイルの名前、および URL コンテキストの名前です。インストールスクリプトによってサーバの環境設定が作成され、デフォルト名で *アプリケーション名*に基づく環境設定が作成されます。ユーザアプリケーションをブラウザから開始する場合は、アプリケーション名を書き留め、アプリケーション名を URL に含めてください。 

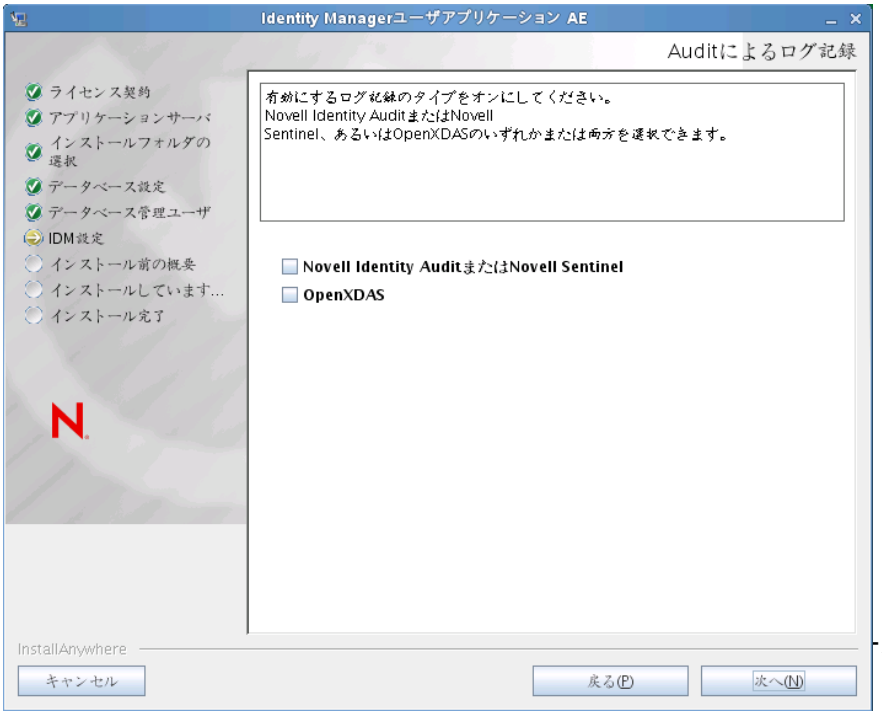
インストール画面	説明
Audit によるログ記録のタイプを選択	ログを有効にするには、*[はい]* をクリックします。ログを無効にするには、*[いいえ]* をクリックします。



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

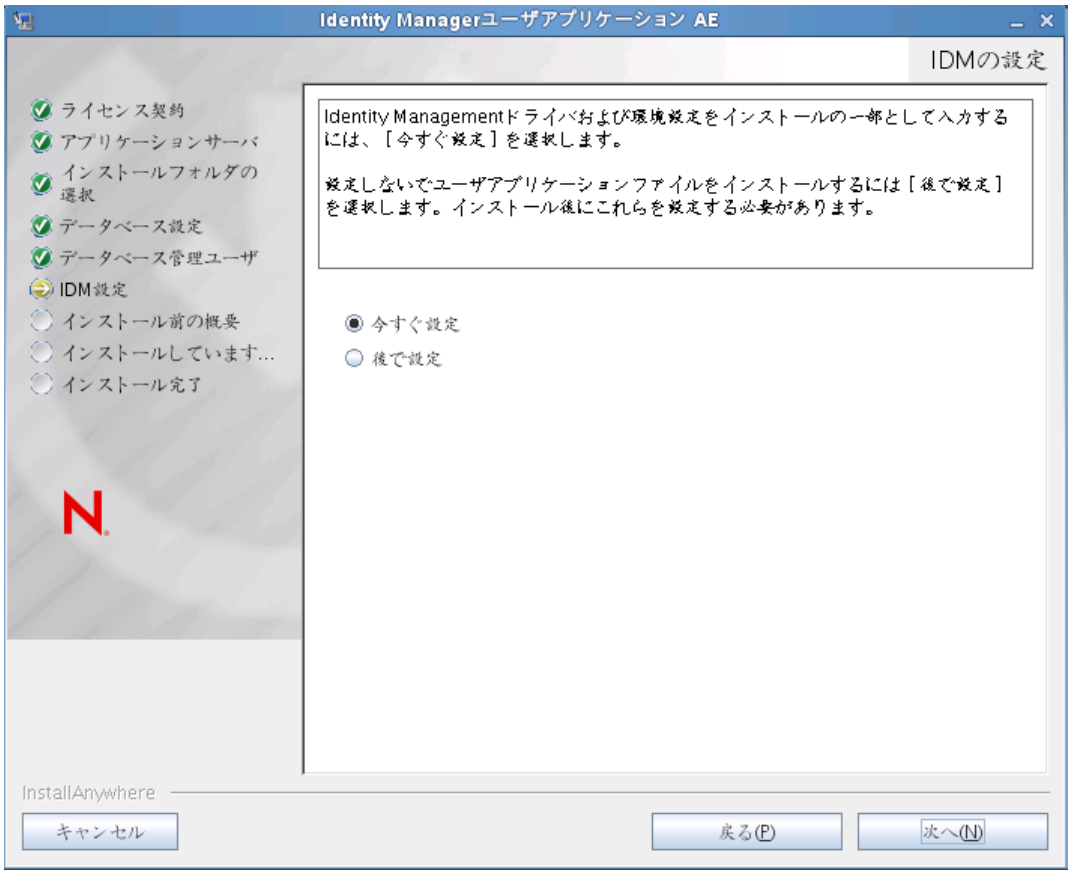
- *Novell Identity Audit または Novell Sentinel*: ユーザアプリケーション用の Novell クライアントを使用してログを有効にします。
- *OpenXDAS*: OpenXDAS ログサーバにイベントが記録されます。

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



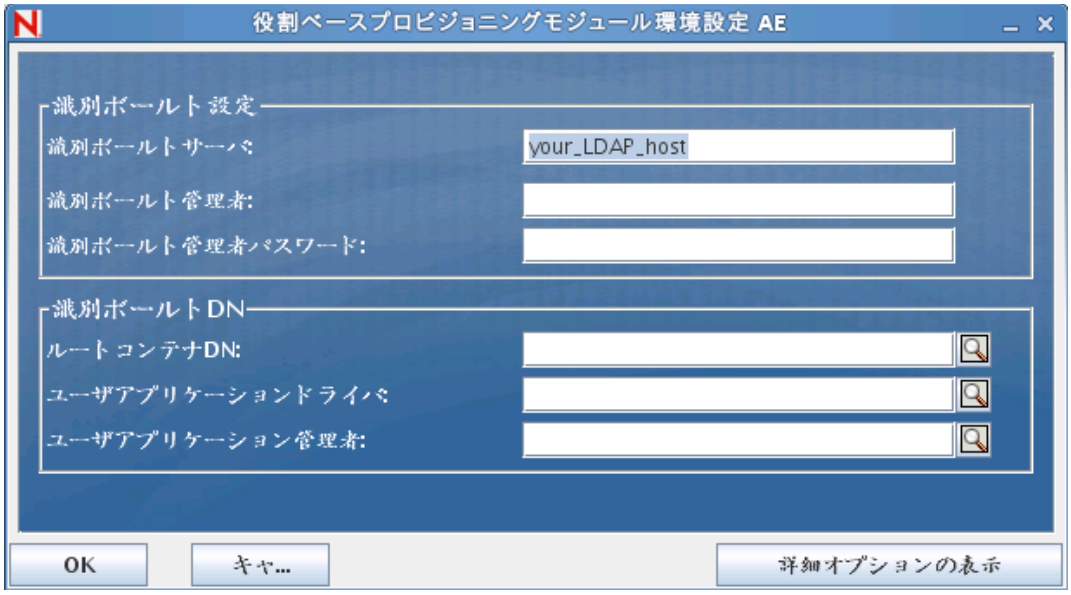
インストール画面	説明
Novell Identity Audit または Novell Sentinel	*サーバ*: ログを有効にする場合、サーバのホスト名または IP アドレスを指定します。ログをオフにする場合は、この値は無視されます。 *ログキャッシュフォルダ*: ログキャッシュのディレクトリを指定します。
セキュリティ - マスタキー	*はい*: 既存のマスタキーをインポートできます。既存の暗号化マスタキーをインポートするよう選択した場合は、該当するキーを切り取ってインストール手順のウィンドウに貼り付けます。 *いいえ*: 新規のマスタキーを作成します。インストール終了後、147 ページのセクション 9.1「マスタキーの記録」で示すように、マスタキーを手動で記録します。 インストール手順で、インストールディレクトリにある master-key.txt ファイルに暗号化マスタキーが書き込まれます。 既存のマスタキーをインポートする理由には、次のようなものがあります。 ◆ インストールファイルをステージングシステムから運用システムに移動中で、ステージングシステムで使用したデータベースへのアクセスを保持する場合。 ◆ ユーザアプリケーションを最初のクラスタのメンバーにインストールしており、現在はクラスタの次のメンバーにインストールしている場合 (同じマスタキーが必要)。 ◆ ディスク故障のため、ユーザアプリケーションを復元する必要がある場合。ユーザアプリケーションを再インストールして、以前のインストールで使用したのと同じ暗号化マスタキーを指定する必要があります。これによって、前に保存した暗号化データにアクセスできます。

7 この時点で RBPM を設定する場合は、*[Configure Now (今すぐ設定)]* を選択し、*[次へ]* をクリックします。



(この情報の入力を求められない場合、30 ページのセクション 2.5「Java Development Kit のインストール」で説明したステップを完了していない可能性があります。)

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



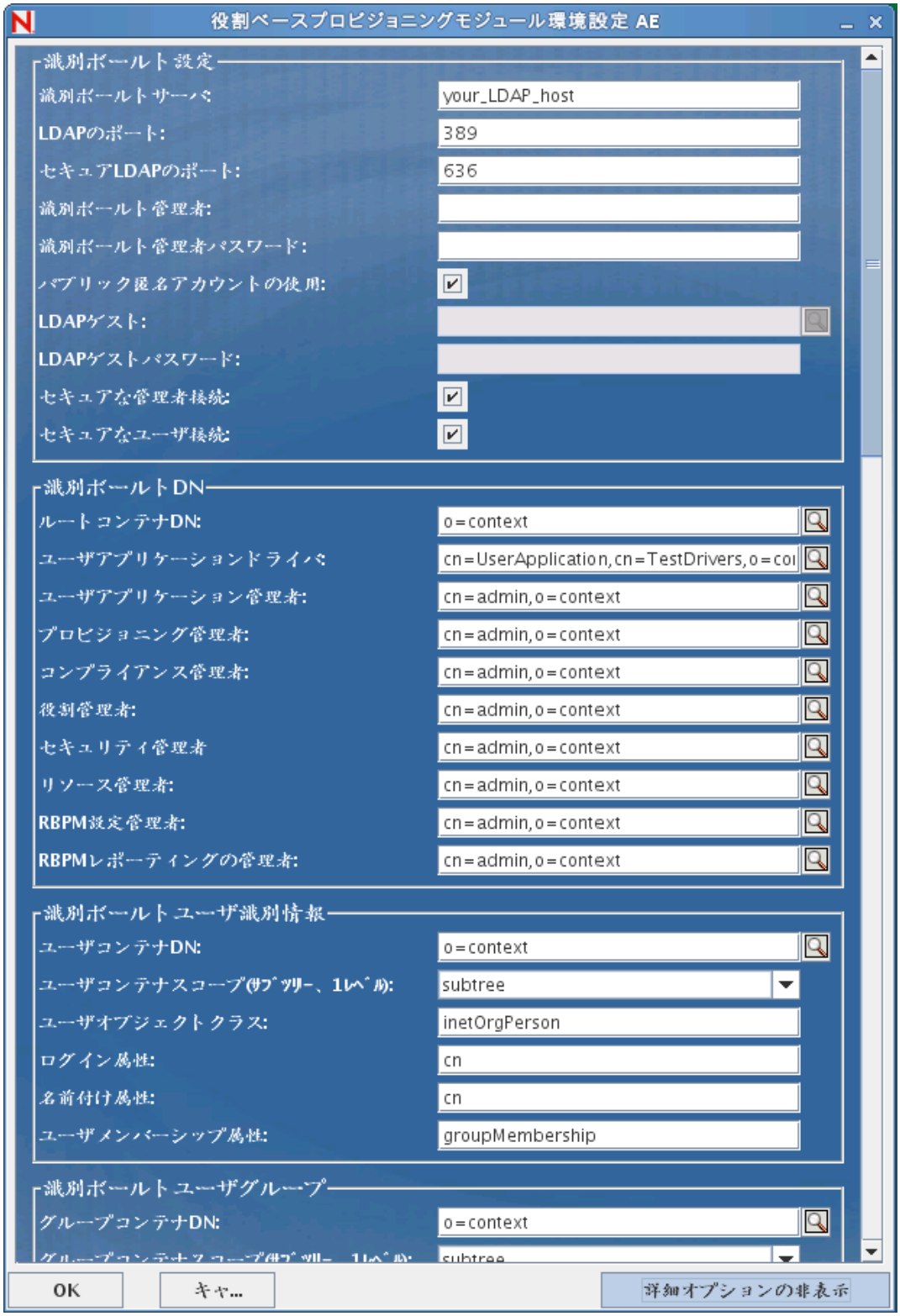
インストールプログラムはルートコンテナ DN から値を取得し、それを次の値に適用します。

- ユーザコンテナ DN
- グループコンテナ DN

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

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

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


役割ベースプロビジョニングモジュール環境設定 AE
識別ボールト設定
識別ボールトサーバ:
your_LDAP_host
LDAPのポート:
389
セキュアLDAPのポート:
636
識別ボールト管理者:
識別ボールト管理者パスワード:
パブリック匿名アカウントの使用:
LDAPゲスト:
LDAPゲストパスワード:
セキュアな管理者接続:
セキュアなユーザ接続:
識別ボールトDN
ルートコンテナDN:
o=context
ユーザアプリケーションドライバ:
cn=UserApplication,cn=TestDrivers,o=co
ユーザアプリケーション管理者:
cn=admin,o=context
プロビジョニング管理者:
cn=admin,o=context
コンプライアンス管理者:
cn=admin,o=context
役割管理者:
cn=admin,o=context
セキュリティ管理者
cn=admin,o=context
リソース管理者:
cn=admin,o=context
RBPM設定管理者:
cn=admin,o=context
RBPMレポーティングの管理者:
cn=admin,o=context
識別ボールトユーザ識別情報
ユーザコンテナDN:
o=context
ユーザコンテナスコープ(サブツリー、1レベル):
subtree
ユーザオブジェクトクラス:
inetOrgPerson
ログイン属性:
cn
名前付け属性:
cn
ユーザメンバーシップ属性:
groupMembership
識別ボールトユーザグループ
グループコンテナDN:
o=context
subtree
OK
キャ...
詳細オプションの非表示

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。

各オプションの詳細については、155 ページの付録 A「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。

8 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
インストール前の概要	［インストール前の概要］ページを読んで、インストールパラメータの選択を確認します。 必要に応じて、*［戻る］* を使用して前のインストールページに戻り、インストールパラメータを変更します。 ユーザアプリケーション環境設定ページでは値は保存されないため、インストールの前のページを再指定した後に、ユーザアプリケーション環境設定の値を再入力する必要があります。インストールおよび環境設定パラメータで納得いく設定ができたら、［インストール前の概要］ページに戻り、*［インストール］* をクリックします。
インストールの完了	インストールの終了が示されます。

6.1.1 インストールログファイルの表示

エラーが発生せずにインストールが完了した場合は、103 ページのセクション 6.2.2「ユーザアプリケーション環境設定ファイルと JVM システムプロパティの追加」に進みます。

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

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

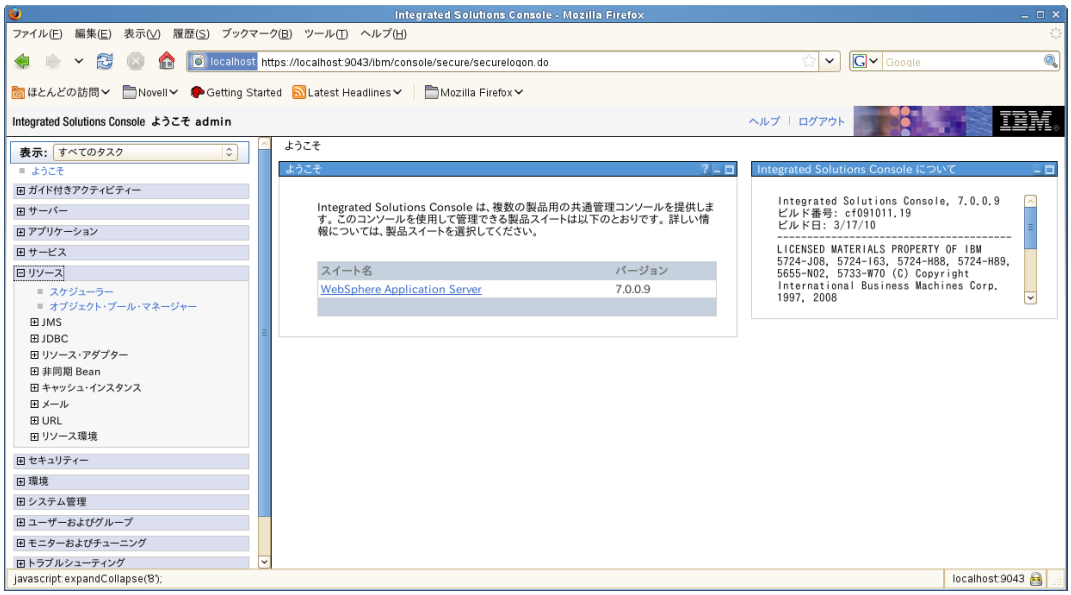
6.2 WebSphere 環境の環境設定

6.2.1 接続プールの設定

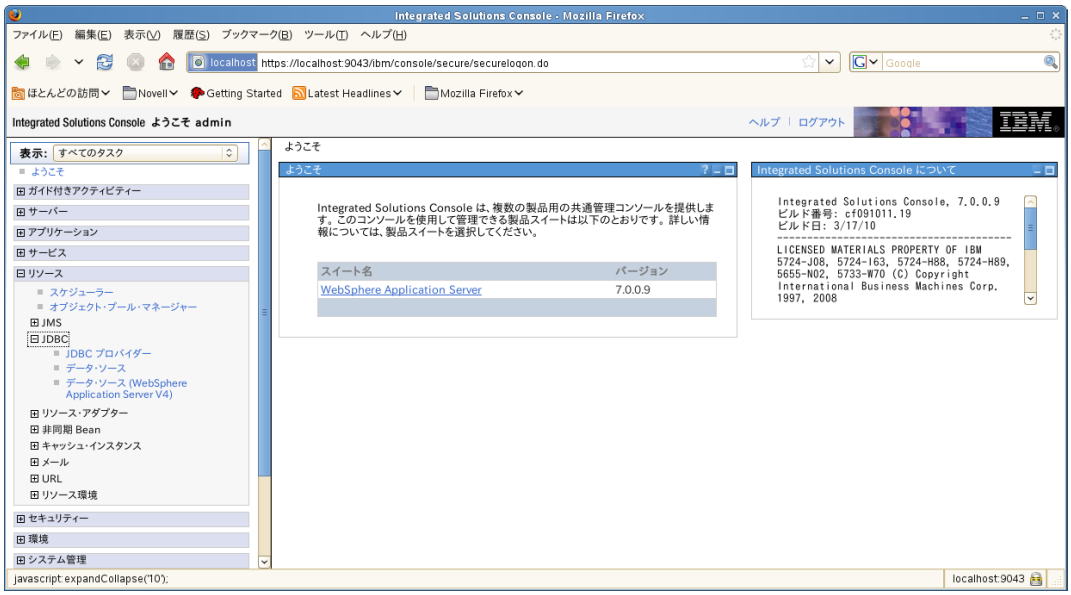
接続プールを WebSphere で使用するように設定するには、JDBC プロバイダとデータソースを作成する必要があります。このセクションでは、プロバイダとデータソースを作成する方法について説明します。

JDBC プロバイダを作成するには

1 ［Integrated Solutions Console］ページの左側にある *［リソース］* を展開します。



2 *［JDBC］* を展開します。



3 *［JDBC プロバイダ］* をクリックします。

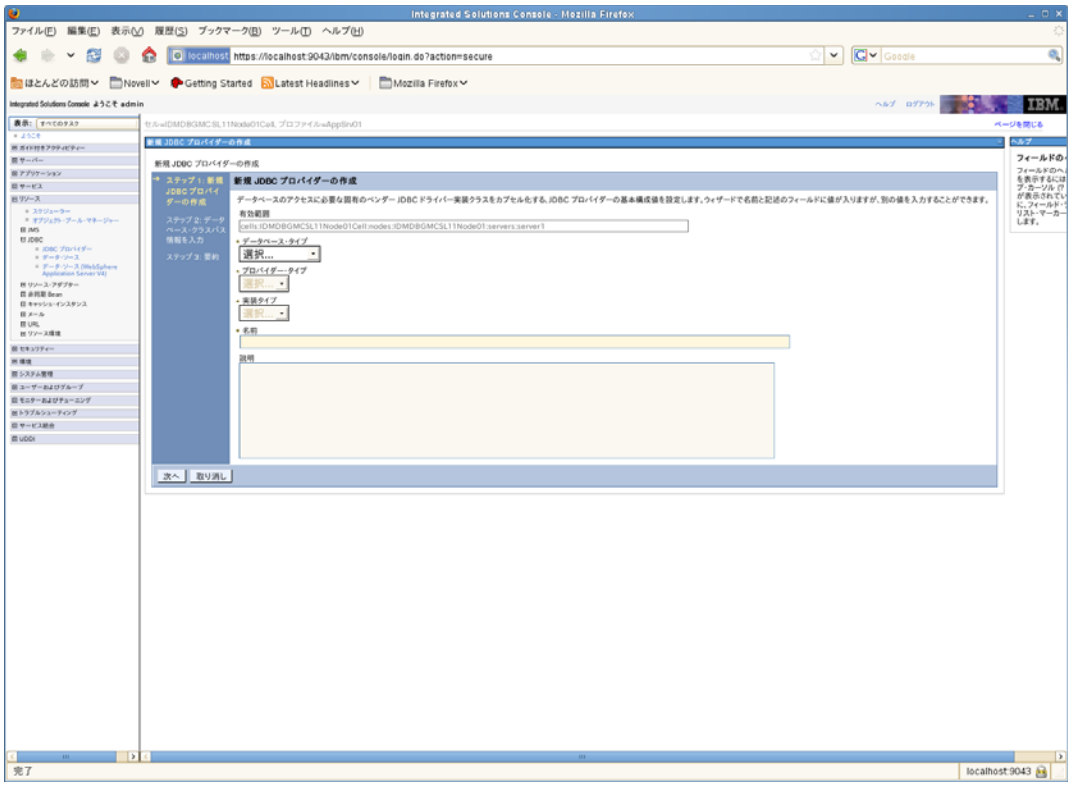
4 *［有効範囲］*を展開します。

5 *［ノード=IDMDBGMCSL11Node01, サーバー=server1］*を選択します。

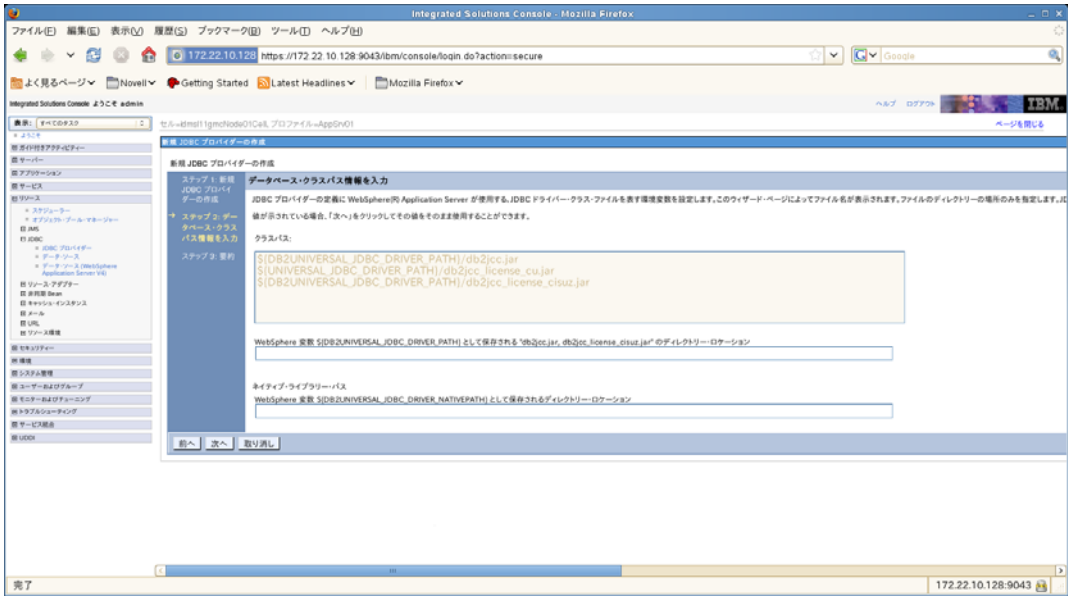
6 *［新規作成］*ボタンをクリックします。

7 *［データベースタイプ］*を選択します (たとえば、DB2 など)。

8 *［次へ］*をクリックします。



9 JDBC のクラスパス情報を入力します。



10 *[次へ]* をクリックします。

11 *[完了]* をクリックします。

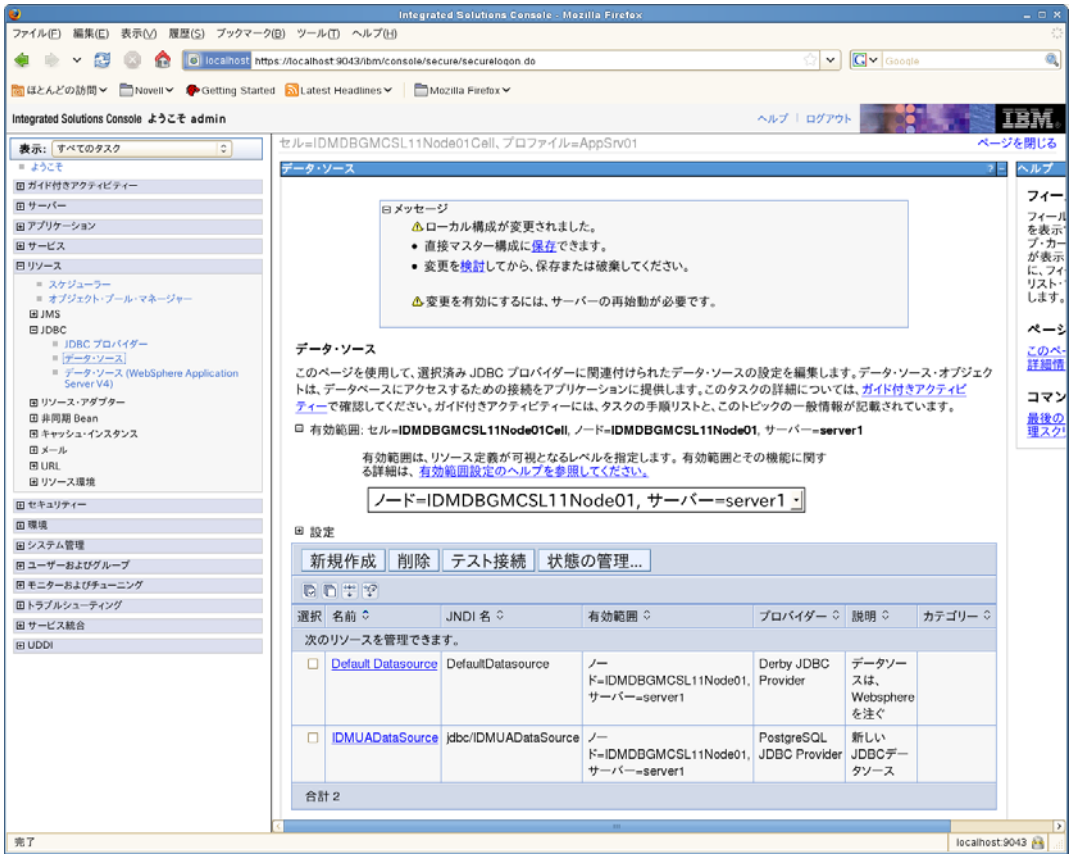
12 *[保存]* リンクをクリックします。

データソースを作成するには

1 ページの左側にある［リソース］を展開します。

2 ［JDBC］を展開します。

3 ［データソース］をクリックします。



4 ［有効範囲］を展開します。

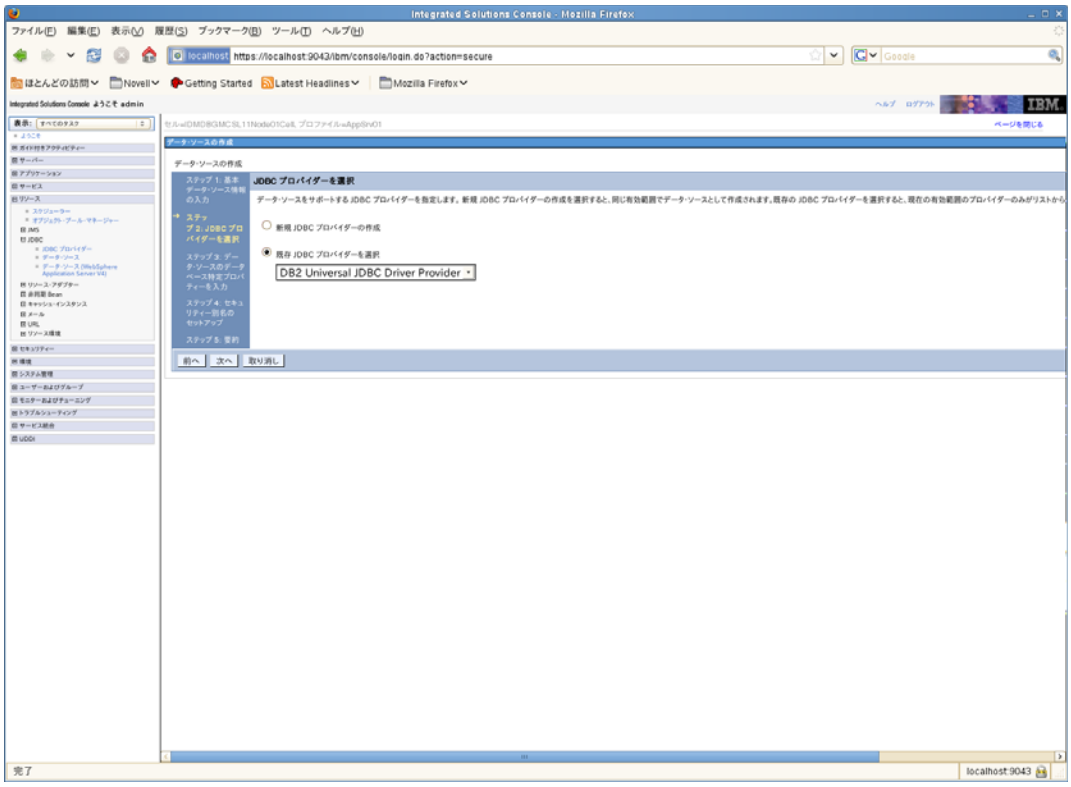
5 ［ノード=*IDMDBGMCSL11Node01*, サーバー=*server1*］を選択します。

6 ［新規］ボタンをクリックします。

7 データソース名と JNDI 名を入力します (たとえば、両方に「IDMUADataSource」と入力します)。

8 ［次へ］をクリックします。

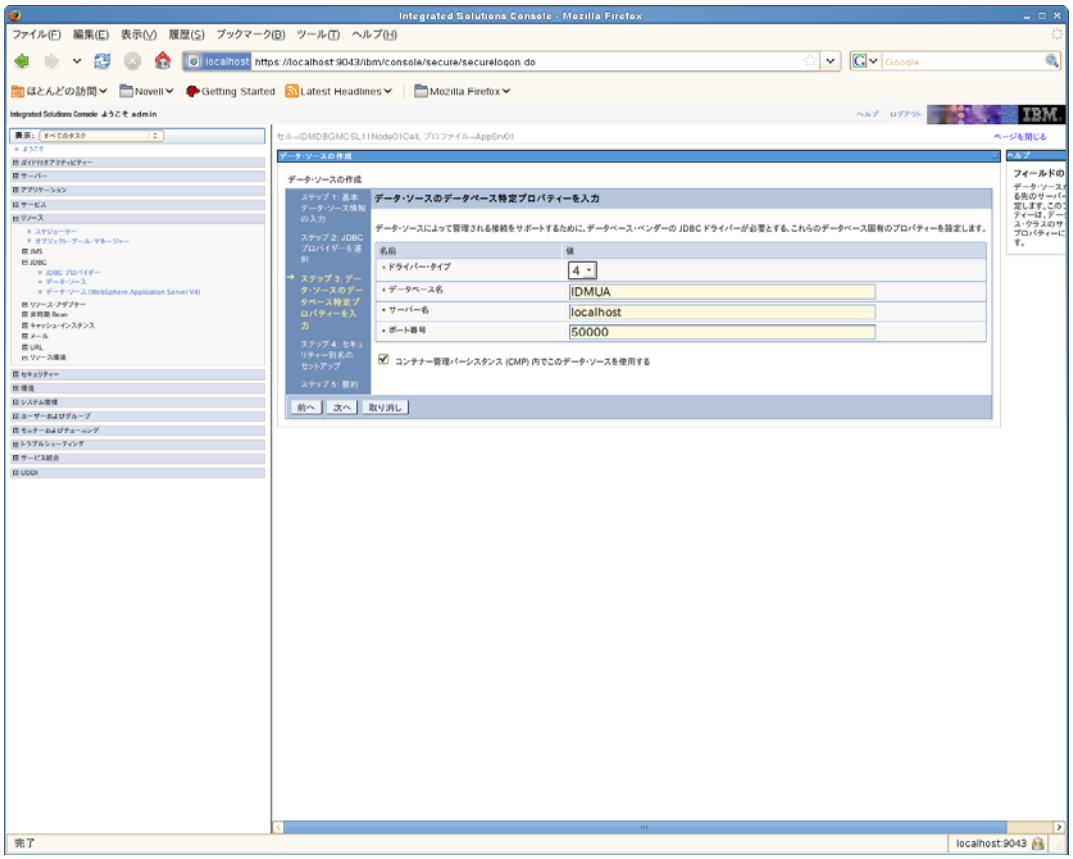
9 ［既存 JDBC プロバイダを選択］をクリックします。



10 上で作成した JDBC プロバイダを選択します。

11 *[次へ]* をクリックします。

12 データソースに必要なデータベース情報 (データソース名、サーバ名、ポート、ユーザ名、およびパスワード) を入力します。



13 *[次へ]* をクリックします。

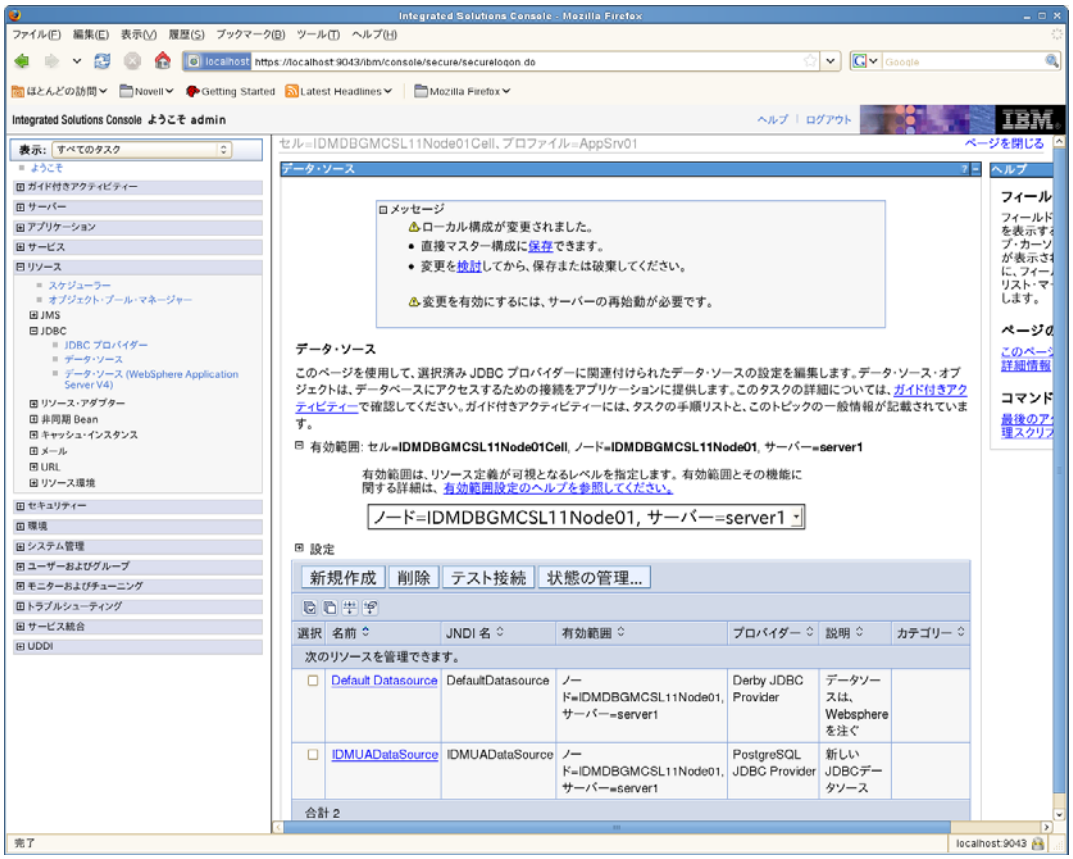
14 セキュリティエイリアス情報を入力するか、デフォルトのままにします。

15 *[次へ]* をクリックします。

16 *[完了]* をクリックします。

17 *[保存]* をクリックします。

18 名前の左側にあるチェックボックスをオンにして新しいデータソースを選択します。



19 *［テスト接続］*ボタンをクリックし、*［成功］*という結果が返されるのを確認します。

6.2.2 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。

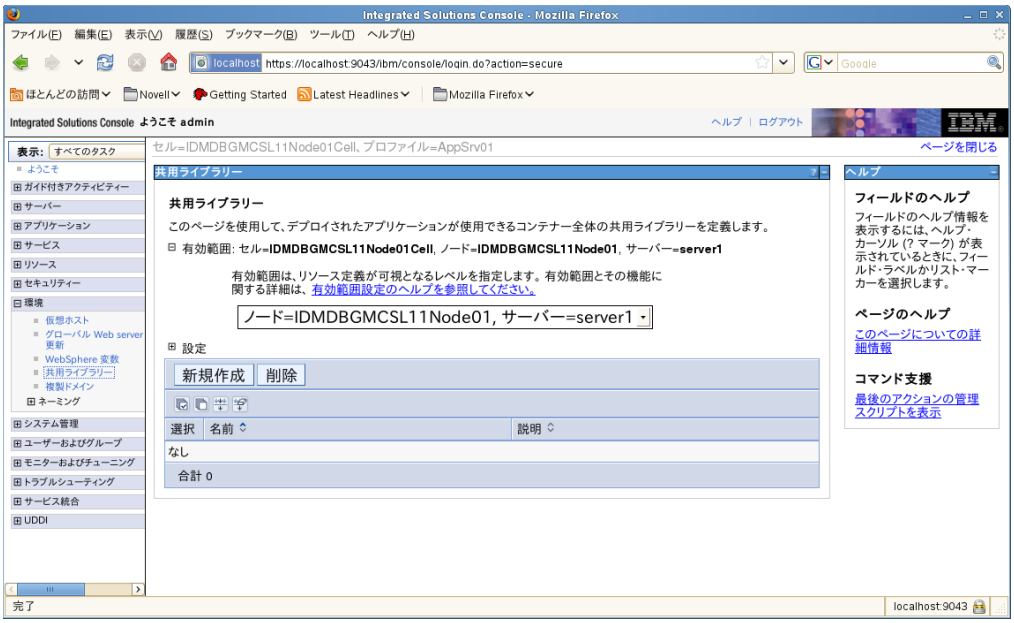
さらに、WebSphere 上のユーザアプリケーション用の共有ライブラリを設定する必要もあります。共有ライブラリは、アプリケーションを正常に実行するために必要なクラスローディングの動作を定義します。

共有ライブラリを設定するには

1 ユーザアプリケーション用の共有ライブラリを作成します。

1a 左側のナビゲーションメニューで *［環境］* をクリックします。

1b *［共用ライブラリ］* をクリックします。



1c *［新規作成］*ボタンをクリックします。

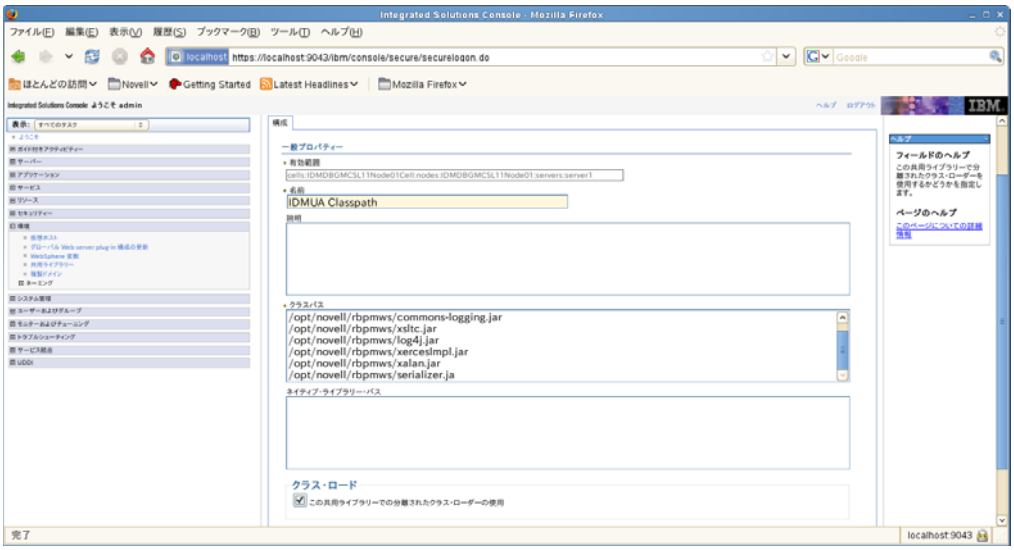
1d 名前を入力します (「IDMUA クラスローダ」など)。

1e ［クラスパス］フィールドに必要な JAR ファイルのリストを入力します。

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

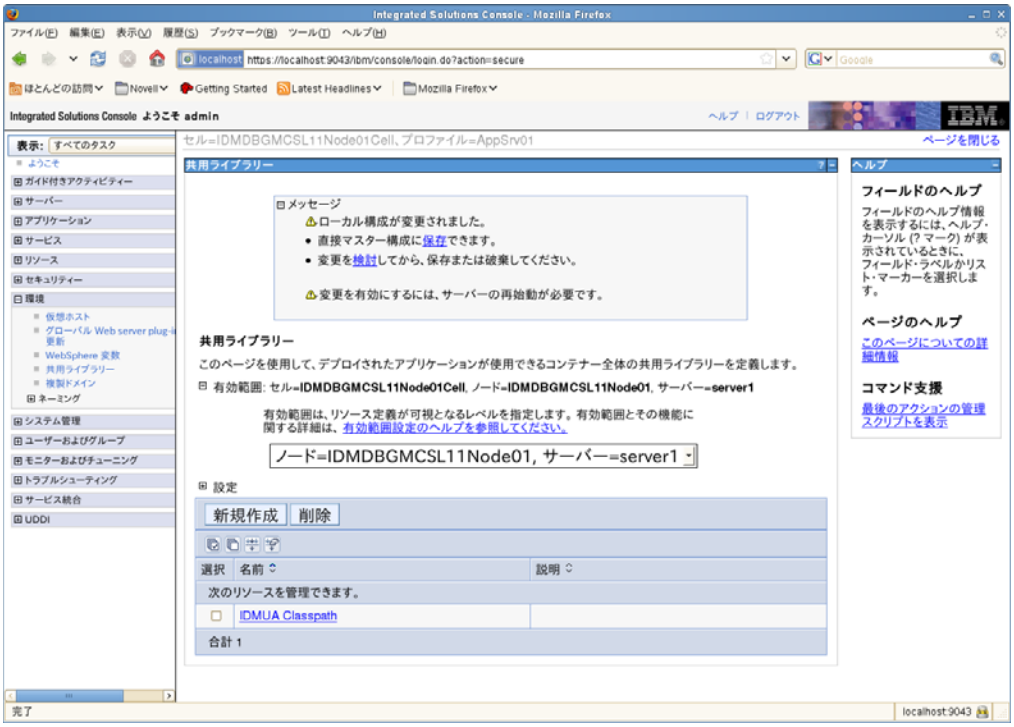
  注 : Apache のサイトからこの JAR ファイルをダウンロードする必要があります。

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



1f *[OK]* をクリックします。

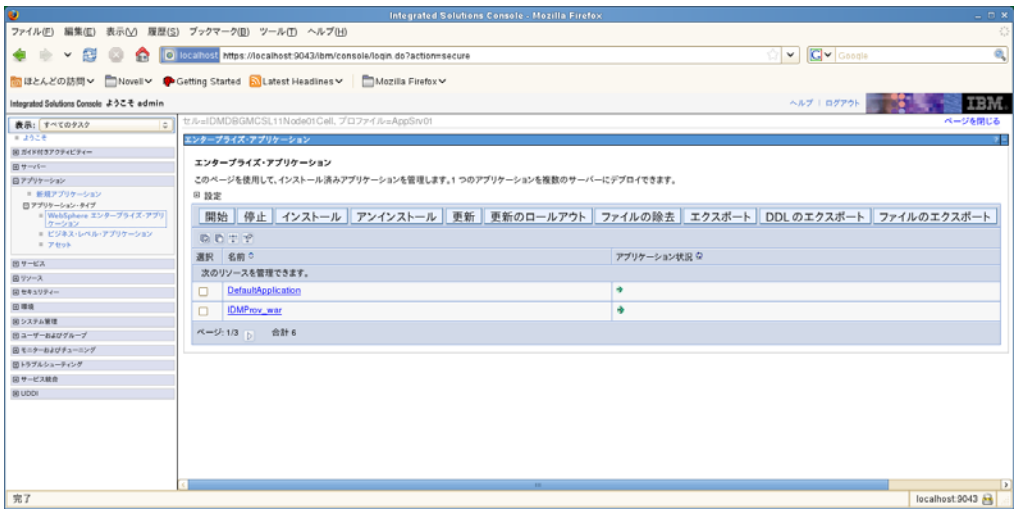
1g *[保存]* リンクをクリックします。



2 IDMProv に共有ライブラリを追加します。

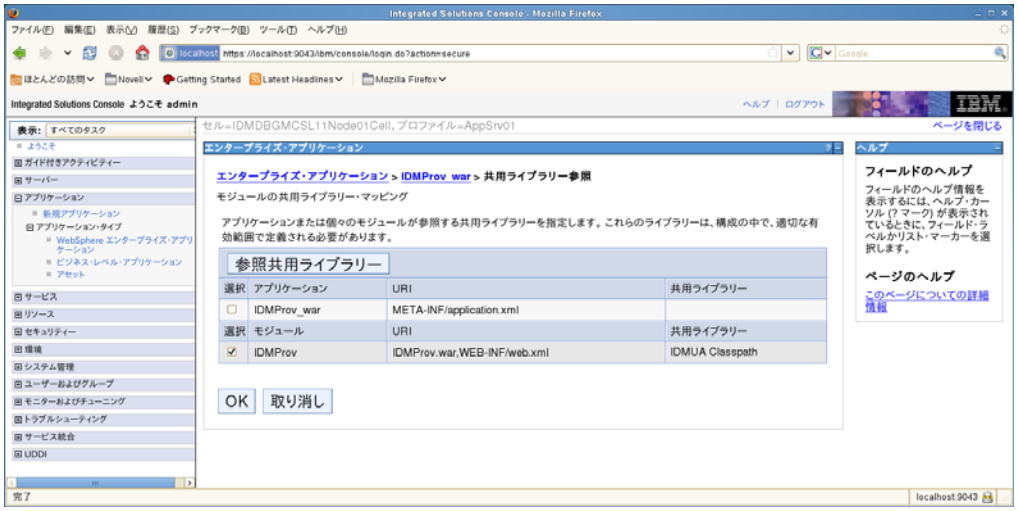
2a 左側で *[アプリケーション]* をクリックします。

2b *[WebSphere エンタープライズ・アプリケーション]* をクリックします。



2c *[IDMProv_war]* という名前をクリックします。

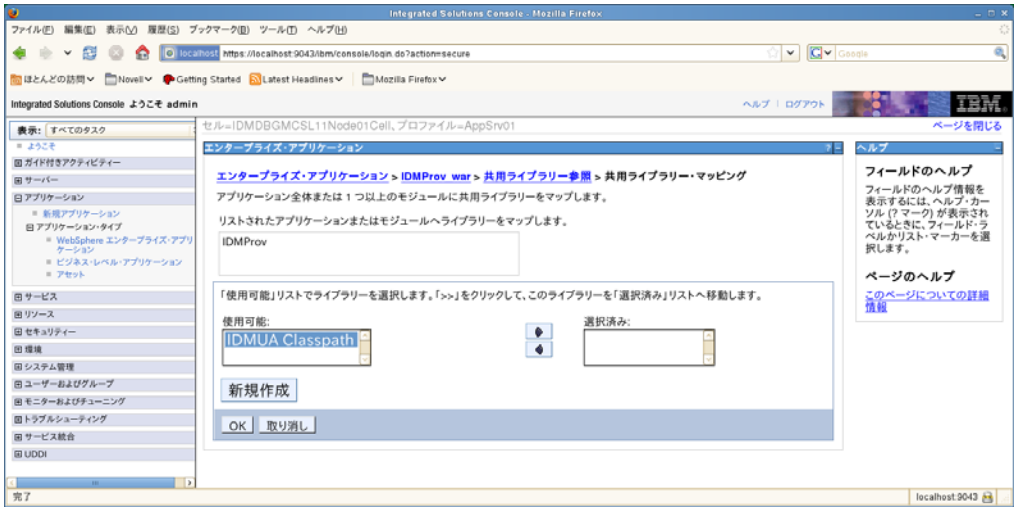
2d ページの最下部の *[参照]* の下から、*[共用ライブラリの参照]* をクリックします。



2e *[IDMProv]* (IDMProv_war ではない) の横にあるチェックボックスをオンにします。

2f *[参照共用ライブラリ]* ボタンをクリックします。

2g *[使用可能]* ボックスの中で共用ライブラリ名 (*[IDMUA Classpath]*) をクリックします。その後、右向き矢印をクリックし、*[選択済み]* ボックスにそれを移動させます。



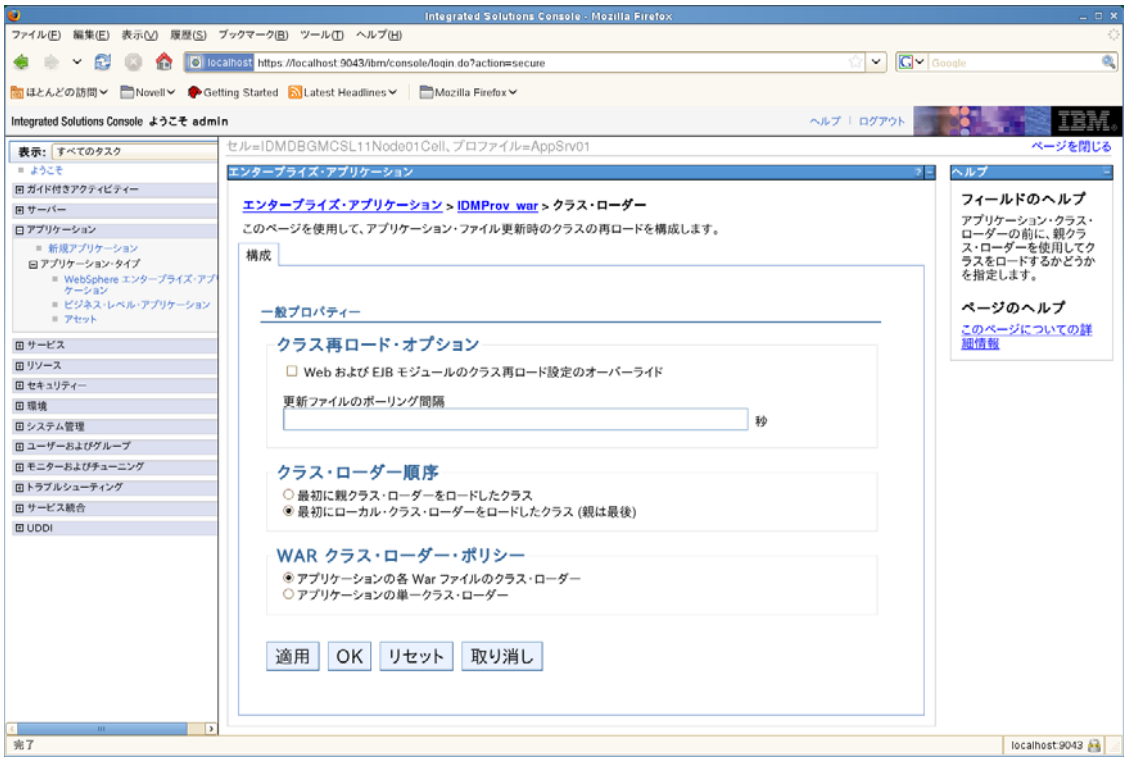
2h *[OK]* をクリックして前のページに戻ります。

2i 再度 *[OK]* をクリックします。

2j *[保存]* をクリックしてサーバ環境設定への変更を保持します。

2k 他のすべての環境設定手順が実行されている場合、サーバを再起動します。

クラスローディングの変更は、モジュールレベルではなく、アプリケーションレベルで行う必要があることに注意してください。WebSphere により展開された WAR 用の EAR が作成され、WAR が EAR 内部のモジュールになります。



6.2.3 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 (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、110 ページのセクション 6.3「WAR ファイルの展開」に進みます。

WebSphere 管理者コンソールを使用した証明書のインポート

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

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

3 右側の設定リストで、*［関連項目］* の下にある *［キーストアと証明書］* 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。

10 画面の一番上にある *［保存］* リンクをクリックします。

コマンドラインを使用した証明書のインポート

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

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

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

次に鍵ツールコマンドの例を示します。

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

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

6.2.4 preferIPv4Stack プロパティを JVM に渡す

ユーザアプリケーションは、キャッシュを実装するのに JGroups を使用します。構成によっては、mcast_addr のバインディングが確実に成功するように、preferIPv4Stack プロパティを true に設定するように JGroups が要求します。このオプションを設定しないと、次のエラーが発生する可能性があり、キャッシングが適切に動作しません。

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

パラメータ java.net.preferIPv4Stack=true は、たとえば extend.local.config.dir のようなその他のシステムプロパティと同じ方法で設定できるシステムプロパティです。システム設定プロパティの設定については 103 ページのセクション 6.2.2「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」、を参照してください。

6.3 WAR ファイルの展開

WebSphere 展開ツールを使用して、WAR ファイルを展開します。

6.3.1 WebSphere 7.0 用の追加の環境設定

RBPM のバージョン 4.0.1 で WebSphere7.0 を使用している場合、RBPM のこのリリースでは、いくつかの JAR ファイル (commons-digester.jar など) が入手可能な最新バージョンにアップグレードされていることに注意する必要があります。したがって、環境を適切に設定していない場合は、WebSphere に付属している JAR ファイルとのバージョンの競合が発生してしまう可能性があります。

正しい JAR ファイルを確実に使用するには、まずは IDMProv.war からクラスをロードするように WebSphere サーバを設定する必要があります。IDMProv.war ファイルには、*［Classes loaded with local class loader first (parent last) (まずはローカルクラスローダを使用してクラスをロード (親は最後))］* オプションを選択する必要があります。

6.4 ユーザアプリケーションの開始およびアクセス

ユーザアプリケーションを起動するには次の処理を行います。

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

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

ユーザアプリケーションへのアクセス方法

1. 展開中に指定したコンテキストを使用してポータルにアクセスします。

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

WebLogic でのユーザアプリケーションのインストール

7

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

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、131 ページの第 8 章「コンソールまたは単一コマンドによるインストール」を参照してください。

ルート以外のユーザとしてインストーラを実行します。

データマイグレーション : 移行の詳細については、『*ユーザアプリケーション : マイグレーションガイド* (http://www.novell.com/documentation/idm40/index.html)』を参照してください。

7.1 WebLogic インストールチェックリスト

- ❑ WebLogic のインストール。

  WebLogic マニュアルのインストール手順に従います。

- ❑ WebLogic が有効な WAR を作成します。

  Identity Manager ユーザアプリケーションインストーラを使用してこのタスクを実行します。詳細については、112 ページのセクション 7.2「ユーザアプリケーション WAR のインストールおよび環境設定」を参照してください。

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

  詳細については、126 ページのセクション 7.3「WebLogic 環境の準備」を参照してください。

- ❑ WAR を展開します。

  詳細については、129 ページのセクション 7.4「ユーザアプリケーション WAR の展開」を参照してください。

7.2 ユーザアプリケーション WAR のインストールおよび環境設定

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

1 インストールファイルが含まれるディレクトリに移動します。

2 JRockit Java 環境 (バージョン 1.6_17) を使用して、コマンドラインから次のプラットフォームのインストーラを開始します。

Solaris:

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

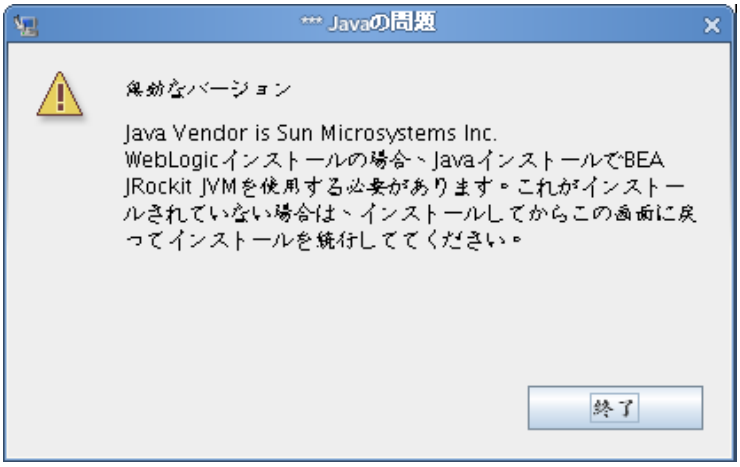
Windows:

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

インストールプログラムを開始すると、言語を入力するよう促されます。

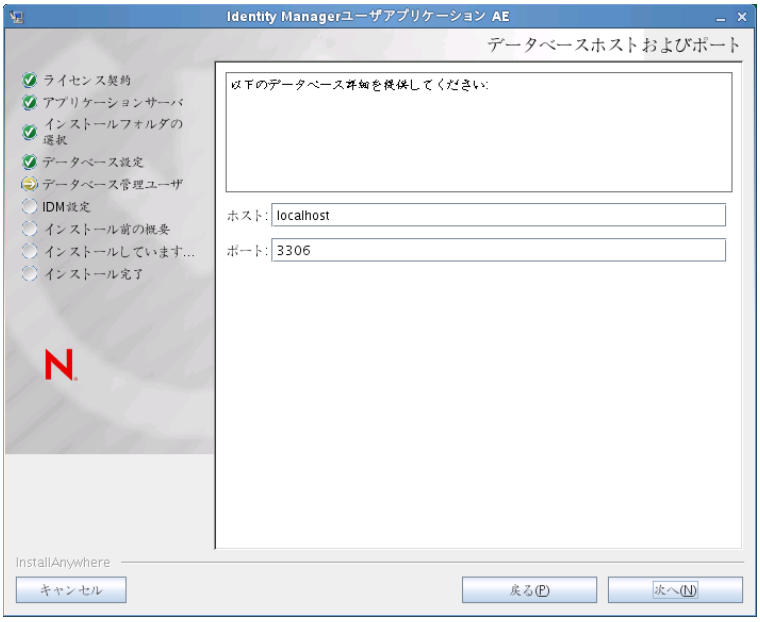
3 言語を選択し、使用許諾契約を確認し、アプリケーションサーバプラットフォームを選択するには、次の情報を使用します。

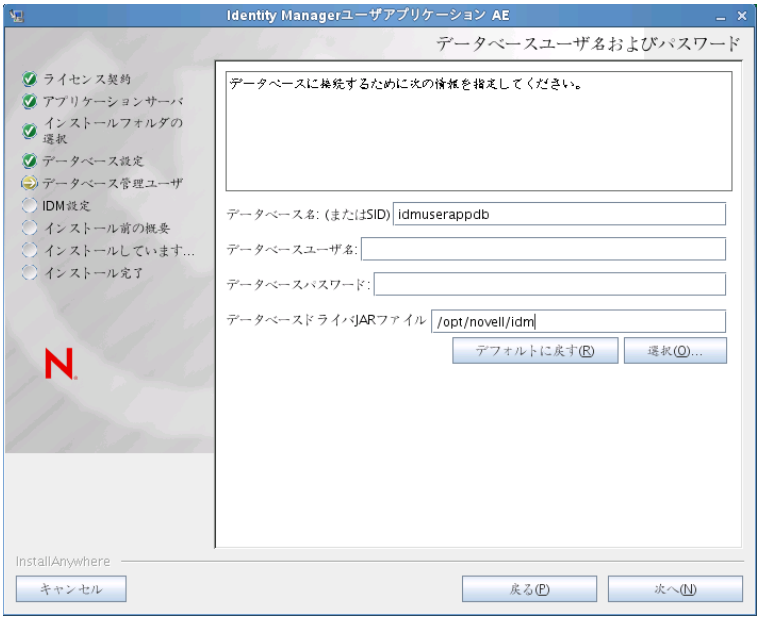
インストール画面	説明
ユーザアプリケーションインストール	インストールプログラムの言語を選択します。デフォルトでは、［英語］が選択されています。
使用許諾契約	使用許諾契約を読み、*［使用許諾契約の条件に同意します］*を選択します。

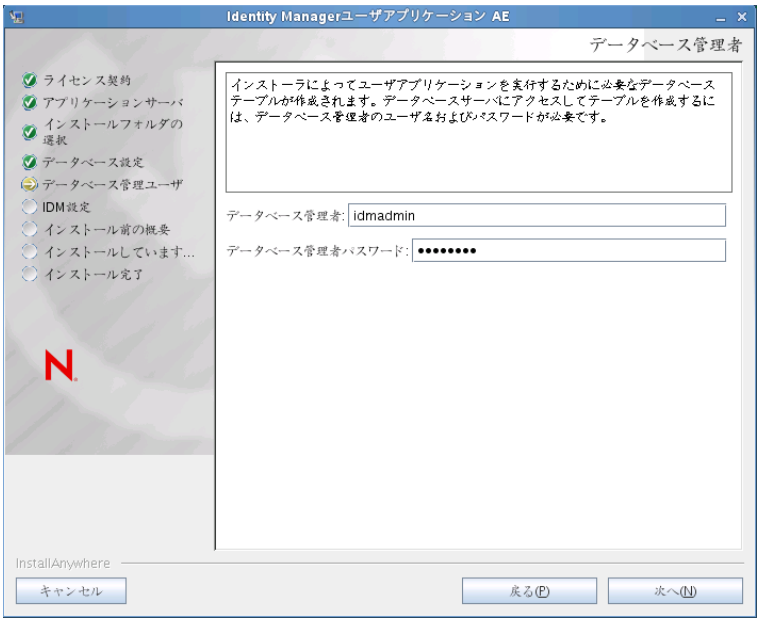
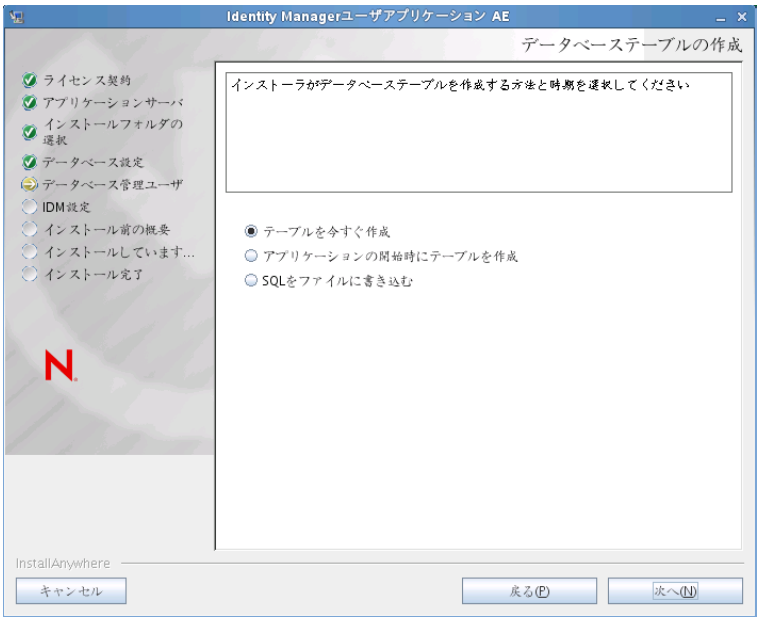
インストール画面	説明
アプリケーションサーバプラットフォーム	*[WebLogic]* を選択します。 ユーザアプリケーションの WAR ファイルがインストーラとは別のディレクトリにある場合は、インストーラによって WAR へのパスを入力するようメッセージが表示されます。 WAR がデフォルトの場所にある場合は、*[デフォルトのファイルに戻す]* をクリックできます。または、WAR ファイルの場所を指定する場合は、*[選択]* をクリックして場所を選択します。 WebLogic でインストールする場合、BEA の Java 環境 (jrockit) を使用することによってインストールプログラ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

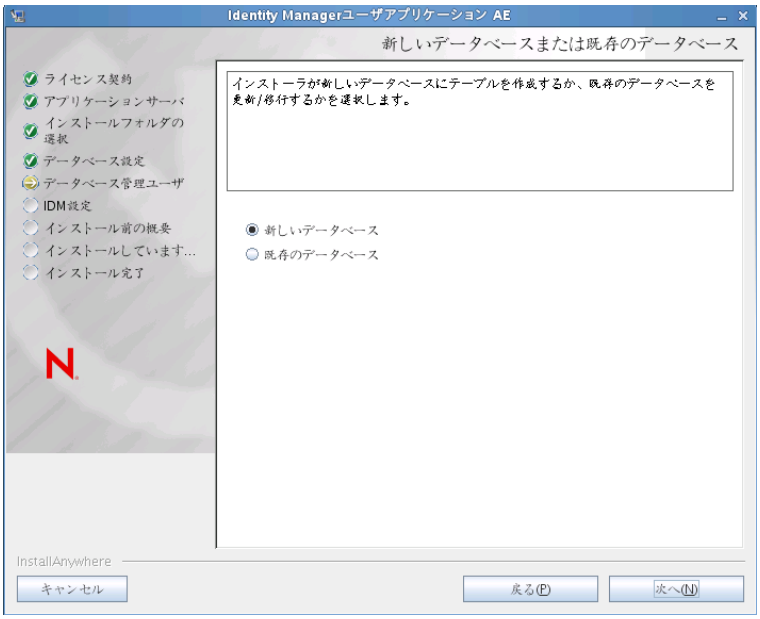
4 次の情報を使用して、インストールフォルダを選択し、データベースを設定します。

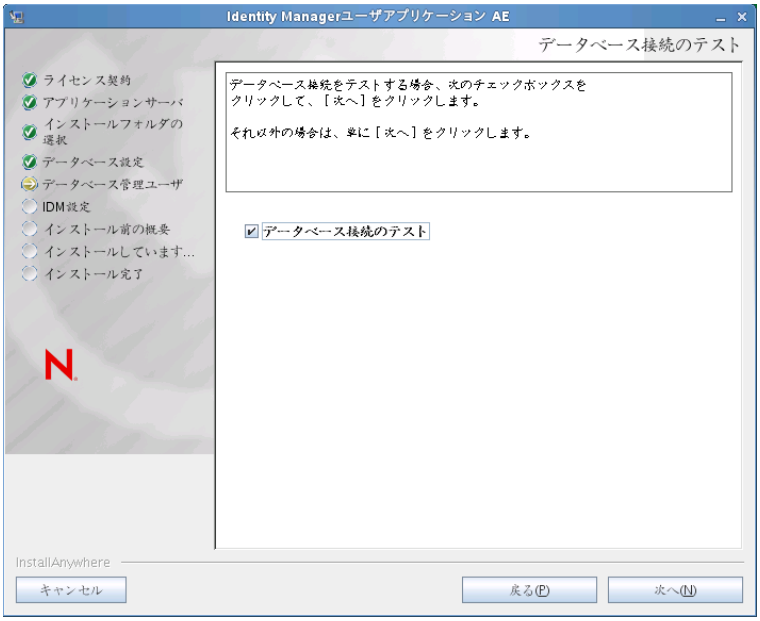
インストール画面	説明
インストールフォルダの選択	インストーラがファイルを配置する場所を指定します。
データベースプラットフォーム	データベースプラットフォームを選択します。データベースおよび JDBC ドライバはすでにインストールされている必要があります。WebLogic の場合、オプションには次のプラットフォームが含まれます。 ◆ Oracle ◆ Microsoft SQL Server ◆ PostgreSQL

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

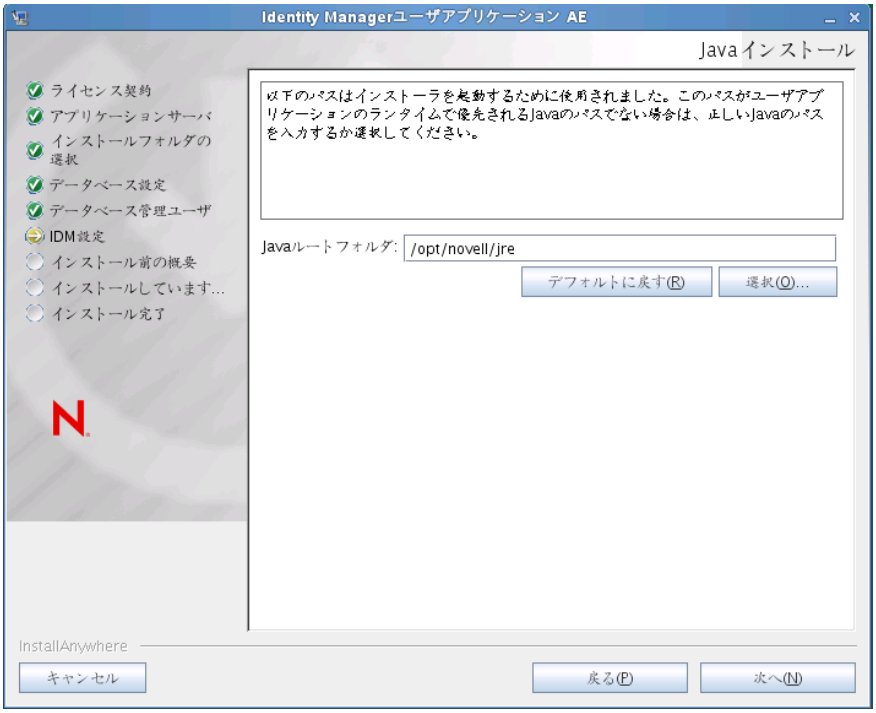
インストール画面	説明
データベースのユーザ名およびパスワード	*データベース名* (または SID): MS SQL Server または PostgreSQL では、事前に設定したデータベース名を入力します。Oracle の場合は、前に作成した Oracle システム ID (SID) を指定します。クラスタでは、クラスタの各メンバーには同じデータベース名または SID を指定します。 *データベースユーザ名* : データベースユーザを指定します。クラスタでは、クラスタの各メンバーには同じデータベースユーザを指定します。 *データベースパスワード*: データベースパスワードを指定します。ク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

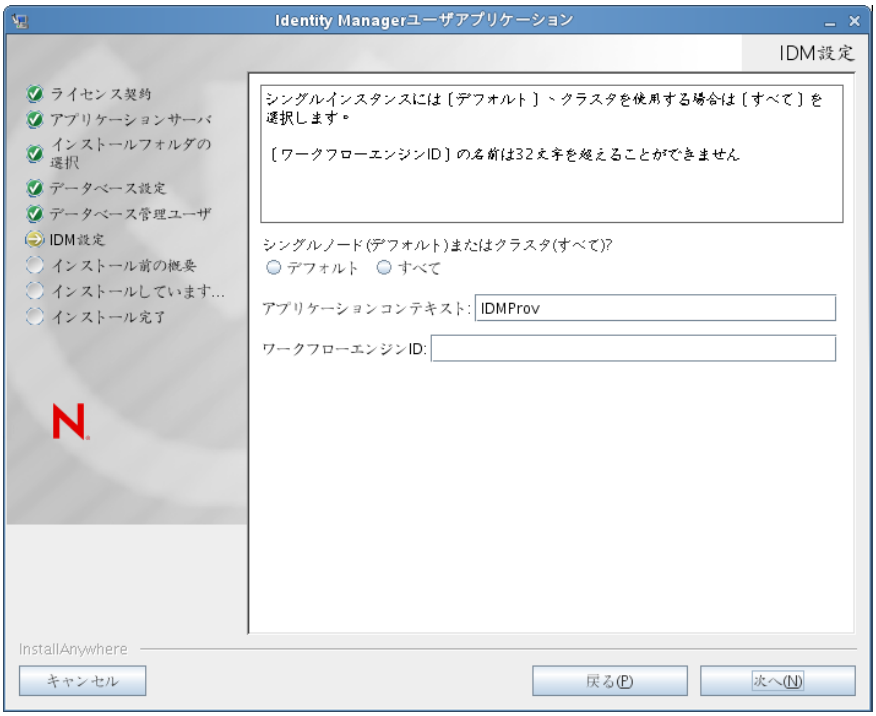
インストール画面	説明
データベース管理者	この画面には、［データベースユーザ名およびパスワード］ページから同じユーザ名とパスワードが事前に入力されています。以前に指定したデータベースユーザがデータベースサーバ内にテーブルを作成するための十分な許可を持っていない場合、必要な権限を持つ別のユーザ ID を入力する必要があります。 
データベーステーブルの作成	データベーステーブルを作成する必要がある場合に指定します。 

インストール画面	説明
新しいデータベースまたは既存のデータベース	使用するデータベースが新規または空の場合、*[新しいデータベース]* ボタンを選択します。データベースが以前のインストールに属する既存のものである場合、*[既存のデータベース]* ボタンを選択します。 

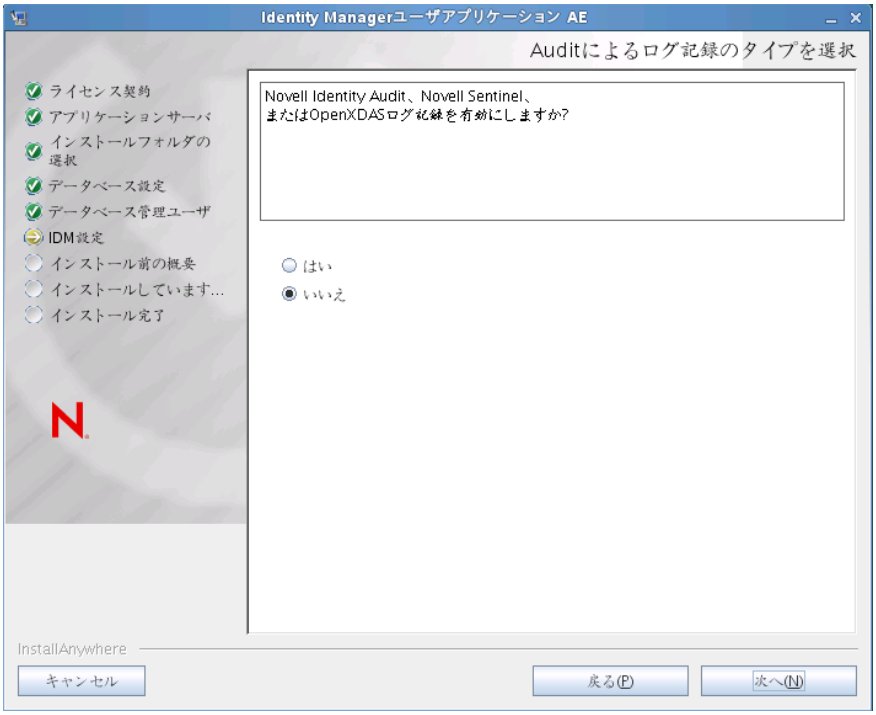
インストール画面	説明
データベース接続のテスト	前の画面で指定した情報が正しかったことを確認するには、*[データベース接続のテスト]* チェックボックスをオンにしてデータベース接続をテストします。  インストーラは、直接テーブルを作成するため、および .SQL ファイルを作成するための両方の場合にデータベースに接続する必要があります。データベース接続をテストして、それが失敗した場合でも、インストールを続行できます。その場合、『*ユーザアプリケーション：管理ガイド* (http://www.novell.com/documentation/idm40/agpro/?page=/documentation/idm40/agpro/data/bncf7rj.html)』で説明されるように、インストール後にテーブルを作成する必要があります。

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

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

インストール画面	説明
IDM 環境設定	*アプリケーションコンテキスト*: アプリケーションサーバの環境設定の名前、アプリケーション WAR ファイルの名前、および URL コンテキストの名前です。インストールスクリプトによってサーバの環境設定が作成され、デフォルト名で *アプリケーション名*に基づく環境設定が作成されます。ユーザアプリケーションをブラウザから開始する場合は、アプリケーション名を書き留め、アプリケーション名を URL に含めてください。 

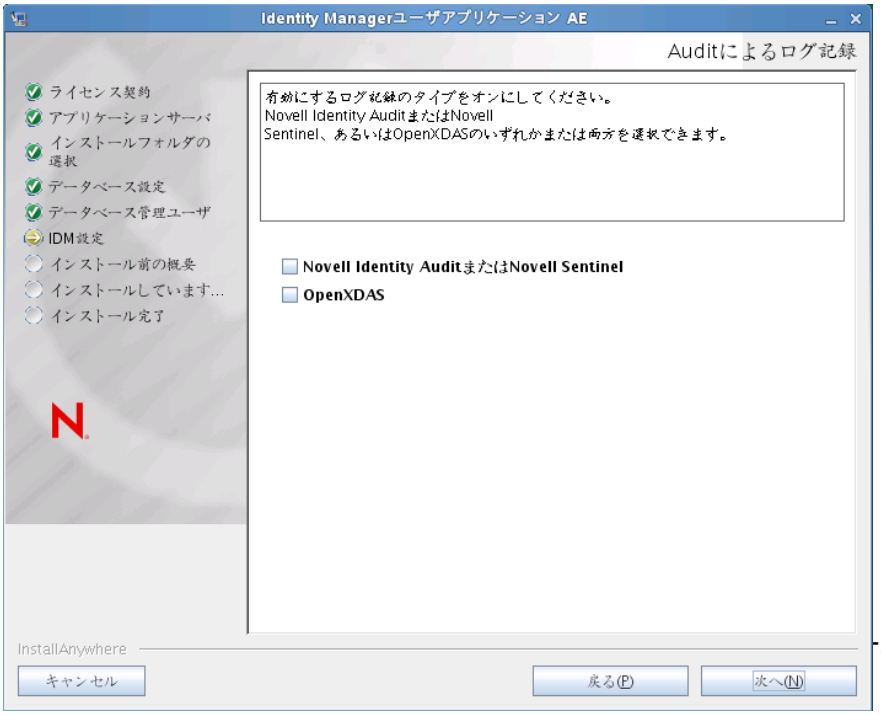
インストール画面	説明
Audit によるログ記録のタイプを選択	ログを有効にするには、*[はい]* をクリックします。ログを無効にするには、*[いいえ]* をクリックします。



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

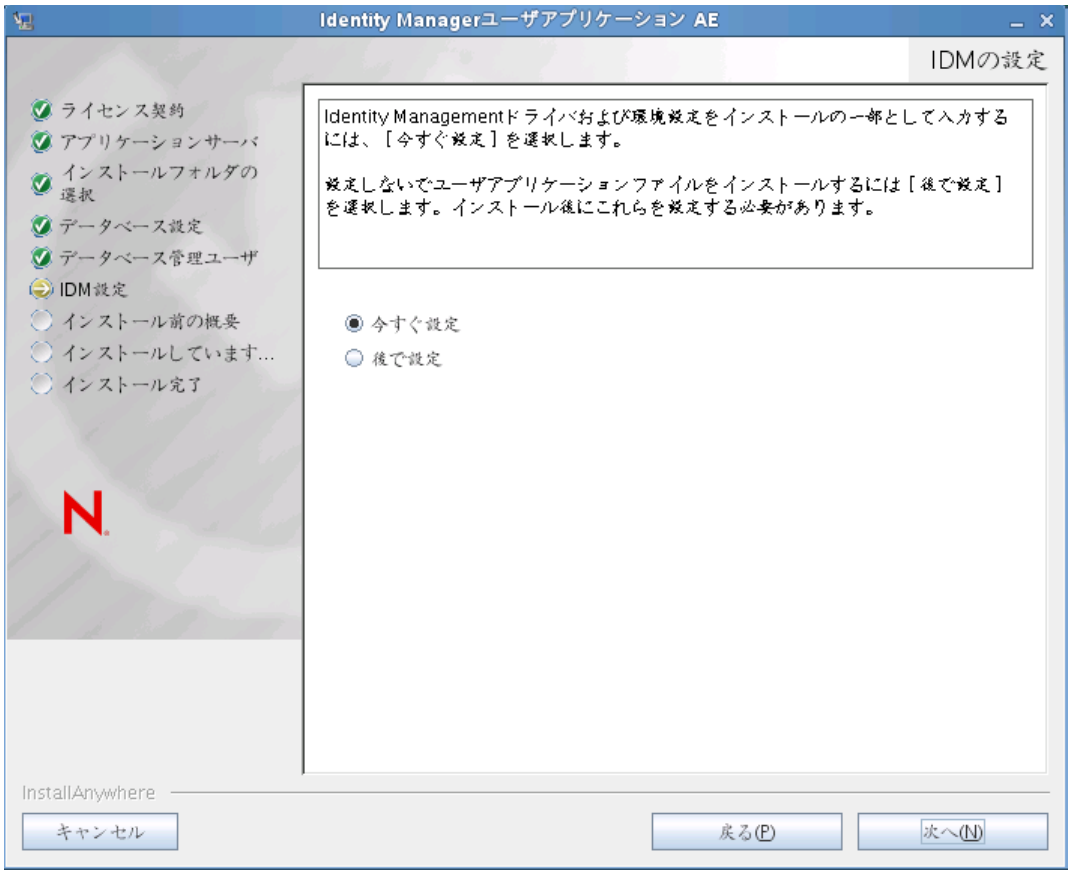
- *Novell Identity Audit または Novell Sentinel*: Novell 監査クライアントを使用してユーザアプリケーションでログを有効にします。
- *OpenXDAS*: OpenXDAS ログサーバにイベントが記録されます。

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



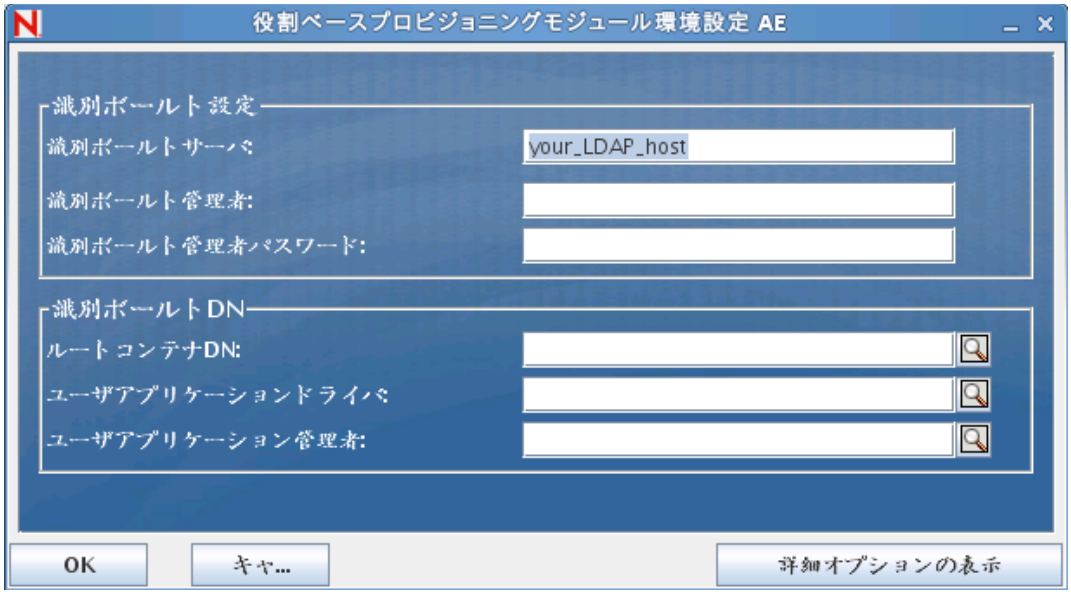
インストール画面	説明
Novell Identity Audit または Novell Sentinel	*サーバ*: ログを有効にする場合、サーバのホスト名または IP アドレスを指定します。ログをオフにする場合は、この値は無視されます。 *ログキャッシュフォルダ*: ログキャッシュのディレクトリを指定します。
セキュリティ - マスタキー	*はい*: 既存のマスタキーをインポートできます。既存の暗号化マスタキーをインポートするよう選択した場合は、該当するキーを切り取ってインストール手順のウィンドウに貼り付けます。 *いいえ*: 新規のマスタキーを作成します。インストール終了後、147 ページのセクション 9.1「マスタキーの記録」で示すように、マスタキーを手動で記録します。 インストール手順で、インストールディレクトリにある master-key.txt ファイルに暗号化マスタキーが書き込まれます。 既存のマスタキーをインポートする理由には、次のようなものがあります。 ◆ インストールファイルをステージングシステムから運用システムに移動中で、ステージングシステムで使用したデータベースへのアクセスを保持する場合。 ◆ ユーザアプリケーションを最初のクラスタのメンバーにインストールしており、現在はクラスタの次のメンバーにインストールしている場合 (同じマスタキーが必要)。 ◆ ディスク故障のため、ユーザアプリケーションを復元する必要がある場合。ユーザアプリケーションを再インストールして、以前のインストールで使用したのと同じ暗号化マスタキーを指定する必要があります。これによって、前に保存した暗号化データにアクセスできます。

6 この時点で RBPM を設定する場合は、*[今すぐ設定]* を選択し、*[次へ]* をクリックします。



(この情報の入力を求められない場合、30 ページのセクション 2.5「Java Development Kit のインストール」で説明したステップを完了していない可能性があります。)

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



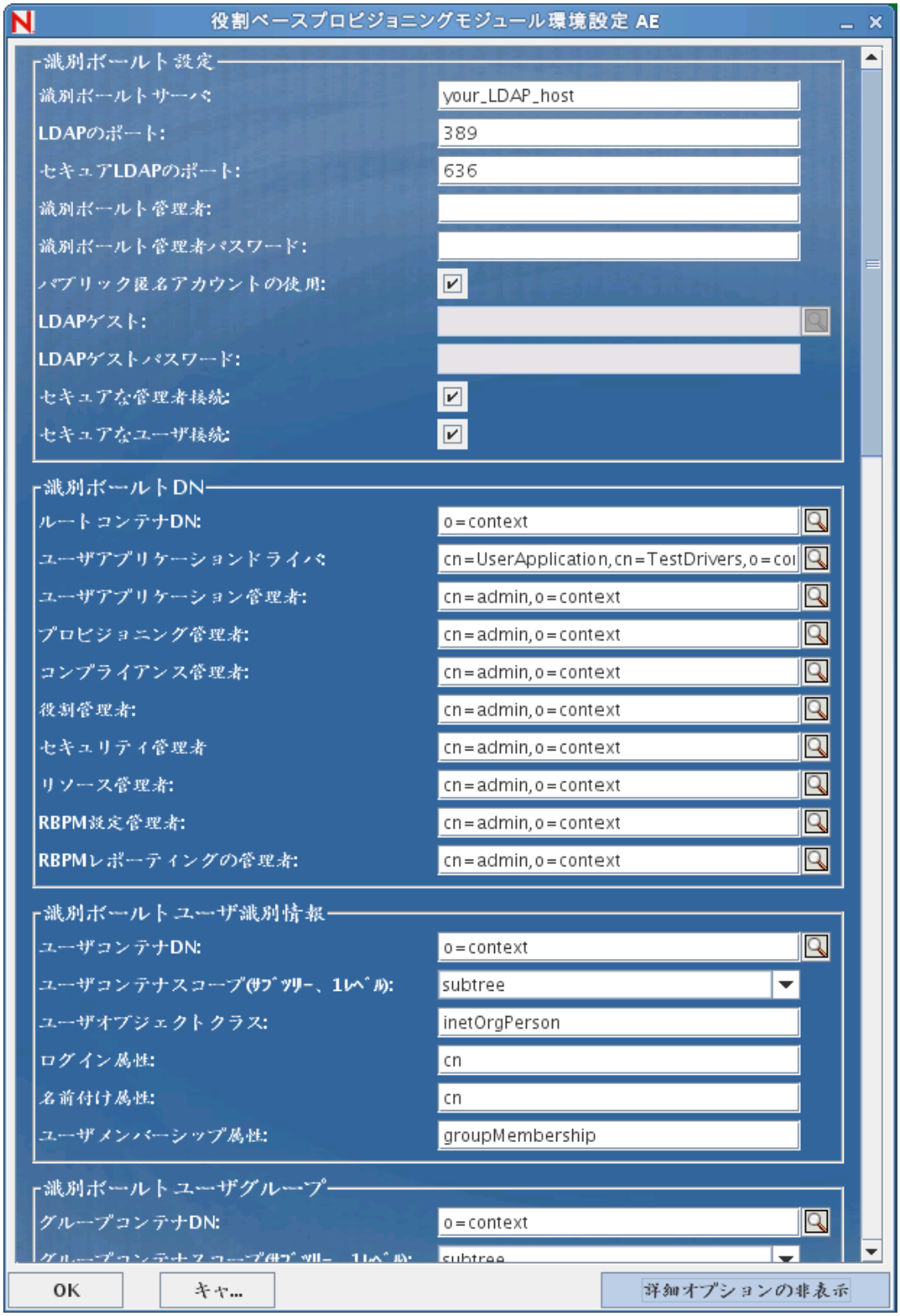
インストールプログラムはルートコンテナ DN から値を取得し、それを次の値に適用します。

- ユーザコンテナ DN
- グループコンテナ DN

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

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

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


役割ベースプロビジョニングモジュール環境設定 AE
識別ボールト設定
識別ボールトサーバ:
your_LDAP_host
LDAPのポート:
389
セキュアLDAPのポート:
636
識別ボールト管理者:
識別ボールト管理者パスワード:
パブリック匿名アカウントの使用:
LDAPゲスト:
LDAPゲストパスワード:
セキュアな管理者接続:
セキュアなユーザ接続:
識別ボールトDN
ルートコンテナDN:
o=context
ユーザアプリケーションドライバ:
cn=UserApplication,cn=TestDrivers,o=co
ユーザアプリケーション管理者:
cn=admin,o=context
プロビジョニング管理者:
cn=admin,o=context
コンプライアンス管理者:
cn=admin,o=context
役割管理者:
cn=admin,o=context
セキュリティ管理者
cn=admin,o=context
リソース管理者:
cn=admin,o=context
RBPM設定管理者:
cn=admin,o=context
RBPMレポーティングの管理者:
cn=admin,o=context
識別ボールトユーザ識別情報
ユーザコンテナDN:
o=context
ユーザコンテナスコープ(サブツリー、1レベル):
subtree
ユーザオブジェクトクラス:
inetOrgPerson
ログイン属性:
cn
名前付け属性:
cn
ユーザメンバーシップ属性:
groupMembership
識別ボールトユーザグループ
グループコンテナDN:
o=context
subtree
OK
キャ...
詳細オプションの非表示

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。

各オプションの詳細については、155 ページの付録 A「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。

7 インストールを完了するには、次の情報を使用します。

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

7.2.1 インストールとログファイルの表示

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

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

7.3 WebLogic 環境の準備

7.3.1 接続プールの設定

- ❑ 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。
- ❑ データソースを作成します。

WebLogic マニュアルのデータソース作成の指示に従います。

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

7.3.2 RBPM 設定ファイルの場所の指定

WebLogic ユーザアプリケーションでは、sys-configuration-xmldata.xml ファイル、idmuserapp_logging.xml ファイル、および wl_idmuserapp_logging.xml ファイルの検索方法を認識している必要があります。したがって、ファイルの場所を setDomainEnv.cmd ファイルに追加する必要があります。

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場所を指定します。

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

   ```
   set JAVA_PROPERTIES
   export JAVA_PROPERTIES
   ```

3. JAVA_PROPERTIES のエントリの下に、次に対してエントリを追加します。
   - Dextend.local.config.dir==<directory-path>: sys-configuration.xml ファイルを含むフォルダ (ファイル自体ではない) を指定します。
   - -Didmuserapp.logging.config.dir==<directory-path>: idmuserapp_logging.xml ファイルを含むフォルダ (ファイル自体ではない) を指定します。
   - -Dlog.init.file==< ファイル名 >: log4j の環境設定に使用される wl_idmuserapp_logging.xml ファイルを指定します。このファイルは、複数のアプリケーションが同じアプリケーションサーバにインストールされているような状況で、ユーザアプリケーションに必要なアペンダとロガーの環境設定を処理します。

   Windows の場合の例 :

   ```
   set JAVA_OPTIONS=-Dextend.local.config.dir=c:\novell\idm
   set JAVA_OPTIONS=%JAVA_OPTIONS% -
   Didmuserapp.logging.config.dir=c:\novell\idm
   set JAVA_OPTIONS=%JAVA_OPTIONS%
   -Dlog.init.file=wl_idmuserapp_logging.xml
   ```

4. 環境変数 EXT_PRE_CLASSPATH を設定し、次の JAR ファイルを指し示します。
   - antlr-2.7.6.jar
   - log4j.jar
   - commons-logging.jar

     注 : Apache のサイトからこの JAR ファイルをダウンロードする必要があります。
   - xalan.jar
   - xercesImpl.jar
   - xsltc.jar
   - serializer.jar
   - IDMselector.jar

注 : これらの JAR ファイルを EXT_PRE_CLASSPATH 変数に追加する別の方法としては、これらのファイルを IDMProv.war ファイルの中の WEB-INF/lib ディレクトリにコピーする方法があります。

4a この行を見つけます。

```
ADD EXTENSIONS TO CLASSPATH
```

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

```
set
EXT_PRE_CLASSPATH=C:\bea\user_projects\domains\base_domain\lib\antlr-
2.7.6.jar;C:\bea\user_projects\domain\base_domain\lib\log4j.jar;C:\be
a\user_projects\domains\base_domain\lib\commons-
logging.jar;C:\bea\user_projects\domains\base_domain\lib\xalan.jar;C:
\bea\user_projects\domains\base_domain\lib\xercesImpl.jar;C:\bea\user
_projects\domains\base_domain\lib\xsltc.jar;C:\bea\user_projects\doma
ins\base_domain\lib\serializer.jar
```

Linux の場合の例 :

```
export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/
lib/antlr-2.7.6.jar:/opt/bea/user_projects/domain/base_domain/lib/
log4j.jar:/opt/bea/user_projects/domains/base_domain/lib/commons-
logging.jar:/opt/bea/user_projects/domains/base_domain/lib/
xalan.jar:/opt/bea/user_projects/domains/base_domain/lib/
xercesImpl.jar:/opt/bea/user_projects/domains/base_domain/lib/
xsltc.jar:/opt/bea/user_projects/domains/base_domain/lib/
serializer.jar
```

5 ファイルを保存して終了します。

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

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

2 次の行をファイル内で探します。

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

3 sys-configuration.xml ファイルへのパスを含めるように既存の行を更新します。

Windows の場合の例 :

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

Linux の場合の例 :

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

4 ファイルを保存して閉じます。

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

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

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

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

7.3.3 OpenSAML JAR ファイルの削除

WebLogic が使用する OpenSAML JAR ファイルが、ユーザアプリケーションに必要な OpenSAML JAR ファイルと競合しています。したがって、ユーザアプリケーションが WebLogic 上で適切に展開されるようにするには、WebLogic /WL103/modules ディレクトリにあるファイルを削除する必要があります。この要件は、SSO が有効でないすべてのユーザアプリケーションに当てはまります。

WebLogic /WL103/modules ディレクトリ内の次の JAR ファイルを必ず削除してください。

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

7.3.4 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. このセクションが終了する直前の <security-configuration> セクションに次の行を追加します。

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-
   credentials>
   </security-configuration>
   ```
3. ファイルを保存して、サーバを再起動します。

この変更を行った後で、ワークフロー管理プラグインにログインできるはずです。

7.4 ユーザアプリケーション WAR の展開

現時点では、標準の WebLogic 展開手順を使用してユーザアプリケーションの WAR ファイルを展開することができます。

7.5 ユーザアプリケーションへのアクセス

- ユーザアプリケーション URL への移動 :

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

  例を次に示します。

  ```
  http://localhost:8180/IDMProv
  ```

コンソールまたは単一コマンドによるインストール

8

このセクションでは、57 ページの第 5 章「JBoss でのユーザアプリケーションのインストール」で説明した GUI を使用したインストール方法の代わりに使用できるインストール方法について説明します。主なトピックは次のとおりです。

- 131 ページのセクション 8.1「コンソールからのユーザアプリケーションのインストール」
- 132 ページのセクション 8.2「単一コマンドによるユーザアプリケーションのインストール」
- 142 ページのセクション 8.3「サイレントモードまたはコンソールモードでの JBossPostgreSQL ユーティリティの実行」
- 144 ページのセクション 8.4「サイレントモードまたはコンソールモードでの RIS インストーラの実行」

8.1 コンソールからのユーザアプリケーションのインストール

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

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

---

1. 15 ページの 表 2-1 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. 57 ページの第 5 章「JBoss でのユーザアプリケーションのインストール」の下にあるグラフィカルユーザインタフェースについて説明されたのと同じステップに従って、コマンドラインのプロンプトを読み、コマンドラインに対する応答を入力して、マスタキーをインポートまたは作成します。
4. ユーザアプリケーション環境設定パラメータを設定するには、手動で configupdate ユーティリティを起動します。コマンドラインで、configupdate.sh (Linux または Solaris) あるいは configupdate.bat (Windows) と入力して、155 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。

6 147 ページの第 9 章「インストール後のタスク」に進みます。

8.2 単一コマンドによるユーザアプリケーションのインストール

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

1 15 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 8-1 を参照してください。ユーザアプリケーション環境設定パラメータは、GUI またはコンソールインストール手順または configupdate ユーティリティで設定したのと同じパラメータです。

5 サイレントインストールは次の方法で起動します。

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

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

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

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_LDAPHOST=	eDirectory 接続設定 : LDAP ホスト。 LDAP サーバのホスト名または IP アドレスを指定します。

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

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

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

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_NOTFSMTPEMAILHOST=	電子メール : 通知 SMTP 電子メールホスト。 必須。プロビジョニング電子メールを使用している SMTP 電子メールホストを指定します。これは、IP アドレスまたは DNS 名が可能です。
NOVL_CONFIG_USEEXTPWDWAR=	パスワード管理 : 外部パスワード WAR の使用。 外部パスワード管理 WAR を使用している場合は、*[True]* を指定します。*[True]* を指定する場合は、*NOVL_CONFIG_EXTPWDWARPTH* および *NOVL_CONFIG_EXTPWDWARRTNPATH* の値も指定する必要があります。 デフォルトの内部パスワード管理機能を使用するには、*[False]* を指定します。/jsps/pwdmgt/ForgotPassword.jsp(最初は http(s) プロトコルなし)。これは、ユーザを、外部 WAR ではなく、ユーザアプリケーションに組み込まれた［パスワードを忘れた場合］機能にリダイレクトします。
NOVL_CONFIG_EXTPWDWARPATH=	パスワード管理 : パスワードを忘れた場合のリンク。 外部または内部のパスワード管理 WAR で、［パスワードを忘れた場合］機能ページ ForgotPassword.jsp の URL を指定します。または、デフォルトの内部パスワード管理 WAR をそのまま使用します。詳細については、150 ページの 「外部パスワードを忘れた場合の管理の環境設定」を参照してください。
NOVL_CONFIG_EXTPWDWARRTNPATH=	パスワード管理 : パスワードを忘れた場合の返信リンク。 ユーザがパスワードを忘れた場合の操作を実行した後でクリックできるように、パスワードを忘れた場合の返信リンクを指定します。
NOVL_CONFIG_FORGOTWEBSERVICEURL=	パスワード管理 : パスワードを忘れた場合の Web サービス URL。 これは、外部の［パスワードを忘れた場合］の War がコアのパスワードを忘れた場合の機能を実行するユーザアプリケーションを呼び戻すために使用する URL です。URL のフォーマットは次のとおりです。 `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
NOVL_CONFIG_USEROBJECTATTRIBUTE=	メタディレクトリユーザ ID: ユーザオブジェクトクラス。 必須。LDAP ユーザオブジェクトクラス (通常は inetOrgPerson)。

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

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

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_CONFIG_CREATEDIRECTORYINDEX	その他 : eDirectory インデックスの作成 サイレントインストーラで、NOVL_CONFIG_SERVERDN で指定した eDirectory サーバ上でマネージャ、ismanager、および srvprvUUID の属性のインデックスが作成されるようにする場合、［true］を指定します。このパラメータが［true］に設定されている場合、NOVL_CONFIG_REMOVEEDIRECTORYINDEX は ［true］に設定できません。 最良のパフォーマンス結果を得るには、インデックス作成が完了している必要があります。ユーザアプリケーションを利用可能な状態にする前にインデックスをオンラインモードにする必要があります。
NOVL_CONFIG_REMOVEDIRECTORYINDEX	その他 : eDirectory インデックスの削除 サイレントインストーラで、NOVL_CONFIG_SERVERDN で指定したサーバのインデックスが削除されるようにする場合、［true］を指定します。このパラメータが ［true］に設定されている場合、NOVL_CONFIG_CREATEEDIRECTORYINDEX は［true］に設定できません。
NOVL_CONFIG_SERVERDN	その他 : サーバ DN。 インデックスを作成または削除する必要のある eDirectory サーバを指定します。
NOVL_CREATE_DB	データベースの作成方法を示します。次の選択肢があります。 ◆ 即時 : データベースをすぐに作成します。 ◆ ファイル : SQL の出力をファイルに書き込みます。 ◆ 起動時 : アプリケーションの起動時にデータベースを作成します。
NOVL_DATABASE_NEW	データベースが新規か既存かを示します。新規データベースの場合、*［True］* を指定します。既存データベースの場合、*［False］* を指定します。

silent.properties にあるユーザアプリケーションのパラメータ名	ユーザアプリケーション環境設定パラメータファイルにある同等のパラメータ名
NOVL_RBPM_SEC_ADMINDN	セキュリティ管理者。 この役割により、メンバーはセキュリティドメイン内のすべての機能を付与されます。 セキュリティ管理者は、セキュリティドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。セキュリティドメインを使用すると、セキュリティ管理者は Roles Based Provisioning Module 内のすべてのドメインへのアクセス許可を設定できます。セキュリティ管理者はチームを構成でき、またドメイン管理者、委任管理者、およびその他のセキュリティ管理者も割り当てることができます。
NOVL_RBPM_RESOURCE_ADMINDN	リソース管理者。 この役割により、メンバーはリソースドメイン内のすべての機能を付与されます。リソース管理者はリソースドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。
NOVL_RBPM_CONFIG_ADMINDN	この役割により、メンバーは構成ドメイン内のすべての機能を付与されます。RBPM 設定管理者は、構成ドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。RBPM 設定管理者は、Roles Based Provisioning Module 内のナビゲーションアイテムへのアクセスを制御します。また、RBPM 設定管理者は委任と代理サービス、ユーザインタフェースのプロビジョニング、およびワークフローエンジンを設定します。
RUN_LDAPCONFIG=	即時または後でなど、いつ LDAP の設定を行うか指定します。次の値があります。 ◆ 即時: 指定されたLDAPの環境設定を使用して WAR ファイルに入力することで、LDAP 設定を即時実行します。 ◆ 後で : LDAP の設定を行わずにユーザアプリケーションのファイルのインストールのみを行います。

8.2.1 サイレントインストールを行う環境でのパスワードの設定

silent.properties ファイルの中にパスワードを指定するのを望まない場合は、代わりに環境内でパスワードを設定できます。この例では、サイレントインストーラが silent.properties ファイルからではなく、環境からパスワードを読み込みます。これにより、セキュリティが増強されます。

ユーザアプリケーションインストーラ用に次のパスワードを設定する必要があります。

- NOVL_DB_USER_PASSWORD
- NOVL_CONFIG_DBADMIN_PASSWORD

- NOVL_CONFIG_LDAPADMINPASS
- NOVL_CONFIG_KEYSTOREPASSWORD

Linux 上でパスワードを設定するには、次の例に示すように export コマンドを使用します。

```
export NOVL_DB_USER_PASSWORD=myPassWord
```

Windows 上でパスワードを設定するには、次の例のように、set コマンドを使用します。

```
set NOVL_DB_USER_PASSWORD=myPassWord
```

8.3 サイレントモードまたはコンソールモードでの JBossPostgreSQL ユーティリティの実行

JBossPostgreSQL ユーティリティは、コンソールモードまたはサイレントモードのいずれかで実行できます。サイレントモードでユーティリティを実行するには、JBossPostgreSQL ユーティリティのプロパティファイルをまず編集する必要があります。いったんプロパティファイルを編集したら、次のコマンドでそれを開始します。

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

例 :

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

JBossPostgreSQL サイレントインストールのプロパティを次に示します。

表 8-2 *JBossPostgreSQL 環境設定プロパティ*

プロパティ	説明
USER_INSTALL_DIR	JBoss および JRE をインストールするパス。 JBoss をインストールする場合に必要。それ以外は空白のままにします。
NOVL_DB_NAME	使用するデータベースの名前です。デフォルトのデータベース名は、idmuserappdb です。 PostgreSQL をインストールする場合は必須です。PostgreSQL をインストールするのでなければ、この値は無視されます。
NOVL_DB_PASSWORD	データベースのルートパスワードです。 PostgreSQL をインストールする場合は必須です。PostgreSQL をインストールするのでなければ、この値は無視されます。
NOVL_DB_PASSWORD_CONFIRM	データベースのルートパスワードを確認します。 PostgreSQL をインストールする場合は必須です。PostgreSQL をインストールするのでなければ、この値は無視されます。

プロパティ	説明
CHOSEN_INSTALL_FEATURE_LIST	インストール対象のインストールセットです。 必須。JBoss と PostgreSQL の両方を選択するか、それらの製品のうちのいずれかをインストールできます。 例 : `CHOSEN_INSTALL_FEATURE_LIST=JBoss, PostgreSQL` `CHOSEN_INSTALL_FEATURE_LIST=JBoss,""`
USER_MAGIC_FOLDER_1	PostgreSQL のインストールディレクトリの名前です。 PostgreSQL をインストールする場合は必須です。このプロパティは、CHOSEN_INSTALL_FEATURE_LIST が PostgreSQL を含まない場合は無視されます。
START_DB	インストーラがインストール時にデータベースを開始するかどうかを示します。インストーラにデータベースを開始させるには、Start という値を割り当てます。それ以外はこのプロパティを空白のままにします。 オプション。

8.3.1 サイレントインストールを行う環境でのパスワードの設定

silent.properties ファイルの中にパスワードを指定するのを望まない場合は、代わりに環境内でパスワードを設定できます。この例では、サイレントインストーラが silent.properties ファイルからではなく、環境からパスワードを読み込みます。これにより、セキュリティが増強されます。

ユーザアプリケーションインストーラ用に次のパスワードを設定する必要があります。

- NOVL_DB_PASSWORD
- NOVL_DB_USER_PASSWORD

Linux 上でパスワードを設定するには、次の例に示すように export コマンドを使用します。

```
export NOVL_DB_USER_PASSWORD=myPassWord
```

Windows 上でパスワードを設定するには、次の例のように、set コマンドを使用します。

```
set NOVL_DB_USER_PASSWORD=myPassWord
```

8.4 サイレントモードまたはコンソールモードでの RIS インストーラの実行

このリリースには、RIS (Rest Information Service) 機能を設定するのに使用できる別のインストーラが付属しています。この機能は、REST をサポートする RIS.war ファイルを設定します。RIS 経由で表示される REST リソースは、SOAP コールを実行し、さまざまな RBPM システムから情報を収集します。

RIS インストーラは、コンソールモードまたはサイレントモードのいずれかで実行できます。インストーラを実行するには、RIS インストーラのプロパティファイルをまず編集する必要があります。いったんプロパティファイルを編集したら、次のコマンドでそれを開始します。

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

例 :

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

インストーラは次の情報を要求します。

- RIS.war がある場所はどこか
- ユーザアプリケーションが実行するように設定してあるポートはどれか
- ユーザアプリケーション向けに定義されているコンテキストはどれか
- RIS.war が展開されるホスト名は何か

RIS のインストールには次のプロパティがあります。

表 8-3 *RIS 環境設定プロパティ*

プロパティ	説明
NOVL_INSTALL_HOST	RIS.war が展開されるホストの名前です。この名前は localhost にはできません。 必須。
NOVL_USERAPP_PORT	RBPM ユーザアプリケーションが実行するように設定してあるポートです。 必須。
NOVL_CONTEXT_NAME	ユーザアプリケーションのコンテキスト名です。 必須。
RIS_INSTALL_DIRECTORY	RIS.war が格納されているディレクトリです。 必須。
RIS_WAR_FILE	RIS.war ファイルの名前です。 この値は変更しないでください。

プロパティ	説明
RIS_INSTALL_LOG	インストーラのログファイルの名前です。このファイルには任意の名前を付けることができます。インストーラは、RIS_INSTALL_DIR プロパティで指定された場所にファイルを書き込みます。 このプロパティを空白のままにすると、RIS-Install.log がデフォルトのログファイルになります。 オプション。

インストール後のタスク

9

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

9.1 マスタキーの記録

インストール後すぐに、暗号化マスタキーをコピーして安全な場所に記録します。

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

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

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

9.2 ユーザアプリケーションの環境設定

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

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

9.2.1 ログの設定

ログを設定するには、『ユーザアプリケーション : 管理ガイド (http://www.novell.com/documentation/idm40/index.html)』の「ログの設定」セクションの手順に従います。

9.3 eDirectory の設定

9.3.1 eDirectory でのインデックスの作成

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

これらのインデックスは、*［ユーザアプリケーション環境設定］*パネルの *［詳細］*タブの［eDirectory インデックスの作成］が選択されている場合、インストール中に自動的に作成できます (158 ページの 表 A-2 で説明されています)。インデックスを作成するためにインデックスマネージャを使用する手順については、『*Novell eDirectory 管理ガイド* (http://www.novell.com/documentation)』を参照してください。

9.3.2 SAML 認証メソッドのインストールおよび環境設定

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

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

     次の例で、Linux 上でこれを実行する方法を説明します。

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

     次の例で、Linux 上でこれを実行する方法を説明します。

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

eDirectory の属性の編集

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

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

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

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

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

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

6d *[OK]* をクリックします。

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

6f *[OK]* をクリックします。

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

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

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

8b *[すべてのオブジェクトクラスの表示]* を再び選択します。

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

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

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

9 オブジェクトビューアに戻ります。

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

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

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

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

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

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

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

   ConfigUpdate ユーティリティのパラメータの詳細については 155 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」、132 ページの 表 8-1 を参照してください。

2. 新しい WAR ファイルをアプリケーションサーバに展開します。

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

9.5 外部パスワードを忘れた場合の管理の環境設定

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

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

9.5.1 外部パスワードを忘れた場合の管理 WAR の指定

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

   ホストおよびポートを含めます。たとえば、http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp。外部パスワード WAR は、ユーザアプリケーションを保護するファイアウォールの外側にできます。
4. *［パスワードを忘れた場合の返信リンク］* では、パスワードを忘れたプロシージャの実行完了後に表示するリンクを指定します。このリンクをクリックすると、指定したリンクにリダイレクトされます。
5. *［パスワードを忘れた場合の Web サービス URL］* では、外部パスワードを忘れた場合の WAR を使用してユーザアプリケーションを呼び戻す Web サービスの URL を指定します。URL のフォーマットは次のとおりです。https://*<idmhost>*:*<sslport>*/*<idm>*/pwdmgt/service.

返信リンクでは、SSL を使用して、ユーザアプリケーションにセキュアな Web サービス通信を確保する必要があります。151 ページのセクション 9.5.4「JBoss サーバ間の SSL 通信の設定」も参照してください。

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

9.5.2 内部パスワード WAR の指定

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

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

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

9.5.3 外部パスワードを忘れた場合の WAR 環境設定のテスト

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

- ブラウザ内で直接アクセスします。外部パスワード WAR で［パスワードを忘れた場合］ページに移動します。たとえば、http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp に移動します。
- ユーザアプリケーションのログインページで、*［パスワードを忘れた場合］*リンクをクリックします。

9.5.4 JBoss サーバ間の SSL 通信の設定

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

9.6 ［パスワードを忘れた場合の設定］の更新

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

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

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

- *［パスワードを忘れた場合のリンク］* (たとえば http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp)

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

9.7 セキュリティ上の考慮事項

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

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

9.8 Identity Manager Java Heap サイズの増加

エンタープライズ環境では、役割とリソースのサービスドライバは、Identity Manager で定義されているデフォルトの量よりも大きな Java の最大ヒープサイズを必要とします。OutOfMemoryError 状態を避けるために Java の最大ヒープサイズを 256MB にすることを推奨します。

Java のヒープサイズは、iManager を使用して、ドライバセットプロパティの［Misc (その他)］セクションから指定するか、DHOST_JVM_INITIAL_HEAP および DHOST_JVM_MAX_HEAP 環境変数を設定することで指定できます。Java VM オプションの設定の詳細については、『Identity Manager Common Driver Administration Guide (http://www.novell.com/documentation/idm40/idm_common_driver/index.html?page=/documentation/idm40/idm_common_driver/data/front.html)』を参照してください。

9.9 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`

項目	推奨されるアクション
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 8180 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 8180 以外のポートを使用する場合は、必ず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、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`

ユーザアプリケーション環境設定の参照

A

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

A.1 ユーザアプリケーション環境設定 : 基本パラメータ

図 A-1 *ユーザアプリケーション環境設定の基本オプション*

表 A-1 *ユーザアプリケーション環境設定の基本オプション*

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

設定のタイプ	オプション	説明
識別ボールト DN	*ルートコンテナ DN*	必須。ルートコンテナの LDAP 識別名を指定します。これは、ディレクトリ抽象化層で検索ルートが指定されない場合に、デフォルトのエンティティ定義検索ルートとして使用されます。
	ユーザアプリケーションドライバ DN	必須。ユーザアプリケーションドライバの識別名を指定します。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。
	RBPM Context name (RBPM コンテキスト名)	現在のコンテキスト名を表示します。
	RBPM Reporting Admin (RBPM レポーティング管理)	レポーティング管理者を指し示します。デフォルトでは、インストーラが他のセキュリティフィールドと同じユーザにこの値を設定します。

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

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

設定のタイプ	オプション	説明
	役割管理者	この役割を使用すると、そのメンバーはすべての役割の作成、削除、変更、およびユーザ、グループ、またはコンテナへの役割の付与または取り消しを行うことができます。さらに役割のメンバーは、任意のユーザに対してレポートを実行できます。デフォルトでは、この役割にはユーザアプリケーション管理者が割り当てられています。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの*［管理］>［管理者の割り当て］*ページを使用します。 configupdate の間、この値への変更は、有効な役割管理者が割り当てられていない場合のみ反映されます。有効な役割管理者が存在する場合は、変更は保存されません。
	セキュリティ管理者	この役割により、メンバーはセキュリティドメイン内のすべての機能を付与されます。 セキュリティ管理者は、セキュリティドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。セキュリティドメインを使用すると、セキュリティ管理者は Roles Based Provisioning Module 内のすべてのドメインへのアクセス許可を設定できます。セキュリティ管理者はチームを構成でき、またドメイン管理者、委任管理者、およびその他のセキュリティ管理者も割り当てることができます。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの*［管理］>［管理者の割り当て］*ページを使用します。
	リソース管理者	この役割により、メンバーはリソースドメイン内のすべての機能を付与されます。リソース管理者はリソースドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの*［管理］>［管理者の割り当て］*ページを使用します。
	RBPM 設定管理者	この役割により、メンバーは構成ドメイン内のすべての機能を付与されます。RBPM 設定管理者は、構成ドメイン内のすべてのオブジェクトで可能なアクションをすべて実行できます。RBPM 設定管理者は、Roles Based Provisioning Module 内のナビゲーションアイテムへのアクセスを制御します。また、RBPM 設定管理者は委任と代理サービス、ユーザインタフェースのプロビジョニング、およびワークフローエンジンを設定します。 ユーザアプリケーションを展開した後でこの割り当てを変更するには、ユーザアプリケーションの*［管理］>［管理者の割り当て］*ページを使用します。
	RBPM Reporting Admin (RBPM レポーティング管理)	レポーティング管理者を指し示します。デフォルトでは、インストーラが他のセキュリティフィールドと同じユーザにこの値を設定します。

設定のタイプ	オプション	説明
	Reinitialize RBPM Security (RBPM セキュリティの再初期化)	セキュリティをリセットできるチェックボックスです。
	IDMReport URL	Identity Reporting Module のユーザインタフェースを指し示す URL です。
識別ボールトユーザ ID	*ユーザ コンテナ DN*	必須。ユーザコンテナの LDAP 識別名 (DN) または完全修飾 LDAP 名を指定します。 このコンテナ内 (およびその下) のユーザが、ユーザアプリケーションにログインできます。 ユーザアプリケーションをホストしているアプリケーションサーバをすでに起動している場合、この設定は configupdate を介して変更できません。 **重要 :** ユーザによるワークフローの実行を可能とさせる場合は、ユーザアプリケーションドライバの設定中に指定したユーザアプリケーション管理者が、確実にこのコンテナに存在するようにしてください。
	ユーザコンテナのスコープ	これにより、ユーザの検索スコープが定義されます。
	ユーザオブジェクトクラス	LDAP ユーザオブジェクトクラス (通常は inetOrgPerson)。
	ログイン属性	ユーザのログイン名を表す LDAP 属性 (たとえば CN)。
	名前付け属性	ユーザまたはグループをルックアップする際に ID として使用する LDAP 属性これはログイン属性と同じではありません。ログイン属性はログイン中にのみ使用し、ユーザおよびグループの検索中には使用しません。
	ユーザメンバーシップ属性	オプション。ユーザのグループメンバーシップを表す LDAP 属性です。この名前にはスペースを使用しないでください。

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

設定のタイプ	オプション	説明
	キーストアタイプPKCS12	使用するデジタル署名のタイプを示します。このフィールドがチェックされている場合、トラステッドストアパスはタイプ PKCS12 です。
Novell Audit デジタル署名および証明書キー		監査サービスのためのデジタル署名キーおよび証明書を含みます。
	Novell Audit デジタル署名証明書	監査サービスのためのデジタル署名証明書を表示します。
	Novell Audit デジタル署名秘密鍵	デジタル署名秘密鍵が表示されます。このキーは、マスタキーに基づいて暗号化されます。
Access Manager の設定	*同時ログアウト有効*	このオプションが選択されている場合は、ユーザアプリケーションによってユーザアプリケーションおよびNovell Access Manager または iChain の同時ログアウトがサポートされます。Novell Access Manager または iChain はログアウト時に Cookie をチェックし、Cookie が存在する場合は、ユーザを ICS ログアウトページに再ルーティングします。
	［同時ログアウト］ページ	Novell Access Manager または iChain ログアウトページへの URL。URL は Novell Access Manager または iChain が期待するホスト名です。ICS ログが有効な場合は、ユーザはユーザアプリケーションからログアウトし、ユーザはこのページを再ルーティングします。

設定のタイプ	オプション	説明
電子メール サーバの設定	*NotificationTemplate ホスト*	Identity Manager ユーザアプリケーションをホストしているアプリケーションサーバを指定します。たとえば、次のようにします。 `myapplication serverServer` この値は、電子メールテンプレートの $HOST$ トークンと置き換えられます。作成される url は、プロビジョニング要求タスクと承認通知へのリンクです。
	通知テンプレート PORT	プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $PORT$ トークンの置き換えに使用されます。
	通知テンプレート SECURE PORT	プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $SECURE_PORT$ トークンの置き換えに使用します。
	通知テンプレート PROTOCOL	非セキュアプロトコル、HTTP を参照してください。プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $PROTOCOL$ トークンの置き換えに使用します。
	通知テンプレート SECURE PROTOCOL	セキュアプロトコル、HTTP を参照してください。プロビジョニング要求タスクと承認通知で使用する電子メールテンプレートの $SECURE_PROTOCOL$ トークンの置き換えに使用されます。
	通知 SMTP 電子メール送信者 :	プロビジョニング電子メール内のユーザからの電子メールを指定します。
	SMTP サーバ名	プロビジョニング電子メールを使用している SMTP 電子メールホストを指定します。これは、IP アドレスまたは DNS 名が可能です。
パスワード管理		
	外部パスワード WAR の使用	この機能によって、外部の［パスワードを忘れた場合］の War にある［パスワードを忘れた場合］ページと、外部の［パスワードを忘れた場合］の WAR が Web サービスを経由してユーザアプリケーションを呼び戻すのに使用する URL を指定できます。 *［外部パスワード WAR の使用］* を選択した場合、*［パスワードを忘れた場合のリンク］*、*［パスワードを忘れた場合の返信リンク］*、および *［パスワードを忘れた場合の Web サービス URL］* に値を入力する必要があります。 *［外部パスワード War の使用］* を選択しない場合は、デフォルトの内部パスワード管理機能が使用されます。/jsps/pwdmgt/ForgotPassword.jsp(最初は http(s) プロトコルなし)。これは、ユーザを、外部 WAR ではなく、ユーザアプリケーションに組み込まれた［パスワードを忘れた場合］機能にリダイレクトします。
	パスワードを忘れた場合のリンク	この URL は［パスワードを忘れた場合］機能ページを指します。外部または内部のパスワード管理 WAR にある ForgotPassword.jsp ファイルを指定します。

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	ユーザがパスワードを忘れた場合の操作を実行した後でクリックできるように、*［パスワードを忘れた場合の返信リンク］*を指定します。
	［パスワードを忘れた場合の Web サービス URL］	これは、外部の［パスワードを忘れた場合］の War がコアのパスワードを忘れた場合の機能を実行するユーザアプリケーションを呼び戻すために使用する URL です。URL のフォーマットは次のとおりです。 `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
その他	*セッションのタイムアウト*	アプリケーションセッションのタイムアウト。
	OCSP URI	クライアントインストールが On-Line Certificate Status Protocol (OCSP) を使用する場合は、Uniform Resource Identifier (URI) を指定します。たとえば、フォーマットは http://host:port/ocspLocal です。OCSP URI によって、トラステッド証明書オンラインの状態は更新されます。
	許可設定パス	許可環境設定ファイルの完全修飾名。
	識別ボールトインデックスの作成	インストールユーティリティでマネージャ、ismanager、および srvprvUUID の属性のインデックスを作成する場合、このチェックボックスを選択します。これらの属性にインデックスがない場合、ユーザアプリケーションのユーザは、特にクラスタ化された環境ではユーザアプリケーションが低いパフォーマンスの状態にあります。ユーザアプリケーションをインストール後、iManager を使用して、手動でこれらのインデックスを作成できます。詳細については、148 ページのセクション 9.3.1「eDirectory でのインデックスの作成」を参照してください。 最良のパフォーマンスを得るには、インデックス作成が完了している必要があります。ユーザアプリケーションを利用可能な状態にする前にインデックスをオンラインモードにする必要があります。
	識別ボールトインデックスの削除	マネージャ、ismanager、および srvprvUUID の属性のインデックスを削除します。
	サーバ DN	インデックスを作成または削除する必要のある eDirectory サーバを選択します。 **注 :** 複数の eDirectory サーバでインデックスの環境設定を行うには、configupdate ユーティリティを複数回実行する必要があります。一度に指定できるのは 1 つのサーバのみです。

設定のタイプ	オプション	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名、LDAP を指定します。
	新規コンテナオブジェクトの追加: コンテナ属性名	コンテナオブジェクトの属性名を指定します。