Oracle® WebCenter Sites

サポート・ソフトウェアの構成

11*g* リリース 1 (11.1.1)

部品番号 : B69695-01

2012 年 4 月

ORACLE®

Oracle® WebCenter Sites: サポート・ソフトウェアの構成 , 11*g* リリース 1 (11.1.1)

部品番号 : B69695-01

原本名 : Oracle® WebCenter Sites: Configuring Supporting Software, 11*g* Release 1 (11.1.1)

原本主著者 : Melinda Rubenau、Sean Cearley

原本協力者 : Eric Gandt、Guthrie Taber、Gaurang Mavadiya、William Habermaas

目次

第 2 部 Web サーバーのインストール

第 3 部 LDAP サーバーのインストールおよび構成

このガイドについて

このガイドでは、Oracle WebCenter Sites により使用されるデータベース、Web サーバー、その他のソフトウェアの事前インストールおよび構成について説明します。

このガイドで説明しているアプリケーションは、旧 FatWire の製品です。命名規則は次のとおりです。

- *Oracle WebCenter Sites* は、以前は *FatWire Content Server* と呼ばれていたアプリケーションの現在の名前です。このガイドでは、*Oracle WebCenter Sites* を *WebCenter Sites* と呼ぶこともあります。
- *Oracle WebCenter Sites: Satellite Server* は、以前は *FatWire Satellite Server* と呼ばれていたアプリケーションの現在の名前です。このガイドでは、*Oracle WebCenter Sites: Satellite Server* を *Satellite Server* と呼ぶこともあります。

対象読者

このガイドは、データベース、データベース・ドライバ、アプリケーション・サーバー、Web サーバー、LDAP サーバーなど、エンタープライズ・レベルのソフトウェアのインストールおよび構成経験のあるインストール・エンジニアを対象としています。

このガイドの構成

このガイドは次の部で構成されています。

- 第 1 部「データベースの作成および構成」では、WebCenter Sites をインストールする前に、サポートされるデータベースを作成および構成する方法について説明します。(この部分は WebCenter Sites インストール・ガイドの補足です。)
- 第 2 部「Web サーバーのインストール」では、サポートされる Web サーバーの使用を選択したときに、このサーバーをインストールおよび構成する方法について説明します。(この部分は WebCenter Sites インストール・ガイドの補足です。)

- 第 3 部「LDAP サーバーのインストールおよび構成」では、WebCenter Sites との統合に備えて、サポートされている LDAP サーバーをセットアップする方法について説明します。(この部分は *『Oracle WebCenter Sites: LDAP との統合』* というガイドの補足です。)
- 第 4 部「認証サービスのインストールおよび構成」では、WebCenter Sites を、認証サービスおよびシングル・サインオンを提供するサポートされたサード・パーティ・アプリケーションと統合する方法について説明します。(この部分は WebCenter Sites インストール・ガイドの補足です。)

関連ドキュメント

詳細は、次のドキュメントを参照してください。

- *Oracle WebCenter Sites: Apache Tomcat Application Server へのインストール*
- *Oracle WebCenter Sites: IBM WebSphere Application Server へのインストール*
- *Oracle WebCenter Sites: Oracle WebLogic Application Server へのインストール*
- *Oracle WebCenter Sites: Satellite Server のインストール*

このガイド内の図

このガイドの図は、インストールまたは構成プロセスでユーザーが操作するダイアログ・ボックスおよび類似ウィンドウのスクリーン・キャプチャを示しています。図は、インストールおよび構成プロセスを理解しやすくするためのものです。パラメータ値、選択するオプション、製品のバージョン番号などの情報を示すことは目的としていません。

表記規則

このガイドでは、次の表記規則を使用します。

- **太字**は、ユーザーが選択するグラフィカル・ユーザー・インタフェース要素を示します。
- *斜体*は、ドキュメントのタイトル、強調、またはユーザーが特定の値を指定する変数を示します。
- 等幅フォントは、ファイル名、URL、サンプル・コード、または画面に表示されるテキストを示します。
- **等幅太字フォント**は、コマンドを示します。

サード・パーティのライブラリ

Oracle WebCenter Sites およびそのアプリケーションには、サード・パーティのライブラリが含まれています。詳細は、*Oracle WebCenter Sites 11gR1: サード・パーティのライセンス*を参照してください。

第 1 部

データベースの作成および構成

WebCenter Sites は、WebCenter Sites 用に特別に構成された、サポートされているデータベースへのアクセスを必要とします。サポートされているデータベースの作成および構成手順は、次の章で説明します。

- 第 1 章「Oracle 11g データベースの作成および構成」
- 第 2 章「MS SQL Server データベースの作成および構成」
- 第 3 章「IBM DB2 9.7 データベースの作成および構成」

上記のデータベースは本番用に構成されていません。これらはすべての権限を持つように設定されています。実際には、WebCenter Sites がデータベースへのアクセスに使用するユーザーに権限を限定できます。ただし、表や索引を作成、変更および削除できる権限は必要です。

サポートされているデータベースのインストール手順については、製品のドキュメントを参照してください。サポートされているデータベースの作成および構成手順については、前述の各章を参照してください。(データベース構成は、異なるアプリケーション・サーバーにわたって同一であることに注意してください。)

第 1 章

Oracle 11*g* データベースの作成および構成

この章では、WebCenter Sites インストールでの、Oracle 11*g* データベースの設定について説明します。データベース構成とユーザーの権限の背景情報は、第 1 部「データベースの作成および構成」を参照してください。

この章は、次の項で構成されています。

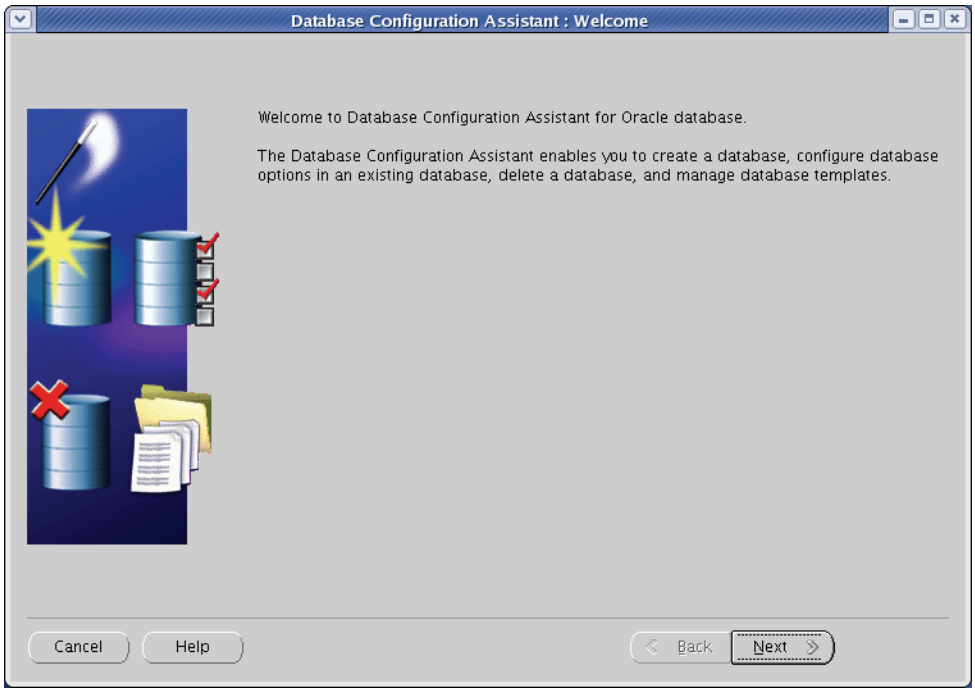
- 手順 I. Oracle 11g データベースの作成
- 手順 II. WebCenter Sites 用新規ユーザーの作成

手順 I. Oracle 11*g* データベースの作成

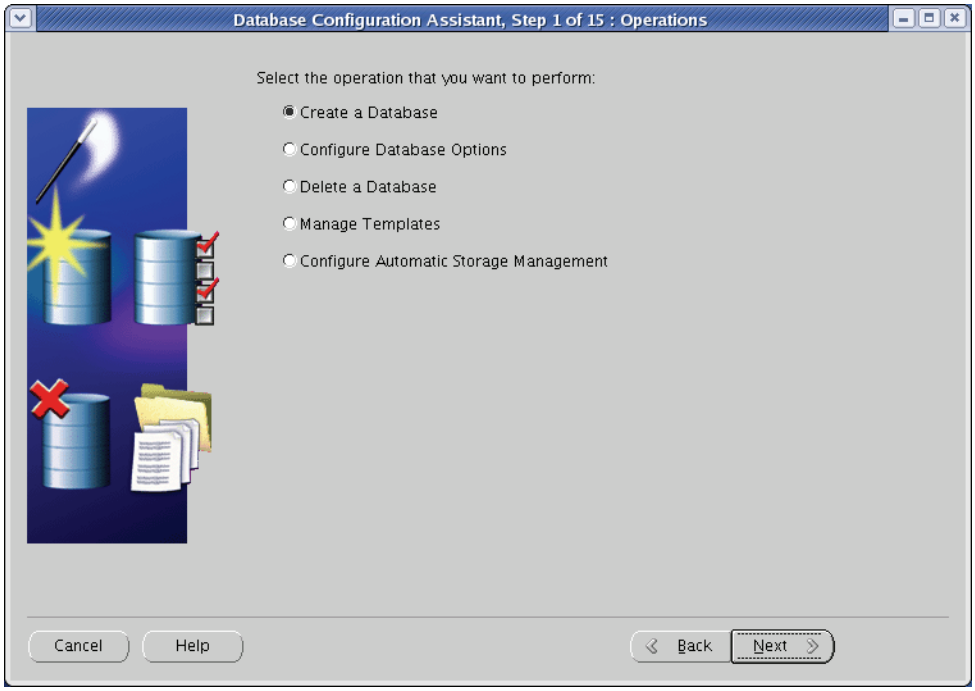
1. 次のコマンドを実行して、Oracle Database Configuration Assistant を起動します。

   <ora_home>/bin/dbca

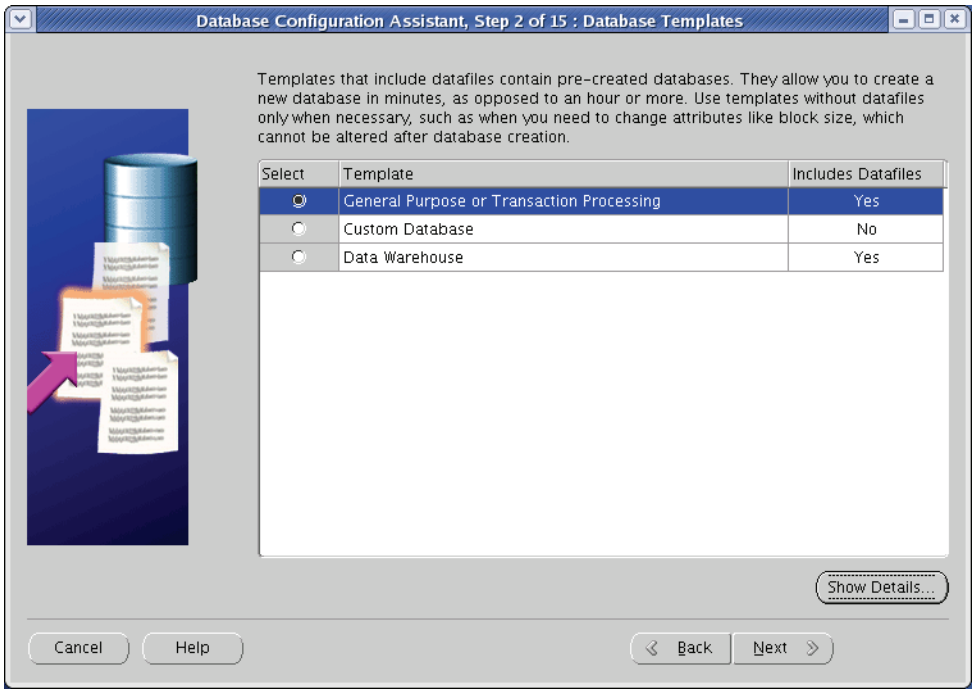
2. 「ようこそ」画面で「**次へ**」をクリックします。



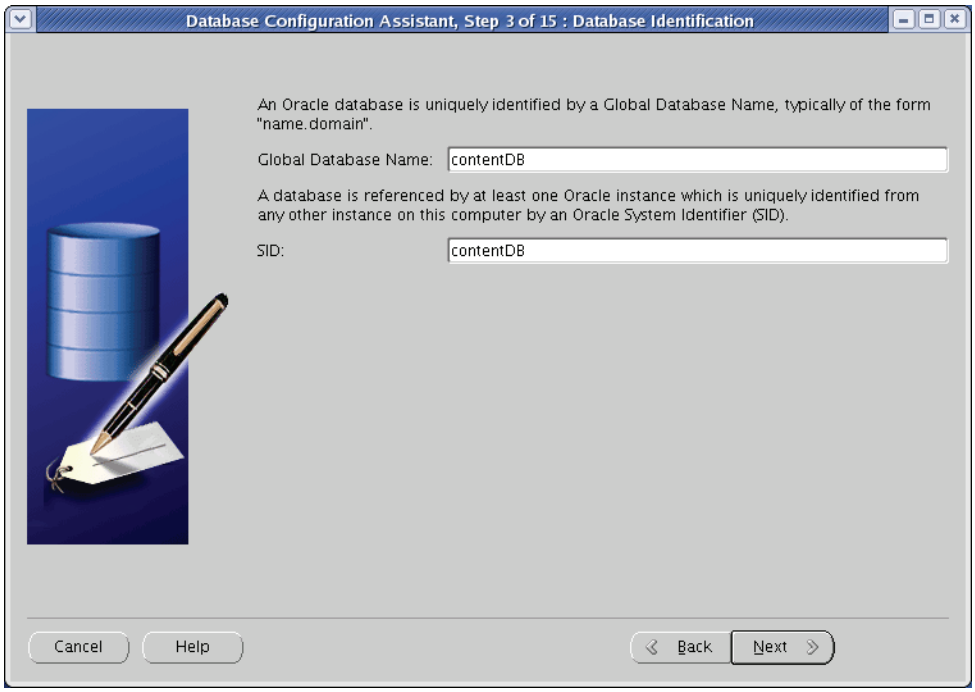
3. 「操作」画面で、**「データベースの作成」**を選択し、**「次へ」**をクリックします。



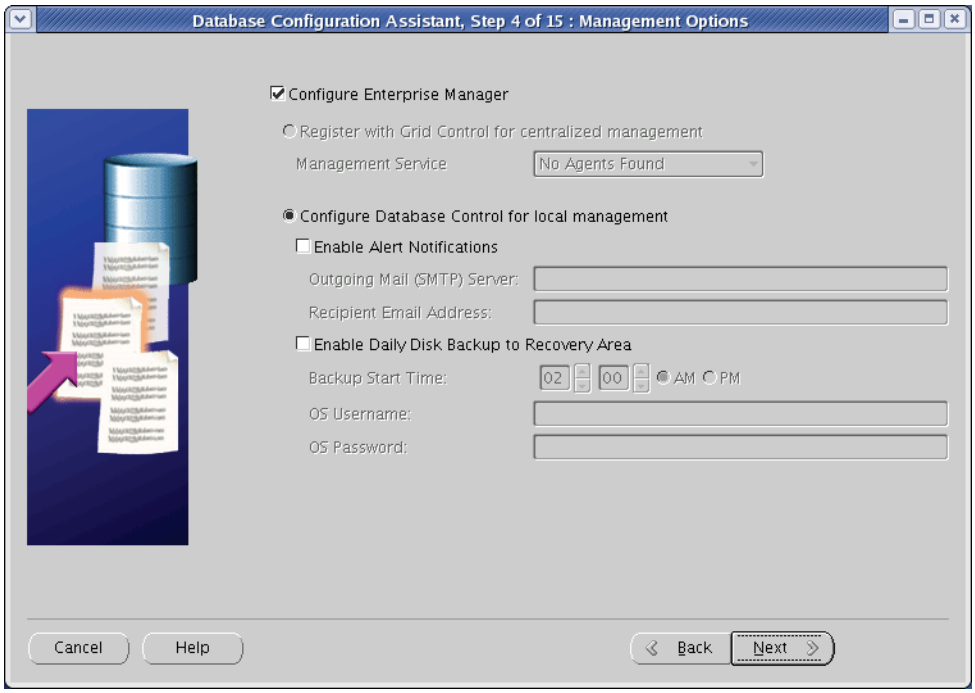
4. 「データベース・テンプレート」画面で、**「汎用またはトランザクション処理」**を選択し、**「次へ」**をクリックします。



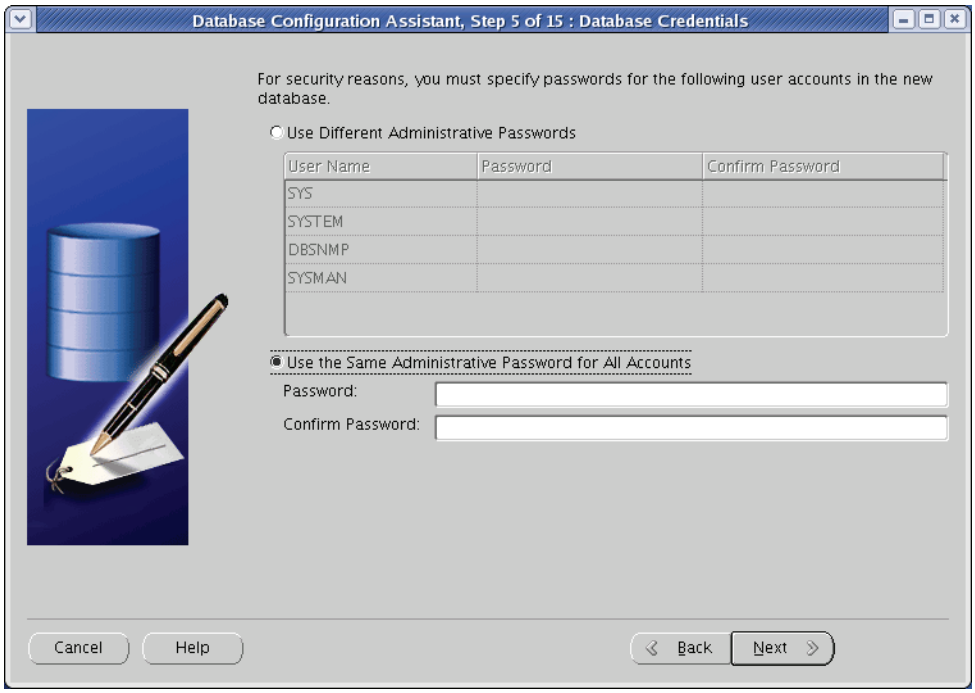
5. 「データベース識別情報」画面に、グローバル・データベース名および SID を入力します。(両方に同じ値を使用することをお薦めします。この例では、`contentDB` を使用しています。) 終了したら、「**次へ**」をクリックします。



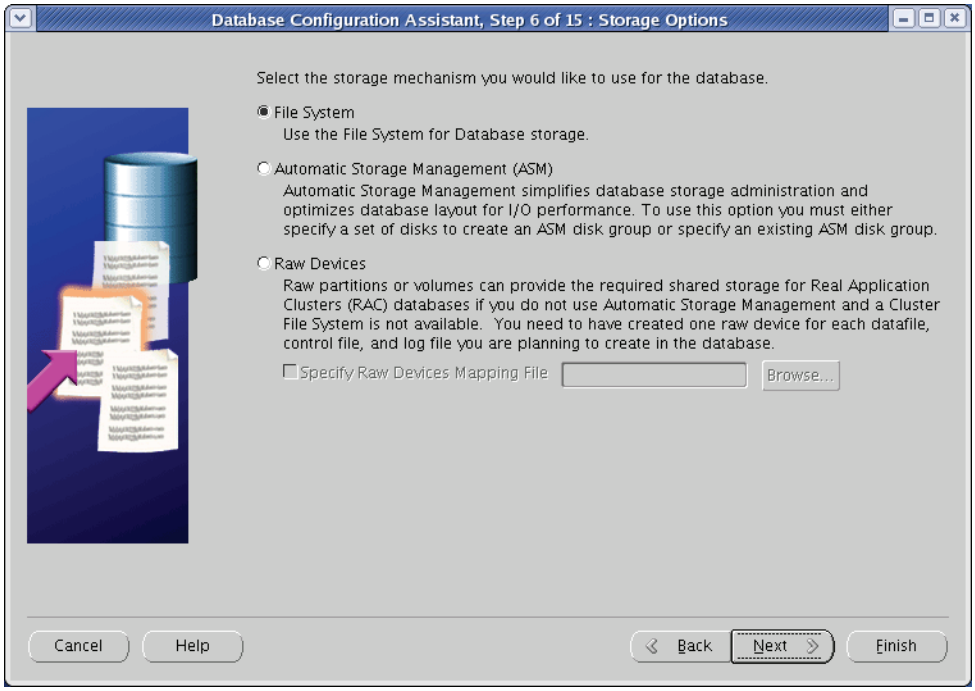
6. 「管理オプション」画面で、「**Enterprise Manager の構成**」チェック・ボックスを選択します。必要に応じて、その他のオプションを選択します。終了したら、「**次へ**」をクリックします。



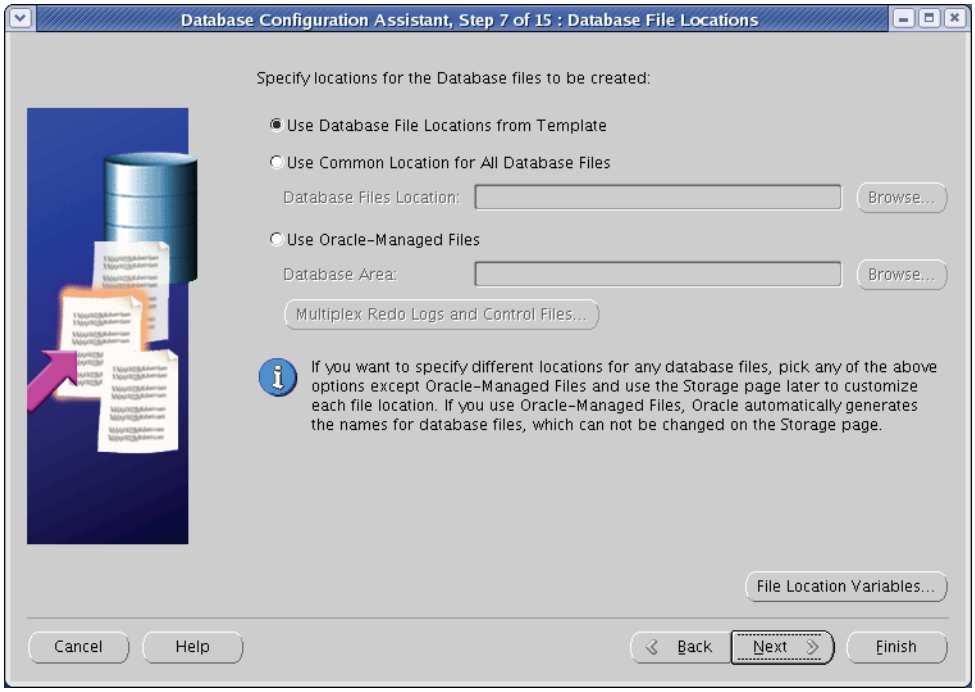
7. 「データベース資格証明」画面で、次のいずれかを実行します。
   - 本番システムをインストールしている場合は、**「別の管理パスワードを使用」**を選択し、表に表示されているデータベース・ユーザーそれぞれに一意のパスワードを入力して、**「次へ」**をクリックします。
   - 非本番システムをインストールしている場合は、**「すべてのアカウントに同じ管理パスワードを使用」**を選択し、パスワードを再入力して、**「次へ」**をクリックします。



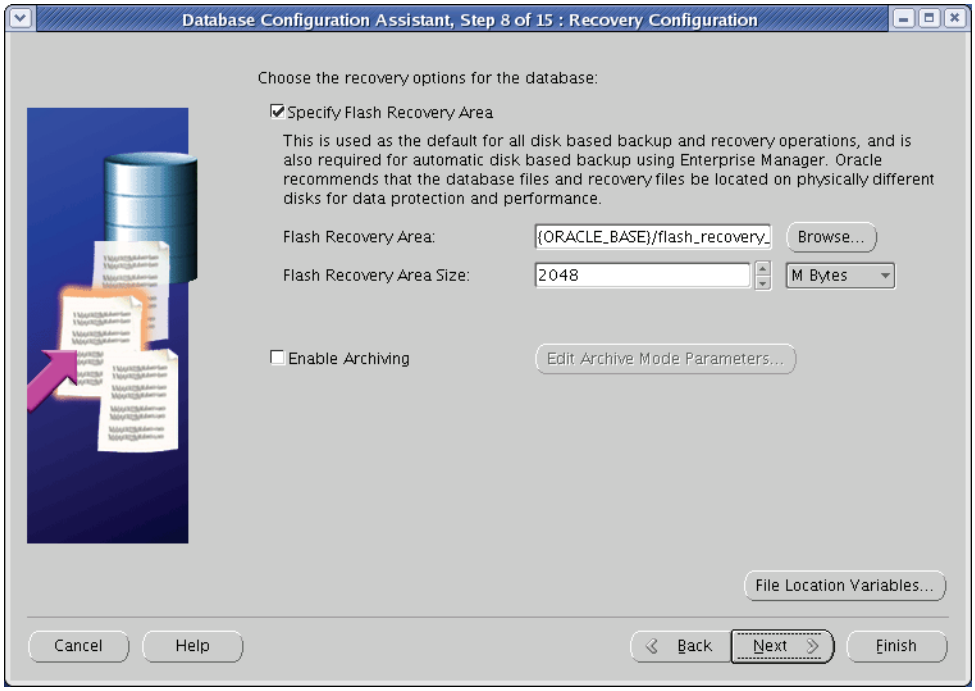
8. 「記憶域オプション」画面で、「**ファイルシステム**」を選択し、「**次へ**」をクリックします。



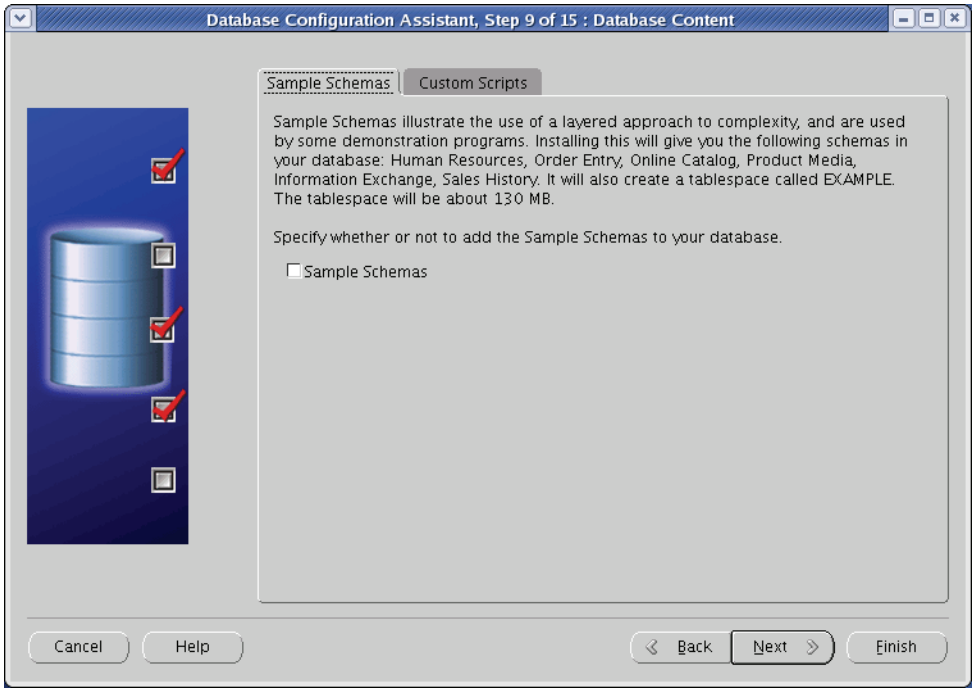
9. 「データベース・ファイルの位置」画面で、(カスタム・ファイル名と場所を使用する場合を除き) 「**テンプレートのデータベース・ファイル位置を使用**」を選択し、「**次へ**」をクリックします。



10. 「リカバリ構成」画面で、デフォルト値をそのまま残し、「**次へ**」をクリックします。

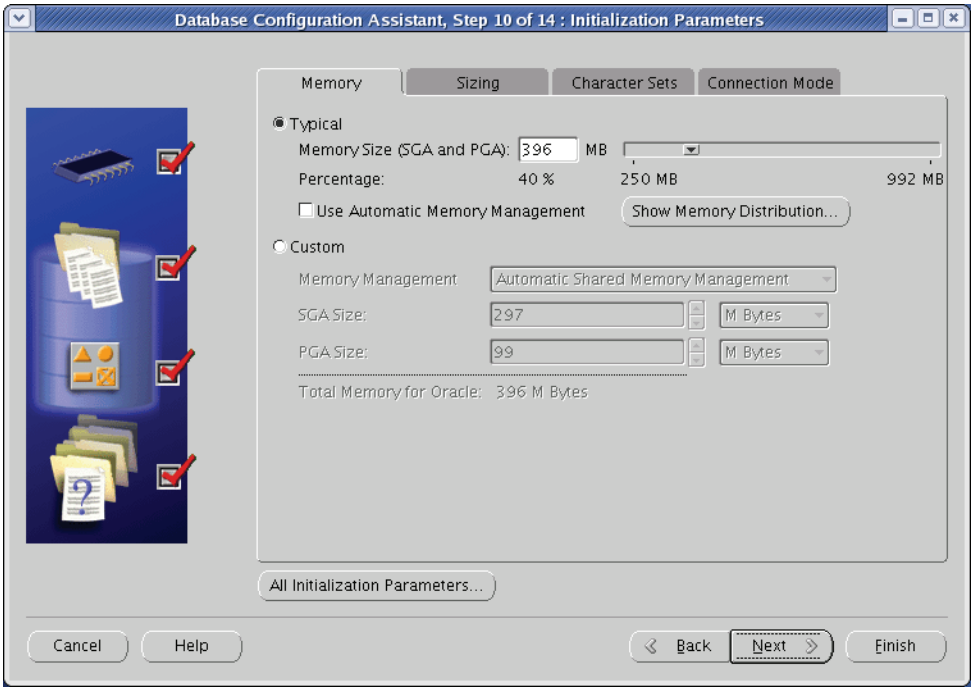


11. 「データベース・コンテンツ」画面で「**次へ**」をクリックします。



12. 「初期化パラメータ」画面で、次の手順を実行します。

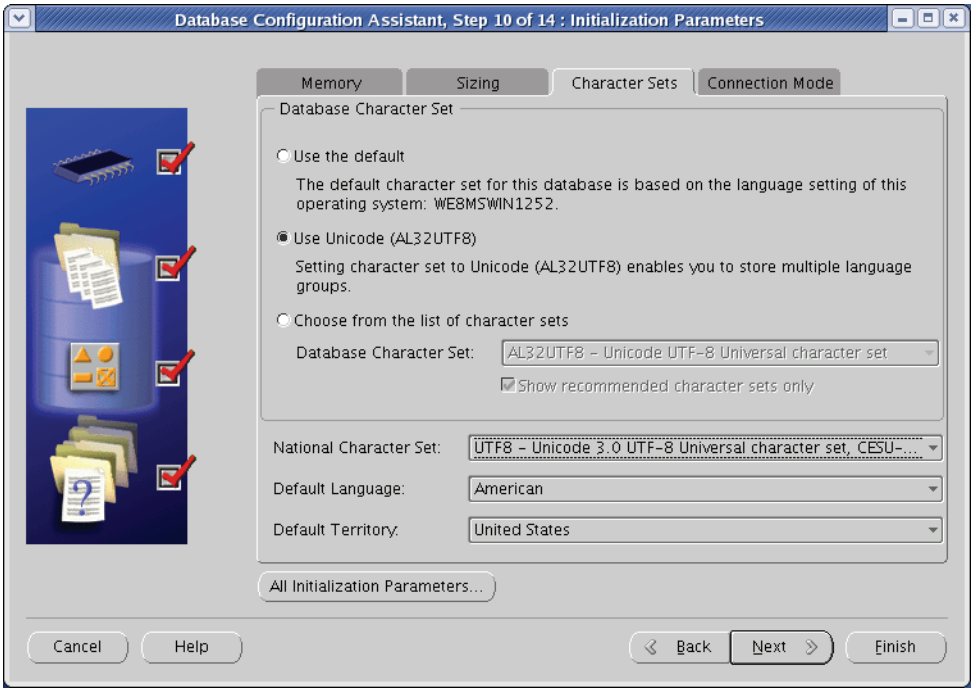
a. 「**メモリー**」タブで、データベースのメモリー・サイズを設定します。ここで入力する値は、データベースのサイズと内容によって異なります。推奨される最小値は 384MB です。



b. 「**キャラクタ・セット**」タブで、次の手順を実行します。

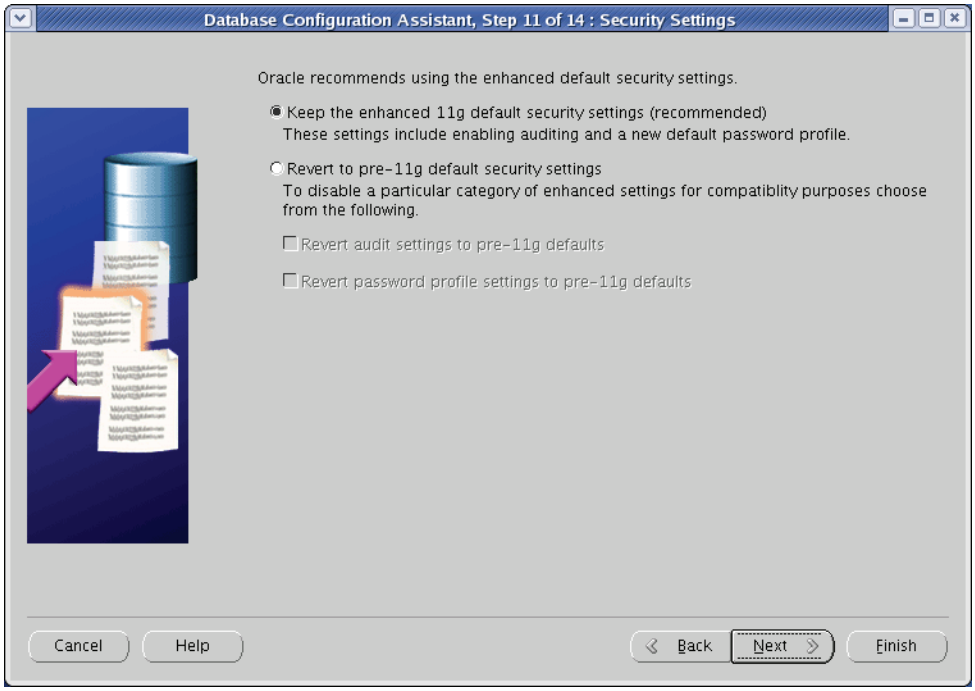
1) 「**Unicode (AL32UTF8) を使用**」ラジオ・ボタンを選択します。

2) 「各国語キャラクタ・セット」ドロップダウン・リストで、**UTF-8 - Unicode 3.0 UTF-8 汎用キャラクタ・セット**を選択します。

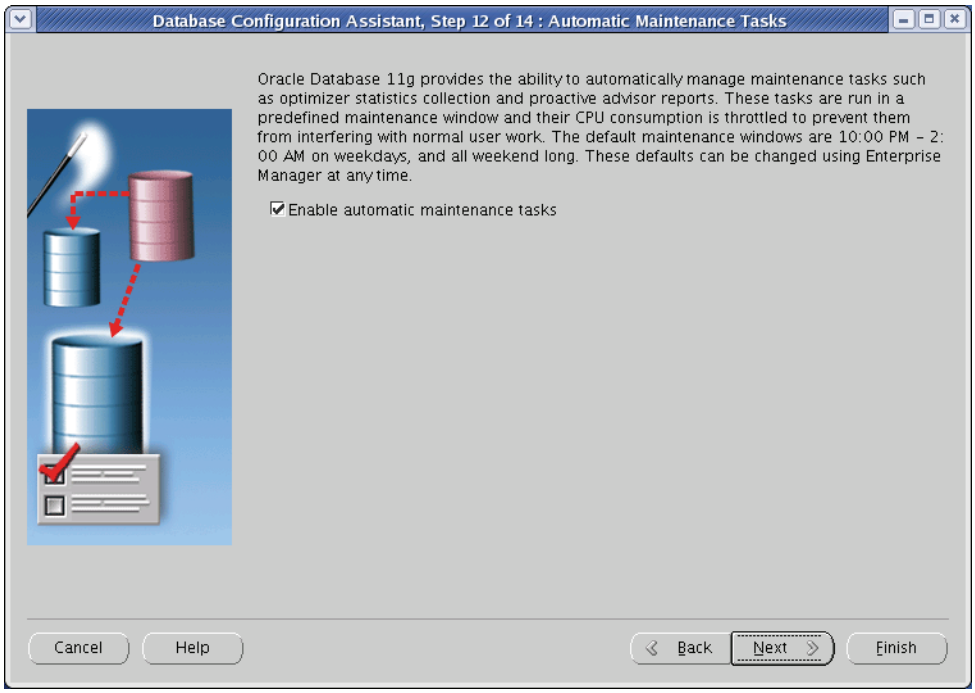


c. 「**次へ**」をクリックします。

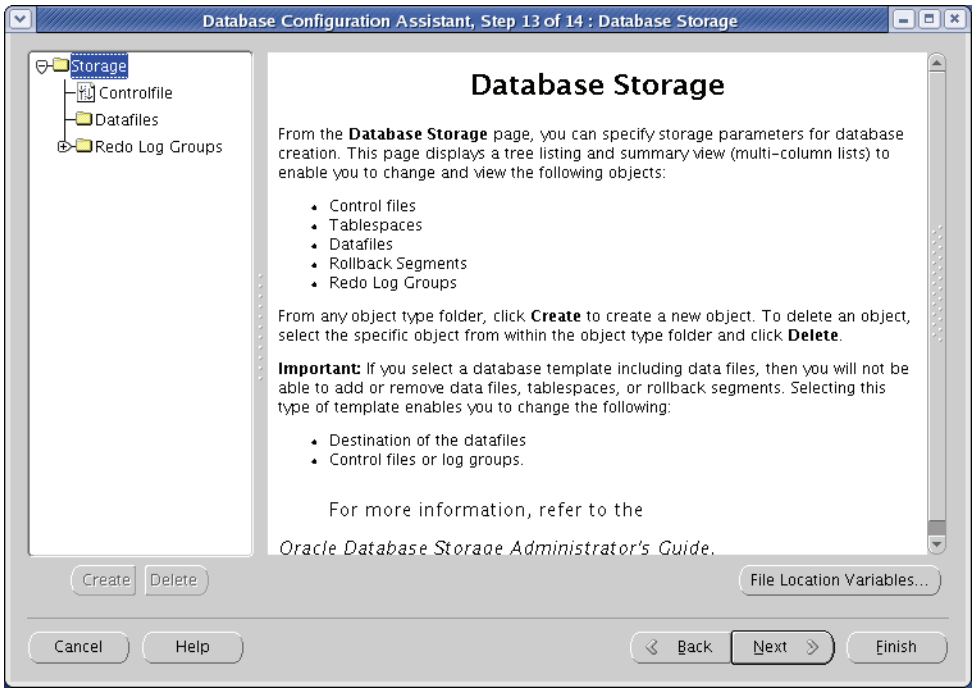
13.「セキュリティ設定」画面で「**次へ**」をクリックします。



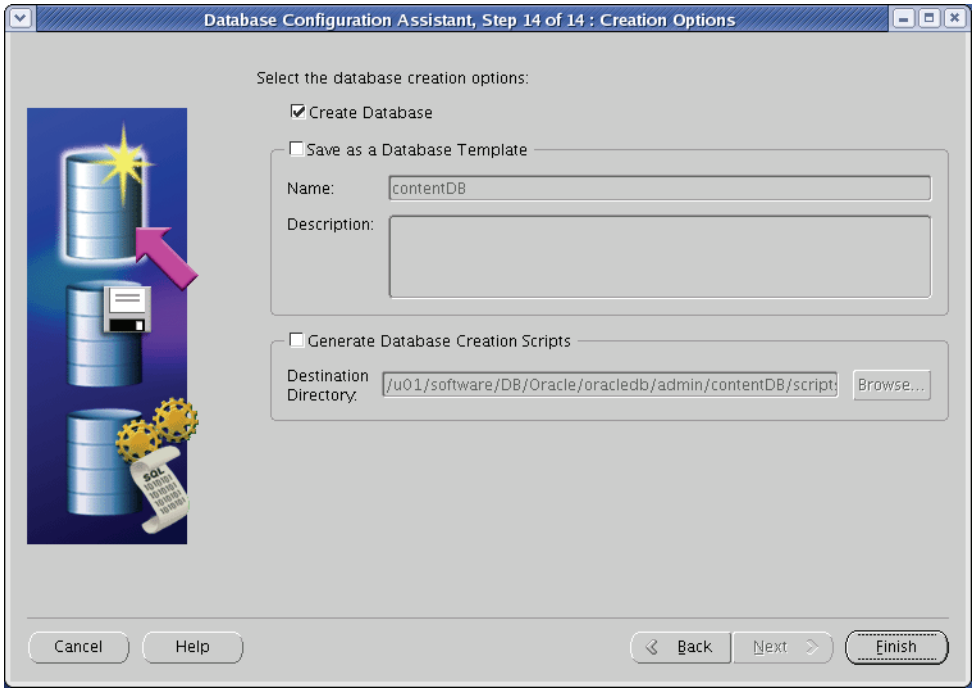
14.「自動メンテナンス・タスク」画面で「**次へ**」をクリックします。



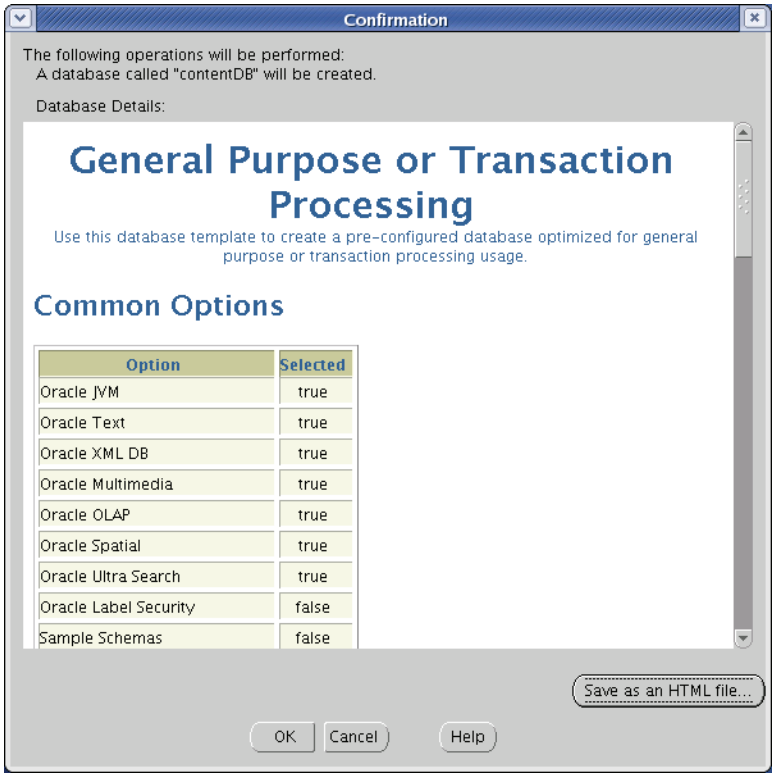
15. 「データベース記憶域」画面で、選択したファイルの場所を確認します。(変更が必要な場合は、**「ファイルの位置変数」**をクリックします。)**「次へ」**をクリックします。



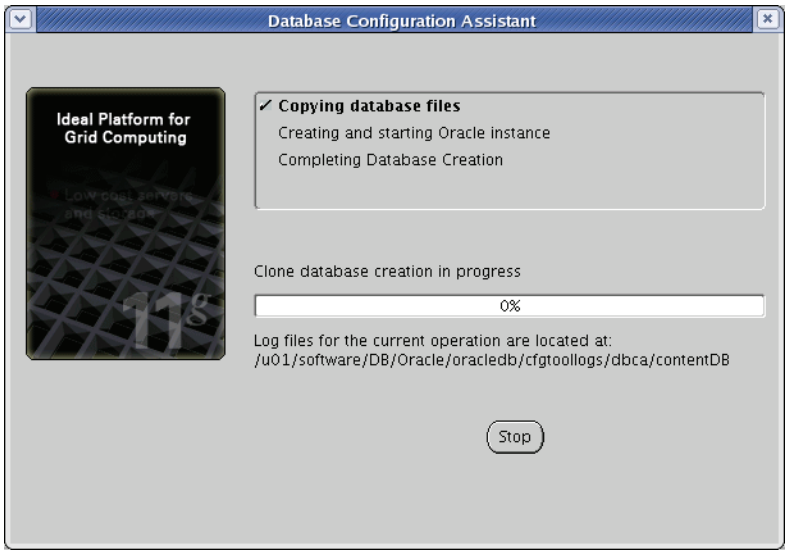
16. 「作成オプション」画面で**「終了」**をクリックします。



17.「確認」画面で、選択したオプションを確認し、「**OK**」をクリックします。



18. データベースの作成タスクが完了するまで待ちます。タスクのいずれかでエラーが発生した場合は、その問題を解決してから続行します。



19. 「サマリー」画面で、データベース SID とデータベース・コントロール URL を記録し、**「終了」**をクリックします。

手順 II. WebCenter Sites 用新規ユーザーの作成

1. コンソール・サーバー・ポートを決定します。
   a. テキスト・エディタで emoms.properties ファイルを開きます。このファイルは次の場所にあります。

      ```
      <ora_home>/<servername>_<SID>/sysman/config/
      ```

   b. 次の行を探します。

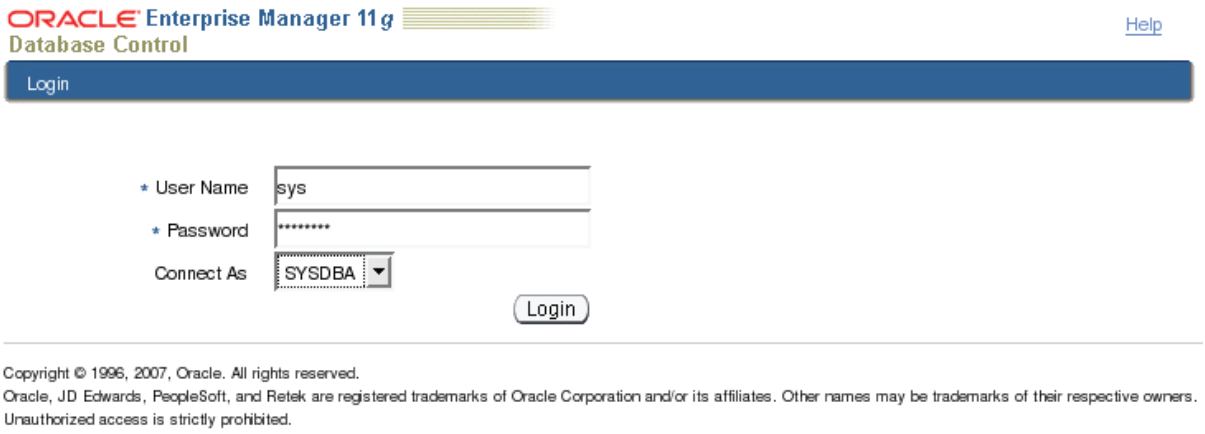
      ```
      oracle.sysman.emSDK.svlt.ConsoleServerPort
      ```

      見つかったら、行の末尾にあるポート番号の値を記録します。
2. Oracle Enterprise Manager コンソールにログインします。
   a. コマンド **emctl status dbconsole** を実行します。

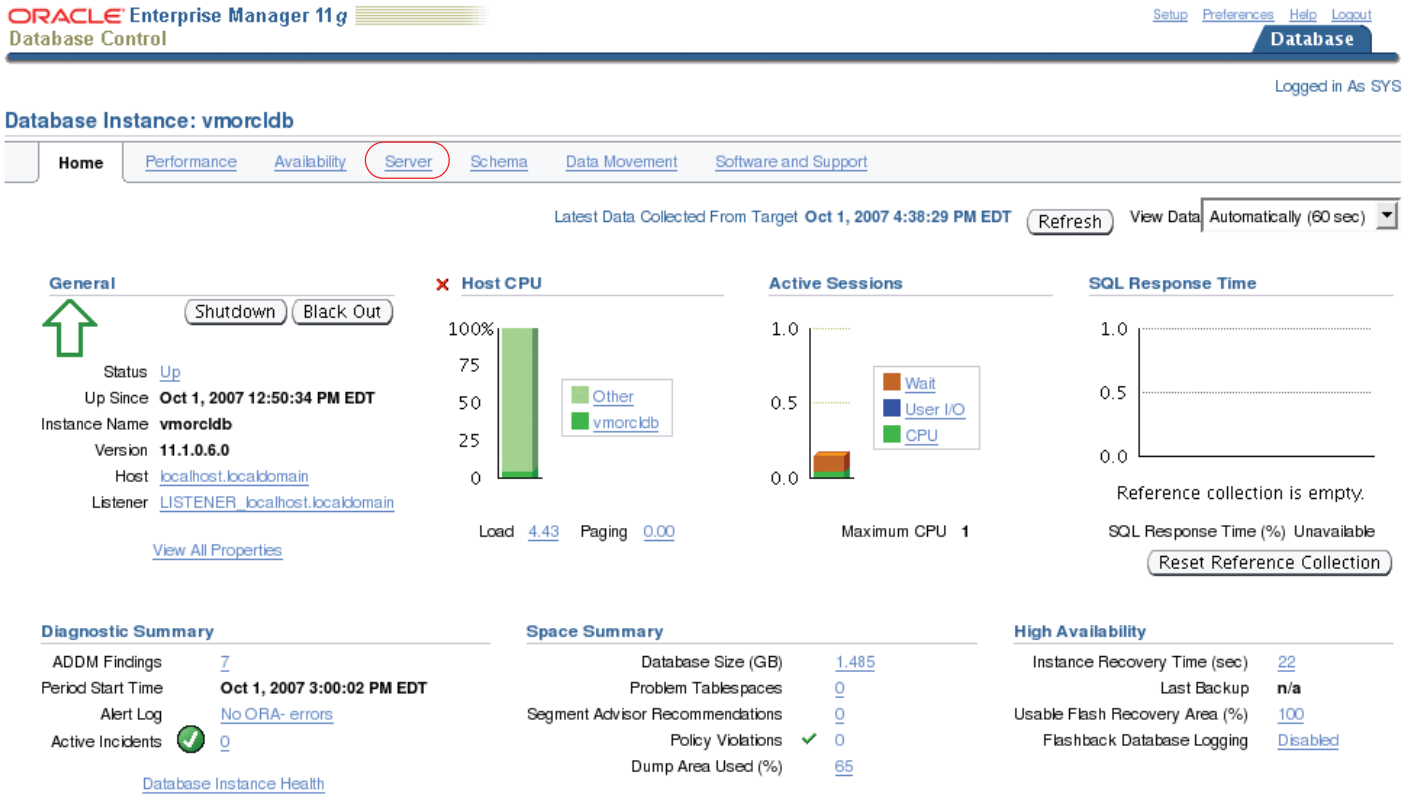
      このコマンドは、次に類似した出力を返します。

      ```
      Oracle Enterprise Manager 11g Database Control Release 11.1.0.6.0
      Copyright (c) 1996, 2007 Oracle Corporation.  All rights reserved.
      https://localhost.localdomain:1158/em/console/aboutApplication
      Oracle Enterprise Manager 11g is running.
      ------------------------------------------------------------------
      Logs are generated in directory /u01/software/DB/Oracle/oracledb/
      product/11.1.0/db_1/localhost.localdomain_vmorcldb/sysman/log
      ```

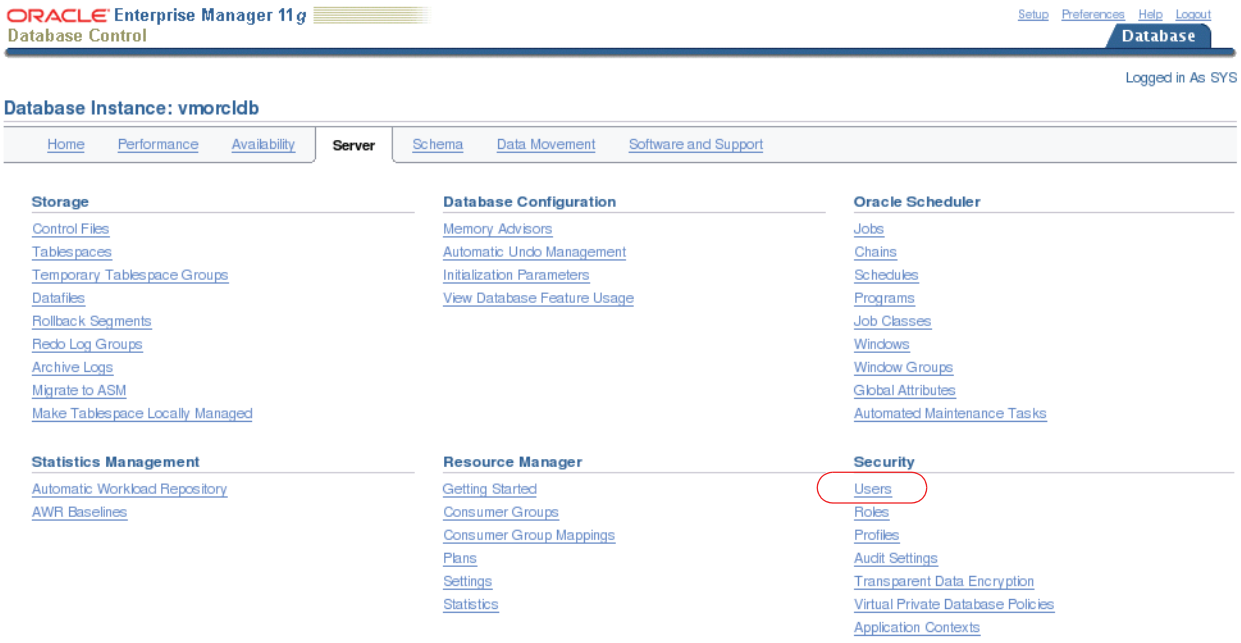
   b. ブラウザを開き、前述の手順 a で太字で表示されている URL に移動します。セキュリティの不一致エラーが発生した場合は無視します (自己署名証明書を使用している場合、このエラーが表示されます)。
   c. **SYSDBA** として接続された sys ユーザーとしてログインします (このユーザーのパスワードは 15 ページの手順 7 で指定しています)。



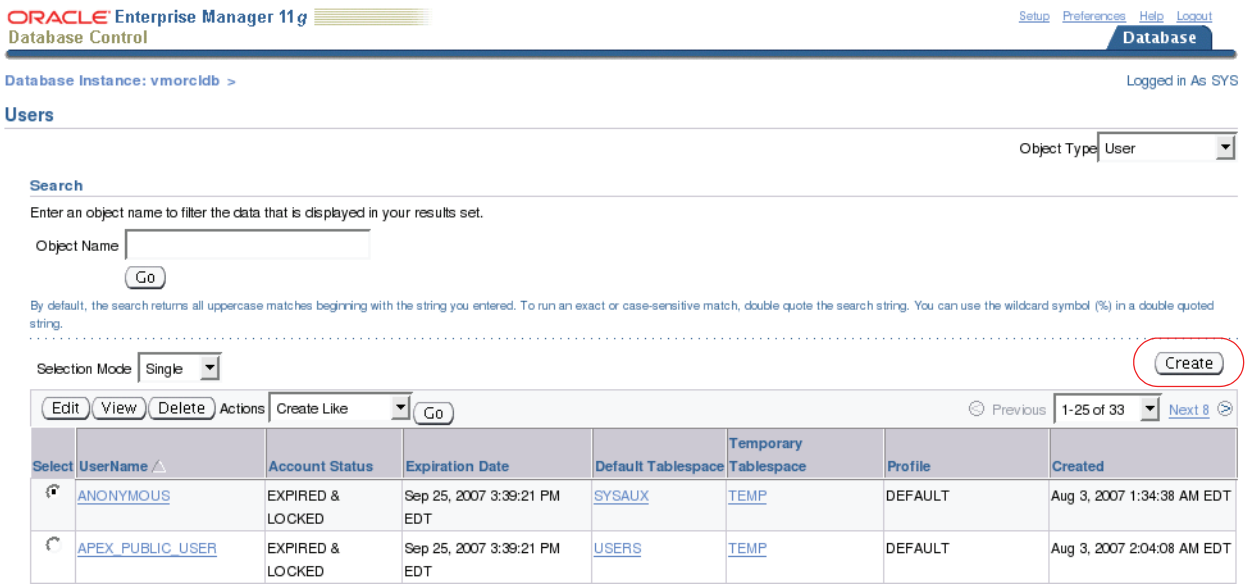
3. タブ・バーで、「**サーバー**」をクリックします。



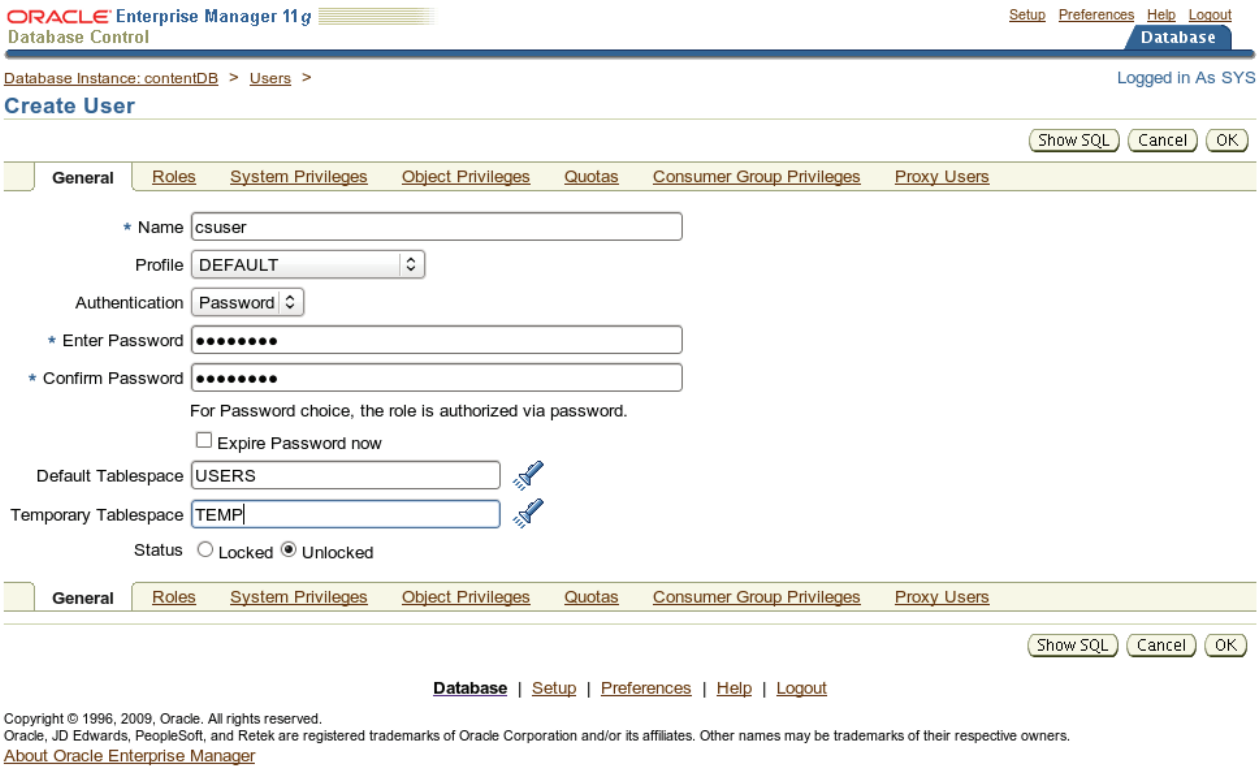
4. 新規ユーザーを作成します。次を実行します。
   a. このページの「セキュリティ」セクションで、**「ユーザー」**をクリックします。



   b. ユーザー・リストの右上隅付近にある**「作成」**をクリックします。

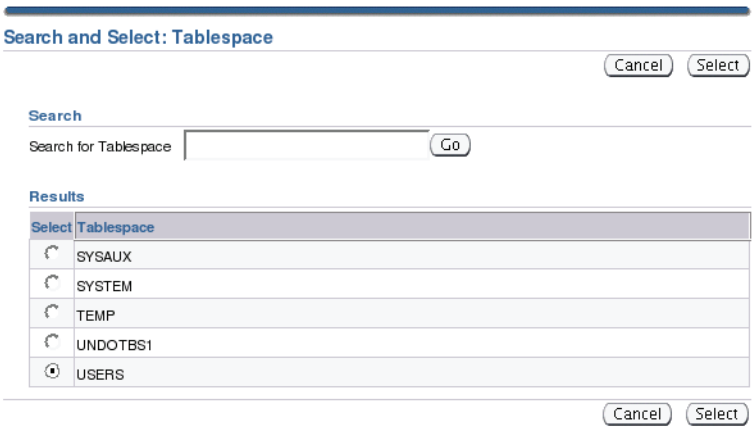


c. 「ユーザーの作成」フォームにあるすべての必須フィールド (アスタリスクが付けられたフィールド) に値を入力します。
その他のすべてのフィールドは、必要に応じて入力します。



5. 新規ユーザーのデフォルト表領域および一時表領域を選択します。次を実行します。
   a. デフォルト表領域を選択します。
      1) 「ユーザーの作成」フォームで、**「デフォルト表領域」**フィールドの隣にある**懐中電灯**ボタンをクリックします。
      2) 表示されるフォームで、**「USERS」**ラジオ・ボタンを選択します。

3) 「**選択**」をクリックします。



b. 一時表領域を選択します。

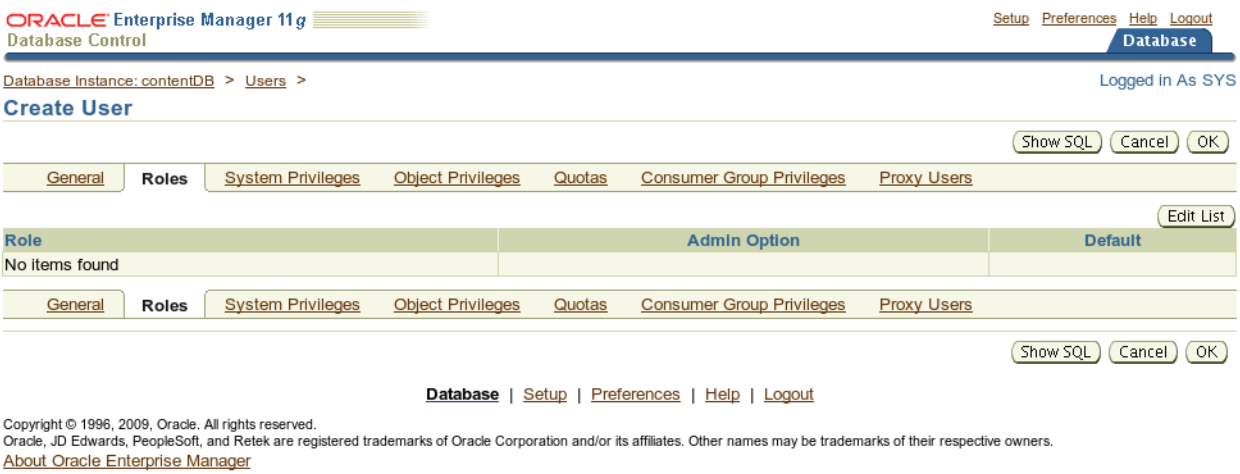
1) 「ユーザーの作成」フォームで、「**一時表領域**」フィールドの隣にある**懐中電灯**ボタンをクリックします。

2) 表示されるフォームで、「**TEMP**」ラジオ・ボタンを選択します。

3) 「**選択**」をクリックします。

6. 必要に応じて、新規ユーザーにロールを割り当てます。

a. タブ・バーで、「**ロール**」をクリックします。



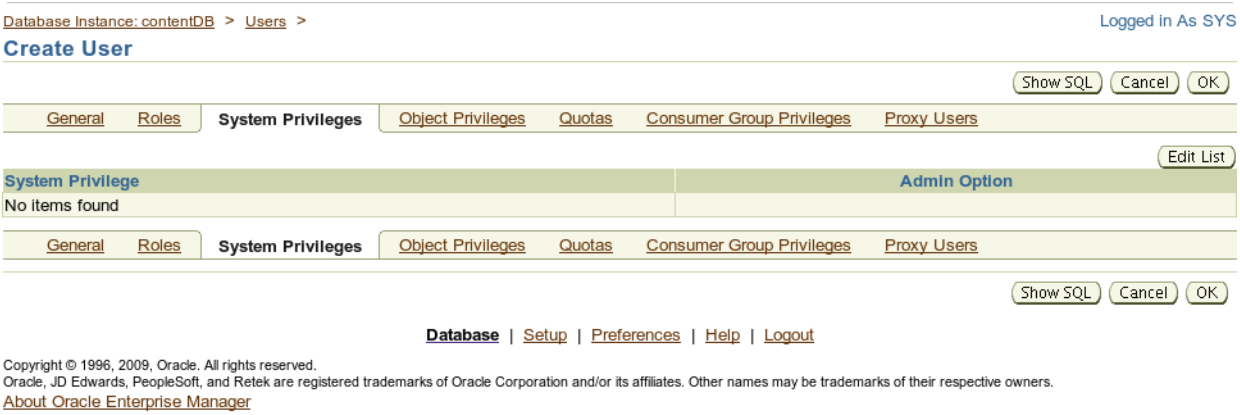
b. ロール・リストの右上隅付近にある「**リストの編集**」をクリックします。

c. 「使用可能なロール」リストで、必要なロールを選択し、「**移動**」をクリックします。

これらのロールが、「選択したロール」リストに表示されます。

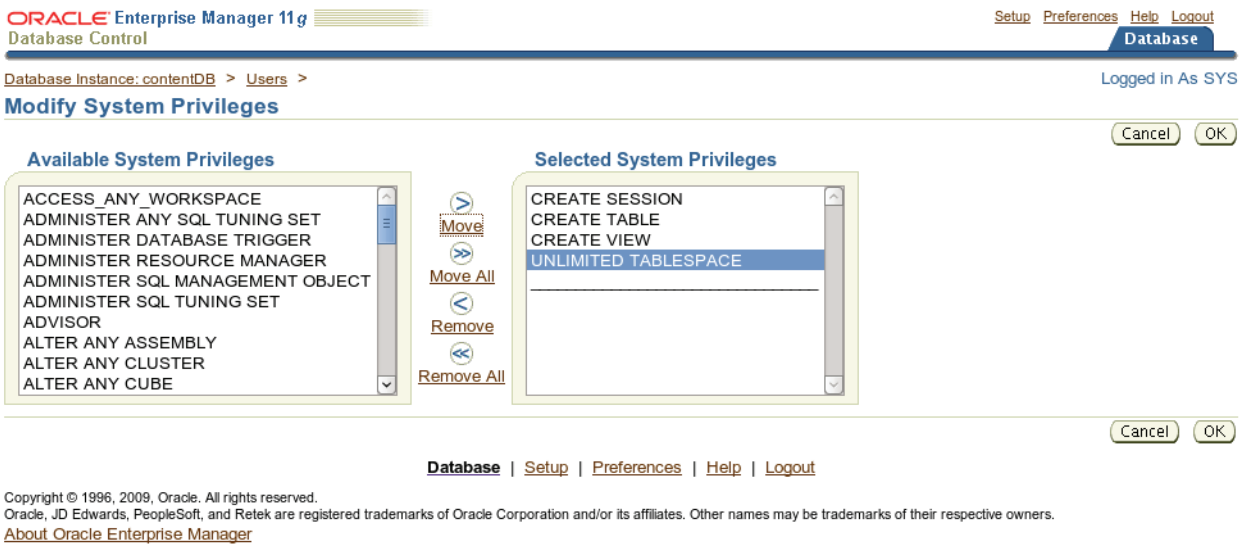
d. 「**OK**」をクリックします。

7. 新規ユーザーにシステム権限を割り当てます。次を実行します。
   a. タブ・バーで、**「システム権限」**をクリックします。

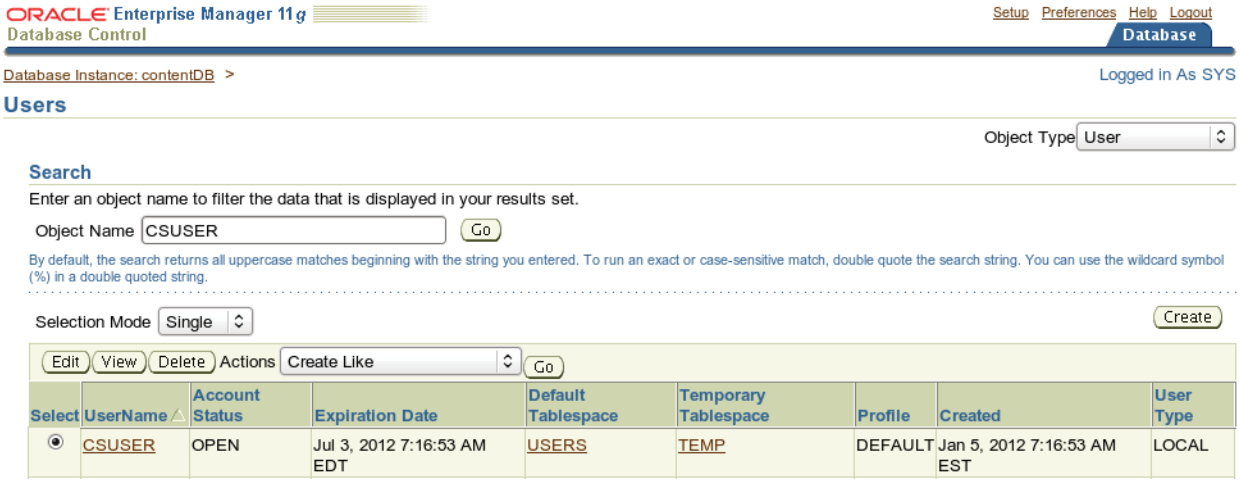


   b. 権限のリストの右上隅付近にある**「リストの編集」**をクリックします。
   c. 「使用可能なシステム権限」リストで、**REATE SESSION、CREATE TABLE、CREATE VIEW** および **UNLIMITED TABLESPACE** を選択し、**「移動」**をクリックします。

      これらの権限が、「選択したシステム権限」リストに表示されます。
   d. **「OK」**をクリックします。



新規ユーザーの作成を確認するメッセージが表示されます。このユーザーが、ユーザーのリストに表示されます。



次の手順

これで、データ・ソースを作成し、構成する準備が整いました。手順については、使用している WebCenter Sites のインストレーション・ガイドを参照してください。

第 2 章

MS SQL Server データベースの作成および構成

この章では、WebCenter Sites インストールでの、MS SQL Server データベースの設定について説明します。データベース構成とユーザーの権限の背景情報は、第 1 部「データベースの作成および構成」を参照してください。

この章は、次の項で構成されています。

MS SQL Server 2008 R2 でのデータベースの作成

MS SQL Server 2008 R2 でデータベースを作成および構成するには

1. Windows Account Manager を使用して、WebCenter Sites データベース・ユーザーのために新しいユーザー・アカウント (たとえば、`csuser`) を作成し、このアカウントにパスワードを割り当てます。
2. SQL Server Manager Studio を開きます。
3. MS SQL Server にログインします。
   a. ユーザー名とパスワードを入力します (デフォルトのユーザー名は `sa` です)。
   b. 「**Connect**」をクリックします。
4. データベースを作成します。
   a. 左側のツリーで、「**Databases**」ノードを展開します。
   b. 「**Databases**」ノードを右クリックし、ポップアップ・メニューから「**New Database**」を選択します。
   c. 「New Database」ウィンドウにデータベース名を入力し、「**OK**」をクリックします。

      新しく作成されたデータベースが、ツリーの「**Databases**」ノードの下に表示されます。
5. このツリーで、新しく作成したデータベースを表しているノードを展開し、その下にある「**Security**」ノードを展開します。
6. 「**Users**」タブをクリックします。
7. 既存ユーザーのリストの下にある空白のスペースを右クリックし、ポップアップ・メニューから「**New User**」を選択します。
8. 「Database User - New」ウィンドウで、「**User name**」および「**Login name**」フィールドに、(この手順の手順 1 で作成した) WebCenter Sites データベース・ユーザーのユーザー名を入力します。
9. 「Owned Schemas」および「Role Members」領域で、「**db_owner**」チェック・ボックスを選択します。
10. 「**OK**」をクリックします。

    データベースが作成されます。
11. データベースの作成後、後述のように「`READ_COMMITTED_SNAPSHOT`」をオンにします。詳細は、ベンダーのドキュメントを参照してください。

```
ALTER DATABASE <your_db_name>
SET ALLOW_SNAPSHOT_ISOLATION ON GO


ALTER DATABASE <your_db_name>
SET READ_COMMITTED_SNAPSHOT ON GO
```

データベースの構成が完了します。これで、この手順の手順 1 で作成した WebCenter Sites データベース・ユーザーのユーザー名とパスワードを使用して、データ・ソースを作成し、構成する準備ができました。手順については、使用している WebCenter Sites のインストレーション・ガイドを参照してください。

第 3 章

IBM DB2 9.7 データベースの作成および構成

この章では、WebCenter Sites インストールでの、サポートされている IBM DB2 データベースの設定について説明します。データベース構成とユーザーの権限の背景情報は、第 1 部「データベースの作成および構成」を参照してください。

この章は、次の項で構成されています。

WebCenter Sites に対応した DB2 9.7 のインストールおよび構成

DB2 9.1 データベースをインストールして構成するには、次の手順を完了します。

A. DB2 のインストール

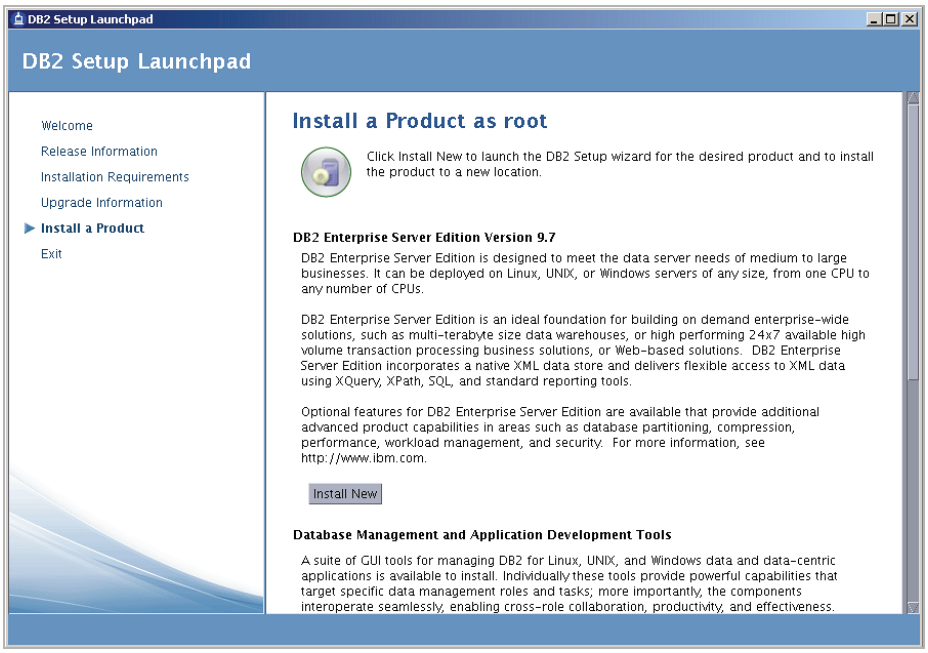
B. 新しい DB2 データベースの作成

C. 新規データベース用のユーザーの作成

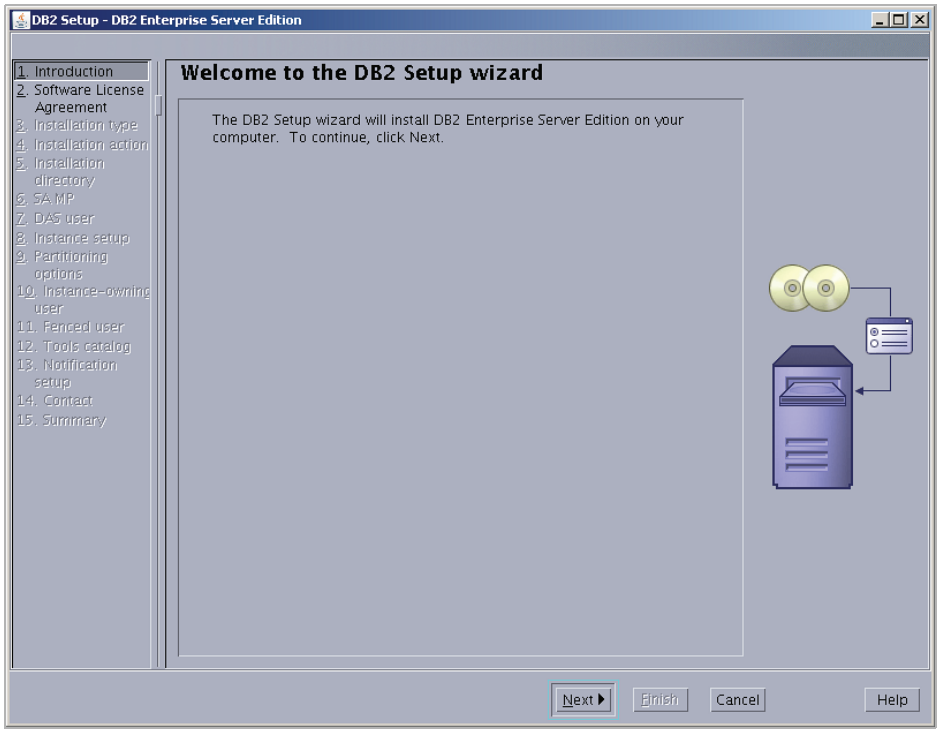
D. データベースの構成

A. DB2 のインストール

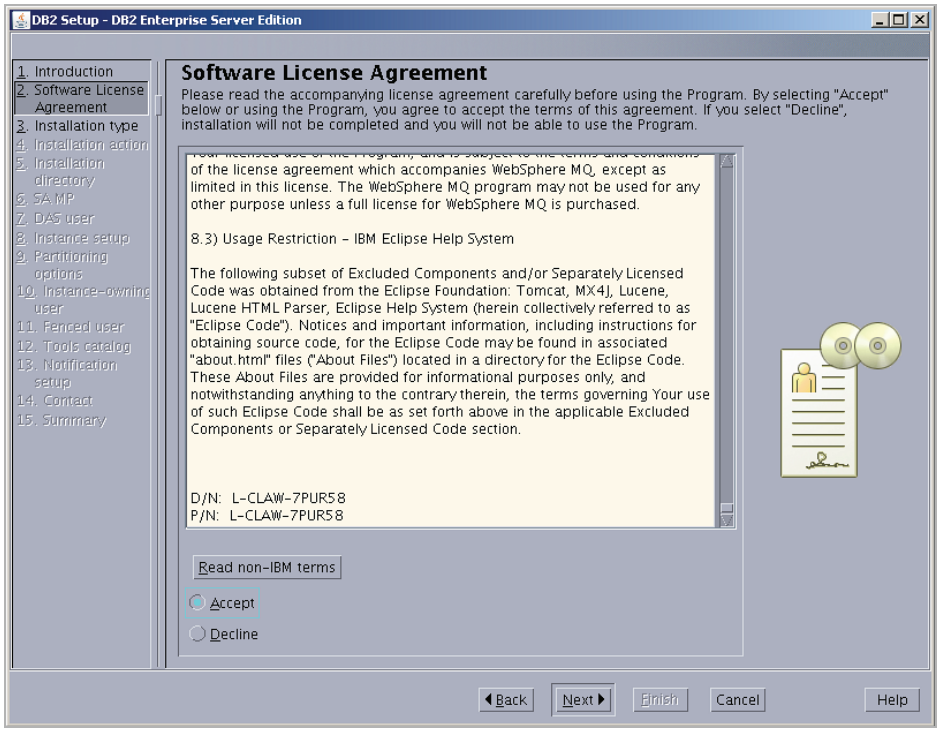
1. 使用しているディストリビューションに適したインストール・ファイルを解凍します。
2. **`./db2setup`** を実行します。
3. 「Information Management Software」画面で、「**Install a Product**」を選択します。
4. 「DB2 Enterprise Server Edition」で、「**Install New**」を選択します。



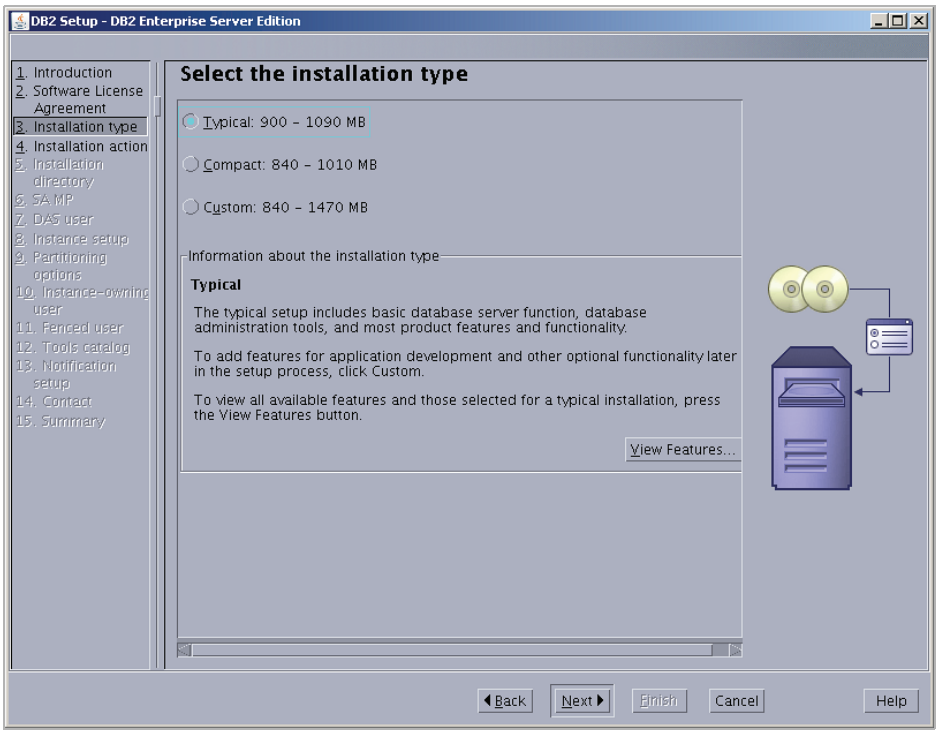
5. 「Welcome to the DB2 Setup Wizard」で「**Next**」をクリックします。



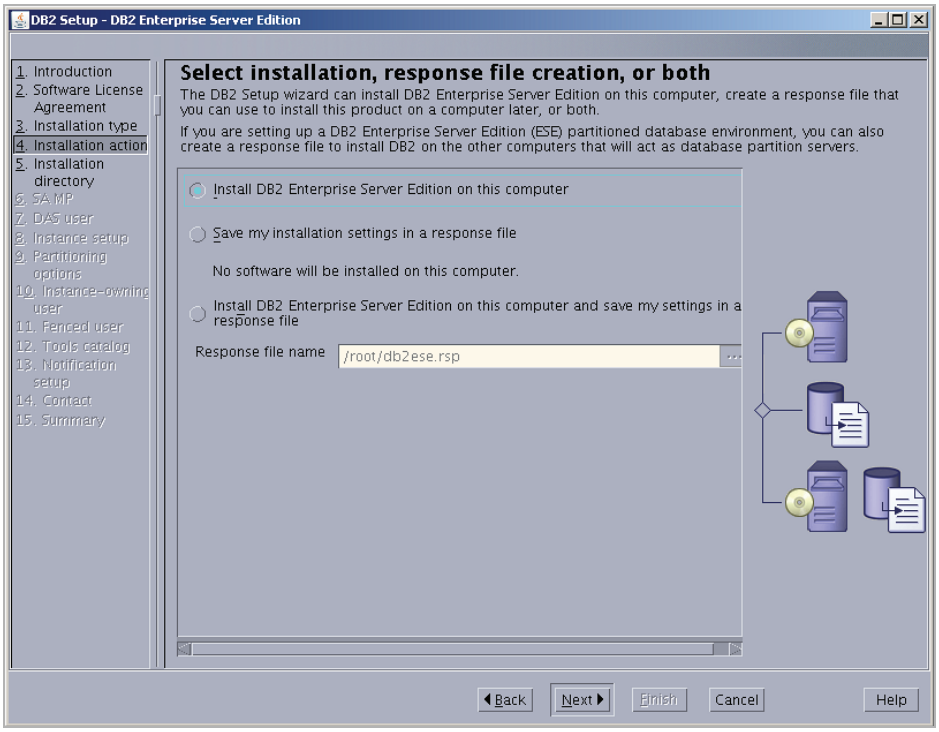
6. 「Software License Agreement」画面で「**Accept**」、「**Next**」の順にクリックします。



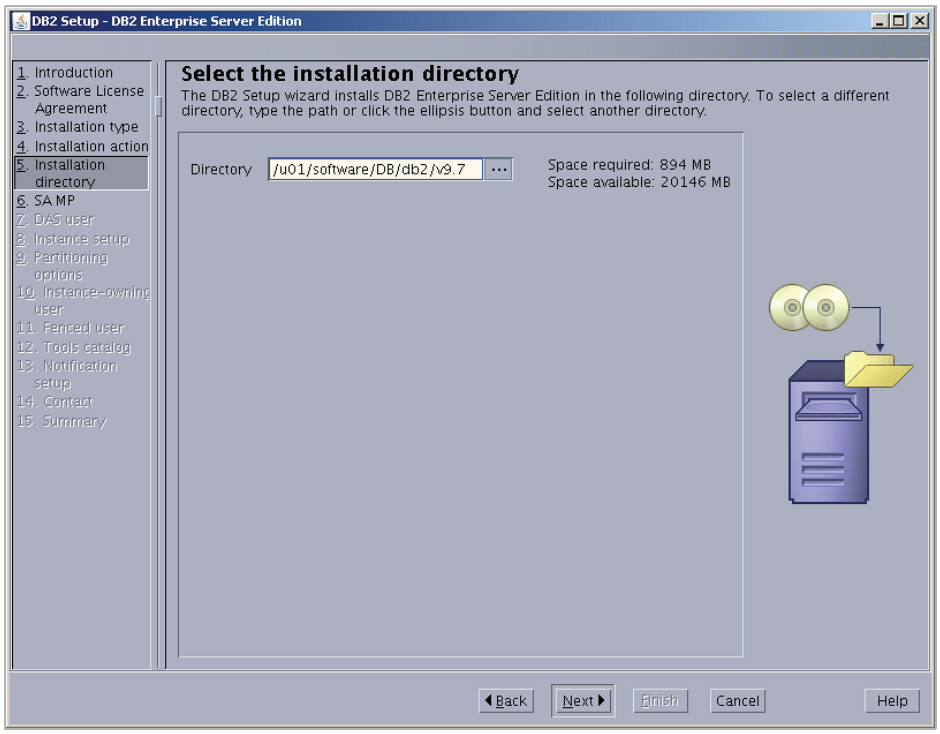
7. 「Select the installation type」画面で、「**Typical**」を選択し、「**Next**」をクリックします。



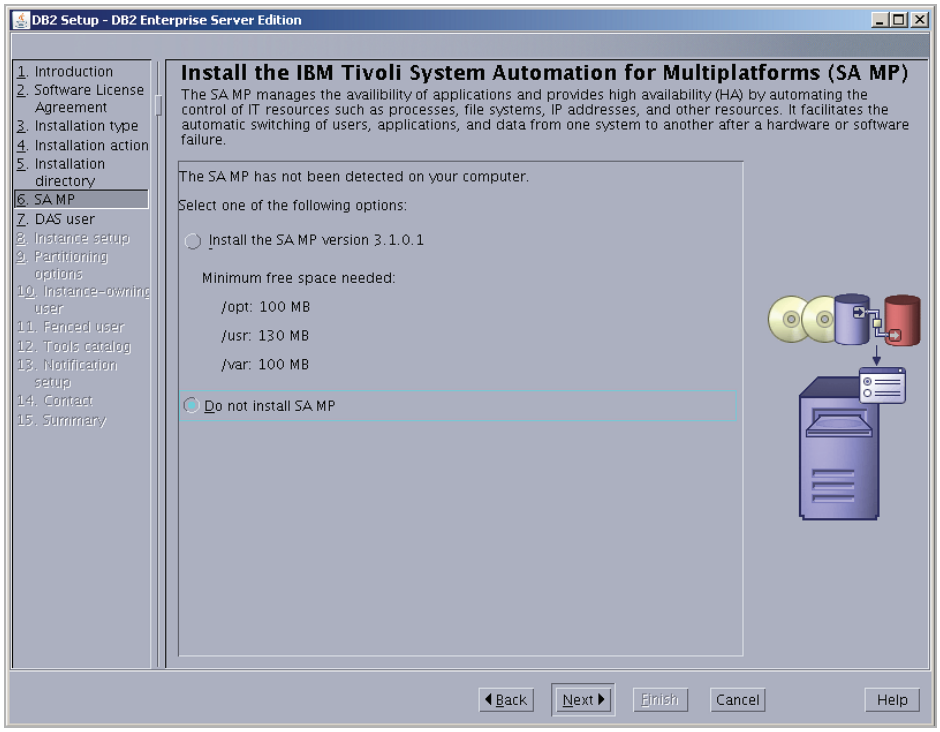
8. 「Select installation, response file creation, or both」で、「**Install DB2 Enterprise Server Edition on this computer**」を選択し、「**Next**」をクリックします。



9. 「Select the installation directory」で、ディレクトリを入力するかデフォルトをそのまま使用して、「**Next**」をクリックします。



10. 「Install the IBM Tivoli System Automation for Multiplatforms (SA MP)」では、使用環境で SA MP が必要な場合を除き、「**Do not install SA MP**」を選択します。

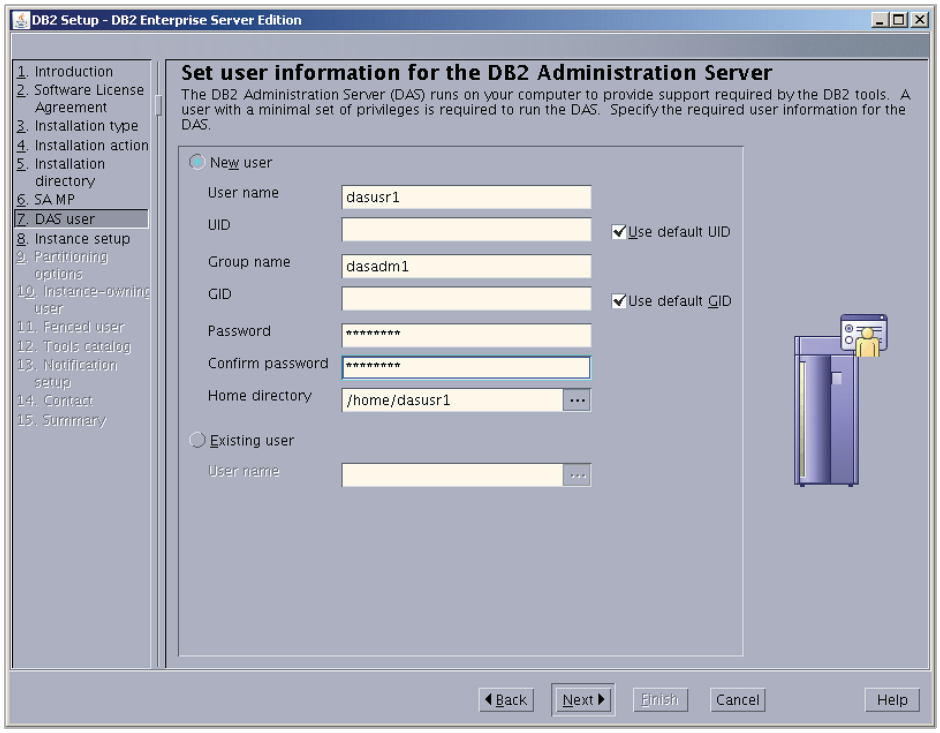


11. 「Set user information for the DB2 Administration Server」では、次のように設定します。

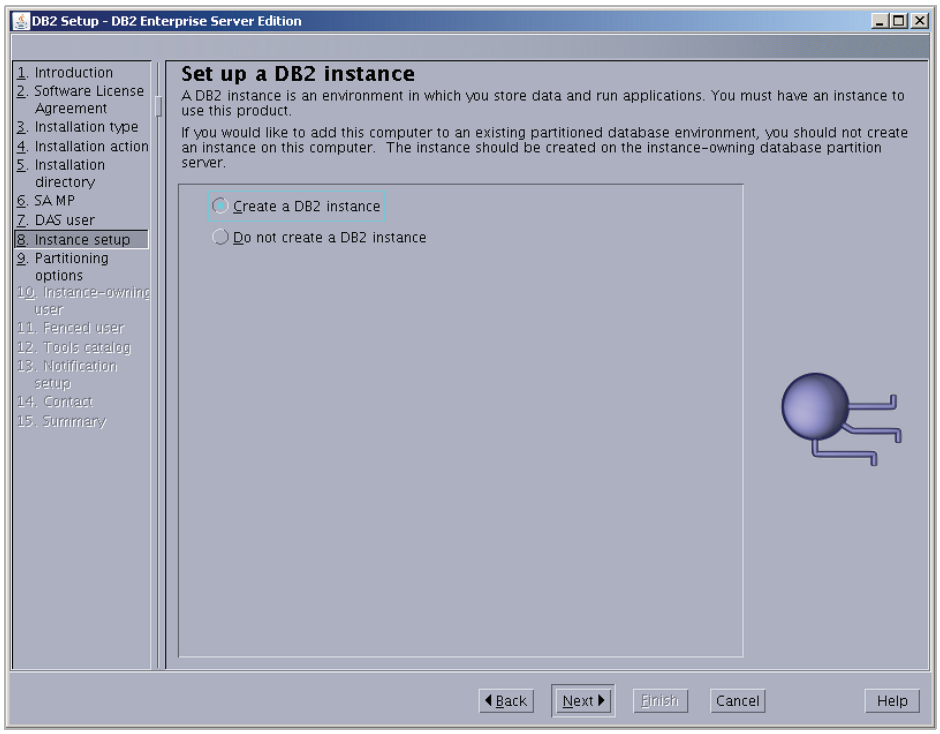
a. 前回 DB2 のインストールに失敗した場合を除き、デフォルトのままにします。

b. パスワードを入力します。

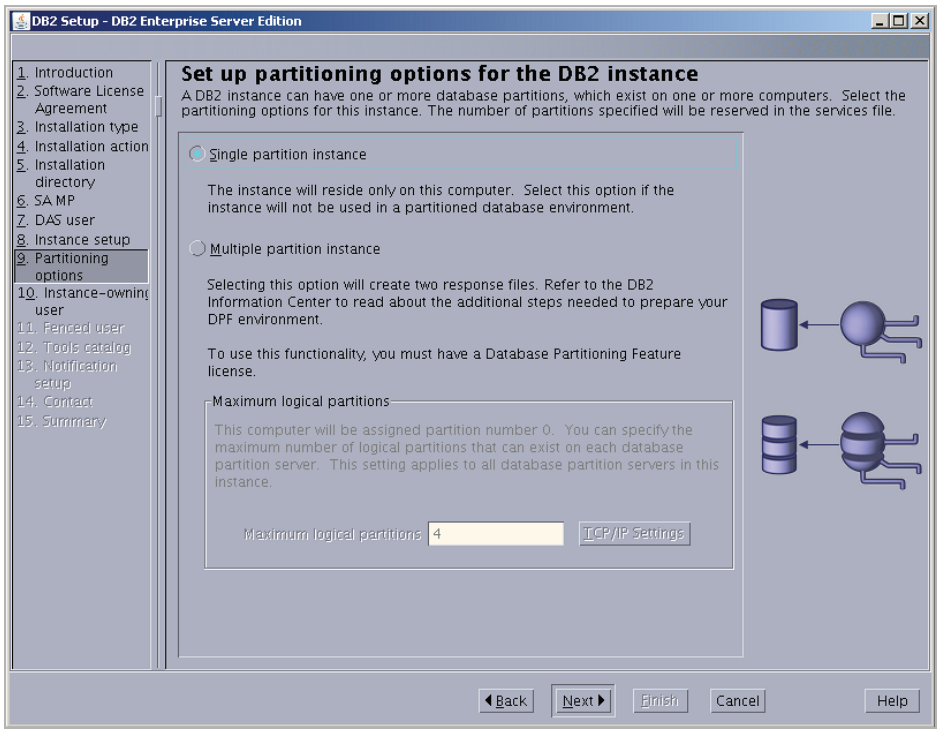
c. 「**Next**」をクリックします。



12. 「Set up a DB2 instance」で、「**Create a DB2 instance**」を選択し、「**Next**」をクリックします。



13. 「Set up partitioning options for the DB2 instance」で、「**Single partition instance**」を選択し、「**Next**」をクリックします。

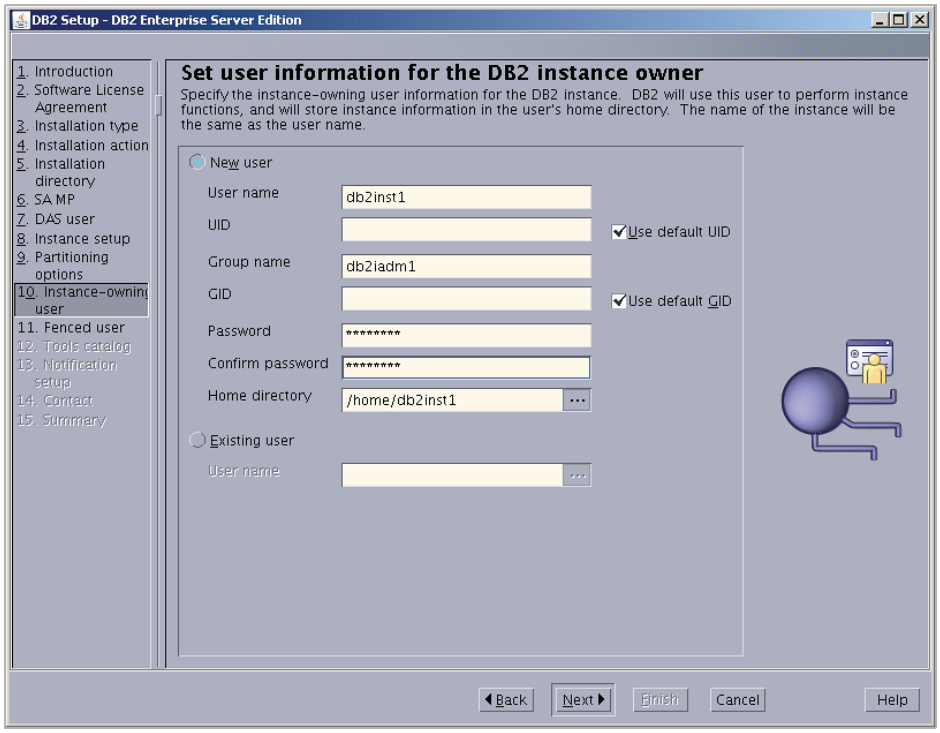


14. 「Set user information for the DB2 instance owner」では、次のように設定します。

a. 前回 DB2 のインストールに失敗した場合を除き、デフォルトのままにします。

b. パスワードを入力します。

c. 「**Next**」をクリックします。

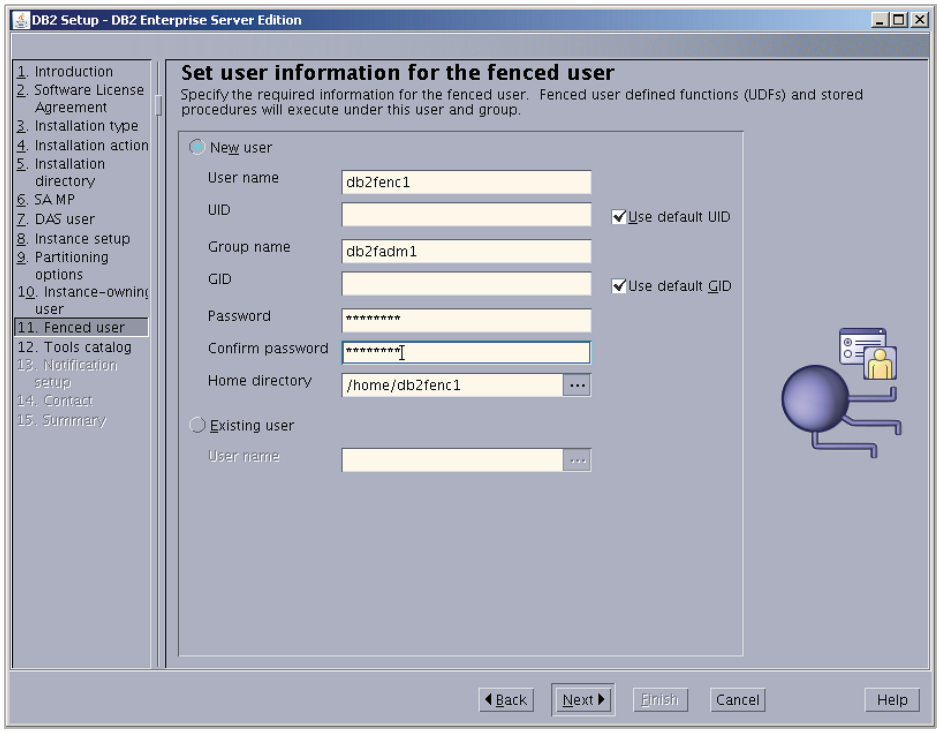


15.「Set user information for the fenced user」では、次のように設定します。

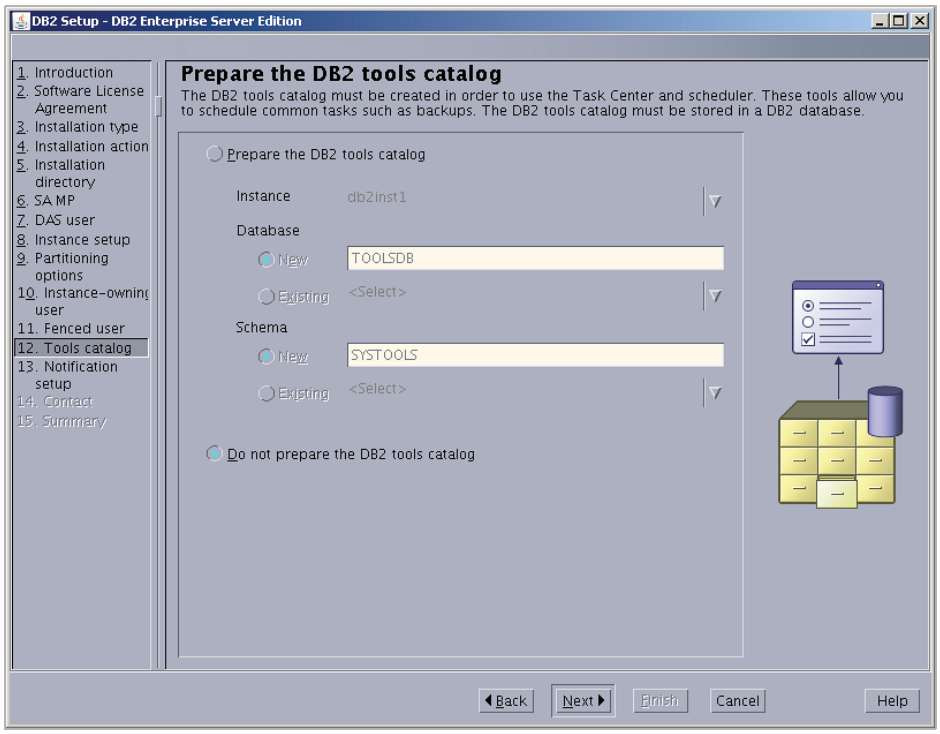
a. 前回 DB2 のインストールに失敗した場合を除き、デフォルトのままにします。

b. パスワードを入力します。

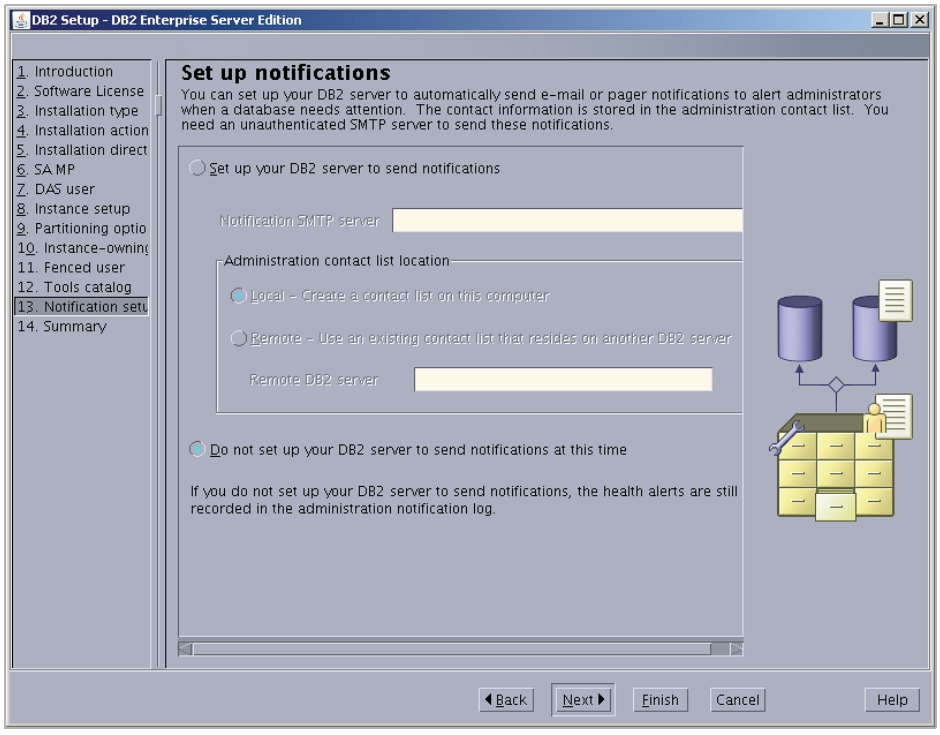
c. 「**Next**」をクリックします。



16. 「Prepare the DB2 tools catalog」で、「**Do not prepare the DB2 tools catalog**」を選択し、「**Next**」をクリックします。

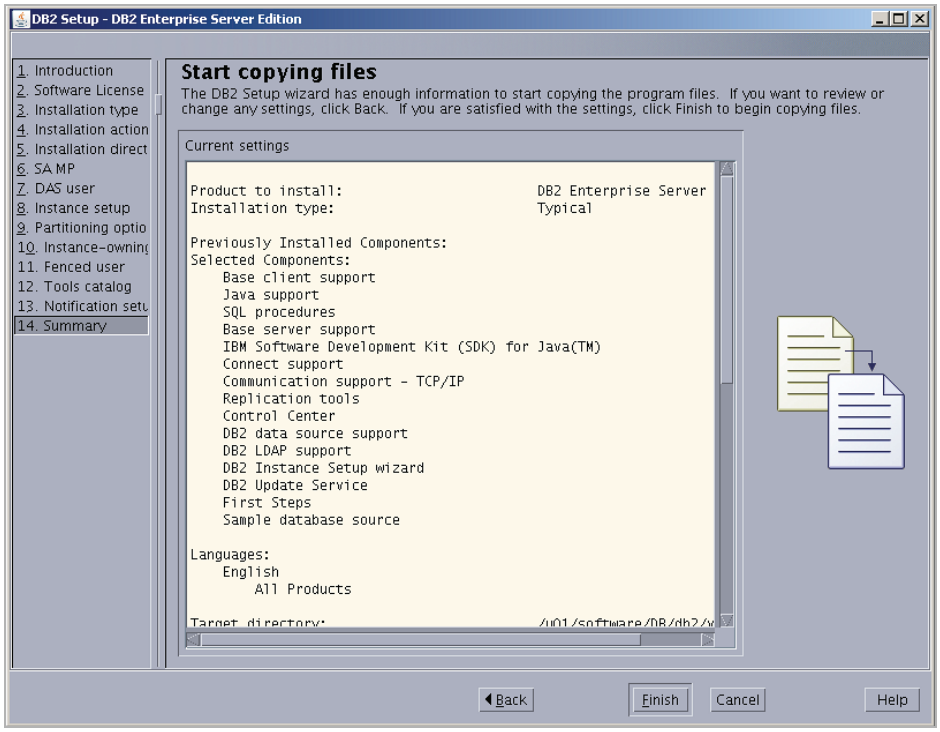


17. 「Set up notifications」で、次のいずれかを実行します。

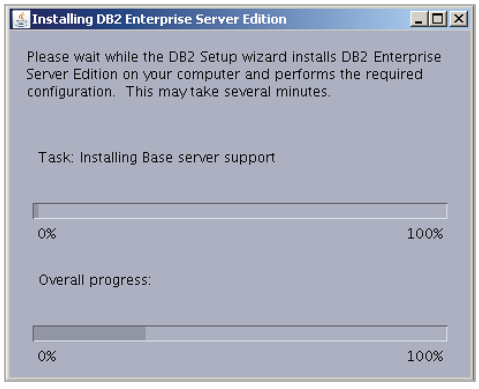


- 使用しているシステムが本番サーバーの場合は、「**Set up your DB2 server to send notifications**」を選択し、ローカル・ホストの正しいアドレスを入力して、「**Next**」をクリックします。
- 使用しているシステムが本番サーバーではない場合は、「**Do not set up your DB2 server to send notifications at this time**」を選択し、「**Next**」をクリックします。

18. 「Start copying files」で、オプションが正しいことを確認し、「**Finish**」をクリックします。



19. インストールが終わるまで待ちます。

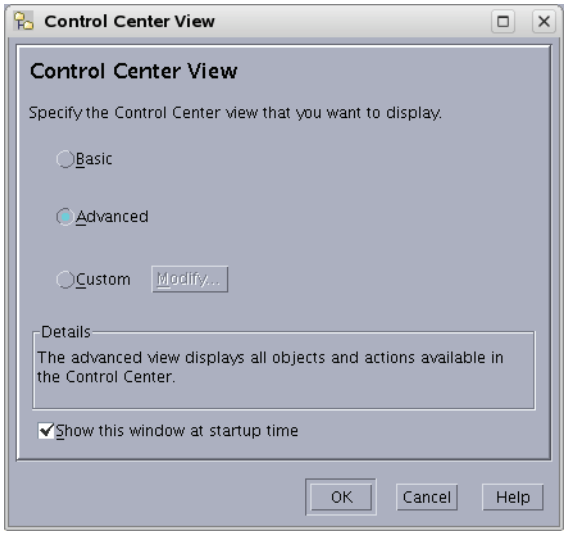


20. 「Setup has completed successfully」で注意事項を読み、ログ・タブを確認して、「**Finish**」をクリックします。

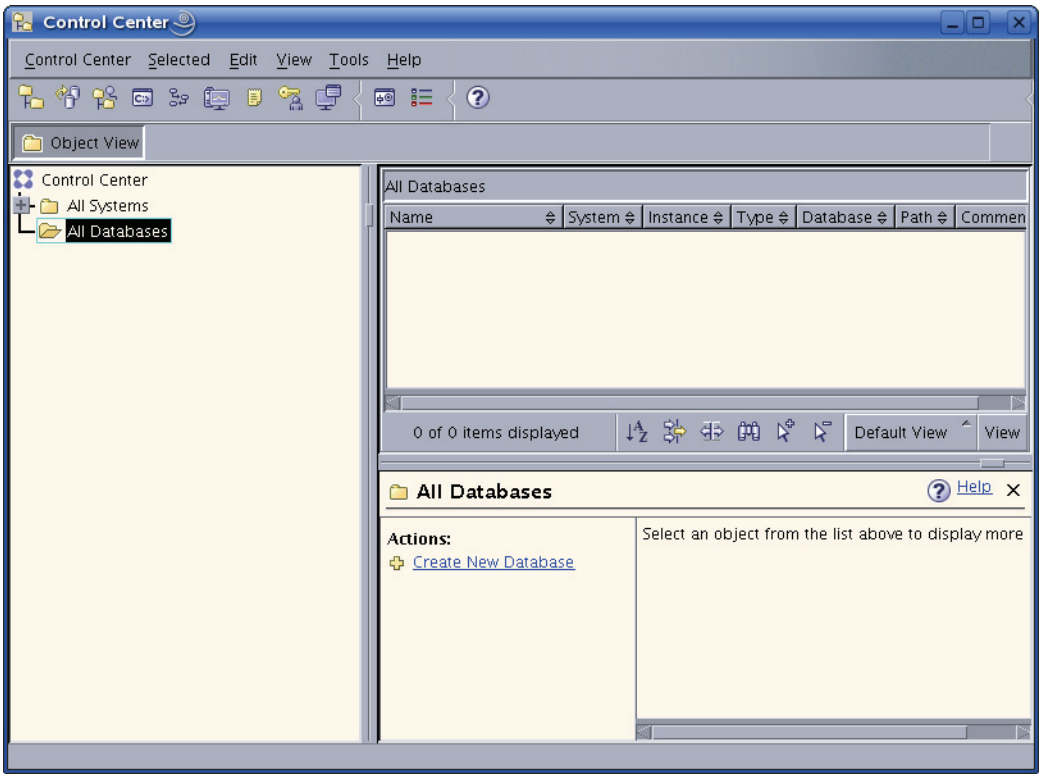
これで DB2 9.7 のインストールは完了です。

B. 新しい DB2 データベースの作成

1. 「db2inst1」(または、インストールの手順 14 で作成したインスタンス・ユーザー) としてログインします。
2. ./sqllib/bin and run db2cc に移動します。
3. 「Control Center View」画面で、「**Advanced**」を選択します。

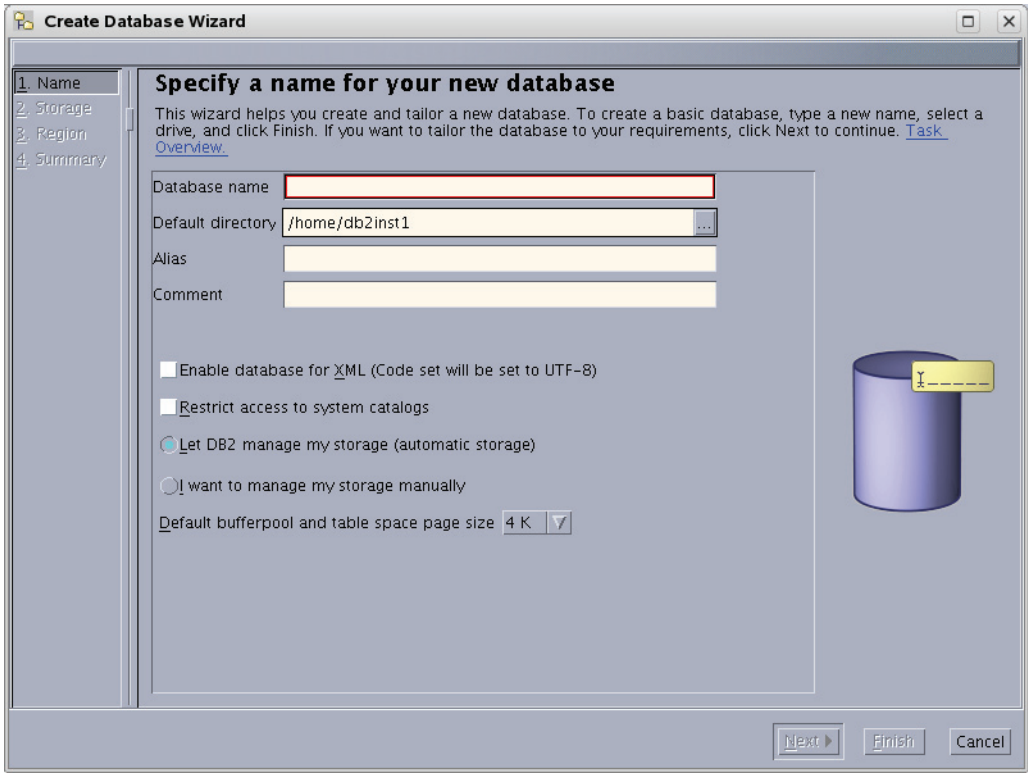


4. 「Control Center」で、データベースを作成するためのアプリケーションを開きます。
   a. ツリー・オプション「**All Systems**」の隣にあるプラス記号をクリックします。

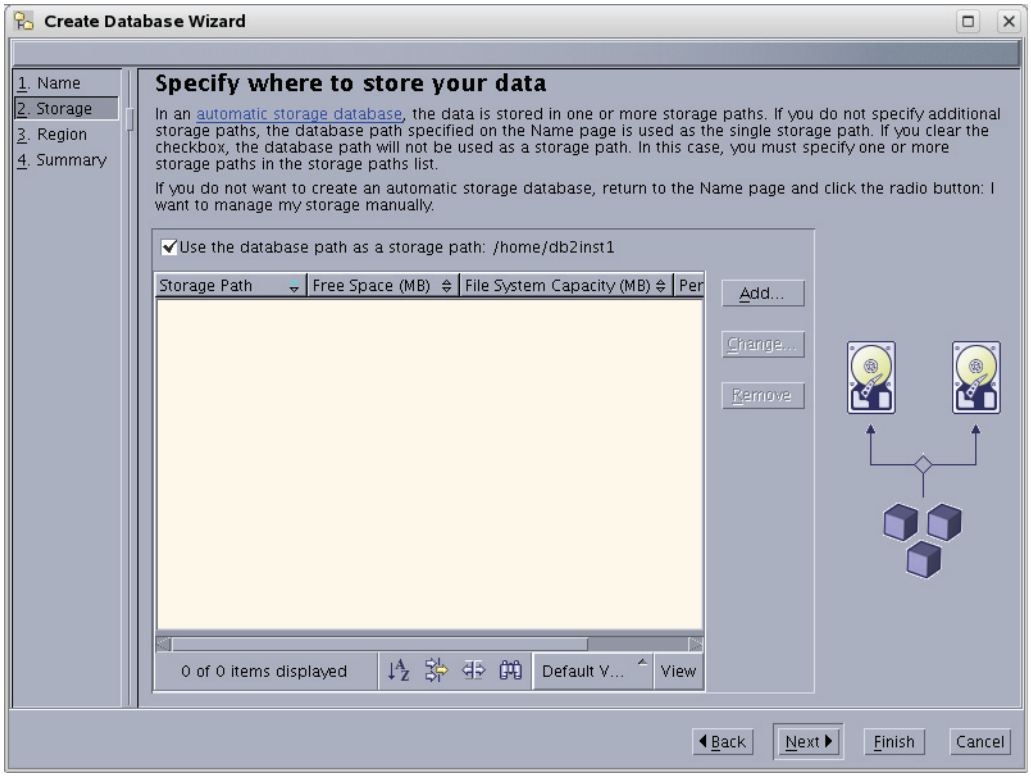


   b. 展開された「**All Databases**」ブランチをクリックします。(事前にデータベースが作成されていない場合、このブランチは空です。)
   c. 「**All Databases**」ブランチを右クリックし、「**Create Database**」→「**Standard**」の順に選択します。
5. 「Specify a name for your new database」で、次の操作を行います。
   a. このデータベースの名前を入力します。
   b. 「**Enable database for XML**」チェック・ボックスを選択します。

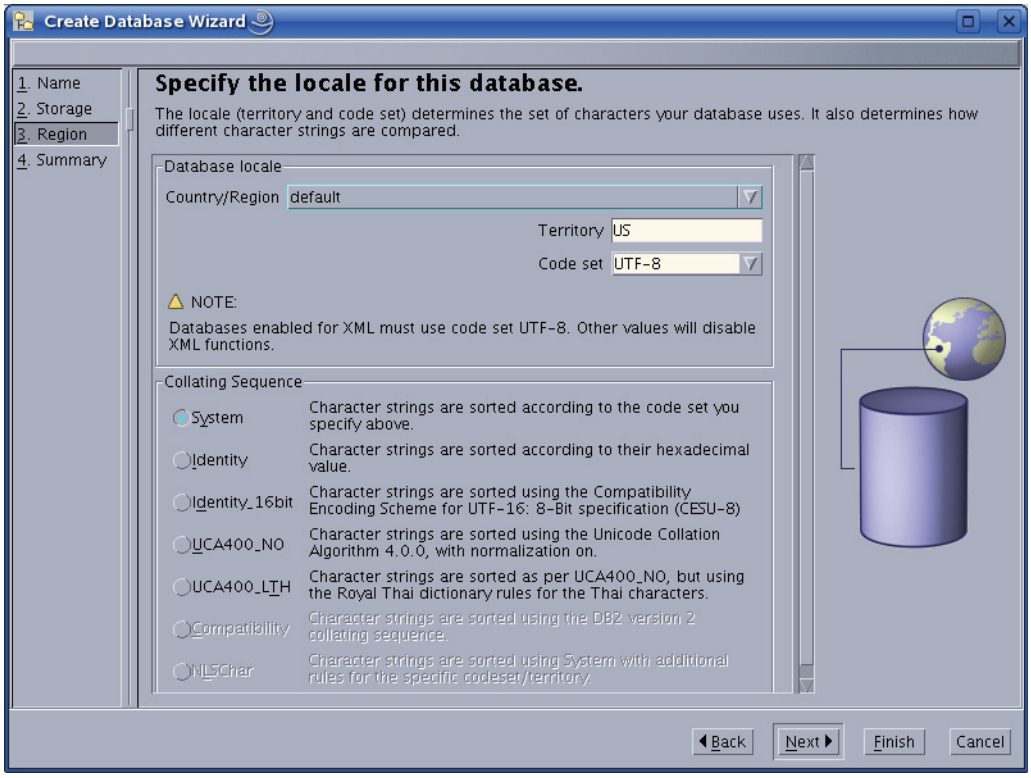
c. 「Default bufferpool and table space page size」ドロップダウンで、「**32**」を選択し、「**Next**」をクリックします。



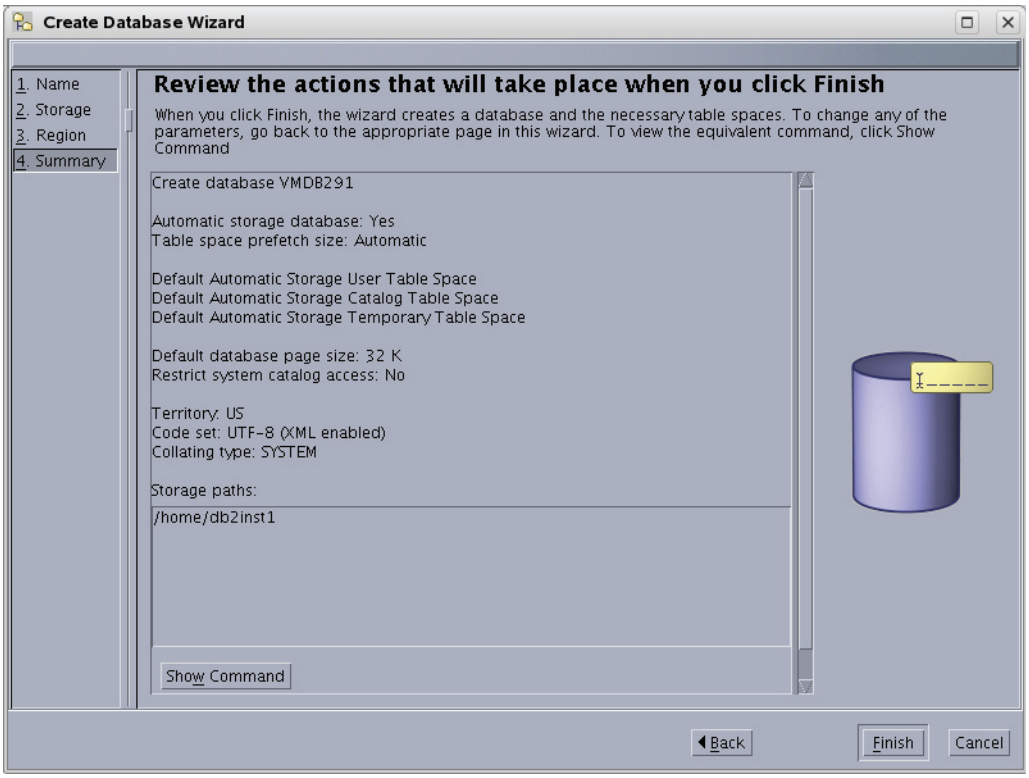
6. 「Specify where to store your data」で、「**Next**」をクリックします (前のページで、デフォルトのオプション「**Let DB2 manage my storage (automatic storage)**」をそのままにしておいたため値は必要ありません)。



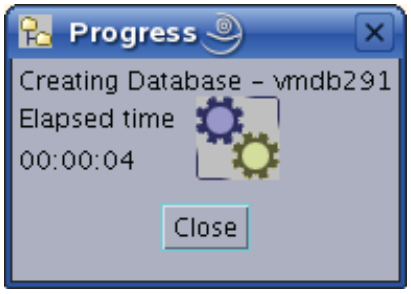
7. 「Specify the locale for this database」で、「Code set」ドロップダウンに「UTF-8」が表示されていることを確認し、「**Next**」をクリックします。



8. 「Review the actions that will take place when you click Finish」で、すべてが適切に設定されていることを確認してから、**「Finish」**をクリックします。

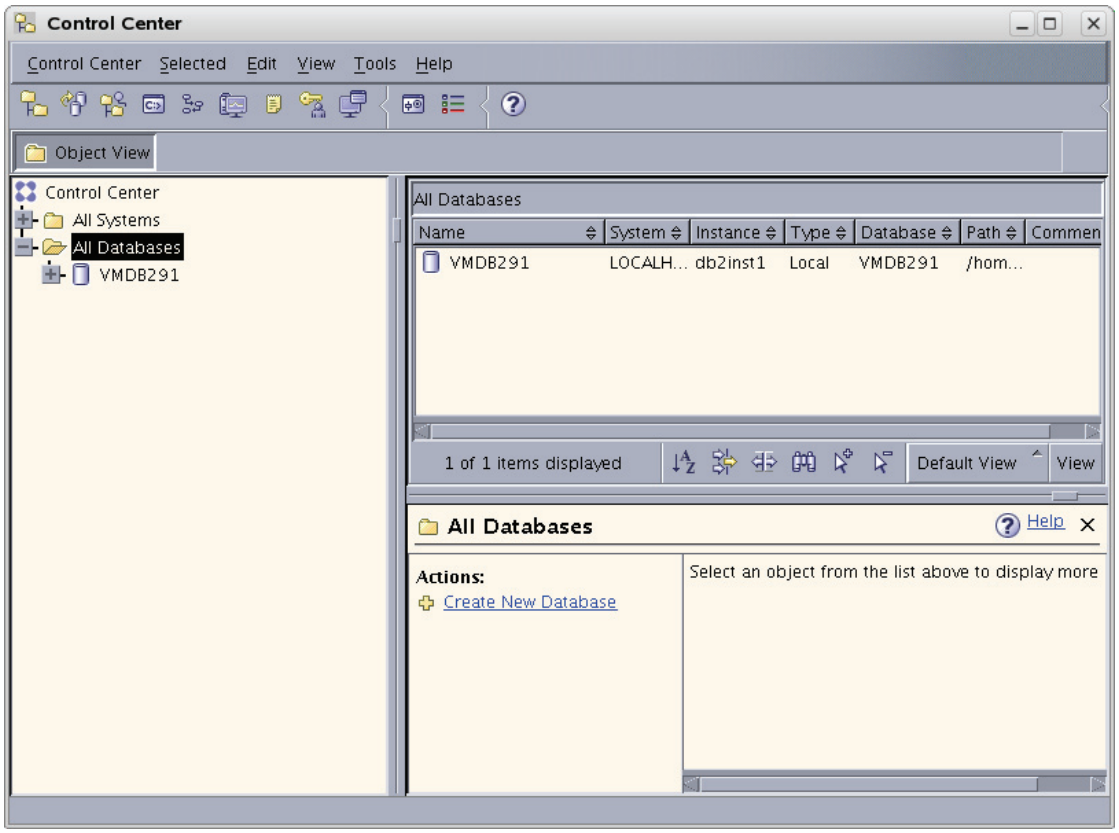


9. 「Progress」ウィンドウでデータベースの作成が完了するまで待ちます。データベースが作成されると、このウィンドウは自動的に閉じられます。



10. これで、データベースが作成され、コントロール・センターに表示されます。

    下の図では、コントロール・センターに「vmdb291」というデータベースが 1 つ存在しています。



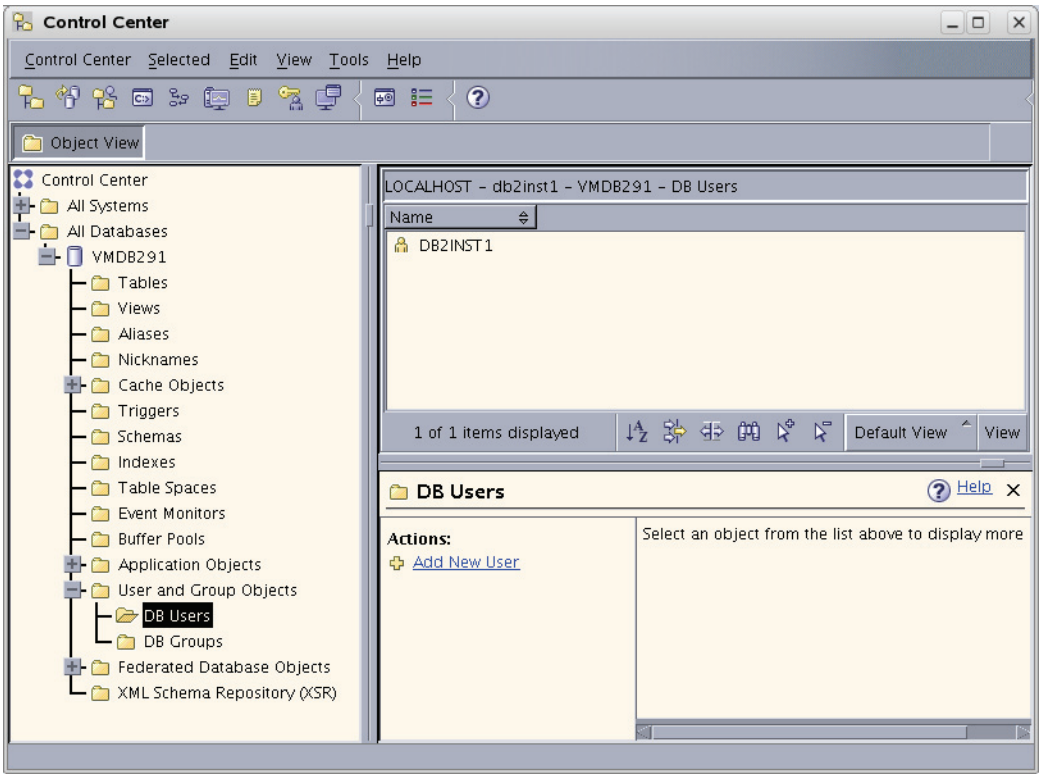
C. 新規データベース用のユーザーの作成

1. コマンドラインに移動します。システム・ユーザーとして、csuser という名前の新しいユーザーを作成します。このユーザーは、Oracle 製品からデータベースにアクセスするために使用されます。

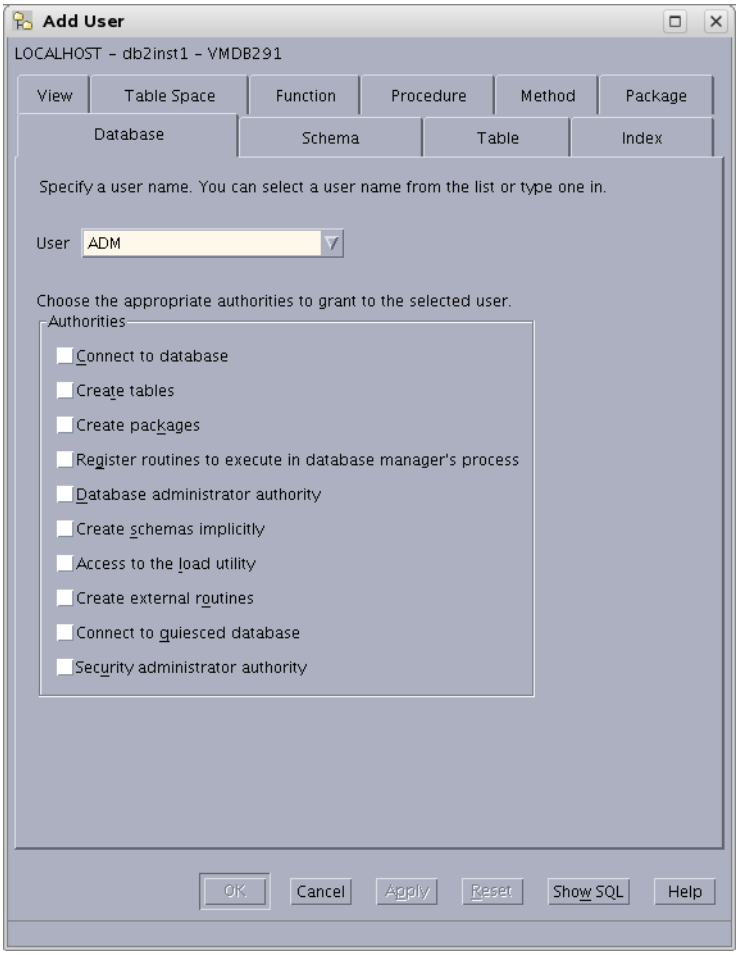
   たとえば、Linux で「csuser」というユーザーを作成するには、次の操作を実行します。

   ```
   useradd -d /home/csuser -m -p demo4132 csuser
   ```

2. 「Control Center」に戻り、ユーザーを追加します。
   a. プラス記号をクリックして、ツリーで新しく作成したデータベースを展開してから、「**User and Group Objects**」ブランチを展開します。
   b. 「**DB Users**」をクリックして、右側のパネルを開きます。
   c. 「**DB Users**」ブランチを右クリックし、「**Add**」オプションを選択します。



3. 「Add User」アプリケーションで、次の操作を実行します。
   a. 50 ページの手順 C で作成したユーザーを選択します。
   b. 「Authorities」で、すべてのチェック・ボックスを選択します。
   c. **「OK」**をクリックします。

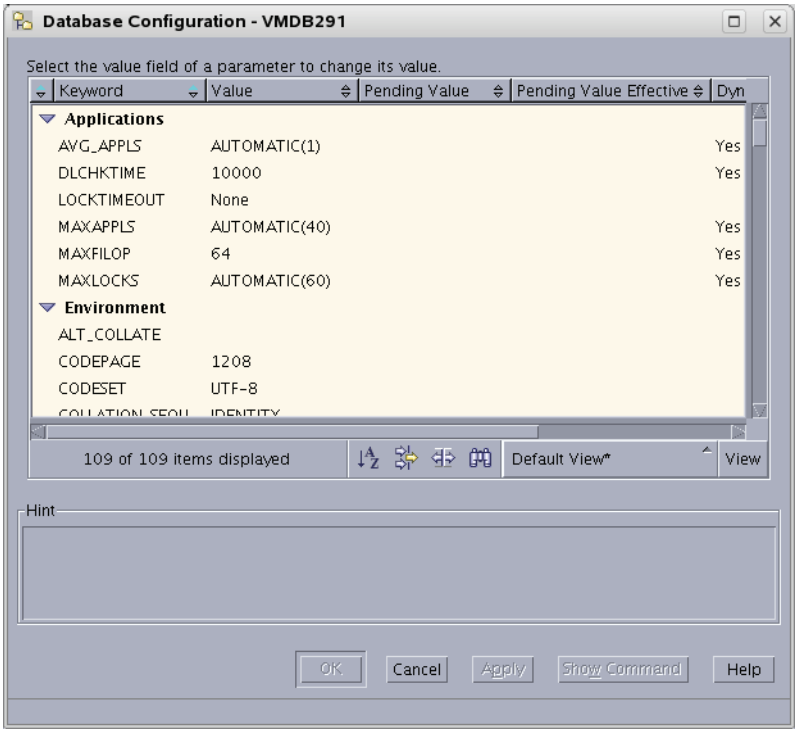


D. データベースの構成

1. 作成したデータベース (データベース・アイコンが表示されているブランチにリストされているもの) を右クリックし、「**Configure Parameters**」を選択します。
2. 「Database Configuration」で、次の操作を実行します。
   a. オプションのリストをスクロールして、次のパラメータをここに示す値で置き換えます。

LOCKTIMEOUT	30
APP_CTL_HEAP_SZ	1024
APPHEAPSZ	1024
LOGFILSIZ	32768 **注意 :** 32768 はこのパラメータに推奨される値です。ただし、大規模なパブリッシュ・ジョブでは、セットアップにあわせてこのパラメータの微調整が必要になる可能性があります。

   b. 「**OK**」をクリックします。



3. 作成したデータベース (データベース・アイコンが表示されているブランチにリストされているもの) を右クリックし、「**Restart**」を選択します。

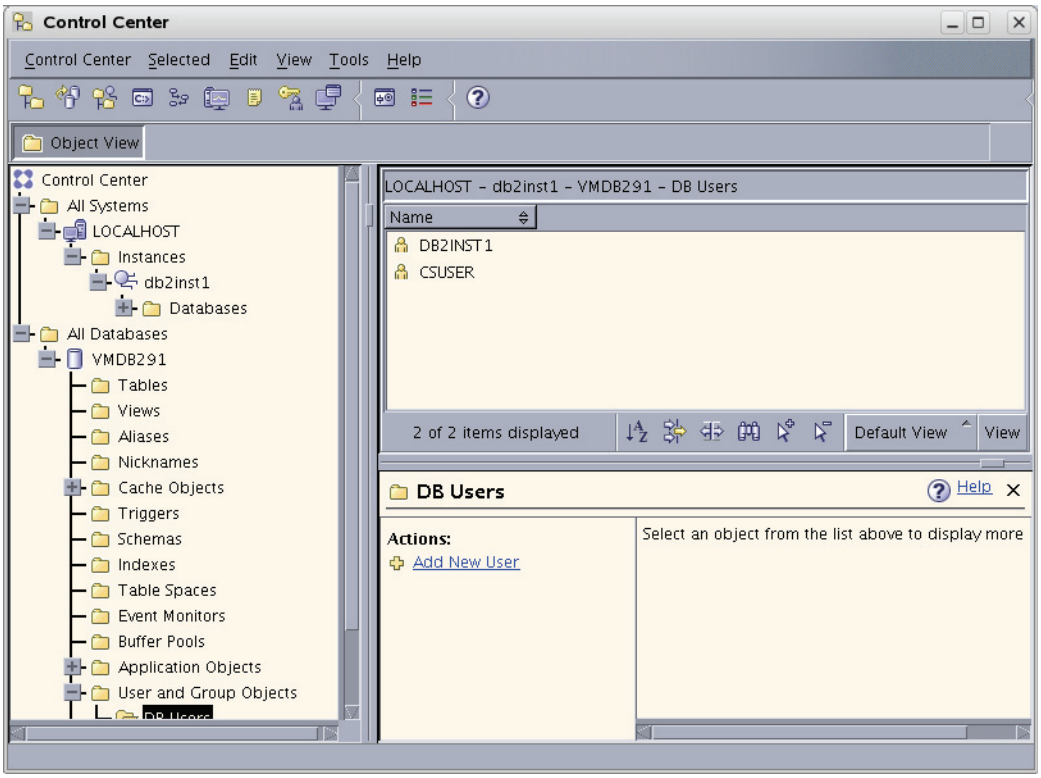
   ステータス・ウィンドウが点滅します。***これは、処理が完了したことを意味するものではありません。***通常、システムが再起動するまで 2、3 分待つ必要があります。

4. インスタンスを停止します。

   a. 「Control Center」ツリーの次のブランチを開きます。「**All Systems**」→「**LOCALHOST**」→「**Instances**」→*自分のインスタンスの名前*

   b. インスタンスを右クリックします。

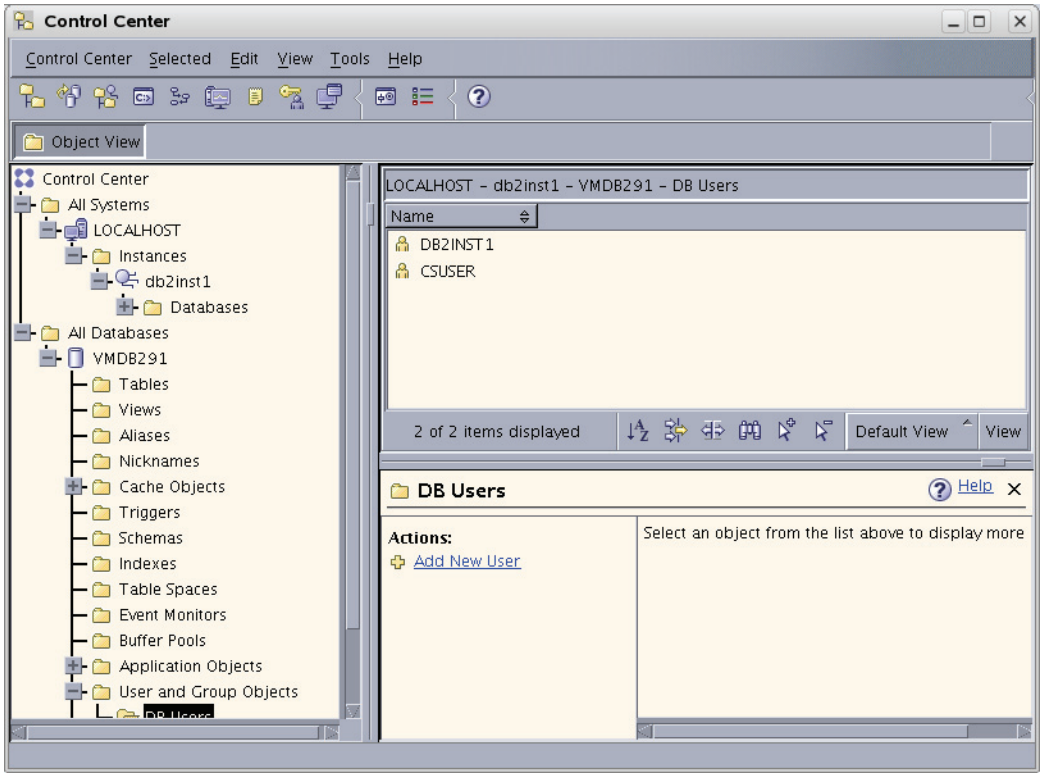
   c. 「**Stop**」を選択します。



   d. 「Confirm Stop」ダイアログ・ボックスで、「**OK**」をクリックします。

   e. このインスタンスが停止したことを知らせるメッセージが表示されるのを待ちます。

5. インスタンスを開始します。
   a. 「Control Center」ツリーの次のブランチを開きます。「**All Systems**」→「**LOCALHOST**」→「**Instances**」→*自分のインスタンスの名前*
   b. インスタンスを右クリックします。
   c. 「**Start**」を選択します。



6. このインスタンスが起動したことを知らせるメッセージが表示されるのを待ちます。***これは、処理が完了したことを意味するものではありません。***通常、システムが再起動するまで 2、3 分待つ必要があります。

   これで、使用しているデータベースで Oracle ソフトウェア製品を使用する準備が整いました。

第 2 部

Web サーバーのインストール

この部では、Web サーバーのインストール方法について説明します。この部は、次の章で構成されています。

- 第 4 章「Web サーバーのインストールをドキュメント化するためのワークシート」
- 第 5 章「IBM HTTP Server 7.0 のインストール」
- 第 6 章「Windows への Internet Information Services のインストール」
- 第 7 章「Solaris および Linux への Apache のインストール」

第 4 章

Web サーバーのインストールをドキュメント化するためのワークシート

この章には、追跡を必要とする Web サーバー・パラメータをリストしたワークシートが用意されています。

この章を印刷してください。その後、ソフトウェアをインストールしながら、これらのワークシートにある空のフィールドを特定のパラメータの値で埋めていきます。これにより、大きく時間を節約できます。さらに、インストール中に何かに失敗した場合のトラブルシューティングでは、これらのワークシートの情報が非常に重要になります。各インストールが完全にドキュメント化されるように、インストール 1 つにつきワークシートのセットを 1 つ使用します。

ワークシートは複数の表から構成され、これらの表は次のカテゴリに分けられます。

- サンプル値に対するキー
- Web サーバー・パラメータ

サンプル値に対するキー

このインストール・ワークシートには、サンプル値とともにパラメータがリストされます。個々のサンプル値は、次のいずれかに分類されます。

- **デフォルト** : 値はインストール時に自動的に作成されます。
- **標準** : この値は簡易インストールに対する標準的な構成を表します。システムから要求があった場合を除き、異なる値を使用しないでください。
- **オプション** : 値はあらかじめ設定されたオプションのリストから選択する必要があります。
- **推奨値** : 特定のパラメータに対して推奨されている値です。

> **注意**
>
> **推奨値**アカウント名には、サンプルのパスワード値が設定されています。このアカウントに対して、使用しているシステムのセキュリティに適したパスワードを選択することを強くお薦めします。

- **例** : この値は単なるサンプルです。使用しているインストールに適した値と置き換える必要があります。サンプル値は、使用している環境では有効ではない可能性があります。

Web サーバー・パラメータ

表 1: IIS Web サーバー・パラメータ

パラメータ	表示	コメント	設定値
Web バージョン	*WebVersion*	例 : Apache 1.3.37	
Web ホスト名	*WebHost*	例 : `jeeves`	
Web ホストの IP アドレス	*WebIP*	例 : `104.222.111.155`	
Web サーバー・ポート	*WebPort*	デフォルト : `80`	
IIS のみ : フィルタ名 (ISAPI プラグイン名)	*FilterName*	推奨 : `iisforwardfilter`	
Apache のみ : Apache ルート・ディレクトリ	*ApacheRoot*	例 : `/usr/apache`	

表 2: Apache Web サーバー・パラメータ

パラメータ	表示	コメント	設定値
Web バージョン	*WebVersion*	例 : Apache 1.3.37	
Web ホスト名	*WebHost*	例 : jeeves	
Web ホストの IP アドレス	*WebIP*	例 : 104.222.111.155	
Web サーバー・ポート	*WebPort*	デフォルト : 80	
IIS のみ : フィルタ名 (ISAPI プラグイン名)	*FilterName*	推奨 : iisforwardfilter	
Apache のみ : Apache ルート・ディレクトリ	*ApacheRoot*	例 : /usr/apache	

第 5 章

IBM HTTP Server 7.0 のインストール

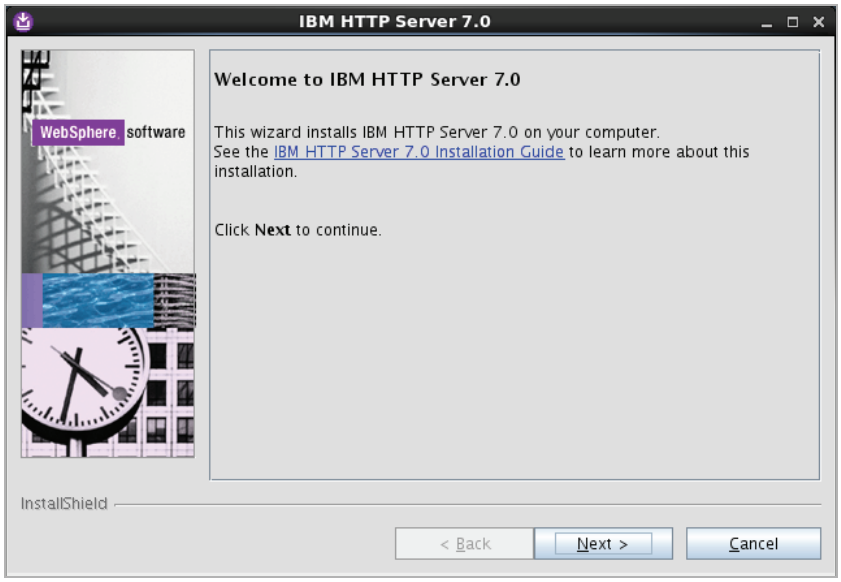
この章は、次の項で構成されています。

注意

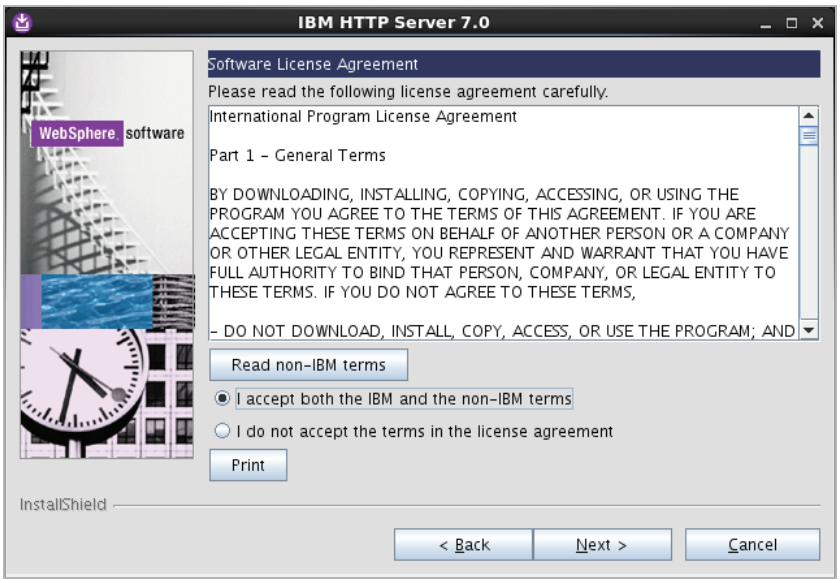
このガイドでは、IBM HTTP Server を「IHS」、WebSphere Application Server を「WAS」と呼びます。

インストール手順

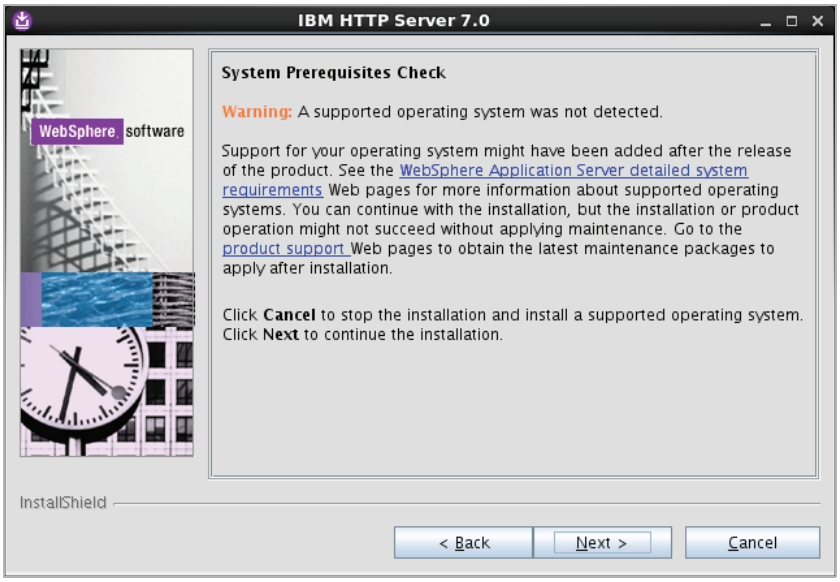
1. 使用している IBM オペレーティング・システムに適した WebSphere Plugins ファイルをダウンロードします。
2. このファイルを一時ディレクトリで解凍します。
   - UNIX の場合 : **`tar -xvf <file name>`**
     例 :
     ```
     gzip -d C87XTML_Plugins.tar.gz
     tar -xvf C87XTML_Plugins.tar
     ```
   - Windows の場合 : **`unzip <file name>`**
     例 :
     ```
     unzip C87XTML_Plugins.zip
     ```
3. `IHS/` ディレクトリに移動します。
   例 :
   ```
   cd IHS/
   ```
4. インストーラを実行します。
   - UNIX の場合 : `./install`
   - Windows の場合 : `install.exe`
5. GUI インストーラが表示されます。「**Next**」をクリックします。



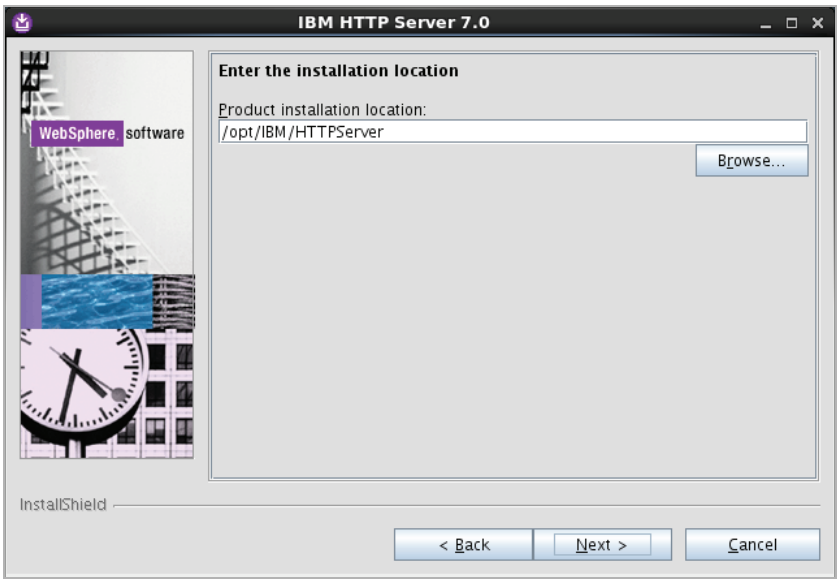
6. 「**I accept the IBM and non-IBM terms**」ラジオ・ボタンをクリックしてライセンス契約を受入れ、「**Next**」をクリックします。



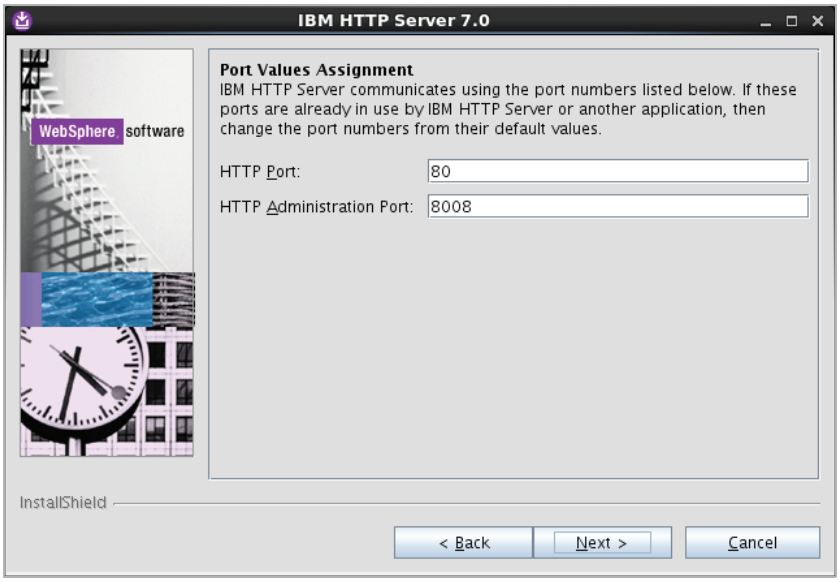
7. 「System prerequisites check」画面で、「**Next**」をクリックします。



8. 「Enter the Install location」画面で、「**Browse**」ボタンを使用して IHS 6.1 をインストールする場所を選択し、「**Next**」をクリックします。



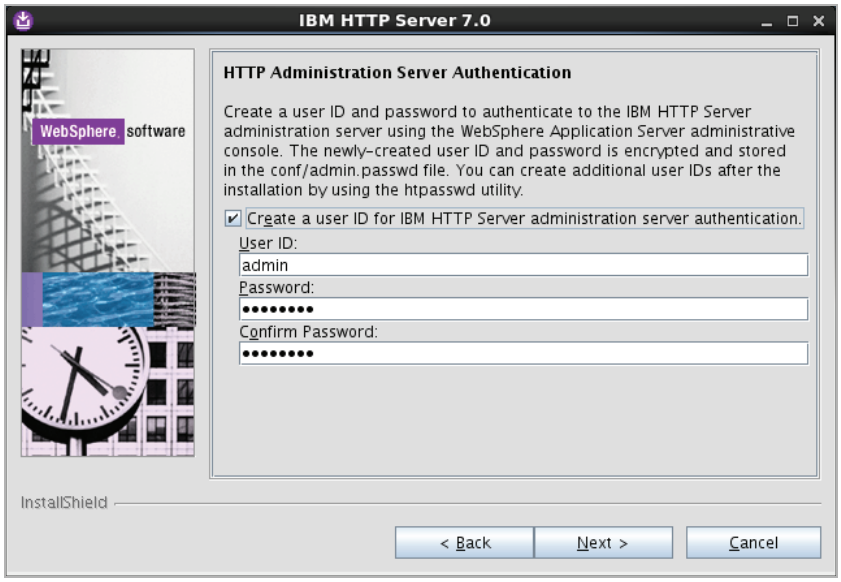
9. 「Port Values Assignment」画面で、IHS を実行するポートを入力します。「**Next**」をクリックします。



注意

このガイドでは、デフォルトのポート、80 および 8008 を使うことを前提にして説明します。これらを変更した場合は、与えられている値を選択したポートで置き換えてください。

10. 「HTTP Administration Server Authentication」画面で、次の操作を行います。
    a. 「**Create a user ID for IBM administration server authentication**」を選択します。
    b. 次のフィールドに入力します。
        - **User ID**: `admin`
        - **Password**: < 入力して確認します >
    c. 「**Next**」をクリックします。

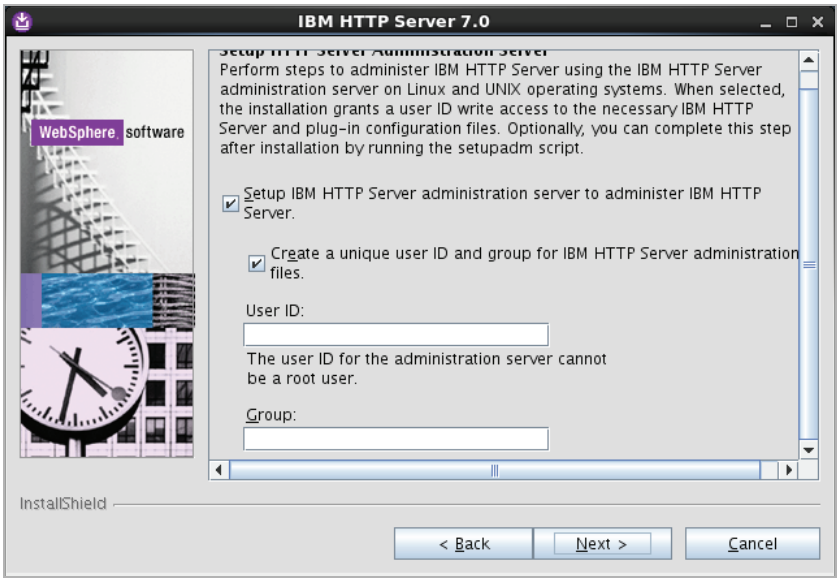


11. 「Setup HTTP Administration Server」画面で、次の操作を行います。
    a. 次の項目を選択します。
        - **Setup IBM HTTP administration server to administer IBM HTTP Server**
        - **Create a unique ID and Group for the IBM HTTP Server administration**
    b. 次のフィールドに入力します。たとえば、次のように指定します。
        - **User ID**: `ihs7`
        - **Group**: `ihs7`

注意

「User ID」および「Group」に指定した一意の名前を記録します。これらは WAS との統合に必要です。「User ID」と「Group」には何を指定してもかまいません。「`ihs61`」は単なる例です。

c. 「**Next**」をクリックします。



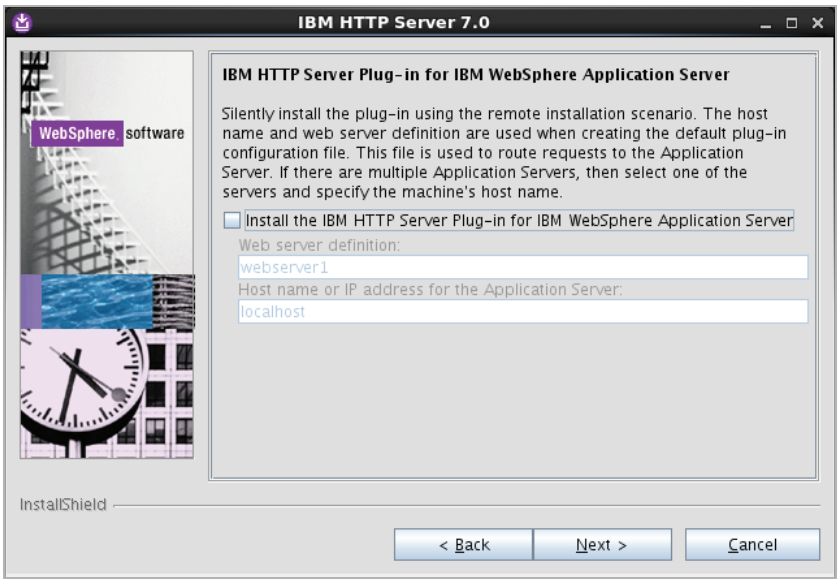
12. 「IBM HTTP Server Plugin for IBM WebSphere Application Server」画面で、次の操作を行います。

a. 「**Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server**」を選択します。

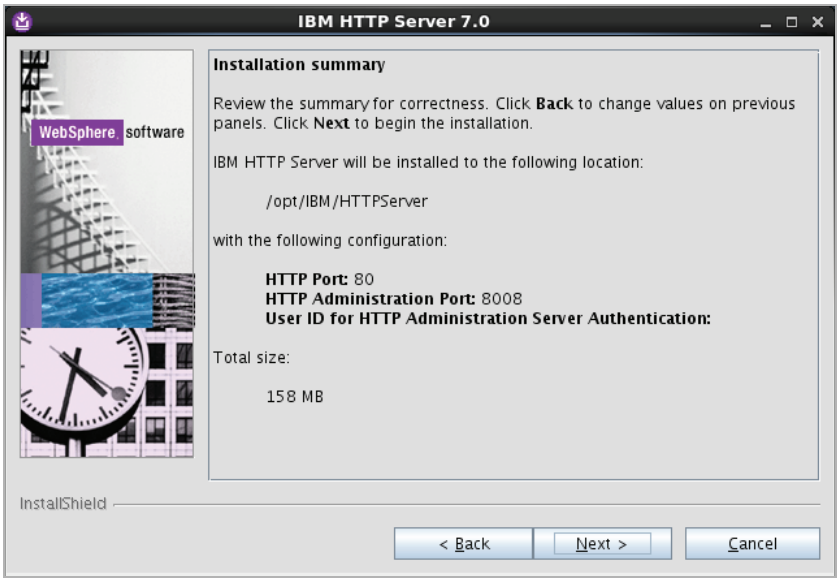
b. 次のフィールドに入力します。

- **Web server definition**: `webserver1`
- **Host name**: アプリケーション・サーバーが検出されたホスト名を入力します。

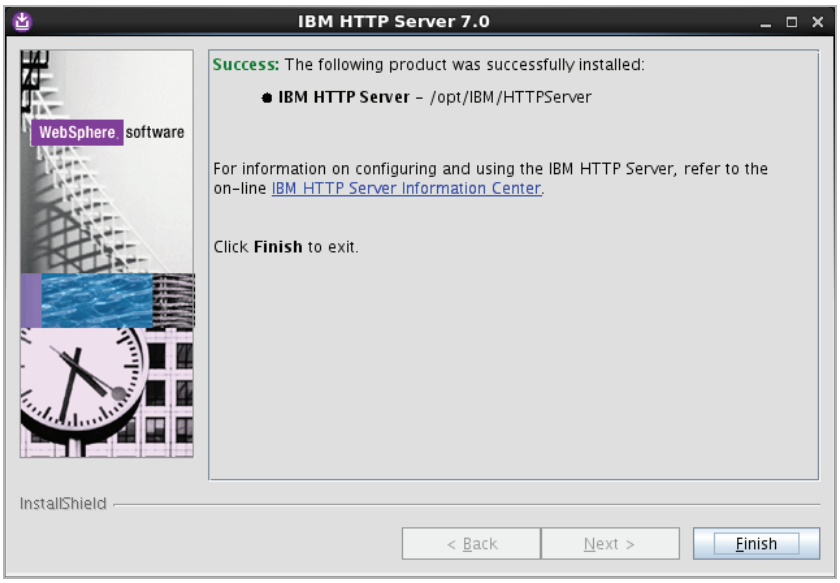
c. 「**Next**」をクリックします。



13.「Installation summary」画面で「**Next**」をクリックします。



14. インストールが終わるまで待ちます。
15. インストールが完了したら、「**Finish**」をクリックします。



注意

ここで、更新インストーラを使用して IBM HTTP Server にパッチを適用し、WebSphere と同じバージョンにします。更新インストーラの使用に関する情報は、更新をダウンロードした IBM サイトにあります。IHS サーバーおよび IHS プラグインの両方を別々に更新してください。そのためには、WebSphere およびプラグインの Fix Pack が必要です。

WebSphere Application Server を使用したローカル・サーバーへの IHS のインストール

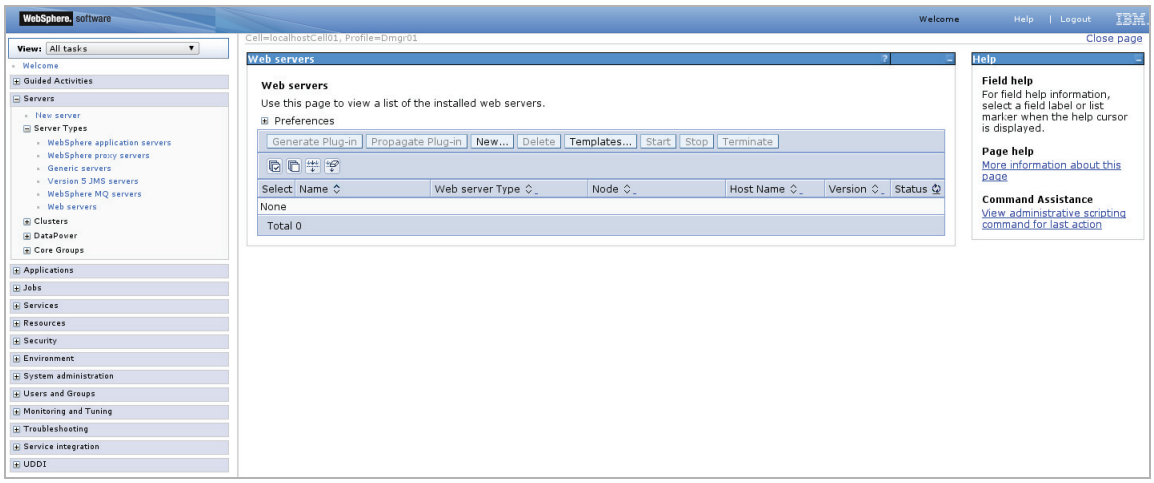
注意

このインストールは、WebCenter Sites のインストール後に実行することをお薦めします。その後、`cfg.xml` プラグインが自動的に更新され、WebCenter Sites に組み込まれます。

1. WAS 管理コンソールを参照します。たとえば、次のようにします。

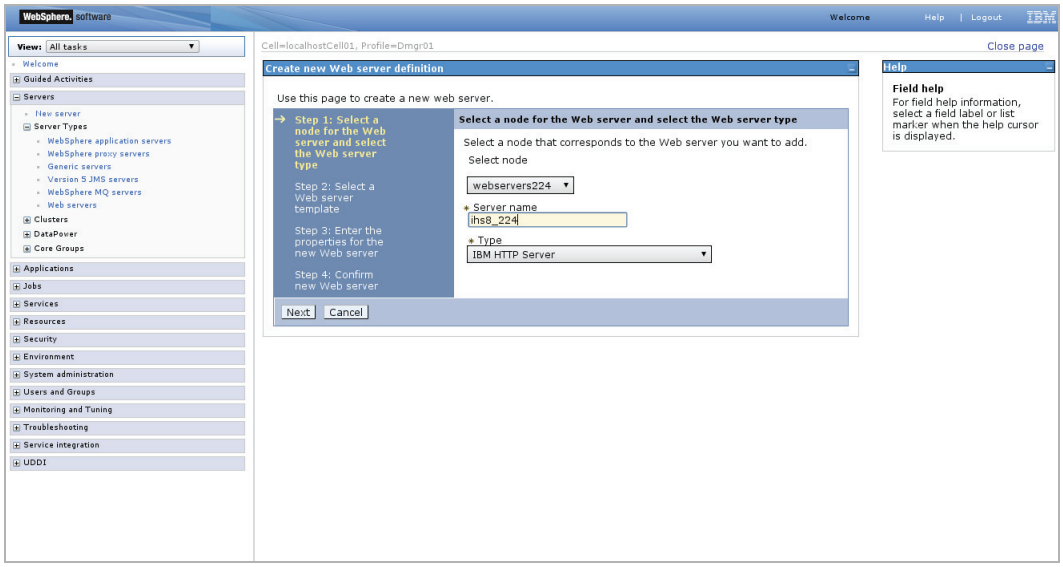
   `http://<DM_host>:<DM_console_port>/ibm/console`

   ここで、`<DM_host>` はデプロイメント・マネージャ・ホストのホスト名または IP アドレス、`<DM_console_port>` はデプロイメント・マネージャ・コンソールが接続をリスニングしているポート番号です。
2. 管理サイトにログインします。
3. 「**Servers**」→「**Web Servers**」を選択します。

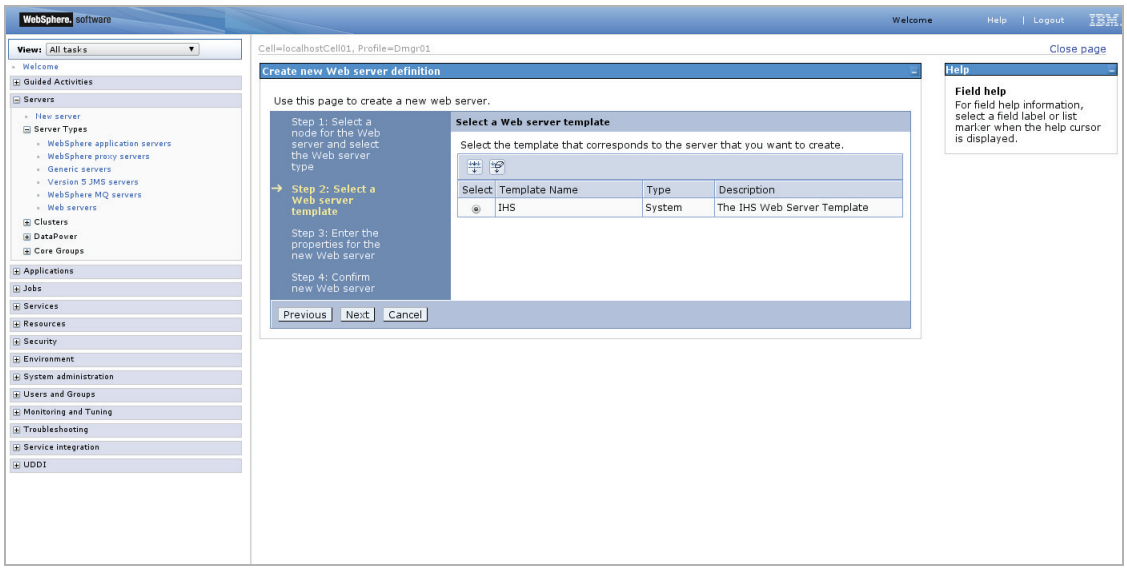


4. 「**New**」をクリックします。

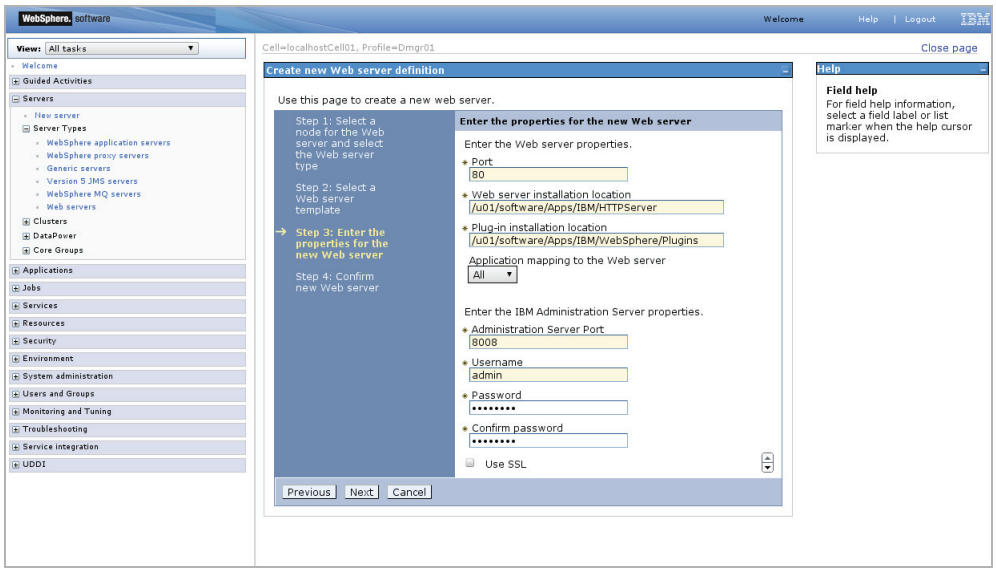
5. IHS を WAS にリンクするには、次の操作を行います。
   a. 次のフィールドに入力します。
      - **Select node**: フェデレーションを行うノードを選択します (通常、これは、WebCenter Sites がインストールされているアプリケーション・サーバーまたはクラスタのノードです)。
      - **Server name**: この Web サーバーに対する一意の名前を入力します。これは、IHS をインストールしたときに入力したものです。
      - **Type**: タイプは「**IBM HTTP Server**」のままにします。
   b. 「**Next**」をクリックします。



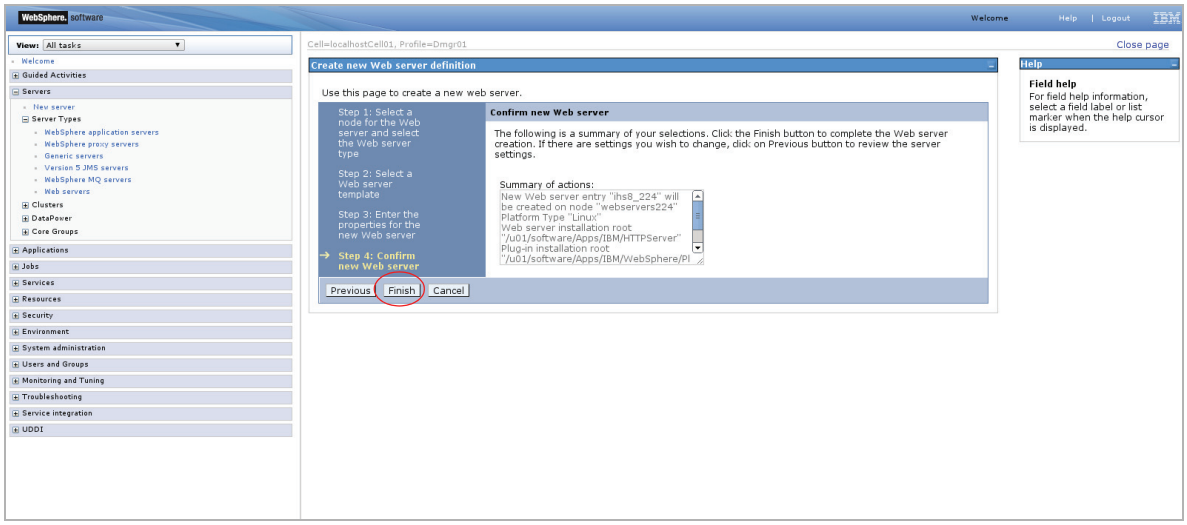
6. 「Select a Web server template」画面で、「**Next**」をクリックします。



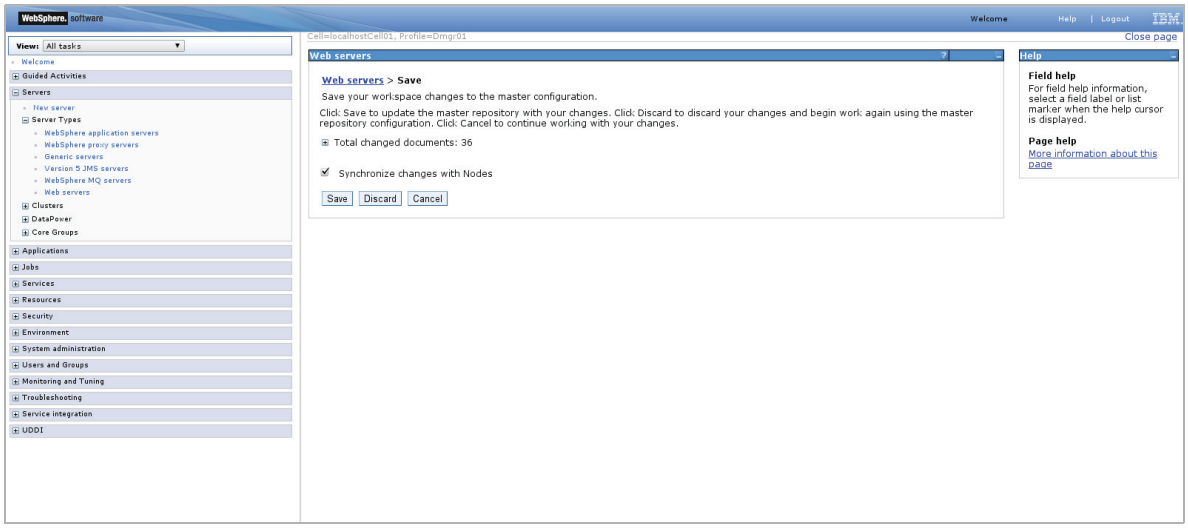
7. 「Property Page」で次の操作を行います。
   a. すべてのエントリが適切であることを確認します。通常変更する必要があるエントリは、IHS サーバーの場所および Plugin Directory のみです。
   b. 「**Next**」をクリックします。



8. 新しい Web サーバーを確認し、「**Finish**」をクリックします。



9. 要求された場合は、変更を保存します。



10. これで、Web サーバーの選択肢を使用して、WAS コンソールから Web サーバーを起動および停止できるようになります。

第 6 章

Windows への Internet Information Services のインストール

この章では、Windows 2008 Server に Microsoft の Internet Information Services (IIS) 7.0/7.5 をインストールし、テストする方法について説明します。

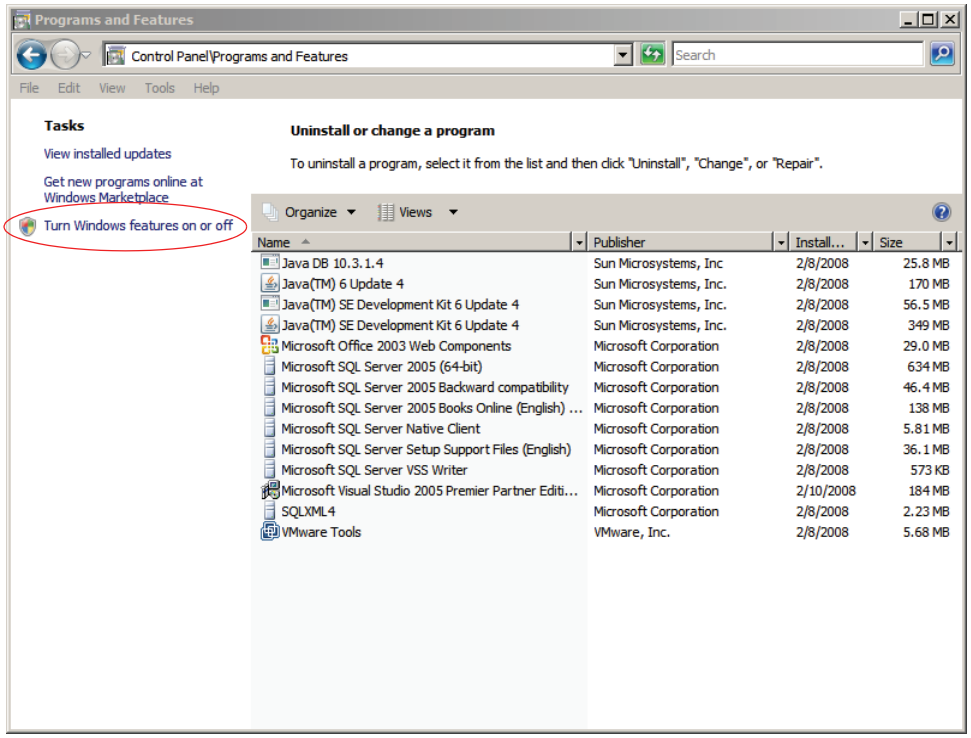
この章は、次の項で構成されています。

手順 I. IIS のインストール

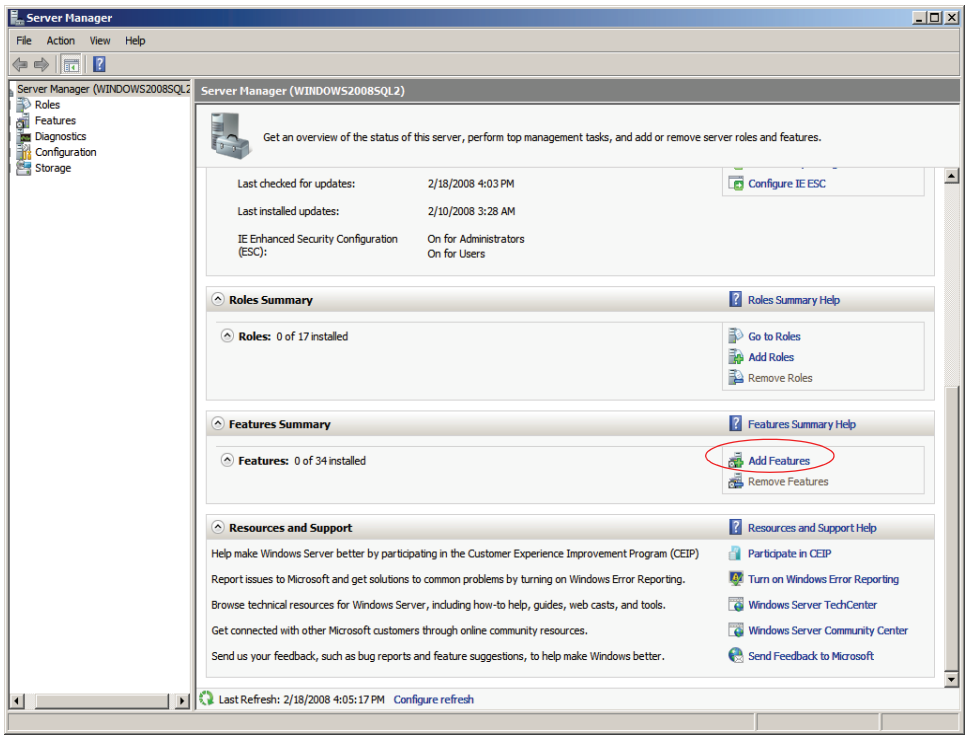
IIS がインストールされていない場合、または一部のみインストールされている場合は、Microsoft の指示に従って、Windows 2008 Server に IIS 7.0 をインストールするか、Windows 2008 R2 Server に IIS 7.5 をインストールしてください。

ここでは手順の概要を説明します。

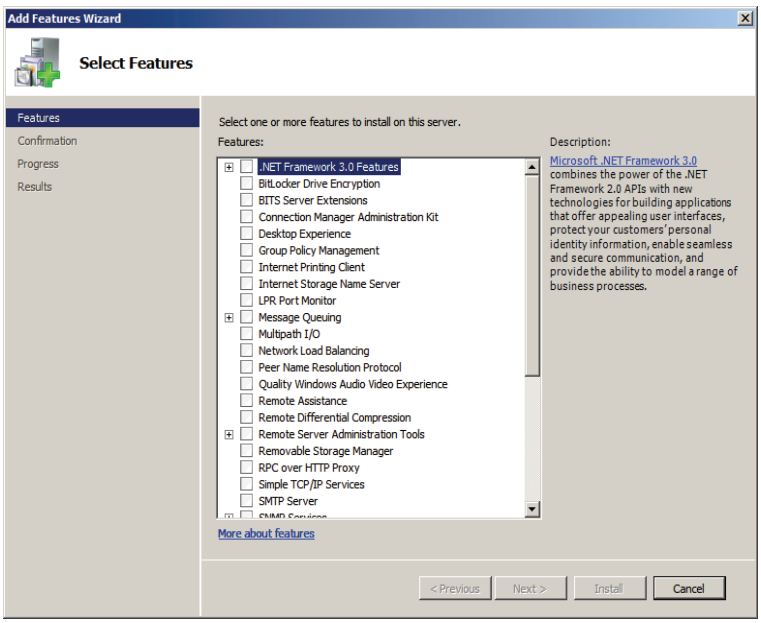
1. 「スタート」→「設定」→「コントロール パネル」を選択します。
2. 「プログラムと機能」を選択します。
3. 「Windows の機能の有効化または無効化」を選択します。



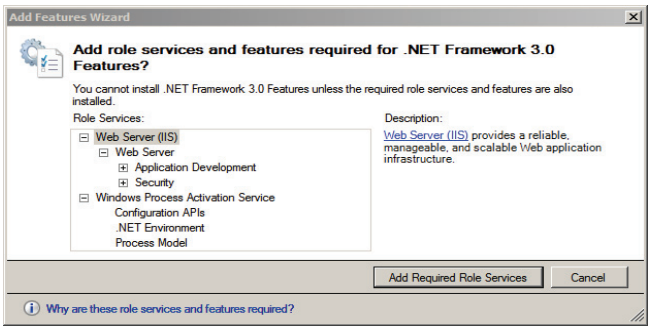
4. 「サーバー マネージャ」ウィンドウで、「機能の概要」セクションにスクロールし、**「機能の追加」**をクリックします。



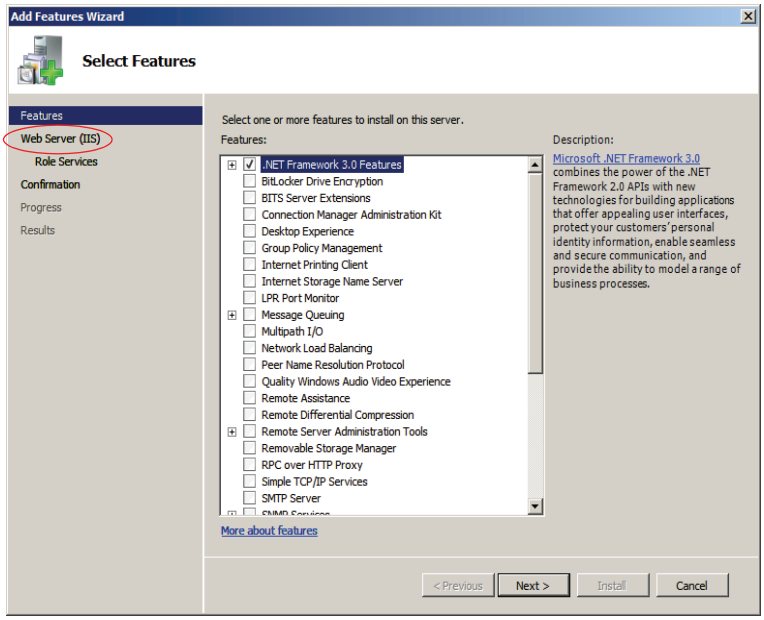
5. 「機能の選択」画面で、**「.NET Framework 3.0 の機能」**を選択します。



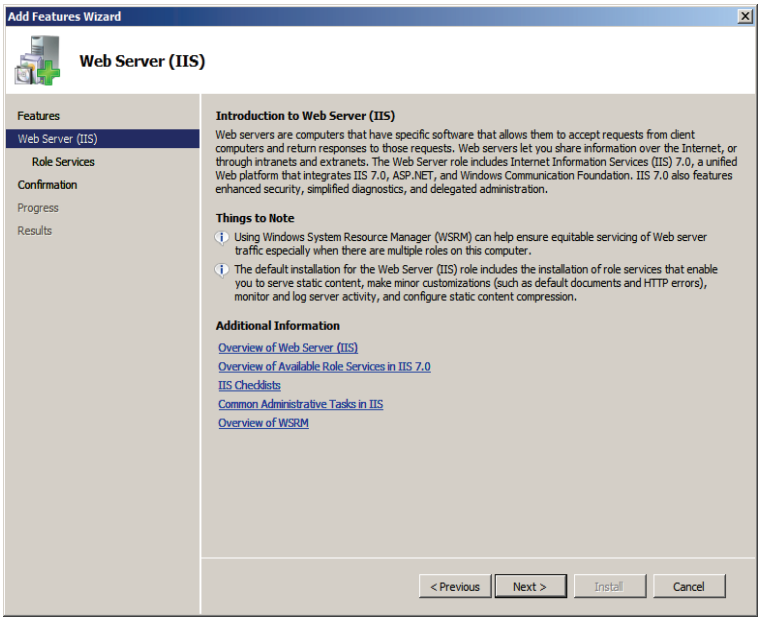
6. 「機能の追加ウィザード」ダイアログ・ボックスで、**「必要な役割サービスを追加」**を選択します。



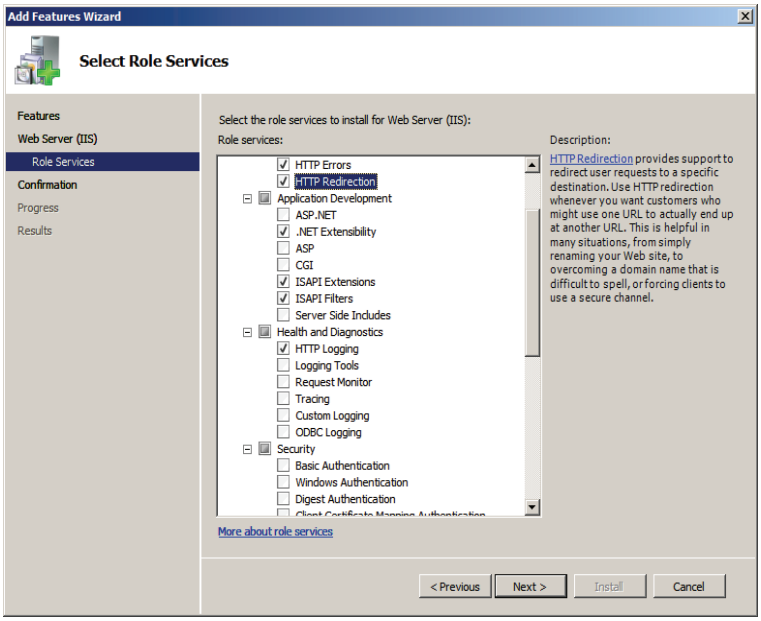
7. 機能の追加ウィザードに、**「Web サーバー (IIS)」**オプションが表示されます。**「次へ」**をクリックします。



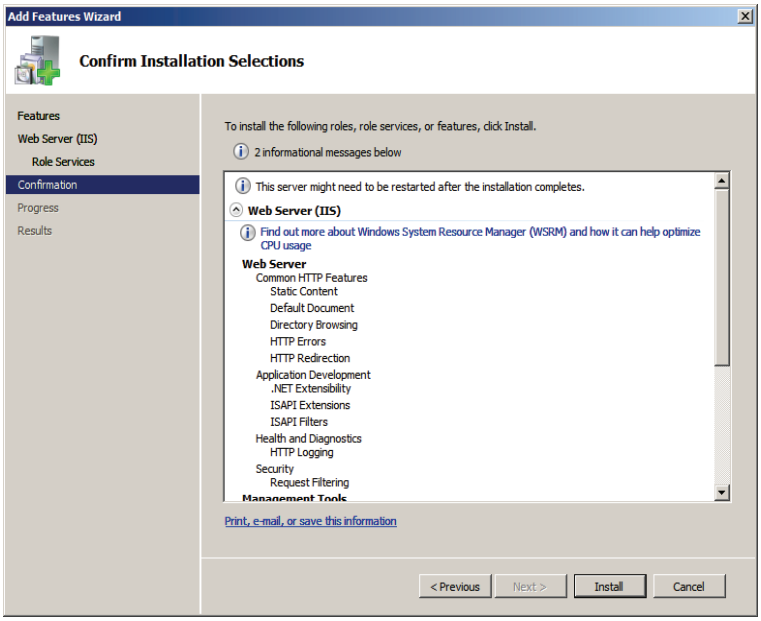
8. 「Web サーバー (IIS) について」画面で、「**次へ**」をクリックします。



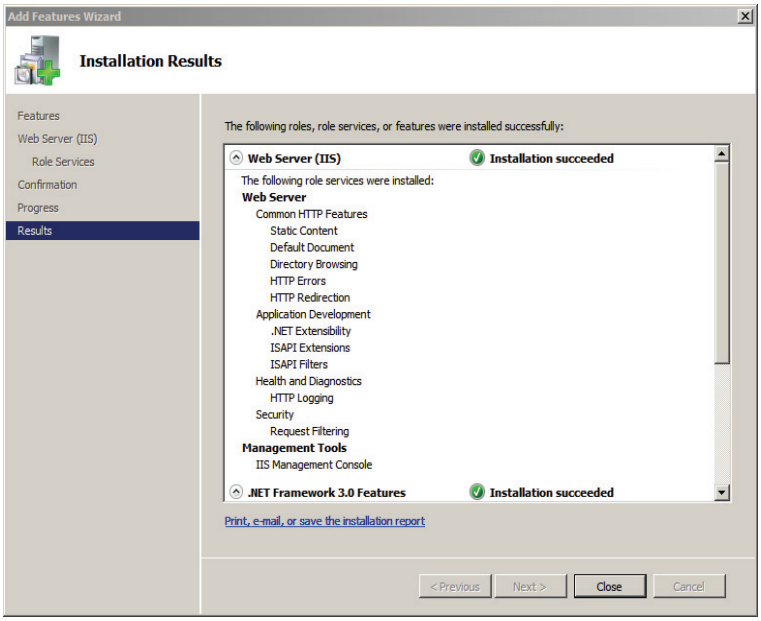
9. 「役割サービスの選択」画面で、次の操作を行います。
   a. 次の項目を選択します。
      - **HTTP 基本機能**
      - **ISAPI 拡張**
      - **ISAPI フィルター**
      - **HTTP ログ**
      - **管理ツール**
      - 「**HTTP リダイレクション**」など、使用しているインストールで必要とされるその他のロールすべて
   b. 「**次へ**」をクリックします。



10. 「インストール オプションの確認」画面で、選択内容を確認し、「次へ」をクリックします。



11. インストールが完了するまで待ちます。その後、結果を確認します。
12. 「閉じる」をクリックします。



13. この時点で再起動を提案されますが、実行する必要はありません。

手順 II. インストールの検証

IIS のインストール後、インストールを検証して、ページに適切なサービスが提供されているかどうかを判断します。インストールした IIS をホストしているサーバー、およびネットワーク上の別のブラウザから、この IIS をテストします。

IIS がページにサービスを提供していることを検証するには、次の操作を実行します。

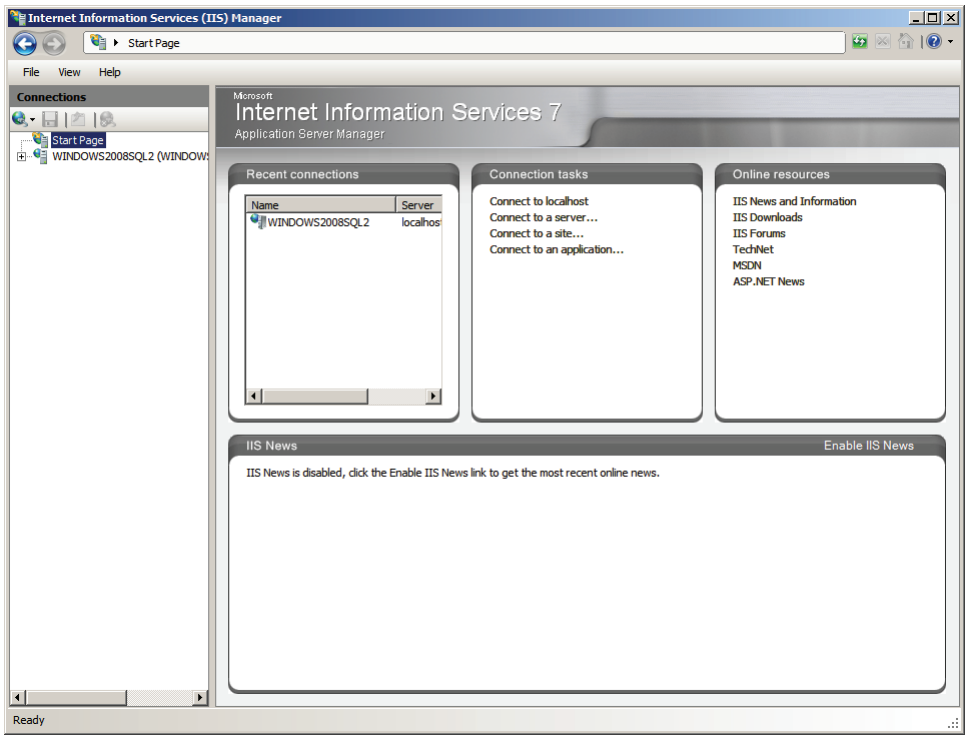
1. IIS が実行されているホストでブラウザを起動します。
2. ブラウザで、URL **`http://localhost/`** に移動します。

   ブラウザに「IIS7」ページが表示されれば、IIS はインストールされ、実行されています。

手順 III. IIS の起動および構成

A. IIS マネージャ

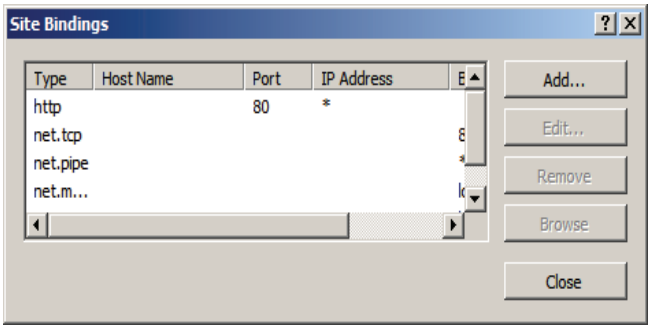
1. 管理コンソールを起動します。どのようなアクションを行う場合でも、最初にこれを実行します。
2. 「スタート」→「すべてのプログラム」→「管理ツール」→「インターネット インフォメーション サービス (IIS) マネージャ」を選択します。
3. インターネット インフォメーション サービス (IIS) マネージャがロードされたら、次の操作を行います。
   a. 現在のシステム名で始まる、左側のツリーを開きます。
   b. 「サイト」エントリ・フィールドで、「Default Web Site」を選択します。



B. IIS ポートの変更

1. 管理コンソールを開き、デフォルト・サイトを参照します。
2. 「Default Web Site」エントリを右クリックし、メニューから「バインドの編集」を選択します。

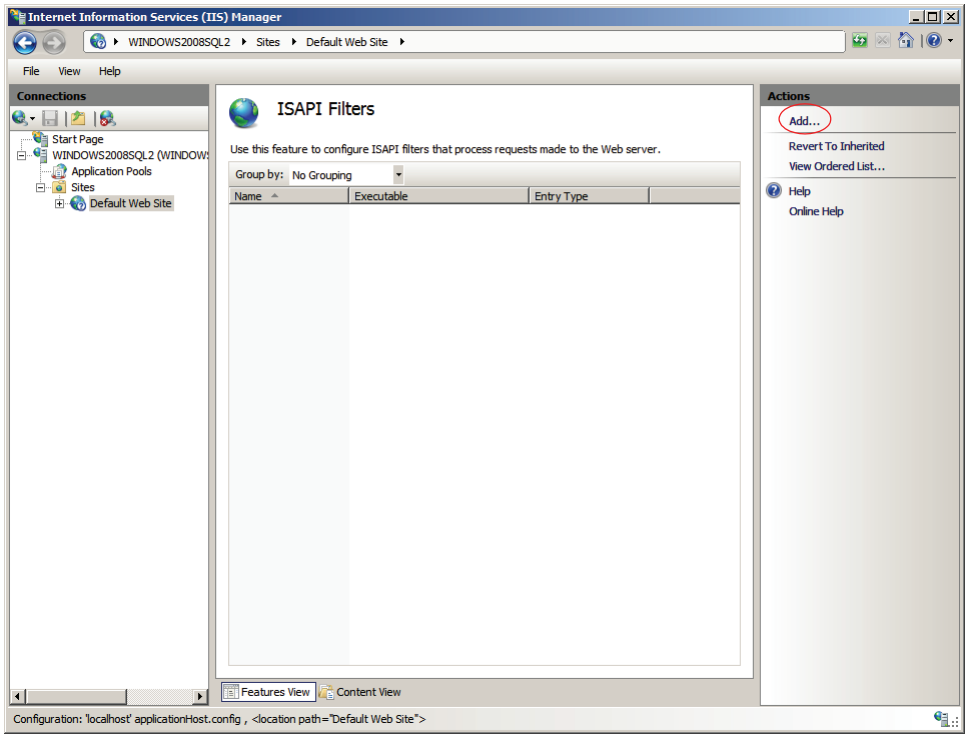
3. 「サイト バインド」ダイアログ・ボックスでは、Server IIS がバインドされるポートおよび IP アドレスの追加または変更ができます。



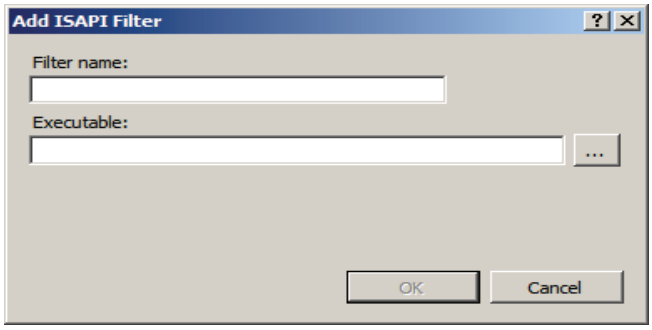
4. すべての変更が終わったら、**「閉じる」**をクリックします。

C. 新しい ISAPI フィルタの追加

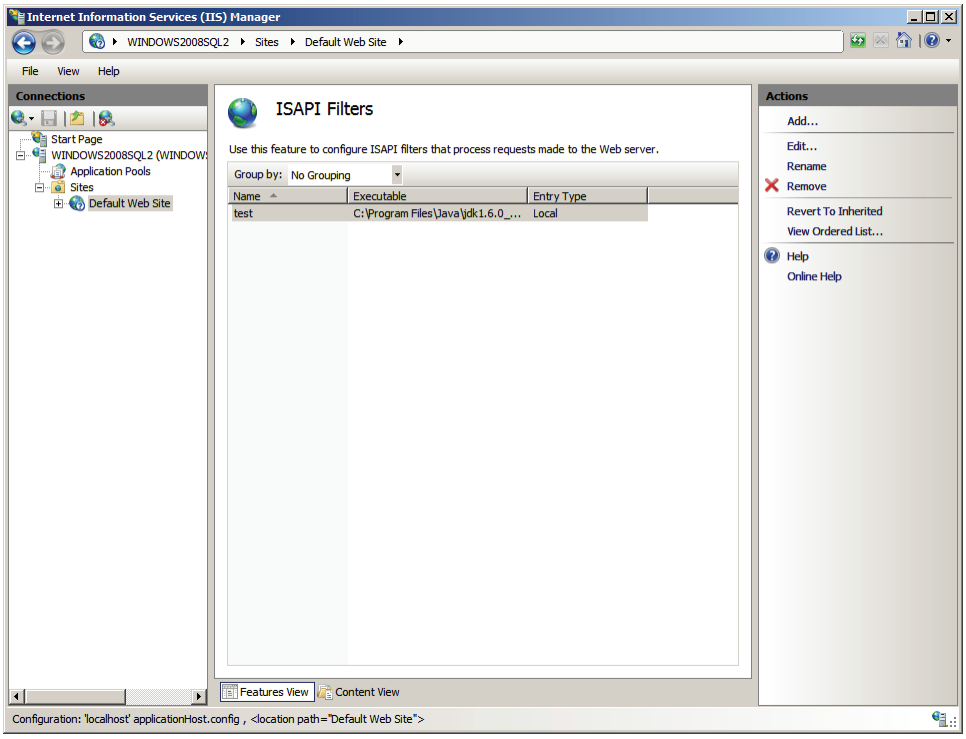
1. 管理コンソールを開き、**デフォルト・サイト**を参照します。
2. 中央のリストで**「ISAPI フィルター」**をクリックし、次に**「追加」**をクリックします。



3. 「ISAPI フィルターの追加」ダイアログ・ボックスが表示されます。
   a. 指定されたフィールドに値を入力します。
      - **フィルター名 :** フィルタの名前を入力します。
      - **実行可能ファイル :** 実行可能ファイルの場所を入力します。
   b. 「**OK**」をクリックします。

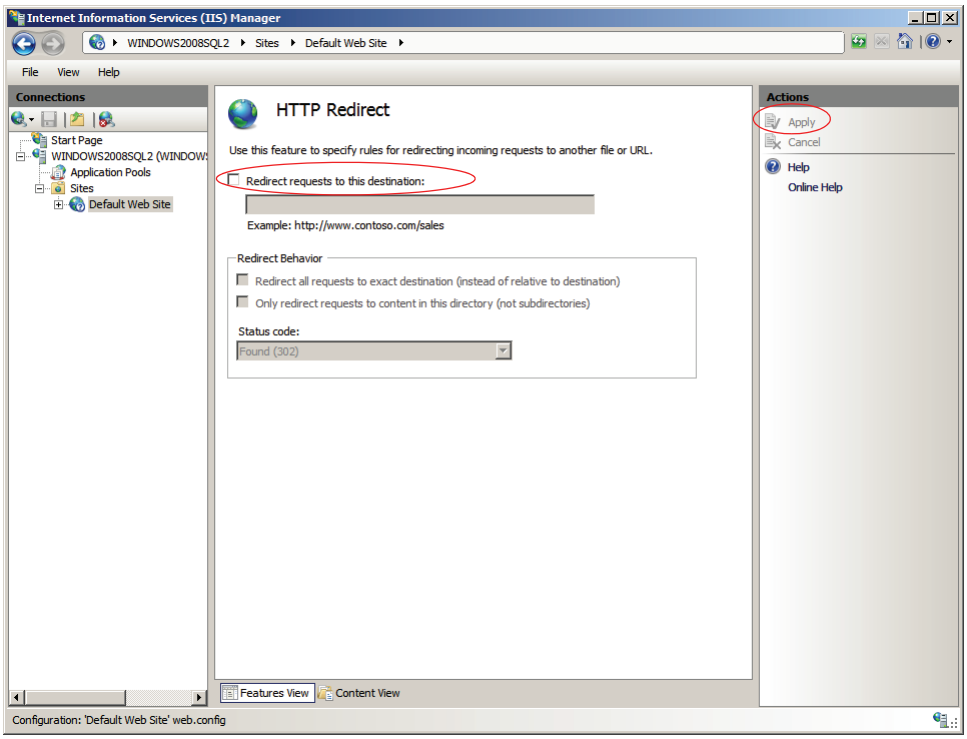


新しいフィルタが「ISAPI フィルター」リストに追加されます。



IIS を使用したプロキシ

1. 管理コンソールを開き、デフォルト・サイトを参照します。
2. 中央のリストで、「**HTTP リダイレクト**」をクリックします。
3. インターネット インフォメーション サービス (IIS) マネージャの中央パネルで、次の操作を行います。
   a. 「**このリダイレクト先に要求をリダイレクト**」オプションを選択します。
   b. テキスト・フィールドに、リモート・サーバーの場所を入力します (WebCenter Sites または Remote Satellite Server については、コンテキスト・ルートを含めます)。
   c. 「**適用**」をクリックします。



第 7 章

Solaris および Linux への Apache のインストール

この章では、Solaris および Linux システムに Apache HTTP サーバーをインストールし、構成する方法について説明します。前述のとおり、Apache は、WebLogic および WebCenter Sites をホストしているマシンにインストールすることも、別のホストにインストールして使用することもできます。

この章は、次の項で構成されています。

手順 I. Apache のインストール

1. Apache HTTP サーバーは、Solaris 8、Solaris 9、Linux RedHat および Linux SuSE システムにあらかじめインストールされている可能性があります。Apache の実行を予定している環境に、Apache がインストールされているかどうかを確認します。
2. 次のいずれかを行います。
   - Apache がすでにインストールされている場合は、88 ページの「手順 II. Apache パラメータのドキュメント化」に進みます。
   - Apache がまだインストールされていない場合は、次のいずれかの操作を行います。
     - ソース・メディアからインストールします。
     - インターネットからダウンロードします。
     - ソースからビルドします。つまり、モジュールを選択し、自分で Apache 実行可能ファイルをコンパイルします。ソースからビルドする場合は、Apache Foundation が URL `http://www.apache.org/` で提供している情報を参照し、その指示に従って操作します。

手順 II. Apache パラメータのドキュメント化

Apache インストールの詳細を、「表 3: Apache のパラメータ」でドキュメント化することを強くお薦めします。

表 3: Apache のパラメータ

パラメータ	保持される内容	設定値
Web サーバーのバージョン (*`WebVersion`*)	ホストで実行されている Apache のバージョン。必ず、WebCenter Sites でサポートされているバージョンを使用してください。	
Web ホスト名 (*`WebHost`*)	ネットワーク上で Apache ホスト・マシンが認識されている名前。	
Web ホストの IP アドレス (*`WebIP`*)	Apache ホスト・マシンに割り当てられている IP アドレス (数値)。	
Web サーバー・ポート (*`WebPort`*)	Apache 通信のために割り当てられたポート番号。デフォルト値は 80 です。	
Apache ルート・ディレクトリ (*`ApacheRoot`*)	Apache がインストールされているトップレベルのディレクトリ。*`ApacheRoot`* 直下のサブディレクトリには、`bin` および `conf` があります。	

手順 III. Apache に正しいモジュールが含まれることを検証

注意

この項は、Apache バージョン 1.3x にのみ適用されます。

Apache はモジュール形式のソフトウェアで、一連のモジュールから構築されています。WebLogic Server では、Apache Web サーバーをホストしているマシンに `mod_so.c` モジュールが必要です。使用している Apache サーバーにこのモジュールが含まれていることを確認してください。そのためには、`httpd` コマンドに `-l` オプションを指定して実行し、出力から `mod_so` を見つけます。

次に例を示します。

```
$ ApacheRoot/bin/httpd -l | grep mod_so
mod_so.c
```

出力を調べて、次のいずれかを行います。

- 直前のコマンドからの出力に「`mod_so.c`」が含まれていれば、使用している Apache のバージョンには正しいモジュールが含まれています。89 ページの「手順 IV. Apache が適切に実行されていることの検証」に進みます。
- 直前のコマンドからの出力に「`mod_so.c`」が含まれていない場合は、Apache を再構築し、再インストールする必要があります。ガイドラインについては、88 ページの「手順 I. Apache のインストール」を参照してください。

手順 IV. Apache が適切に実行されていることの検証

この手順では、Apache を起動して、適切に実行されていることを検証します。検証方法については、Apache Web サイトを参照してください (88 ページの「手順 I. Apache のインストール」に記載されています)。

次の手順

WebLogic および WebCenter Sites で実行するように Apache を構成します。手順については、使用している構成のインストレーション・ガイドを参照してください。

第 3 部

LDAP サーバーのインストールおよび構成

LDAP の使用を選択した場合、WebCenter Sites では、WebCenter Sites 用に特別に構成された、サポートされている LDAP サーバーへのアクセスを必要とします。この部では、サポートされている LDAP サーバーをインストールおよび構成して、WebCenter Sites と統合する方法について説明します。

注意

- サポートされている LDAP サーバーは、WebCenter Sites-LDAP インテグレータを実行する**前に**セットアップする必要があります。
- LDAP と統合するけれども、WebCenter Sites にコンテンツ管理サイトが 1 つも存在しない場合は、LDAP 統合が完了した時に、*『Oracle WebCenter Sites: LDAP との統合』* のコンテンツ管理サイトがインストールされていない場合の統合後の手順に関する項を参照してください。

この部は、次の章で構成されています。

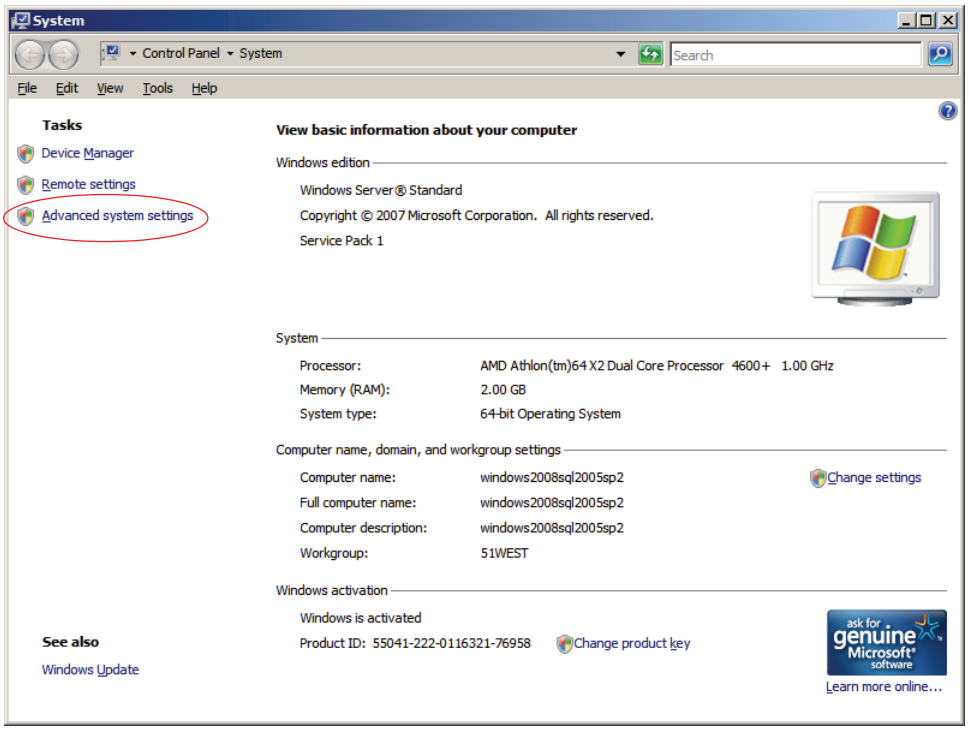
第 8 章

Active Directory Server 2008 のインストール

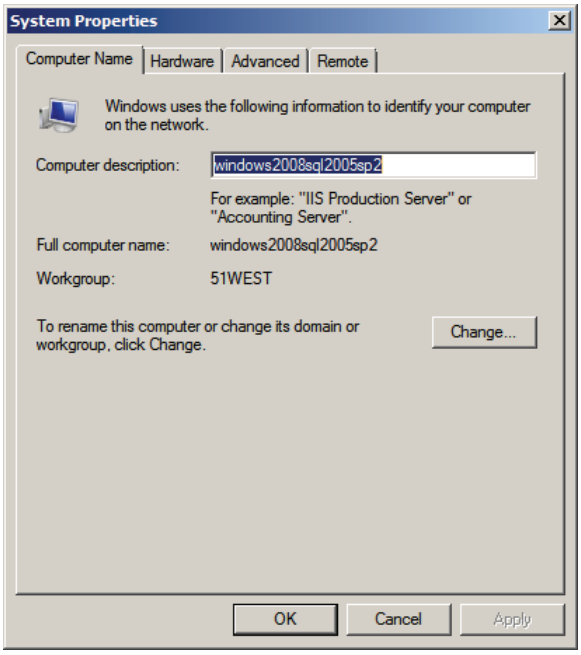
この章には次の項が含まれます。

インストール手順

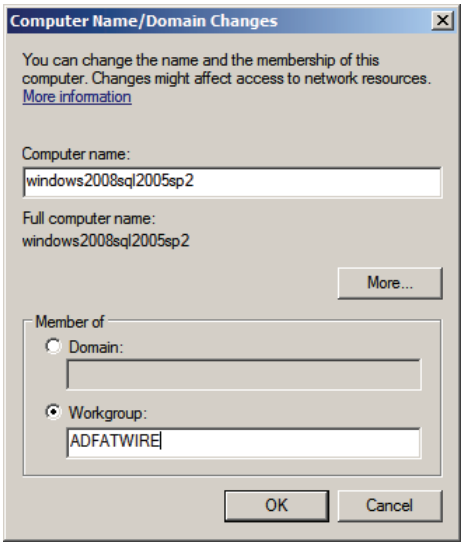
1. オペレーティング・システムをインストールします。
   a. Windows Server 2008(Web を除く Windows サーバー) をインストールします。
   b. インストールが完了しても、インストール・ディスクはドライブに入れたままにしてください。ADS のインストールを完了するには、このディスクが必要です。
   c. コンピュータの**名前**および**サフィックス**を設定します。
2. 「システムのプロパティ」ダイアログ・ボックスを開きます。**「スタート」**をクリックし、コンピュータ・アイコンを右クリックします。
3. 「システム」ウィンドウで、**「システムの詳細設定」**を選択します。



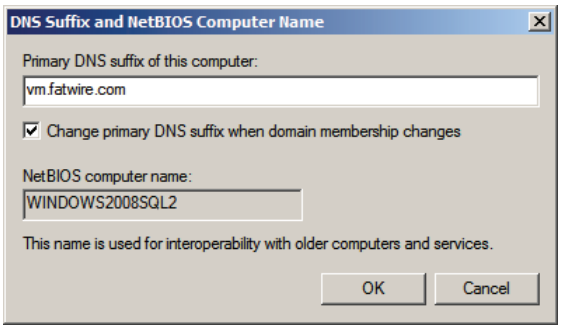
4. 「コンピューター名」タブを選択します。
   a. 「変更」をクリックします。



5. ポップアップ・ウィンドウが表示されたら、次のフィールドに入力します。
   - **コンピューター名**: コンピュータに割り当てる名前を入力します (この名前を記録しておきます)。
   - **所属するグループ**: 「**ワークグループ**」ラジオ・ボタンを選択し、一意のワークグループ名を入力します (この名前を記録しておきます)。



a. 「**詳細 ...**」をクリックします。

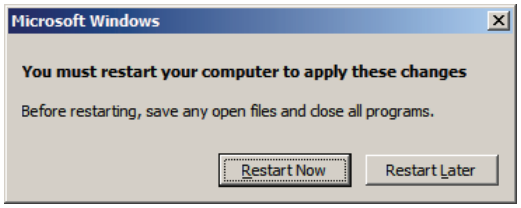


b. 「DNS サフィックスと NetBIOS コンピューター名」ダイアログ・ボックスで、次の手順を実行します。

- **このコンピューターのプライマリ DNS サフィックス**: コンピュータの DNS サフィックスを入力します (このサフィックスを記録しておきます)。
- **ドメインのメンバーシップが変更されるときにプライマリ DNS サフィックスを変更する**: チェック・ボックスが選択されている場合は、選択を解除します。

c. 「**OK**」をクリックしてダイアログ・ボックスを閉じます。

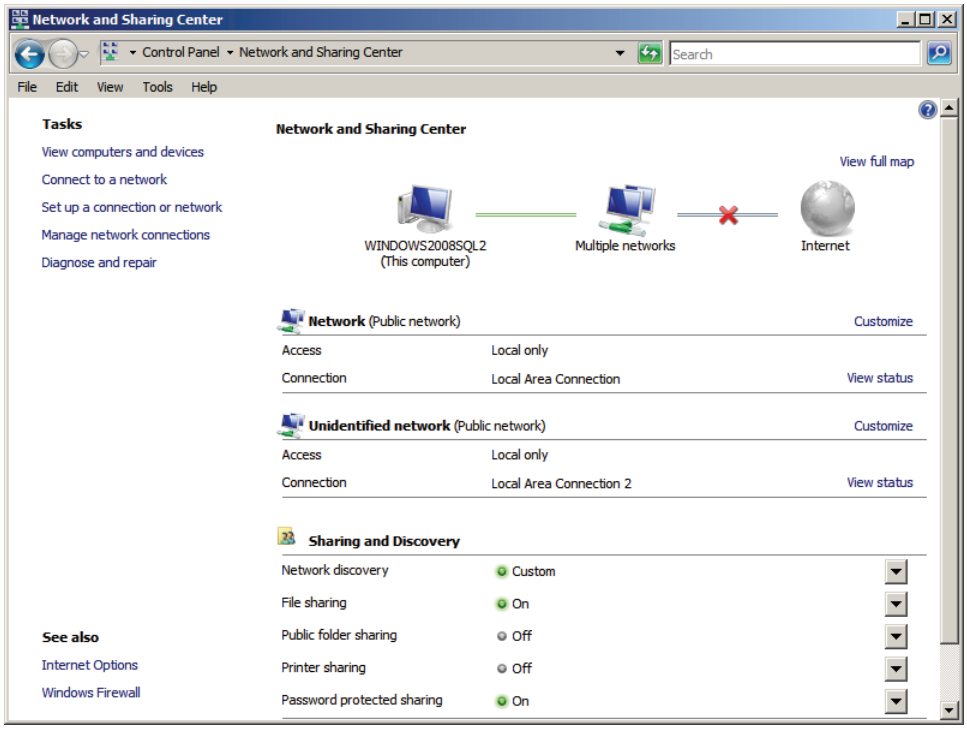
6. 「コンピューター名 / ドメイン名の変更」ダイアログ・ボックスで、「**OK**」をクリックします。
7. 「システムのプロパティ」ウィンドウで、「**閉じる**」をクリックします。
8. 再起動ダイアログ・ボックスで、「**後で再起動する**」をクリックします。



ネットワーク設定の構成

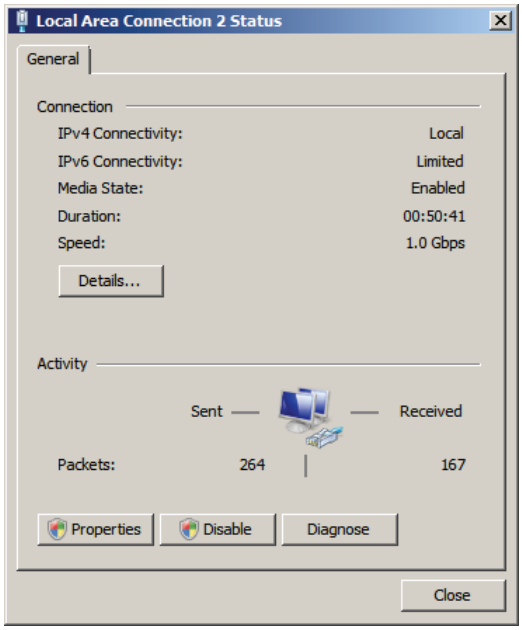
ネットワーク設定を構成するには、次の手順を実行します。

1. 「ネットワークのプロパティ」を開きます。
   a. 「スタート」→「コントロール パネル」を選択します。
   b. 「ネットワークと共有センター」アイコンをクリックします。
   c. 編集するネットワーク接続を選択します (`see ipconfig` 結果が複数ある場合は、必ず正しい接続を選択してください)。

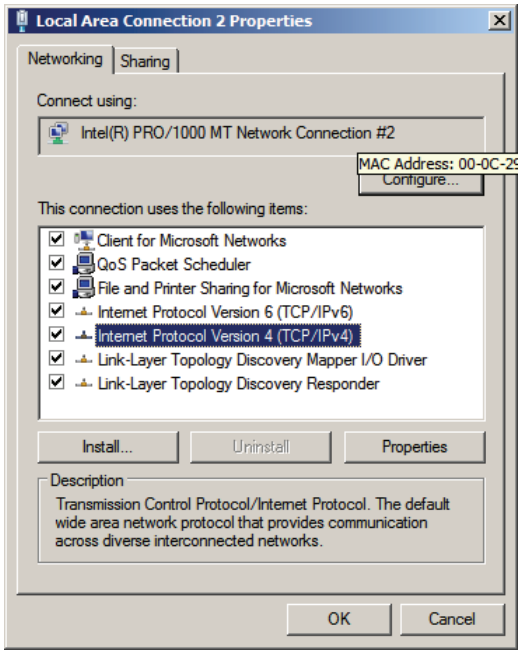


2. 選択したネットワーク接続の隣にある「状態の表示」を選択します。

3. 「プロパティ」をクリックします。

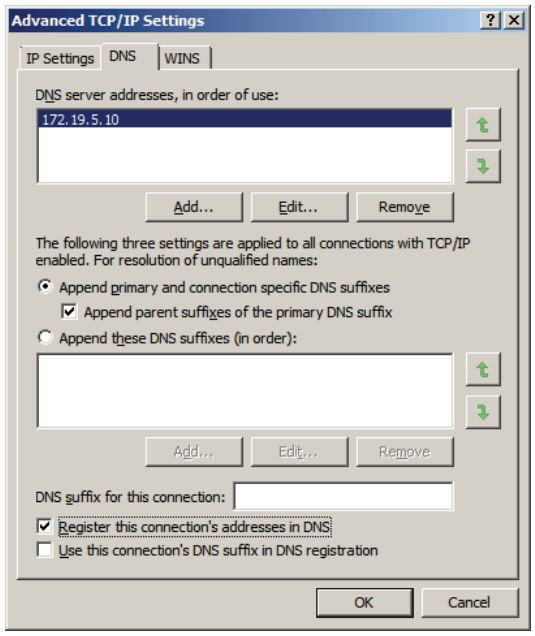


4. 「インターネット プロトコル バージョン 4 (TCP/IPv4)」を選択します。



   a. IP アドレスに、未使用の静的 IP アドレスを設定します。
   b. コンピュータの IP アドレスに、目的の DNS サーバーを設定します。

c. 「**詳細設定**」をクリックします。

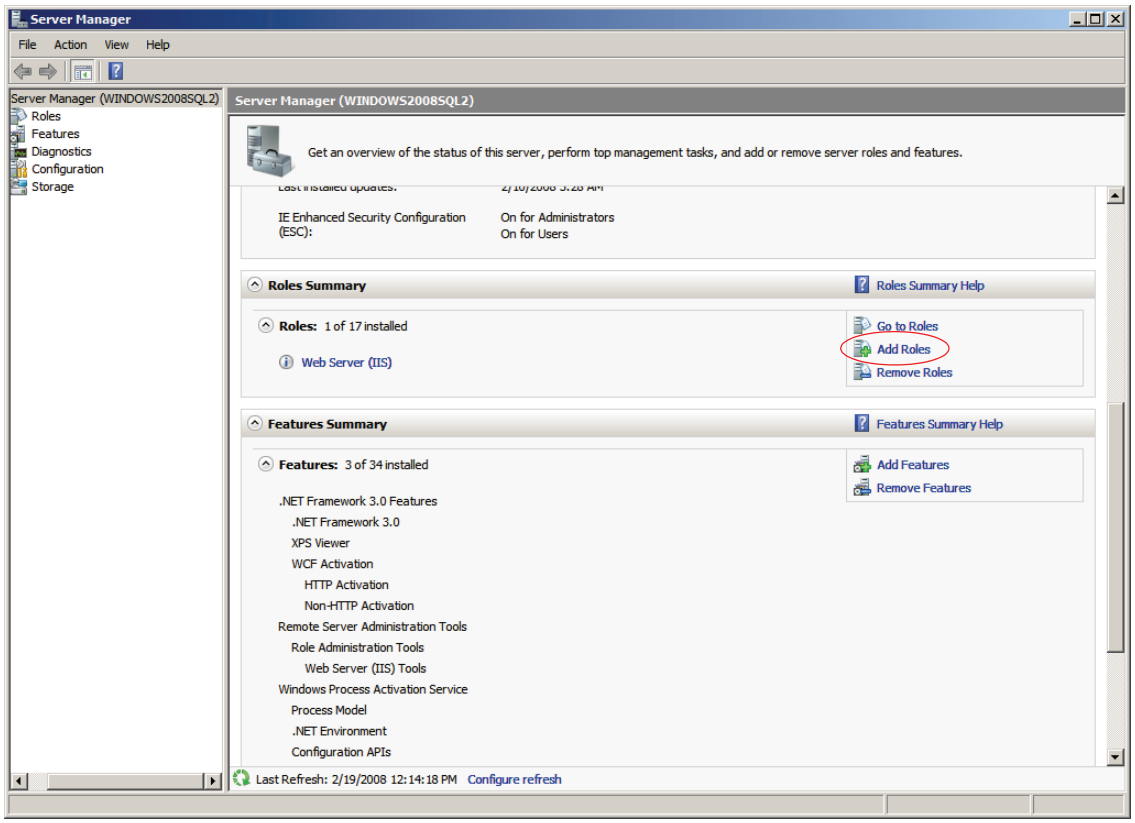


- 「**プライマリおよび接続専用の DNS サフィックスを追加する**」チェック・ボックスを選択します。
- 「**プライマリ DNS サフィックスの親サフィックスを追加する**」チェック・ボックスを選択します。

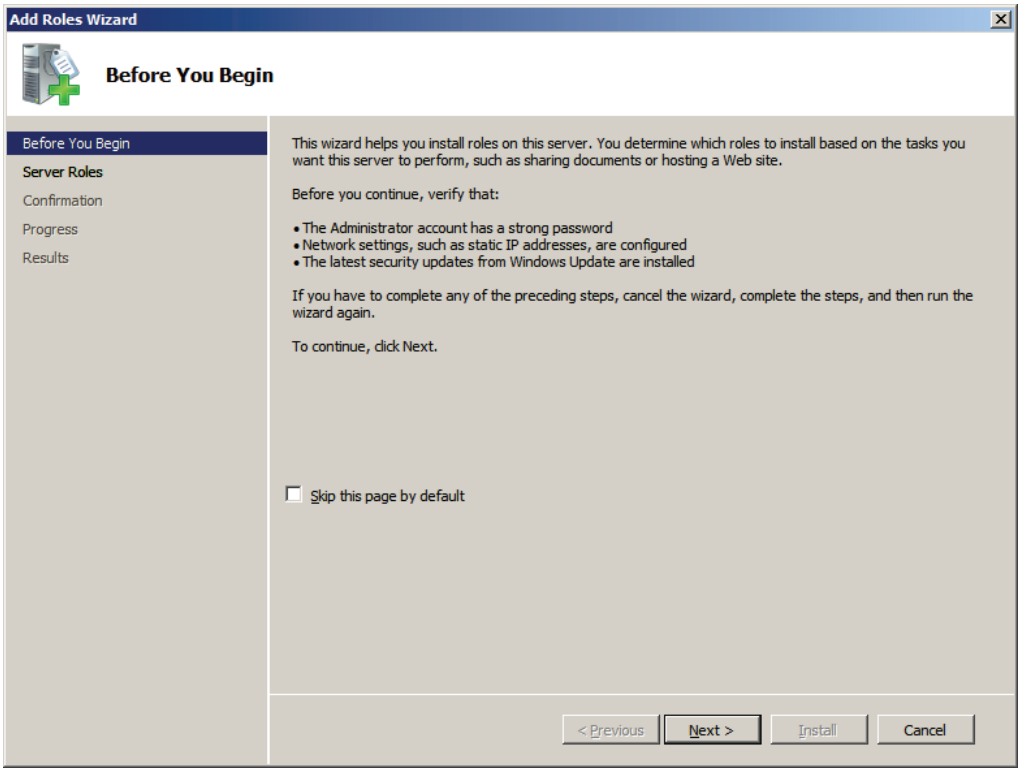
5. プロパティ・ペインが閉じられるまで「OK」をクリックし、最後に「**閉じる**」をクリックします。
6. コンピュータを再起動します。

Active Directory 2008 サービスのインストール

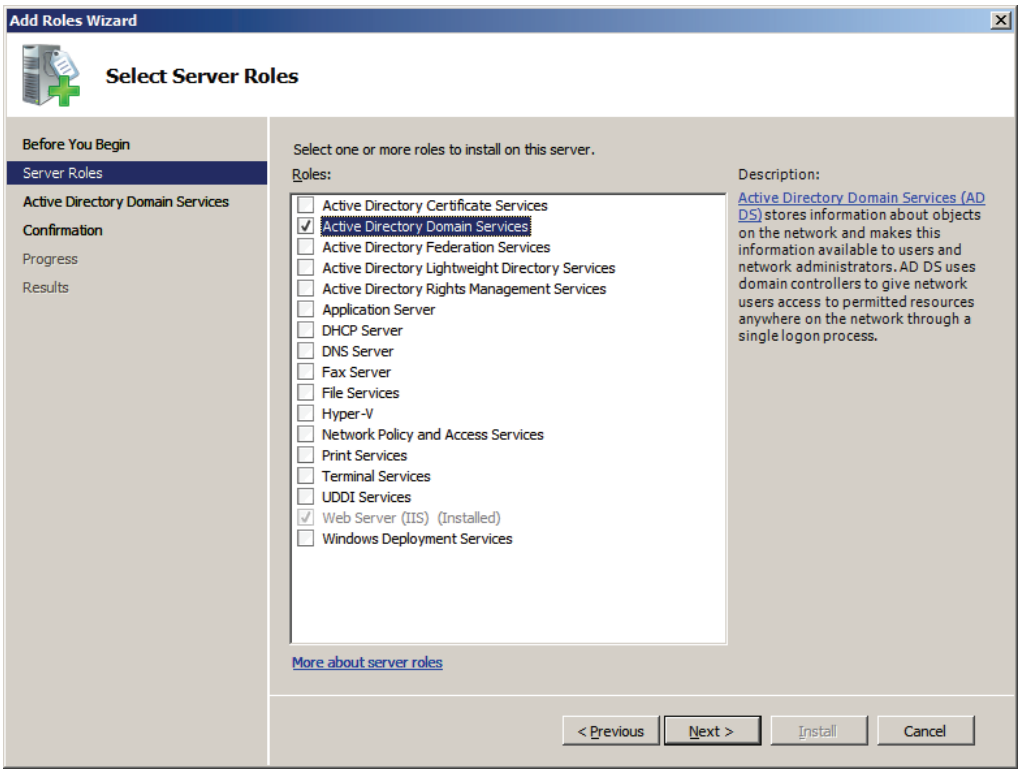
1. 「スタート」→「サーバー マネージャ」を選択します。
2. 「役割」セクションで、「**役割の追加**」をクリックします。



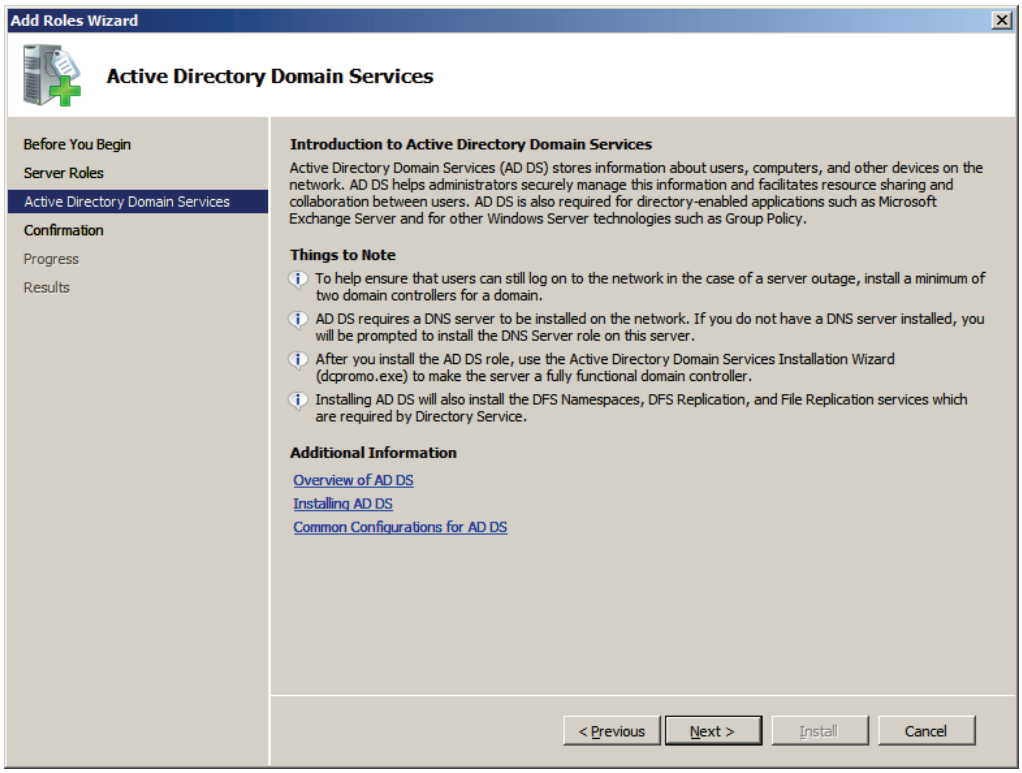
3. 「役割の追加ウィザード」で「**次へ**」をクリックします。



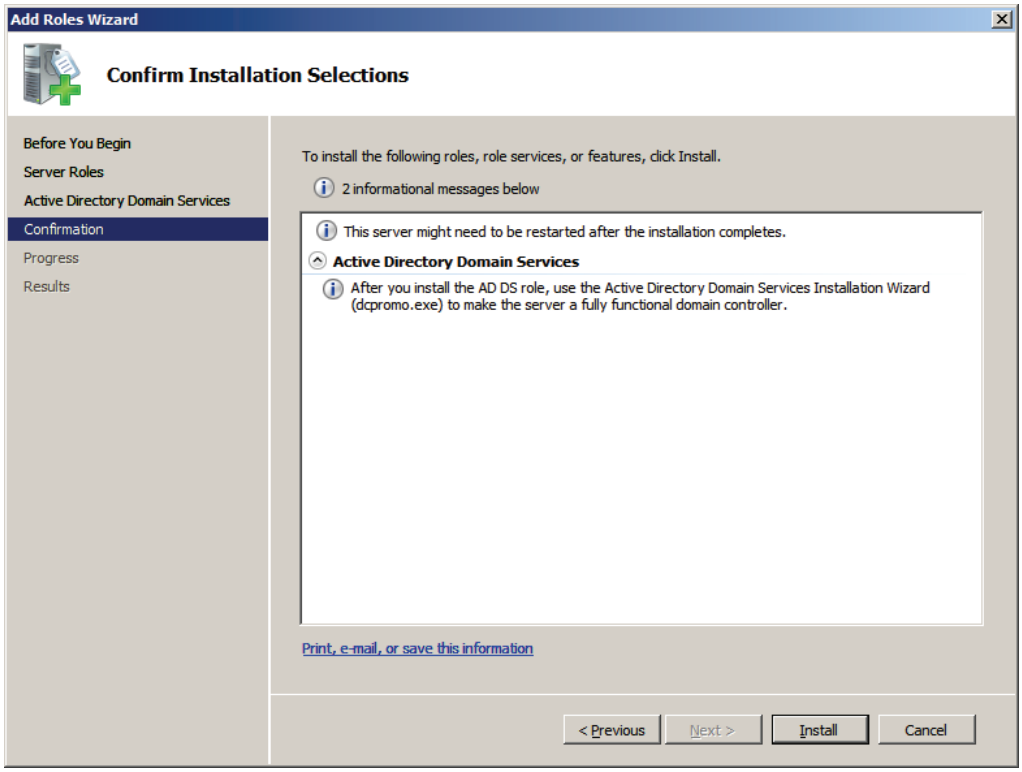
4. 「**Active Directory ドメイン サービス**」を選択し、「**次へ**」をクリックします。



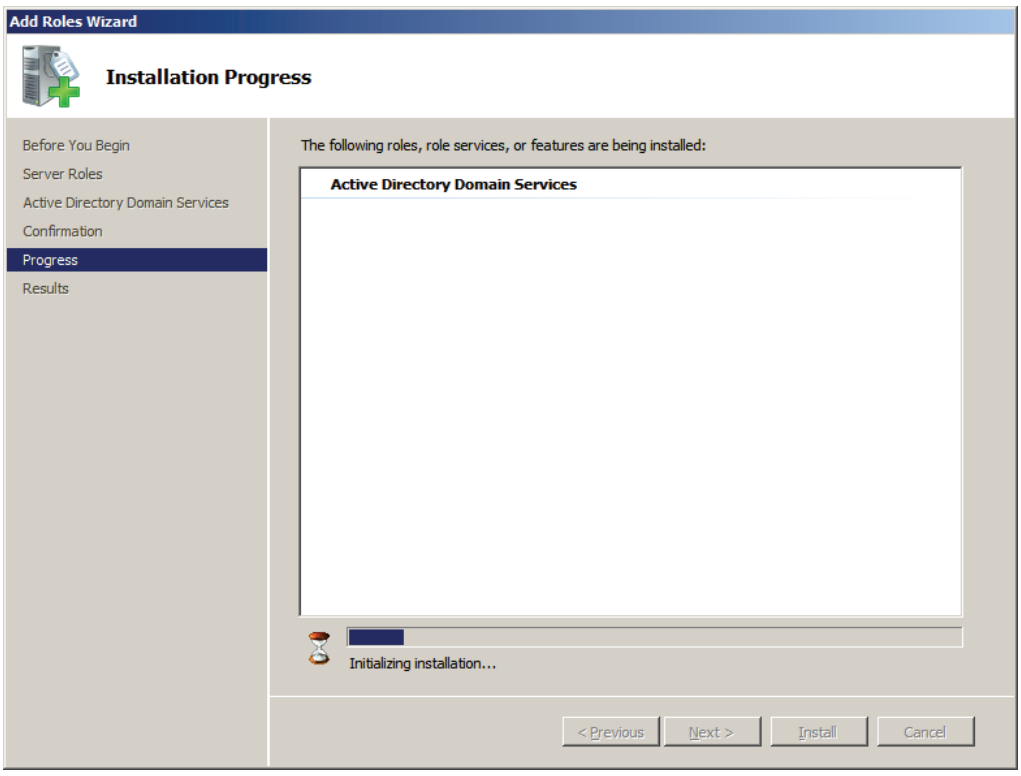
5. Active Directory とともにインストールされる追加サービスのリストを確認し、「次へ」をクリックします。



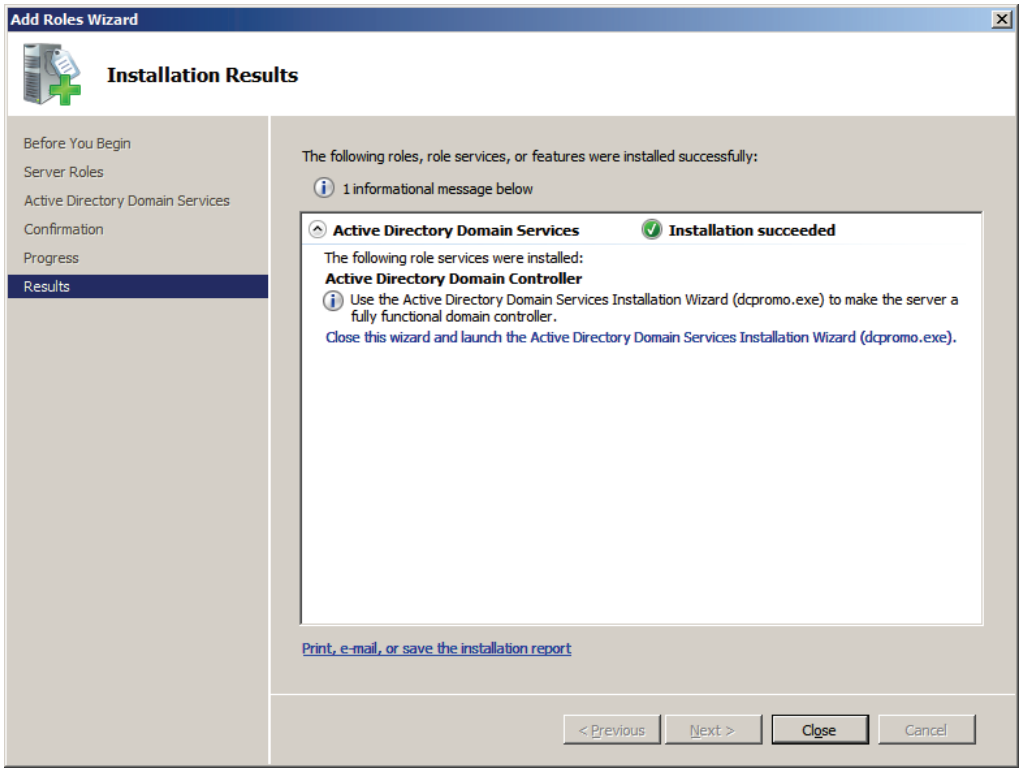
6. 「インストール」をクリックして、Active Directory 2008 のインストールを開始します。



7. インストールが完了するまで待ちます。



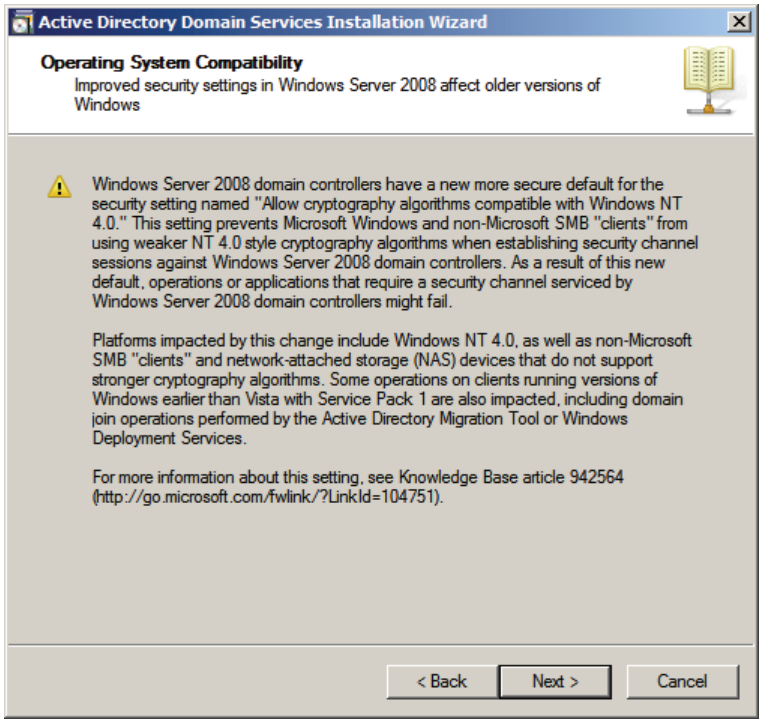
8. 「役割の追加ウィザード」ページの結果を確認します。**「このウィザードを終了し、Active Directory ドメイン サービス インストール ウィザード (dcpromo.exe) を起動します」**をクリックします。



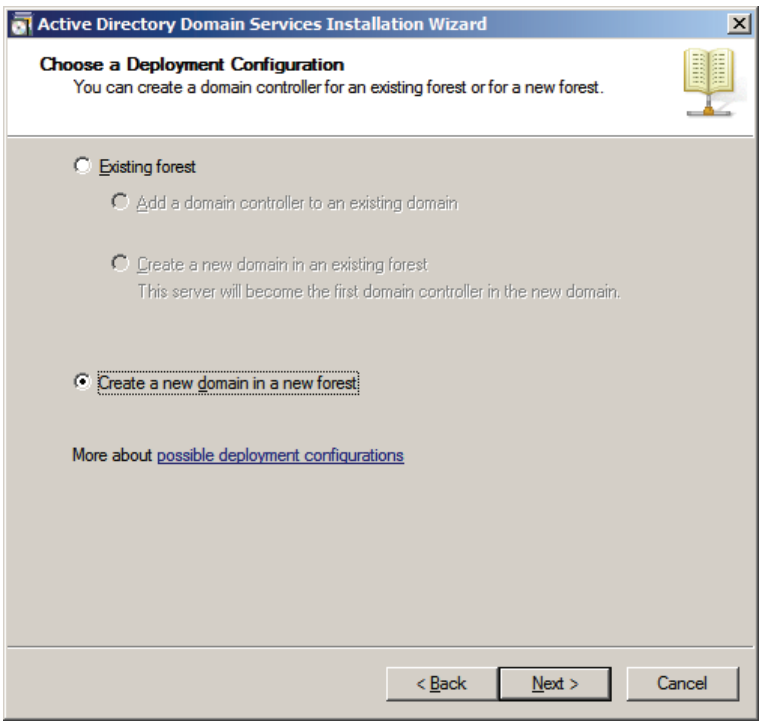
Active Directory 2008 インストール・ウィザードのインストール

1. 「ようこそ」画面で「**次へ**」をクリックします。

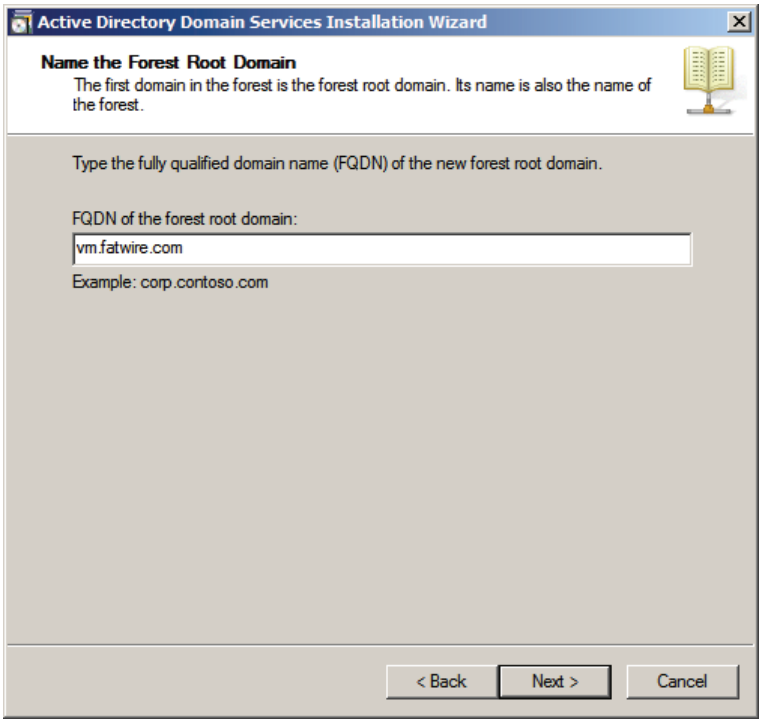
2. 「オペレーティング システムの互換性」画面で、「**次へ**」をクリックします。



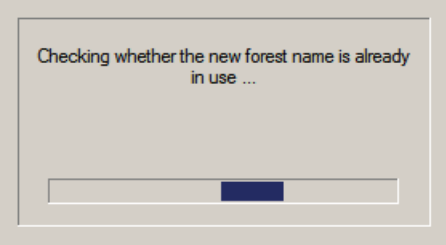
3. 「展開の構成の選択」画面で、**「フォレストに新しいドメインを作成する」**を選択し、**「次へ」**をクリックします。



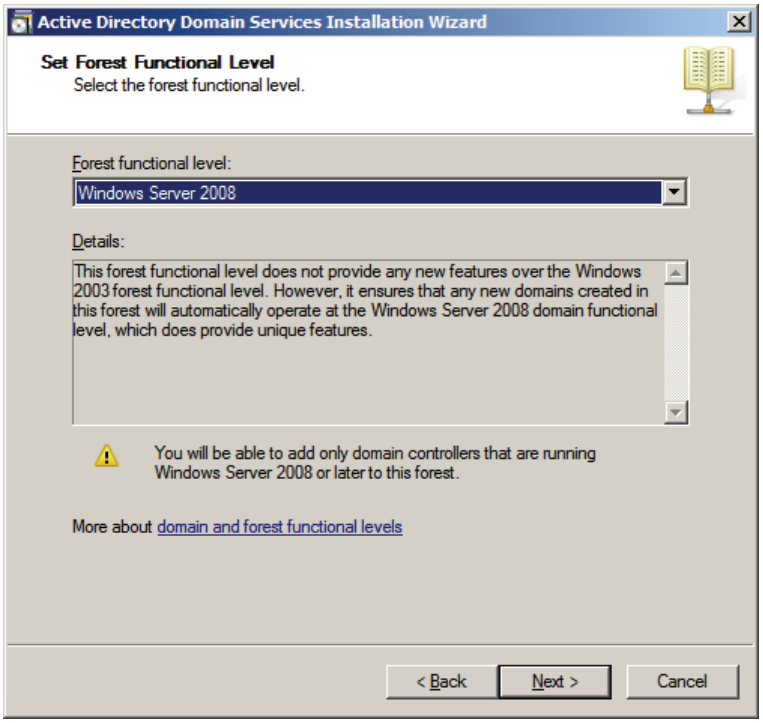
4. フォレスト ルート ドメインに名前を付けます。
   a. 新しいフォレストの名前を入力します。これは、先ほど作成した DNS ルート・ドメインです。**「次へ」**をクリックします。



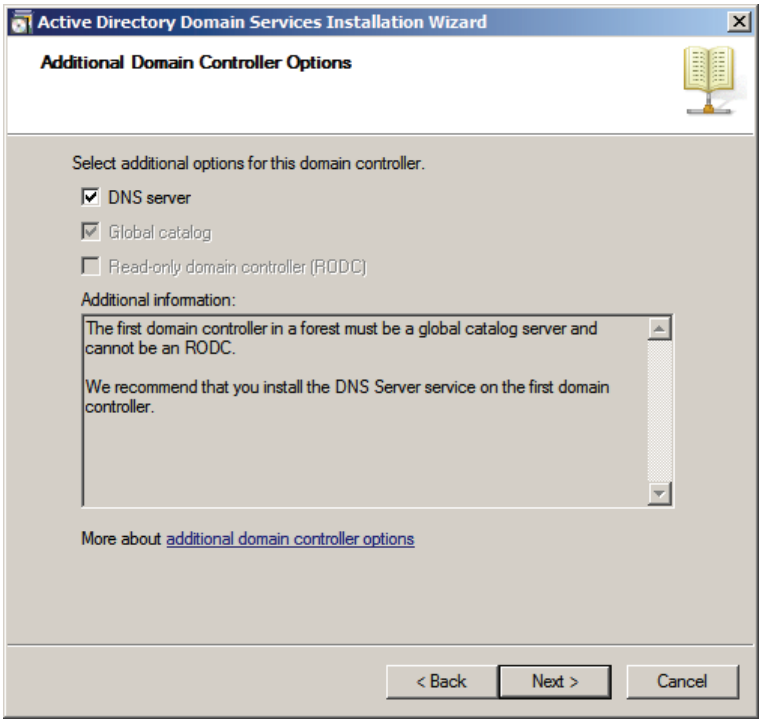
b. チェック・ダイアログが完了するまで待ちます。



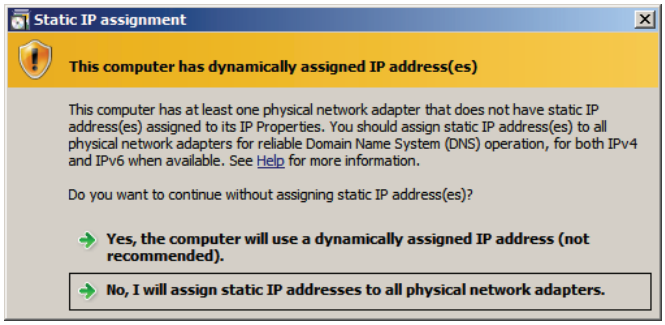
5. 「フォレストの機能レベルの設定」で、「**Windows Server 2008**」を選択し、「**次へ**」をクリックします。



6. 「追加のドメイン コントローラ オプション」画面で、「**DNS サーバー**」が選択されていることを確認し、「**次へ**」をクリックします。



DHCP ベースのアダプタを使用している場合、次のポップアップ・メッセージが表示されます。

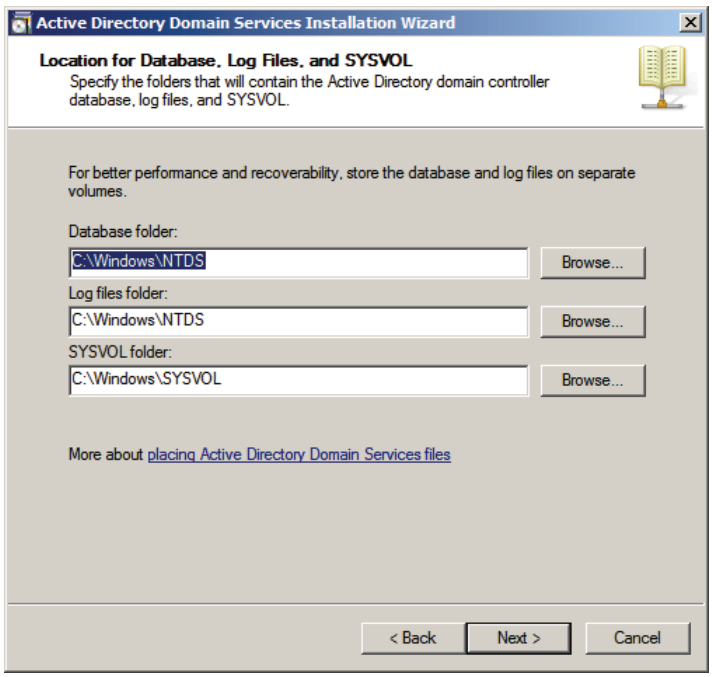


「**いいえ すべての物理ネットワーク アダプタに静的 IP アドレスを割り当てます**」を選択し、インストールを続行します。インストールの完了後、どの DHCP アダプタでも元に戻すことができます。

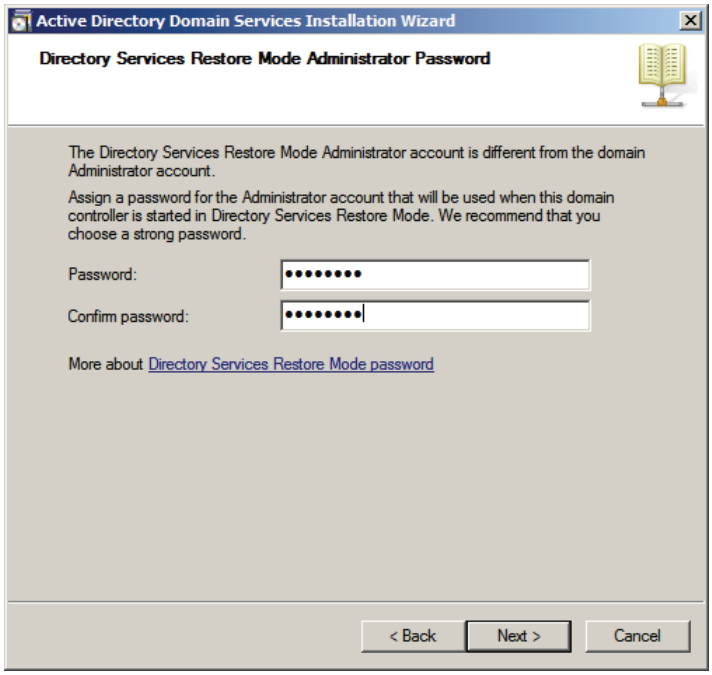
7. 作成している DNS ゾーンが権威のある親ゾーンを持たない場合、次のポップアップ・メッセージが表示される可能性があります。

「**はい**」を選択して、インストールを続行します。

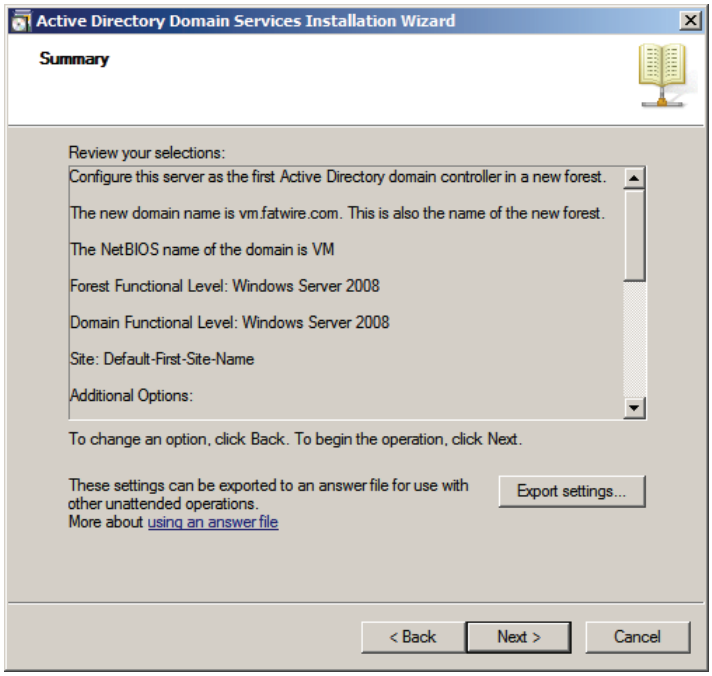
8. 「データベース、ログ ファイル、および SYSVOL の場所」画面の「**データベースのフォルダ**」フィールドでデフォルトを選択するか、システムで必要とされるフォルダに変更してから、「**次へ**」をクリックします。



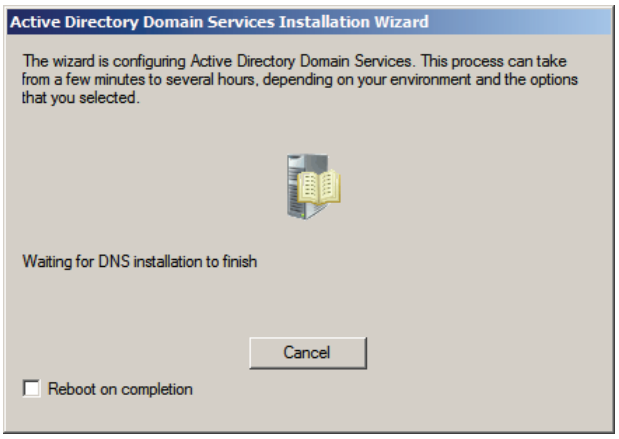
9. 「ディレクトリ サービス復元モード Administrator パスワード」画面にパスワードを入力し、これを記録します。



10. 「概要」画面で次の操作を行います。
    a. 設定を確認します。
    b. 設定をエクスポートします。
    c. 「次へ」をクリックします。



11. インストールが完了するまで待ちます。

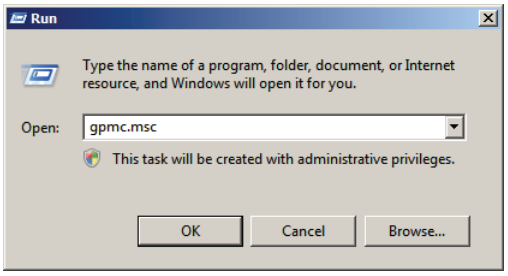


12.「Active Directory ドメイン サービス インストール ウィザード」で、「完了」をクリックし、インストールを終了します。

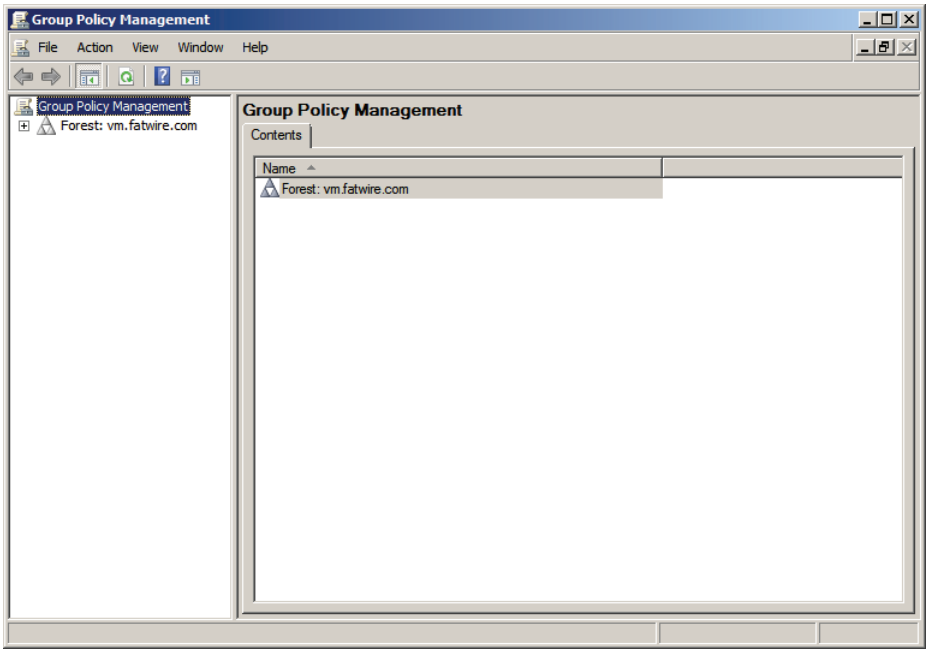
13. システムを再起動します。

グループ・ポリシーの確認

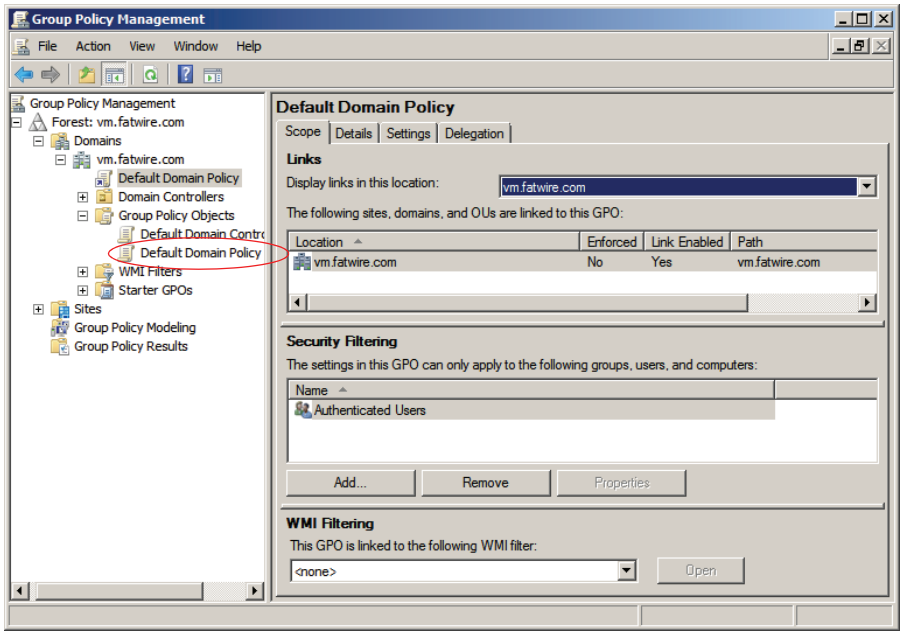
1. 「スタート」→「ファイル名を指定して実行」を選択します。
   a. 表示されたフィールドに、gpmc.msc と入力します。
   b. 「OK」をクリックします。



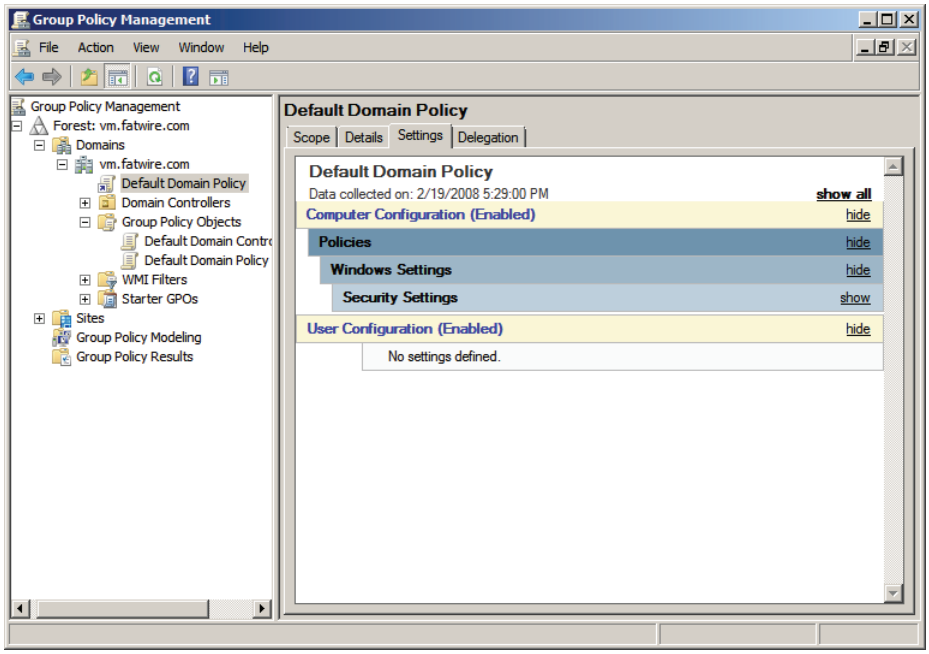
2. 「グループ ポリシーの管理」が開きます。



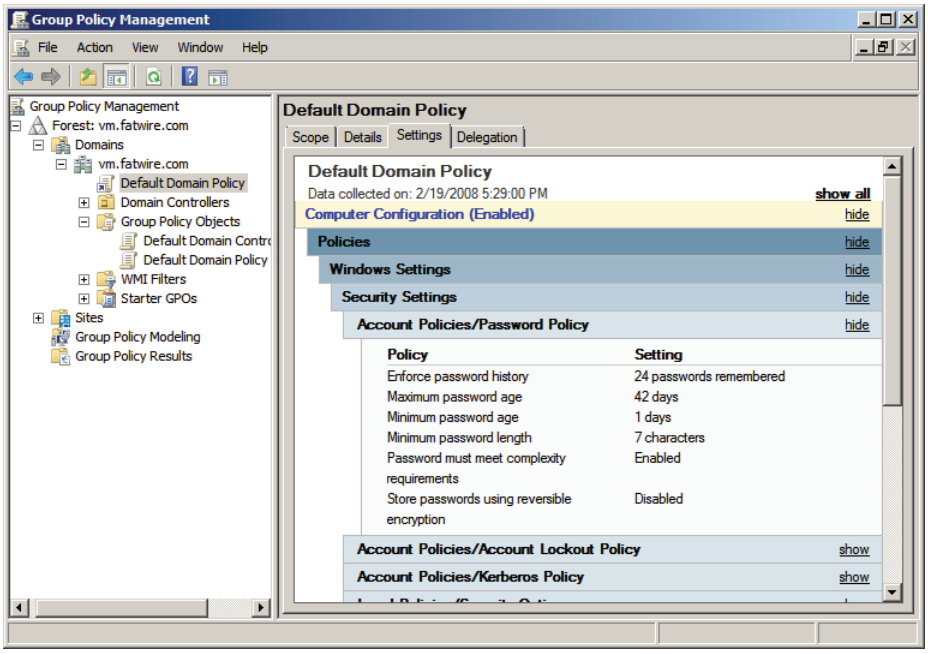
a. 「**ドメイン**」→ *ドメイン名*の順にツリーを展開し、「グループ ポリシーの管理」画面の左側パネルにある「**Default Domain Policy**」を選択します。



b. 「**設定**」タブを選択します。



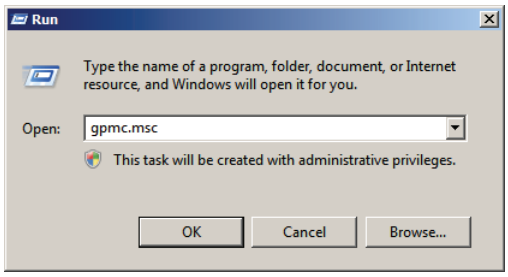
c. 「表示」をクリックして、「セキュリティ」→「アカウント ポリシー / パスワード ポリシー」セクションを展開します。



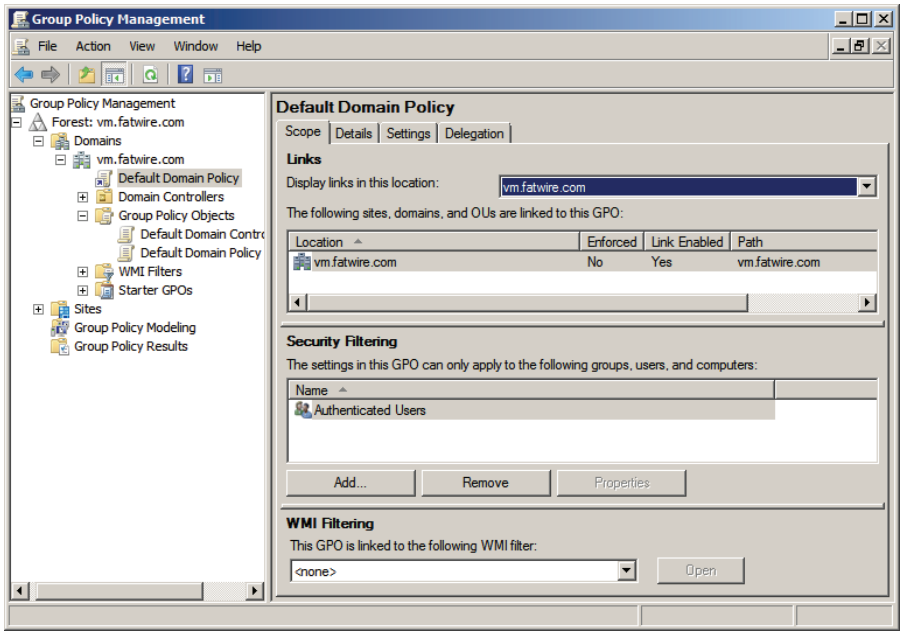
3. 「ポリシー」リストを確認します。オプション**「複雑さの要件を満たす必要があるパスワード」**はデフォルトで「有効」に設定されています。このオプションを**「無効」**に変更します (デフォルトの WebCenter Sites パスワードはこれらの要件を満たしません)。

グループ・ポリシーの変更

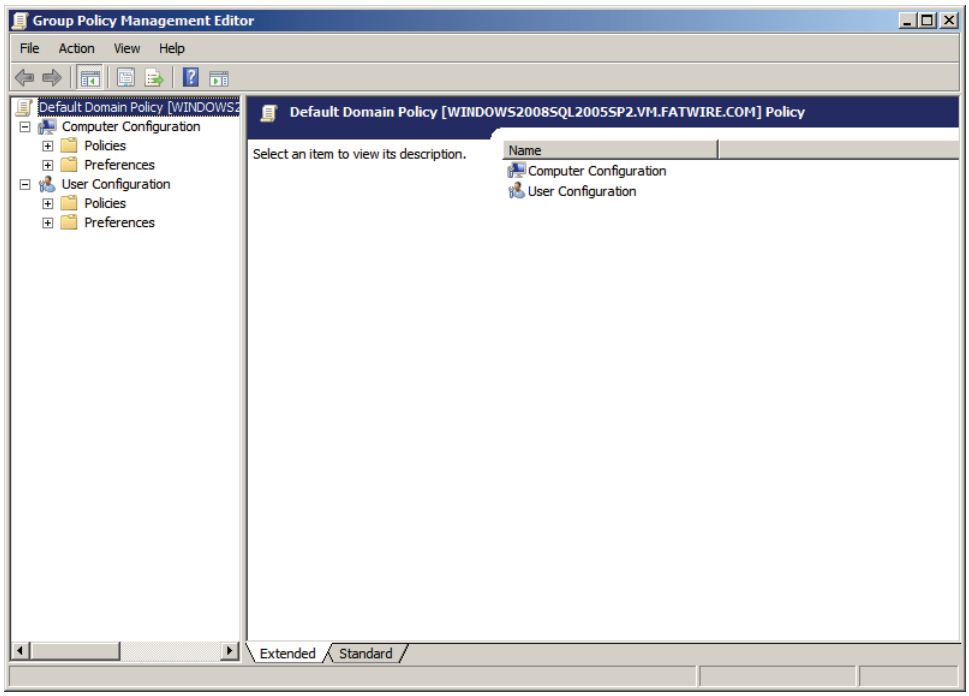
1. **「スタート」→「ファイル名を指定して実行」**を選択します。
   a. 表示されたフィールドに、`gpmc.msc` と入力します。
   b. **「OK」**をクリックします。



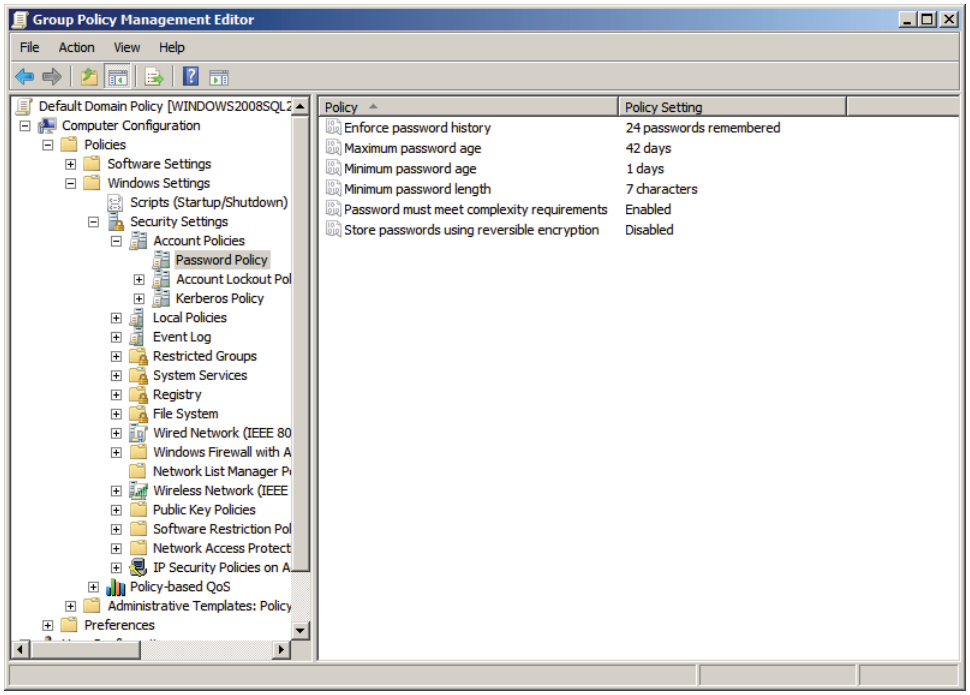
2. 「グループ ポリシーの管理」画面で、「**ドメイン**」→ *ドメイン名*の順にツリーを展開します。画面の右側にある「**Default Domain Policy**」を選択して、「**編集**」を選択します。



3. 「グループ ポリシー管理エディター」が開きます。

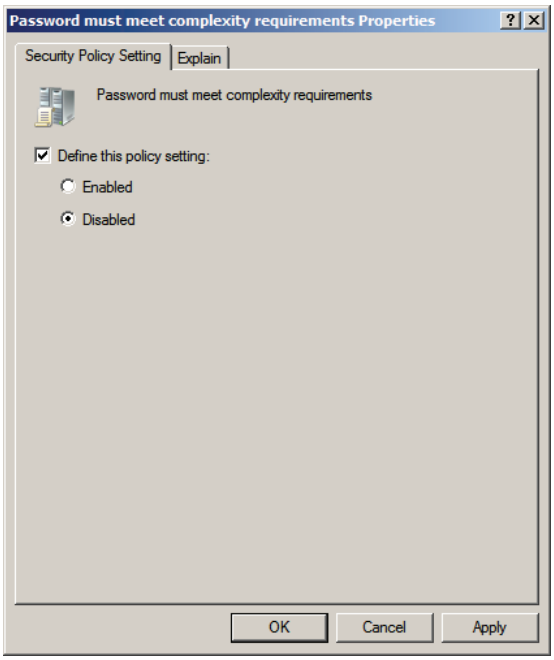


a. 左側のツリーで、「**コンピューターの構成**」→「**ポリシー**」→「**Windows の設定**」→「**セキュリティの設定**」→「**アカウントの設定**」→「**パスワードのポリシー**」の順に展開します。



b. 画面の右側にある「**複雑さの要件を満たす必要があるパスワード**」を右クリックし、「**プロパティ**」を選択します。

c. 「複雑さの要件を満たす必要があるパスワードのプロパティ」ダイアログ・ボックスで、「**無効**」ラジオ・ボタンを選択し、「**OK**」をクリックします。



d. 「グループ ポリシー管理エディター」および「グループ ポリシーの管理」ウィンドウを閉じます。

4. これにより、ドメインはパスワードの複雑さを確認しなくなります。WebCenter Sites のデフォルト・パスワードを使用できるようになりました。

   WebCenter Sites がインストールされているとき、「**有効**」をクリックしてステップ 2 をリバースすれば、セキュリティ設定を再び元に戻すことができます。

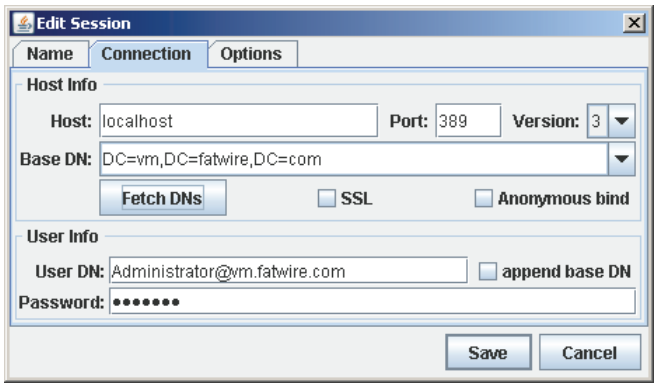
LDAP ブラウザを使用した ADS への接続

この項では、LDAP ブラウザを使用して Active Directory Server に接続する方法を示します。

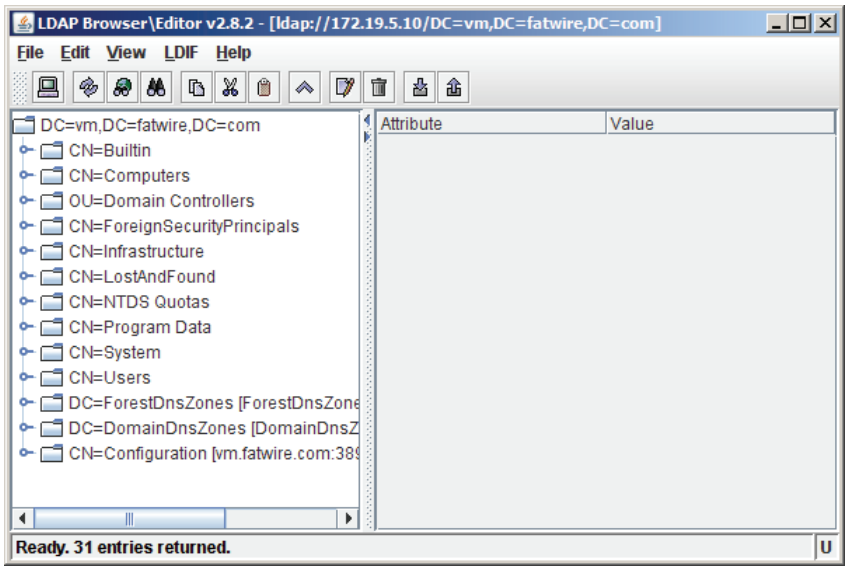
注意

LDAP ブラウザでは、グループの追加、パスワードの設定およびアカウントの有効化はできません。

1. LDAP ブラウザを開きます。
2. 「**Quick Connect**」タブを選択します。
3. 次の情報を入力します。
   - **Host:** `localhost` (リモートで接続している場合は、実際のホスト名を入力します)
   - **Base DN:** `<DNS_suffix>` (DNS 名のホスト名に続く部分)
   - **Anonymous bind:** 選択解除
   - **User DN:** `administrator@<DNS_suffix>`
   - **Append base DN:** 選択解除
   - **Password:** `<ADS_password>` (111 ページのステップ 9 で作成したパスワード)
4. 「**Connect**」をクリックします。



5. LDAP ツリーにデフォルト・ビューが表示されます。



第 9 章

IBM Tivoli Directory Server 6.x のセットアップ

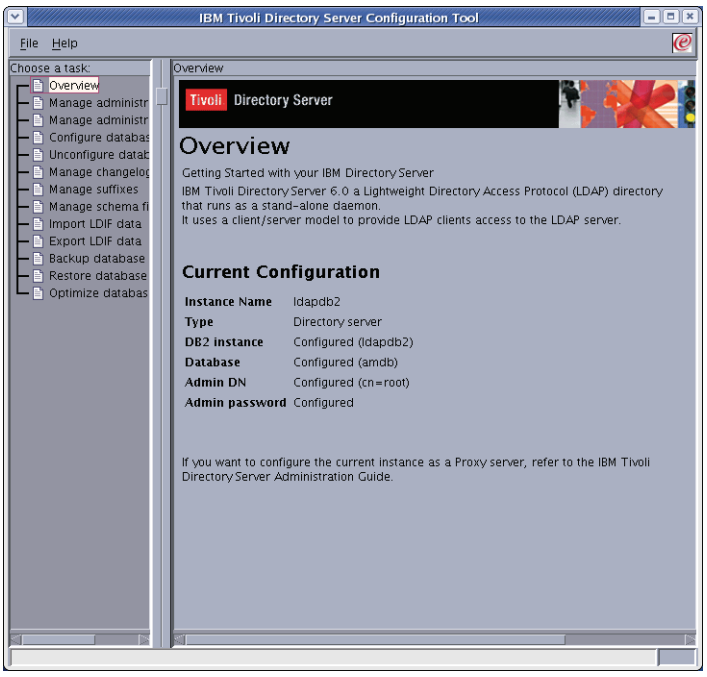
この章は、次の項で構成されています。

注意

このガイドでは、Tivoli Directory Server は「TDS」とも呼ばれます。

IBM Tivoli Directory Server のコマンド

表 4: IBM Tivoli Directory Server のコマンド

アクション	コマンド
インスタンスを開始	`<LDAP Install directory>/sbin/idsslapd -I <instance name>`
インスタンスを停止	`<LDAP Install directory>/bin/ibmdirctl stop -h localhost -D cn=root -w <password for cn=root>`
インスタンスをチェック	`<LDAP Install directory>/bin/ibmdirctl status -h localhost -D cn=root -w <password entered for cn=root>`
インスタンスのリストを表示	`<LDAP Install directory>/sbin/idsilist`
インスタンス管理ツールをロード	`<LDAP Install directory>/sbin/idsxinst`
インスタンスの構成ツールをロード	`<LDAP Install directory>/sbin/idsxcfg -I <name of instance>` 

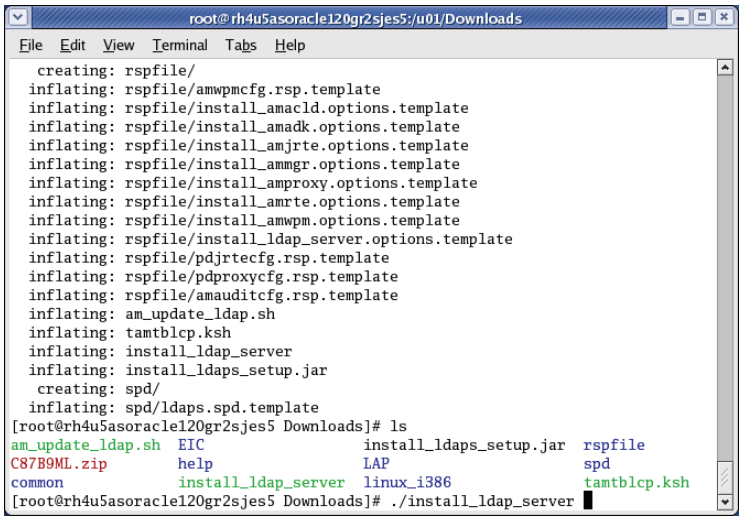
IBM Tivoli Directory Server をインストールする前に

1. グループ `idsldap` を作成します。
2. LDAP インスタンス用のユーザーを作成します。パスワード (例 : `ldapdb2`) はメモしておきます。このパスワードは、「IBM Tivoli Directory Server のインストール」の手順 7 で使用します。
3. **`pdksh`** がインストールされていることを確認します。

IBM Tivoli Directory Server のインストール

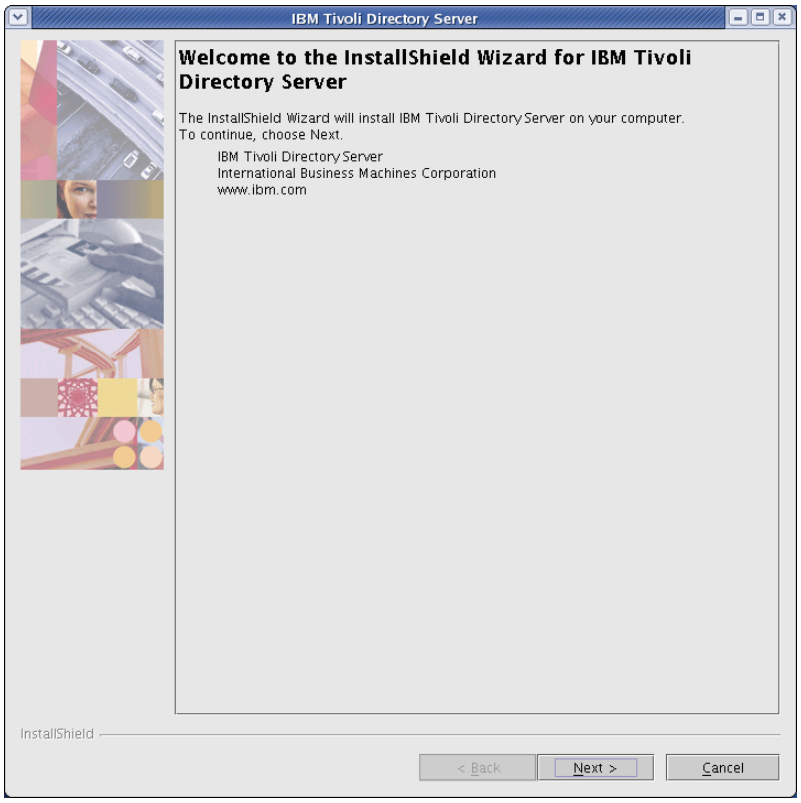
1. IBM から Tivoli Directory Server をダウンロードします。
2. アーカイブを一時ディレクトリで解凍します。
3. 一時ディレクトリに移動し、次のコマンドを実行します。

   `./install_ldap_server`.

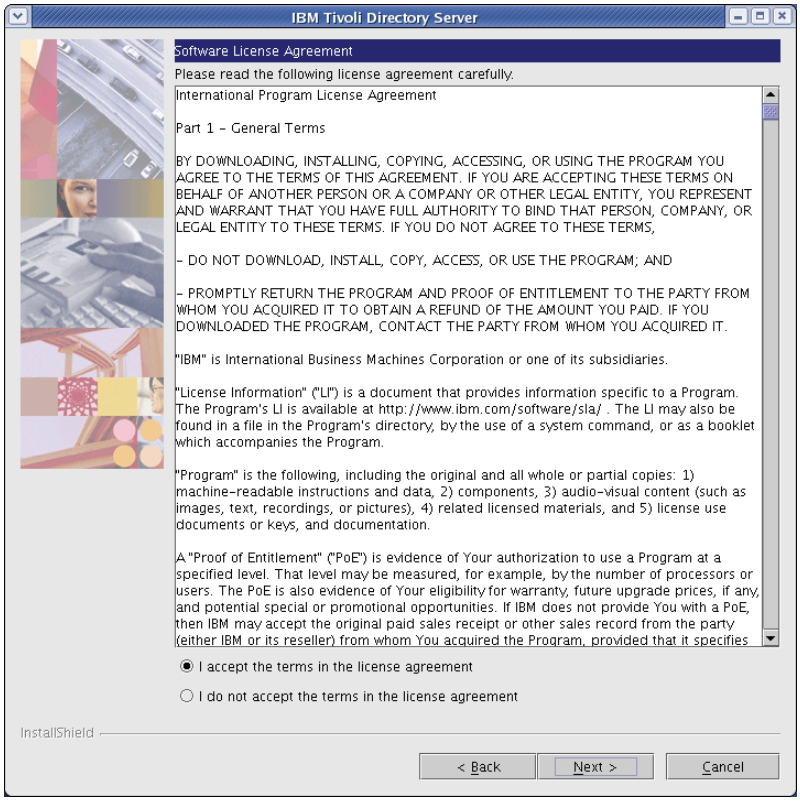


4. インストール・ダイアログ・ボックスが表示されたら、言語を選択し、「**OK**」をクリックします。

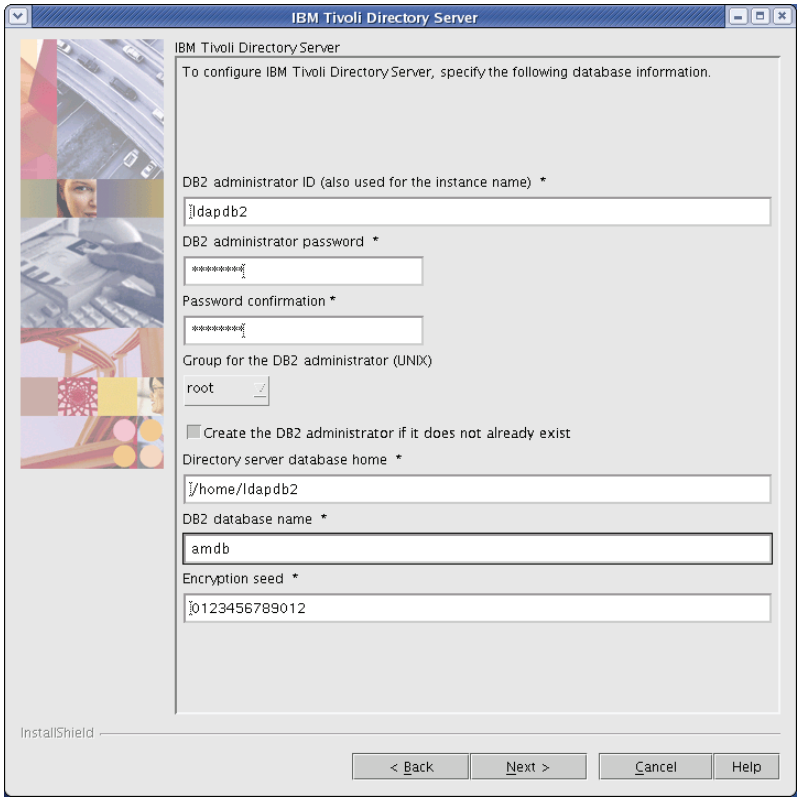
5. 「**Next**」をクリックします。



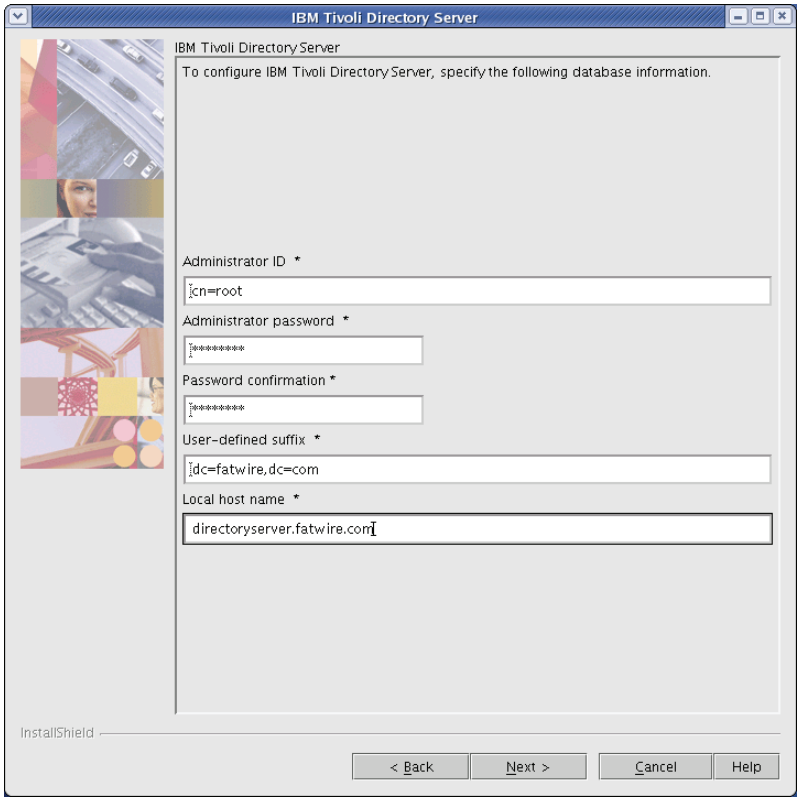
6. 「License Agreement」画面で、「**I Accept the terms in this license agreement**」を選択し、「**Next**」をクリックします。



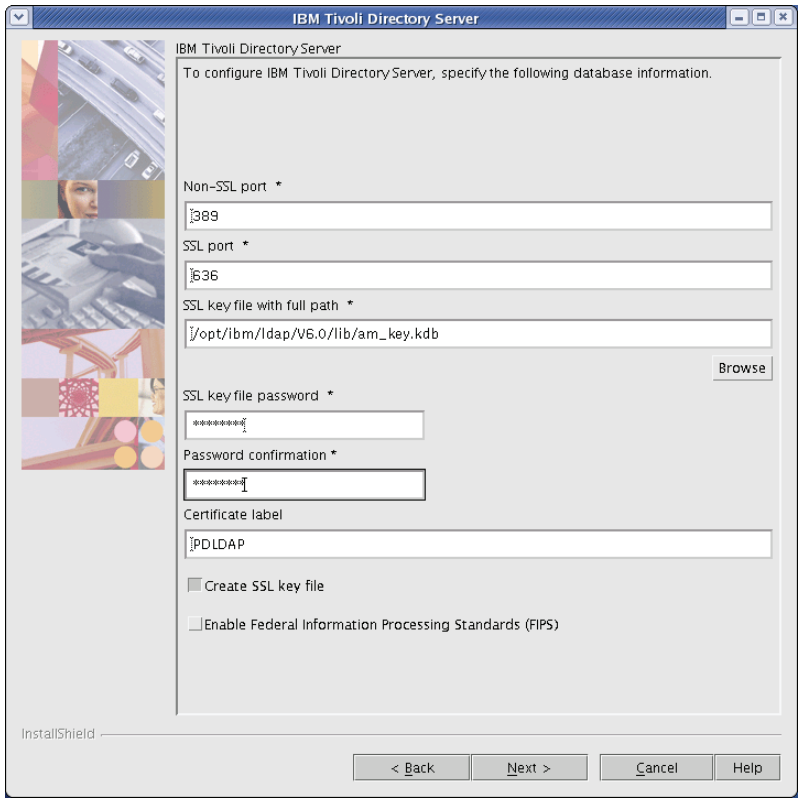
7. 1 つめの構成画面で、次のフィールドに値を入力します。
   - **DB2 administrator ID**: LDAP インスタンス用に作成したユーザーの名前。
   - **DB2 administrator password**: 「IBM Tivoli Directory Server をインストールする前に」の手順 2 で LDAP インスタンス・ユーザーに指定したパスワード (`ldapdb2`) を入力します。
   - その他のフィールドはデフォルト値のままにします。
   - 「**Next**」をクリックします。



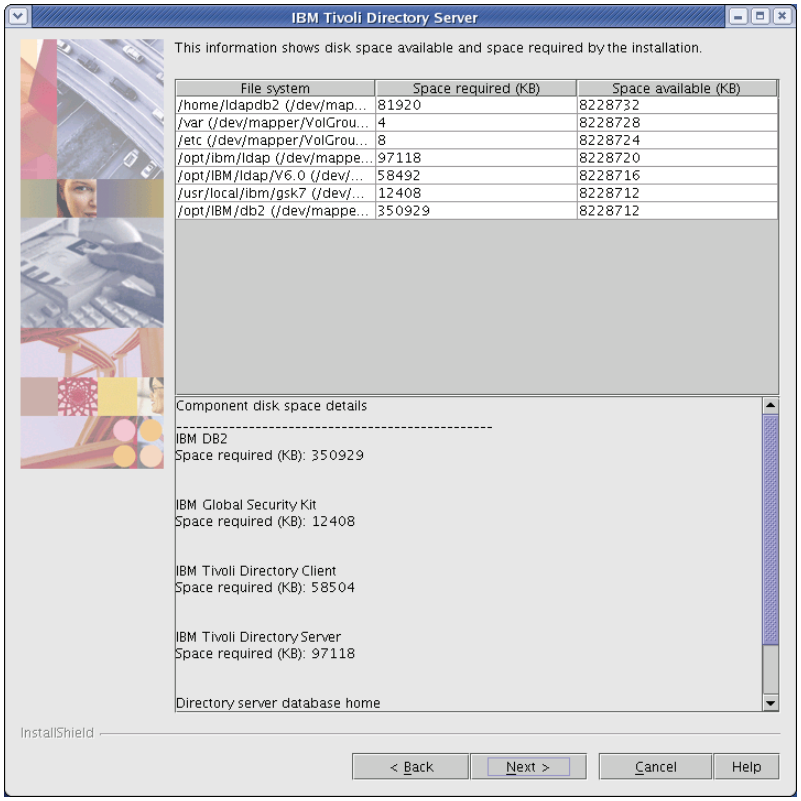
8. 2 つめの構成画面で、次のフィールドに値を入力します。
   a. **Administrator password**: パスワードを入力してメモします。このパスワードは構成中に繰り返し使用され、`sn=root` の形式で表示されます。
   b. **User-defined suffix**:
      `dc=<`**domain**`>,dc=<`**ext**`>`
      たとえば、ドメインが `fatwire.com` である場合、「User-defined suffix」は `dc=fatwire,dc=com` となります。
   c. 「**Local hostname**」が正しいことを確認します。
   d. 「**Next**」をクリックします。



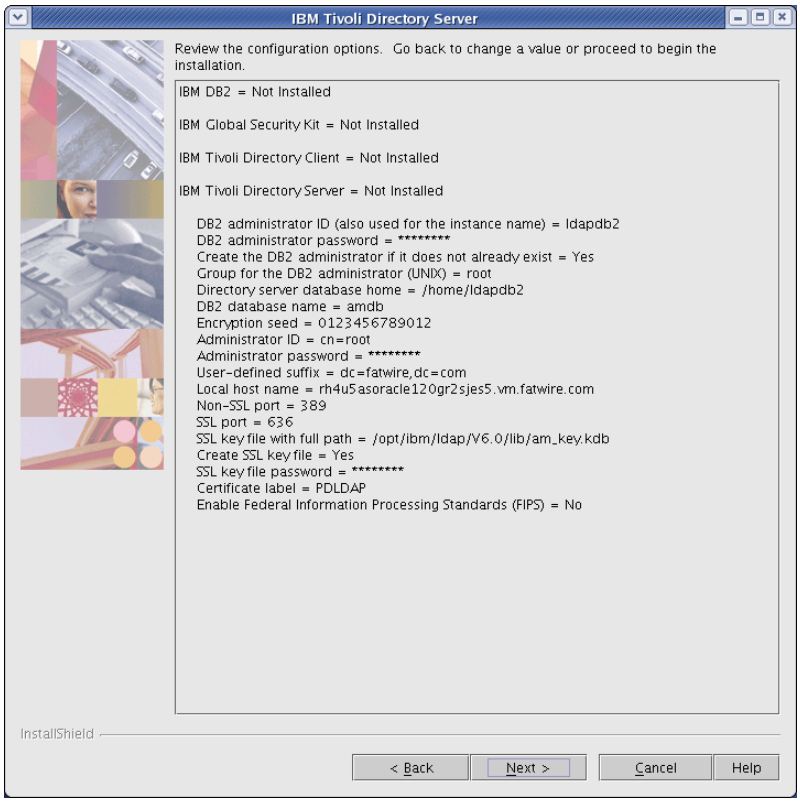
9. 3 つめの構成ページで、次の操作を行います。
   a. 次のフィールドに入力します。
      - **SSL key file password**: SSL のパスワードを入力します。
      - **Non-SSL port**: 「Non-SSL port」の値が 389 に設定されていることを確認します。非 SSL が変更されている場合は、WebCenter Sites をインストールするときに、この新しい値を使用します。
   b. 「**Next**」をクリックします。



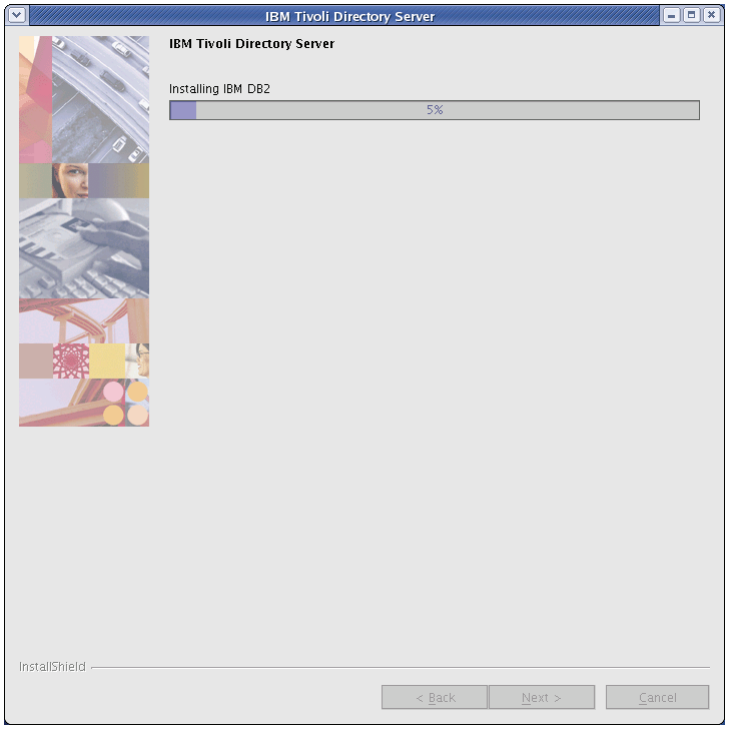
10. インストールを正常に行うために十分なディスク領域があることを確認し、「**Next**」をクリックします。



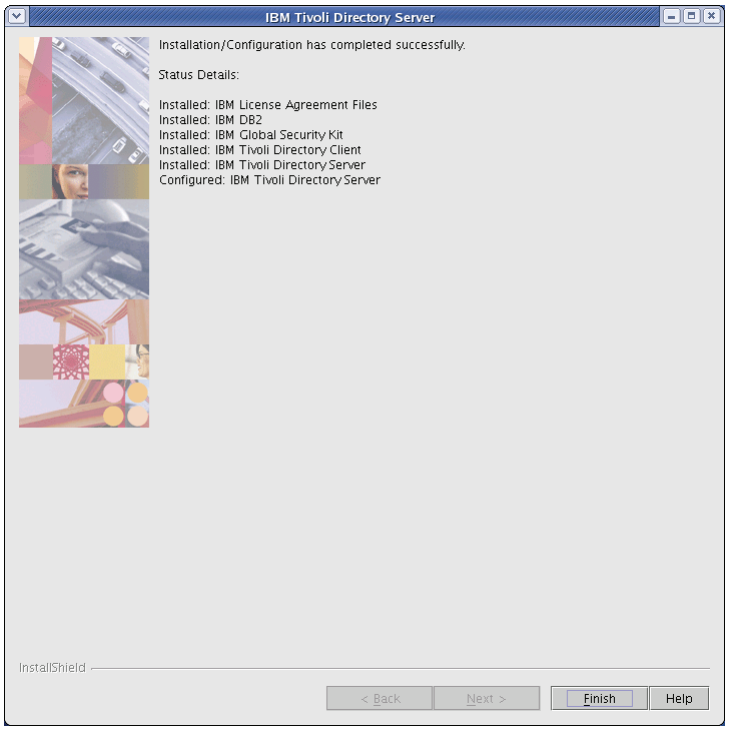
11. サマリーを確認し、「**Next**」をクリックします。



12. インストールが完了するまで待ちます。



13. 「**Finish**」をクリックします。これでインストールは完了です。



Tivoli Directory Server の構成

注意

WebCenter Sites では、sha 暗号化を使用している IBM TDS のみサポートされます。

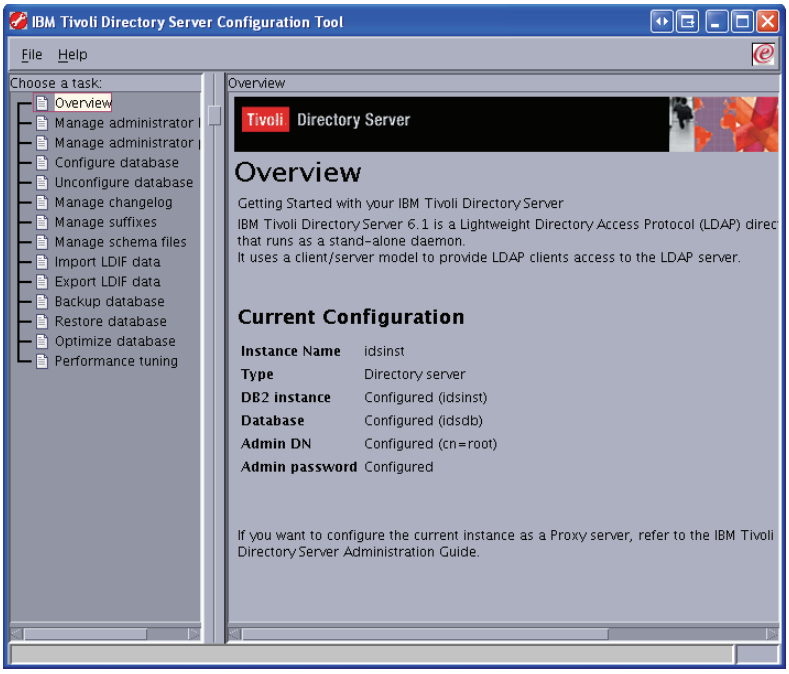
1. テキスト・エディタで、次のファイルを開きます。
   /home/<ldap user>/idsslapd-<ldap user>/etc/ibmslapd.conf.
2. ibm-slapdPwEncryption パラメータを見つけ、その値を sha に変更します。
3. テキスト・エディタで変更を保存します。

LDAP の構成の完了および検証

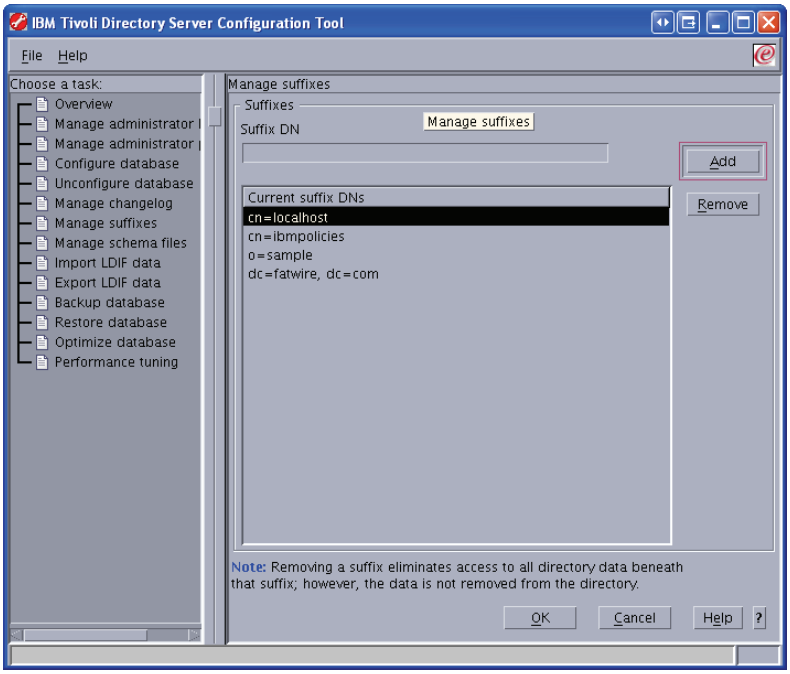
1. IBM TDS インスタンスを開始します。
   <**LDAP Install directory**>/sbin/idsslapd -I <**instance name**>

2. IBM TDS インスタンス構成ツールを開始します (構成プロセスを続行するには、ディスプレイを設定しておく必要があります)。

   <LDAP Install directory>/sbin/idsxcfg -I **<name of instance>**



3. 「**Manage suffixes**」を選択します。



4. インストール中に指定したユーザー定義接尾辞がリストに表示されていることを確認し、「**OK**」をクリックします。

LDIF ファイル (LDAP ブラウザ) のインポート

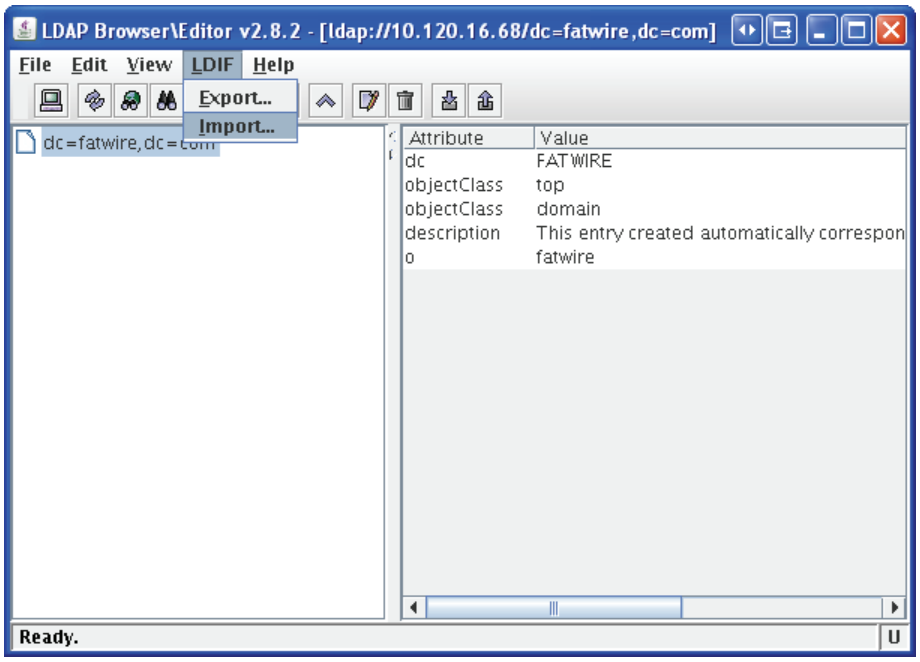
1. IDM TDS インスタンスを開始します。

   ```
   <LDAP Install directory>/sbin/idsslapd -I <instance name>
   ```

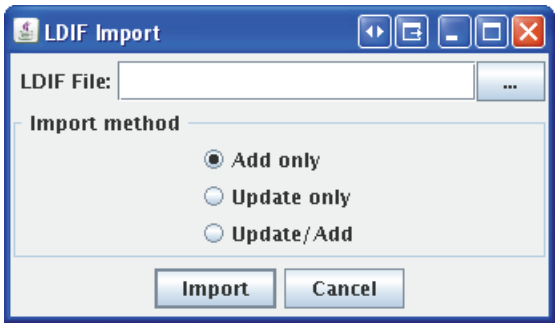
2. LDAP ブラウザを使用して IBM TDS に接続します。手順については、138 ページの「LDAP ブラウザを使用した IBM TDS へ接続」を確認してください。

3. dc=<**domain**>,dc=<**ext**> を選択します。

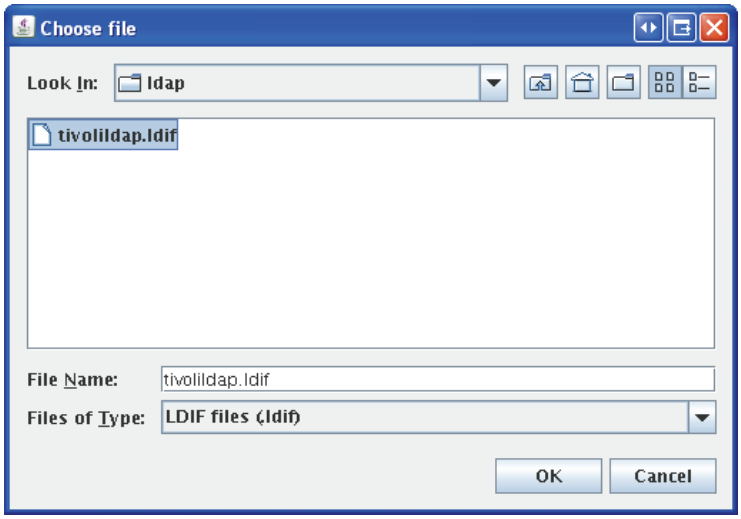
   a. 「**LDIF**」メニューをクリックし、「**Import**」を選択します。



4. 「**Add only**」ボタンをクリックします。



5. LDIF ファイル <cs_install_dir/ldap>/tivolildap.ldif を参照し、「**OK**」をクリックします。



6. 「**Import**」をクリックします。

> **注意**
>
> root エントリはすでに存在するため、インポートに失敗しますが、その他のエントリは正常にインポートされます。

7. 「**OK**」をクリックします。

LDIF ファイル (構成ツール) のインポート

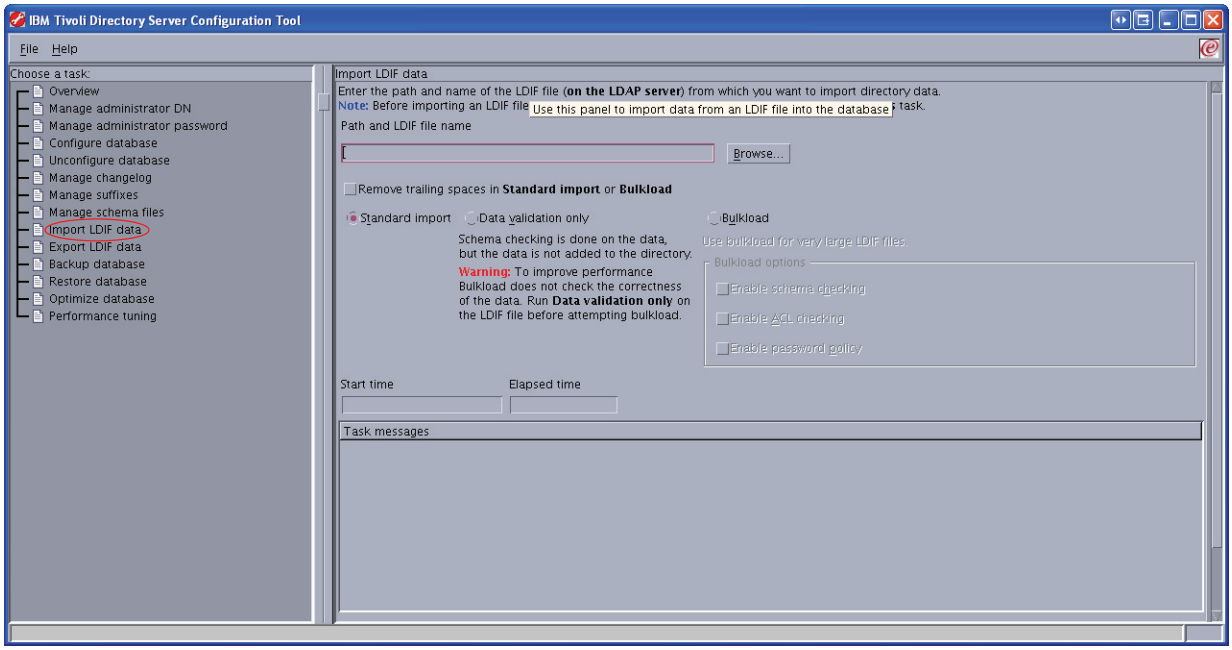
1. dos2unix ユーティリティを使用して、LDIF ファイルを UNIX 形式に変換します。
   - **Linux**:
     dos2unix <tivolildap.ldif>
   - **Solaris**:
     mv tivolildap.ldif > tivolildap2.ldif
     dos2unix tivoli.ldap2.ldif > tivolildap.ldif
2. IBM TDS インスタンスを停止します。

   <**LDAP Install directory**>/bin/ibmdirctl stop -h localhost -D cn=root -w <**password for cn=root**>

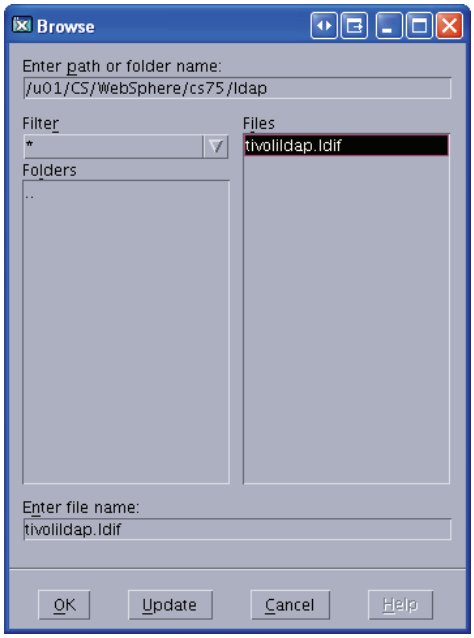
3. IBM TDS インスタンス構成ツールを開始します (インポート・プロセスを続行するには、ディスプレイを設定しておく必要があります)。

   <LDAP Install directory>/sbin/idsxcfg -I **<name of instance>**

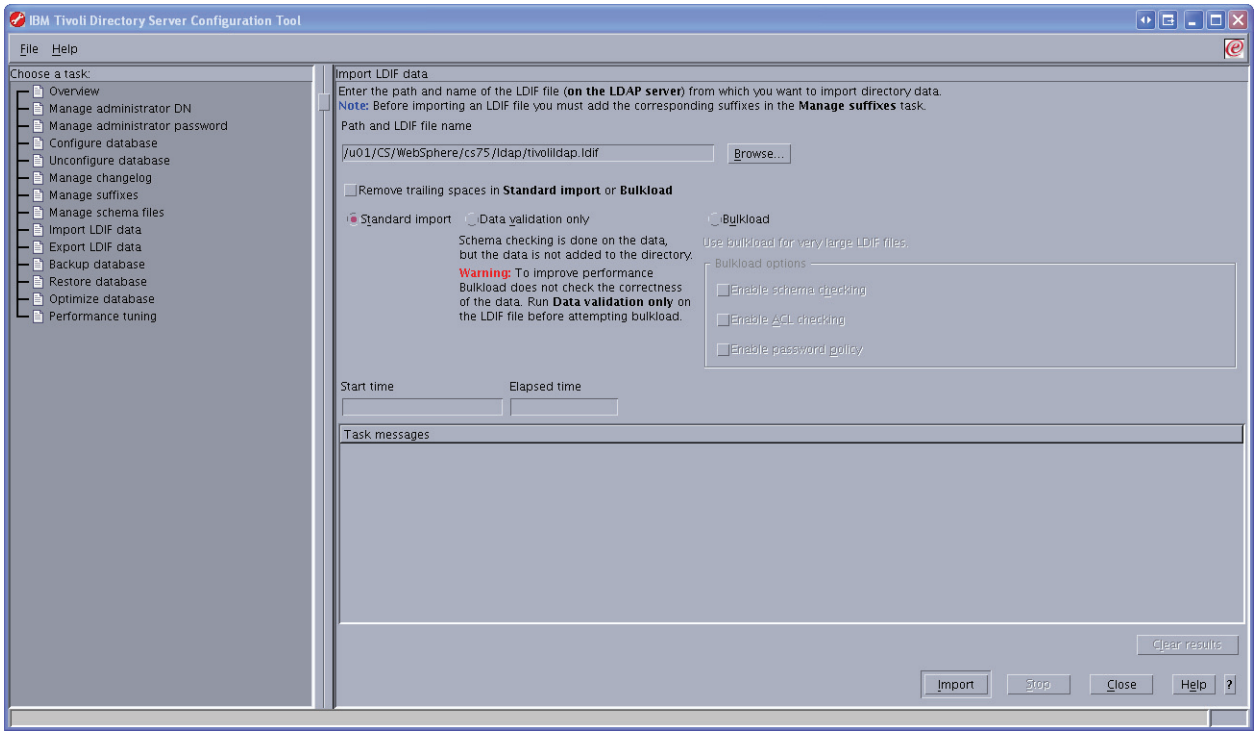
4. 「**Import LDIF data**」を選択します。



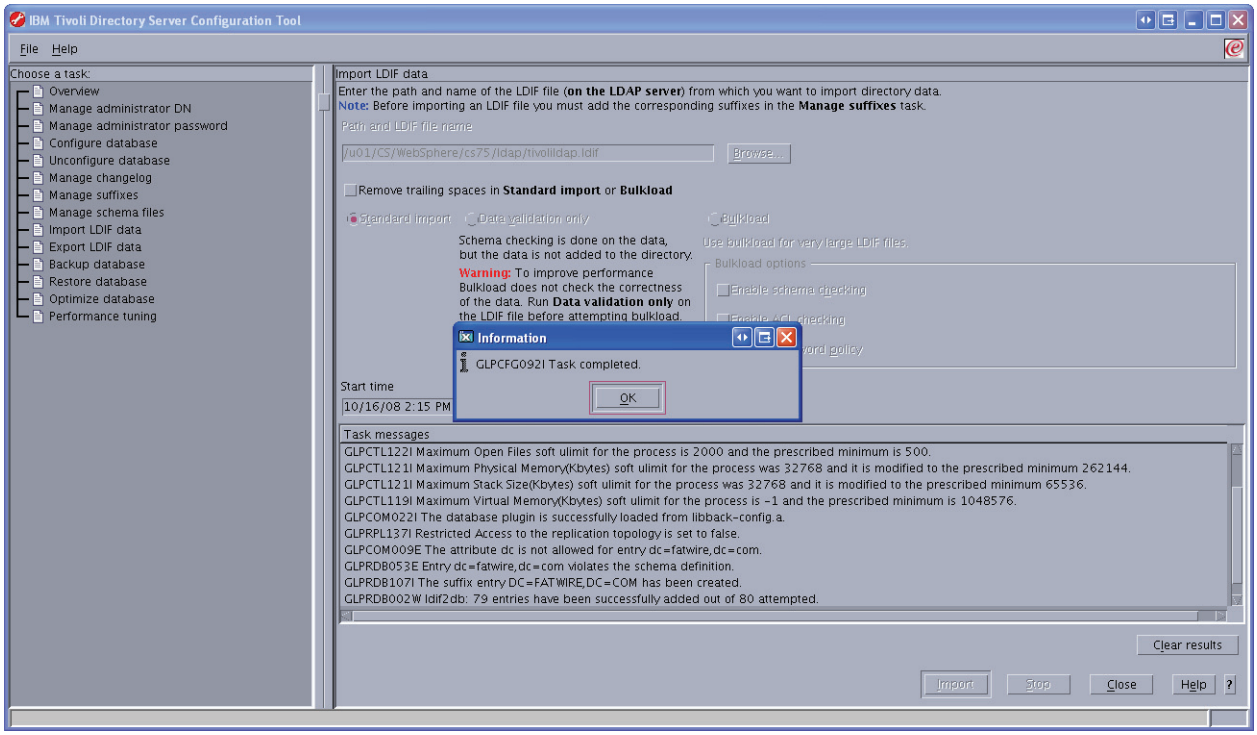
5. 「**Browse**」をクリックします。
6. インポートする LDIF ファイルを参照し、「**OK**」をクリックします。



7. 「**Import**」をクリックします。



8. インポートが完了したら、「**OK**」をクリックします。



LDIF ファイルを使用したユーザーおよび ACL の追加

1. 空の LDIF ファイルを作成します (例 : `addstuff.ldif`)。
2. 追加するユーザーそれぞれについて、LDIF ファイルに次の行を追加します。

   dn: uid=<**User_Name**>,cn=users,dc=<**domain**>,dc=<**ext**>

   userPassword: <**password**>

   uid:<**User_Name**>

   objectClass:top

   objectClass: person

   objectClass: organizationalPerson

   objectClass: inetOrgPerson

   sn:<**User_Name**>

   cn:<**User_Name**>
3. 追加する ACL それぞれについて、LDIF ファイルに次の行を追加します。

   dn: cn=<**ACL Name**>,cn=groups,dc=<**domain**>,dc=<**ext**>

   objectClass:top

   objectClass: groupOfNames

   member:uid=<**User_Name 1**>,cn=users,dc=<**domain**>,dc=<**ext**>

   member:uid=<**User_Name 2**>,cn=users,dc=<**domain**>,dc=<**ext**>

   .

   .

   .

   member: uid=<**User_Name** *n*>,cn=users,dc=<**domain**>,dc=<**ext**>
4. 133 ページの「LDIF ファイル (LDAP ブラウザ) のインポート」または 134 ページの「LDIF ファイル (構成ツール) のインポート」の手順に従って、LDIF ファイルをインポートします。

LDAP ブラウザを使用した IBM TDS へ接続

1. LDAP ブラウザをダウンロードしてインストールします。
2. LDAP ブラウザを起動します。

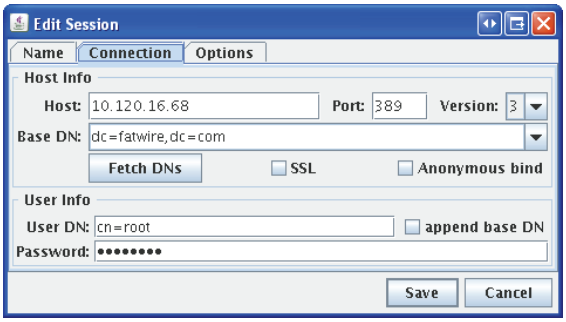
   ```
   ./lbe.sh
   ```

3. 必須フィールドに入力します。
   - **Host**: IBM TDS の IP またはホスト名を入力します。

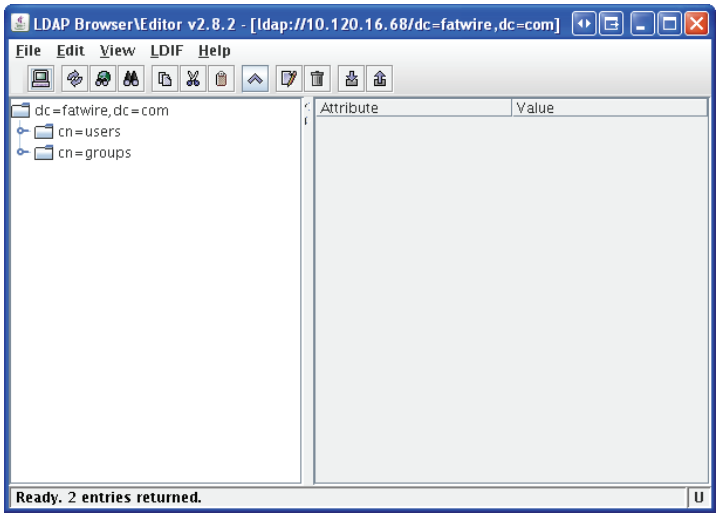
   注意

   IBM TDS が実行されるデフォルト・ポートは 389 です。

   - **Port**: IBM TDS が実行されるポートを入力します。
   - **Base DN**: IBM TDS のインストール中に入力した、ユーザー定義接尾辞を入力します (ユーザー定義接尾辞の詳細は、127 ページの手順 8 を参照)。
   - **Anonymous bind**: チェック・ボックスの選択を解除します。
   - **User DN**: `cn=root` と入力します。
   - **Password**: `cn=root` のパスワードを入力します。



4. 「**Save**」をクリックします。



第 10 章

OpenLDAP 2.3.*x* のセットアップ

この章では、WebCenter Sites で使用できるように OpenLDAP をセットアップする方法について説明します。

注意

OpenLDAP は、WebCenter Sites-LDAP インテグレータを実行する**前に**設定する必要があります。

この章は、次の項で構成されています。

OpenLDAP のコマンド

この項では、最も一般的に使用される OpenLDAP コマンドについて説明します。WebCenter Sites で使用できるように OpenLDAP をセットアップする際に参照してください。

OpenLDAP の開始

注意

この項では、`slapd` デーモンが `/usr/local/libexec` にあることを前提にしています。インストールによってはデーモンが別の場所にある可能性があります。このような場合は、この項に掲載されているコマンドで使用されているパスを正しいパスで置き換えてください。

- 通常どおりに OpenLDAP を開始するには、次のコマンドを使用します。

  ```
  /usr/local/libexec/slapd
  ```

- フル・デバッグを指定して OpenLDAP を開始するには、次のコマンドを使用します (フル・デバッグは、構成の問題の診断や WebCenter Sites のインストールに便利です)。

  ```
  /usr/local/libexec/slapd -h 'ldap:///' -d 0x5001
  ```

OpenLDAP サーバーの検索

OpenLDAP サーバーを検索するには、次の手順を実行します。

1. 次のコマンドを実行します。

   ```
   ldapsearch -x -D "cn=Manager,dc=<domain>,dc=<extension>" -W
      -b '' -s base '(objectClass=*)' namingContexts
   ```

   ここで、`<domain>` と `<extension>` は 144 ページの手順 a で指定した値です。

2. パスワードの入力を求められたら、145 ページの手順 d で指定したルート DN ユーザー・パスワードを入力します。

   通常、**ldapsearch** コマンドからは次のような応答が返されます。

   ```
   Enter LDAP Password:
   # extended LDIF
   #
   # LDAPv3
   # base <> with scope baseObject
   # filter: (objectClass=*)
   # requesting: namingContexts
   #


   #
   dn:
   ```

```
namingContexts: dc=fatwire,dc=com
# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

OpenLDAP サーバーへの LDIF ファイルの追加

整形式の LDIF ファイルを OpenLDAP サーバーに追加するには、**ldapadd** コマンドを使用します。

```
ldapadd -D 'cn=Manager,dc=<domain>,dc=<extension>'
   -w <root_dn_password> -f <LDIF_file_name>
```

ここで、

- <domain> と <extension> は、144 ページの手順 a で指定した値です。
- <root_dn_password> は、145 ページの手順 d で指定したルート DN ユーザーのパスワードです。
- <LDIF_file_name> は、追加する LDIF ファイルの名前です。

OpenLDAP のインストール

この項では、OpenLDAP のインストール方法について説明します。

注意

OpenLDAP は、ほとんどの Linux ディストリビューションにバンドルされています。システムに OpenLDAP がすでにインストールされている場合は、この項をスキップしてください。

OpenLDAP をインストールするには

1. 次の OpenLDAP Web サイトから、OpenLDAP `tgz` アーカイブをダウンロードします。

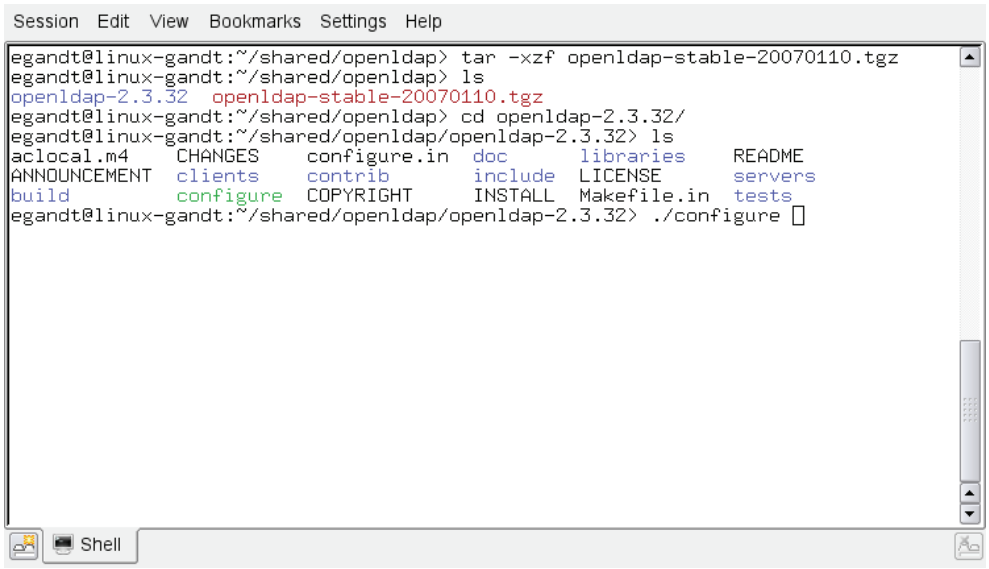
   `http://www.openldap.org/`

   例：`openldap-stable-20070110.tgz`

2. アーカイブを解凍します。
   - GNU を使用している場合は、次のコマンドを使用します。

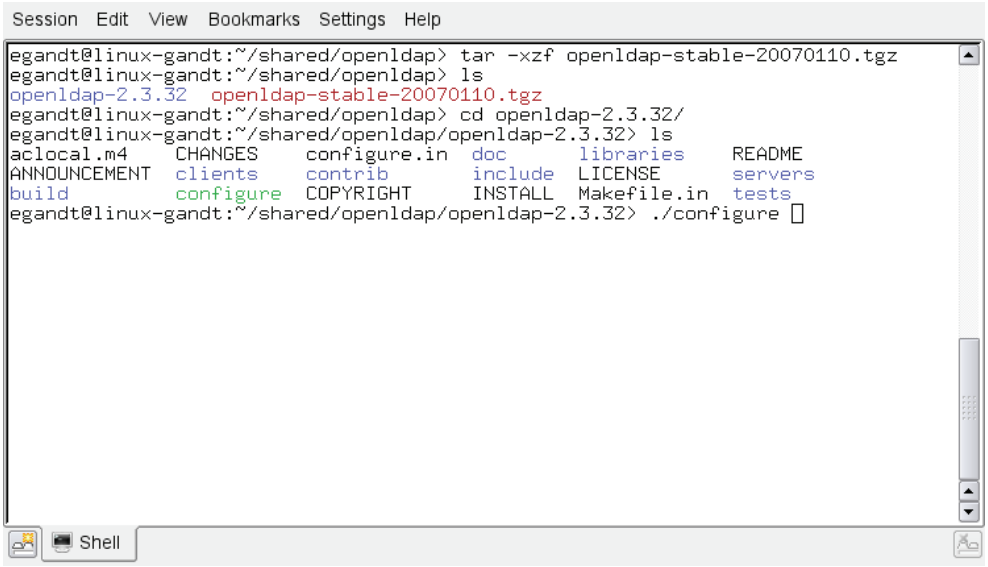
     `tar-xvzf openldap-stable-20070110.tgz`
   - GNU を使用していない場合は、次のコマンドを使用します。

     `gzip -d openldap-stable-20070110.tgz ; tar -xvf openldap-stable-20070110.tar`



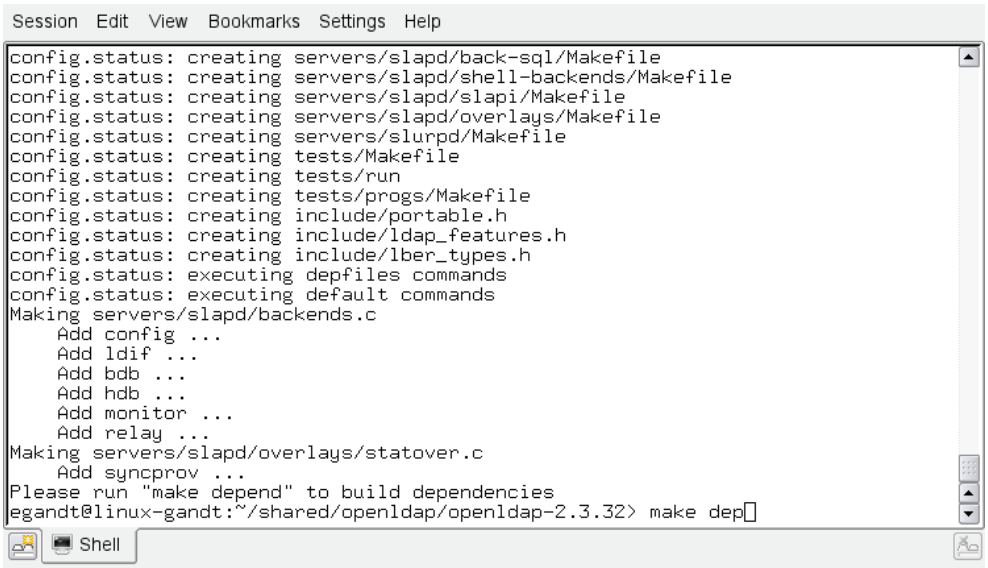
3. OpenLDAP ソースが入っているディレクトリに移動します。例:

```
cd openldap-2.3.32
```



4. 次のように OpenLDAP ソースを構成します。

```
./configure --enable-crypt --with-tls
```



提案されるオプションは次のとおりです。

- **`--enable-crypt`**: パスワードの暗号化を可能にします

- **`--with-tls`**: TLS/SSL サポートを可能にします

注意

システムにあわせて OpenLDAP をカスタマイズする場合、**`./configure --help`** を実行すると構成オプションの一覧が表示されます。

5. OpenLDAP 依存性をコンパイルします。**`make depend`**
6. OpenLDAP をコンパイルします。**`make`**
7. OpenLDAP をインストールします。**`make install`**

注意

デフォルトでは、OpenLDAP は `/usr/local` にインストールされます。

OpenLDAP の構成

この項では、OpenLDAP インストールの構成方法について説明します。

1. `ldap.conf` ファイルを次のように編集します。

注意

前項の手順に従って OpenLDAP を手動でインストールした場合、`ldap.conf` は `/usr/local/etc` にあります。

a. ベース DN を指定します。次の行を探します。存在しない場合は作成します。

```
BASE dc=<domain>,dc=<extension>
```

ここで、`<domain>` は LDAP サーバーのドメイン、`<extension>` はこのサーバーの TLD です。

OpenLDAP のベース DN の長さは、必ず dc 2 つ分になります。たとえば、フル・ドメインが `vm.fatwire.com` の場合、ベース DN は `fatwire.com` で、`BASE` 行は次のようになります。

```
BASE dc=fatwire,dc=com
```

b. URI を指定します。次の行を探します。存在しない場合は作成します。

```
URI ldap://<hostanme_or_IP> ldap://<hostanme_or_IP>
```

OpenLDAP が接続をリスニングしているホスト名または IP アドレス、あるいはその両方を入力します。複数のエントリを指定する場合はスペースで区切ります。次に例を示します。

```
URI ldap://127.0.0.1 ldap://localhost ldap://172.19.1.2
```

2. sldapd.conf ファイルを次のように編集します。

> **注意**
>
> 前項の手順に従って OpenLDAP を手動でインストールした場合、sldapd.conf は /usr/local/etc にあります。

a. 次のセクションを見つけます。

```
access to *
    by self write
    by users read
```

これを次で置き換えます。

```
access to *
    by dn="cn=Manager,dc=<domain>,dc=<extension>" write
    by self write
    by users read
    by anonymous auth
```

ここで、<domain> と <extension> は手順 1a で指定した値です。

b. 接尾辞を指定します。次の行を探します。存在しない場合は作成します。

```
suffix dc=<domain>,dc=<extension>
```

ここで、<domain> と <extension> は手順 1a で指定した値です。

c. ルート DN ユーザーを指定します。(ルート DN ユーザーは LDAP サーバーへのアクセスに使用されます。) 次の行を探します。存在しない場合は作成します。

```
rootdn cn=<user_name>,dc=<domain>,dc=<domain>
```

ユーザー名に Manager と入力し、<domain> および <extension> を手順 1a で指定した値に置き換えます。

d. ルート DN ユーザーのパスワードを指定します。次の行を探します。存在しない場合は作成します。

```
rootpw<password>
```

> **注意**
>
> パスワードは暗号化することも、暗号化しないこともできます。(暗号化されたパスワードは、{SSHA} で始まります)。暗号化されたパスワードを使用する場合は、次の操作を行います。
>
> 1. **slappasswd** コマンドを使用して、暗号化されたパスワード (ハッシュ) を生成します。このコマンドは、暗号化された有効なパスワード (ハッシュ) を生成し、端末に表示します。
> 2. 次の手順 e を実行します。

e. (オプション) 直前の手順で、暗号化されたパスワードの使用を選択した場合は、パスワードのタイプを SHA に設定します。次の行を探します。存在しない場合は作成します。

```
password-hash {SSHA}
```

これにより、パスワードのタイプが SHA (デフォルト) に設定されます。パスワードにはその他のタイプも設定できます。詳細は、OpenLDAP のドキュメントを参照してください。

3. `core.schema` ファイルを次のように編集します。

注意

前項の手順に従って OpenLDAP を手動でインストールした場合、`core.schema` は `/usr/local/etc/schema` にあります。

a. 次のセクションを見つけます。

```
objectclass ( 2.5.6.17 NAME 'groupOfUniqueNames'
   DESC 'RFC2256:a group of unique names (DN and Unique
      Identifier)'
   SUP top STRUCTURAL
   MAY ( businessCategory $ seeAlso $ owner $ ou $ o
      $ description $ uniqueMember)
   MUST ( uniqueMember $ cn ))
```

b. 各行の先頭に # 文字を入力して、セクションをコメント化します。その後ろに、次の修正したセクションを挿入します。

```
objectclass ( 2.5.6.17 NAME 'groupOfUniqueNames'
   DESC 'RFC2256:a group of unique names (DN and Unique
      Identifier)'
   SUP top STRUCTURAL
   MAY ( businessCategory $ seeAlso $ owner $ ou $ o
      $ description $ uniqueMember)
   MUST ( cn ))
```

元のセクションと修正後のセクションは最後の行が違います。

`MUST ( uniqueMember $ cn )` が `MUST ( cn )` になっています。

これで、OpenLDAP が構成されました。

OpenLDAP への WebCenter Sites スキーマの追加

この項では、WebCenter Sites スキーマを OpenLDAP サーバーに追加する方法について説明します。

注意

次のサンプル LDIF ファイルの内容をコピーする場合は、dn セクションの間と、ファイルの最後に必ず空白行を挿入してください。

WebCenter Sites 用に OpenLDAP を構成するには

1. 次の内容の LDIF ファイルを作成し、pre_cs_openldap.ldif という名前を付けます。

```
dn: dc=<domain>,dc=<extension>
objectClass: dcObject
objectClass: organization
dc: fatwire
description: OpenLDAP pre_cs_setup
o: Fatwire Software

# LDAP Manager Role
dn: cn=Manager,dc=<domain>,dc=<extension>
objectclass: organizationalRole
cn: Manager

# add the organizational Unit People
dn: ou=People,dc=<domain>,dc=<extension>
objectClass: organizationalUnit
objectClass: top
ou: People

# add the organizational Unit Group
dn: ou=Groups,dc=<domain>,dc=<extension>
objectClass: organizationalUnit
objectClass: top
ou: Groups
```

ここで、<domain> と <extension> は 144 ページの手順 a で指定した値です。

このファイルは、2 つのサブ組織 (Groups および People) と Manager ユーザーを持つ、新しい組織 (fatwire) を作成します。Manager ユーザーは、LDAP サーバーへのアクセスに使用されます。

2. OpenLDAP サーバーに pre_cs_openldap.ldif ファイルを追加します。次のコマンドを実行します。

   ```
   ldapadd -D 'cn=Manager,dc=<domain>,dc=<extension>'
      -w <root_dn_password> -f pre_cs_openldap.ldif
   ```

   ここで、

   - <domain> と <extension> は、144 ページの手順 a で指定した値です。
   - <root_dn_password> は、145 ページの手順 d で指定したルート DN ユーザーのパスワードです。

3. OpenLDAP サーバーをテストします。次のコマンドを実行します。

   ```
   ldapsearch -x -b 'ou=Groups,dc=<domain>,dc=<extension>'
      '(objectclass=*)'
   ```

   ここで、<domain> と <extension> は 144 ページの手順 a で指定した値です。

   たとえば、**ldapsearch** コマンドからは次のような応答が返されます。

   ```
   # extended LDIF
   #
   # LDAPv3
   # base <ou=Groups,dc=fatwire,dc=com> with scope subtree
   # filter: (objectclass=*)
   # requesting: ALL
   #

   # search result
   search: 2
   result: 0 Success

   # numResponses: 1
   ```

   pre_cs_openldap.ldif ファイルが LDAP サーバーに正常に挿入された場合、result: 行には success と表示されます。この時点で、WebCenter Sites LDAP インテグレータの実行準備は完了です。手順については、*『Oracle WebCenter Sites: LDAP との統合』* を参照してください。

ユーザー・パスワードの変更

WebCenter Sites LDAP インテグレータを実行したとき、(`fwadmin`、`ContentServer` および `DefaultReader` を除く) WebCenter Sites ユーザーすべてに WebCenter Sites 構成画面で入力したパスワードが割り当てられています。セキュリティ上の理由から、これらのユーザーには一意のパスワードを手動で割り当てる必要があります。

注意

OpenLDAP の構成時に、暗号化されたパスワードの使用を選択した場合は、WebCenter Sites システム上のすべてのユーザーのパスワードを変更する**必要があります**。変更しないと、WebCenter Sites インストールは適切に動作しません。これは、WebCenter Sites-LDAP インテグレータはユーザー・パスワードを平文として OpenLDAP に書き込みますが、OpenLDAP はパスワード・ハッシュを予期しているためです。

次の表は、WebCenter Sites ユーザーと、そのユーザーに割り当てるべきパスワードをまとめたものです。

ユーザー	パスワード
`DefaultReader`	`SomeReader`
`ContentServer`	WebCenter Sites のインストール時に指定したパスワード
`fwadmin`	WebCenter Sites のインストール時に指定したパスワード
WebCenter Sites システムのその他すべてのユーザー	WebCenter Sites と LDAP の統合時に指定したパスワード

この項では、OpenLDAP でパスワードを変更する方法について説明します。

- LDAP ブラウザを使用したユーザー・パスワードの変更
- ldapmodify コマンドを使用したユーザー・パスワードの変更

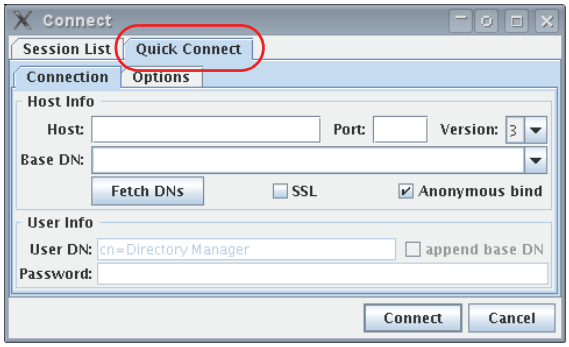
LDAP ブラウザを使用したユーザー・パスワードの変更

この項では、`http://www-unix.mcs.anl.gov/~gawor/ldap/` から入手可能な無料の LDAP ブラウザやエディタ・プログラムを使用して、ユーザー・パスワードを変更する方法について説明します。

OpenLDAP で LDAP ブラウザを使用してユーザー・パスワードを変更するには

1. LDAP ブラウザをダウンロードしてインストールします。
2. LDAP ブラウザを起動します。**`./lbe.sh`**

3. 「**Quick Connect**」タブをクリックします。

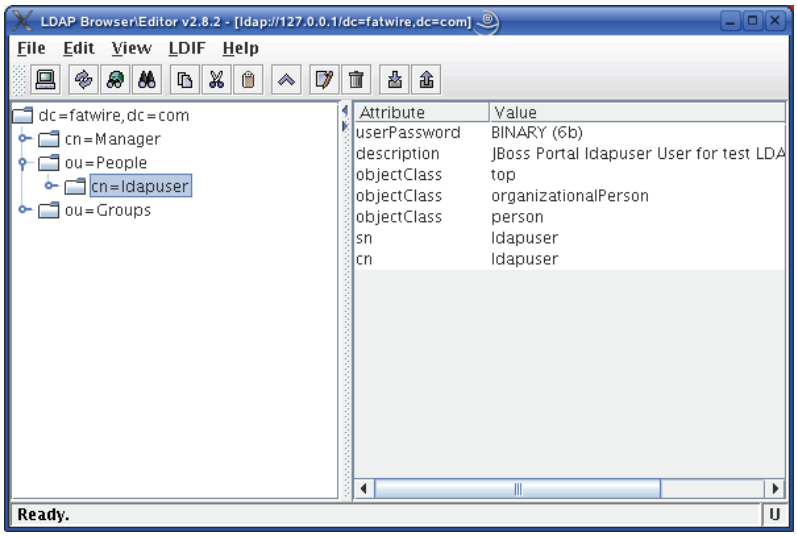


4. 次のようにフィールドに入力します。

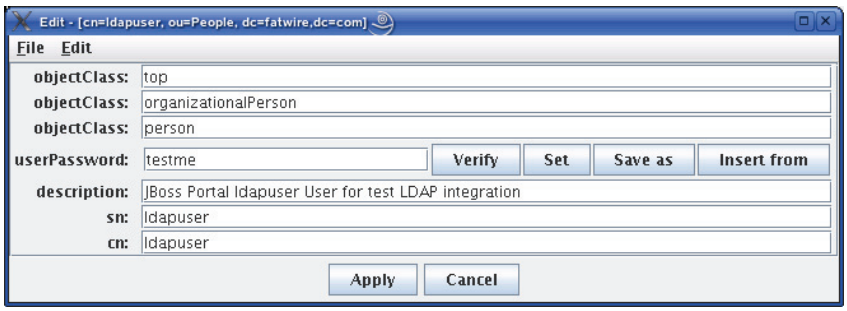
フィールド	値
Hostname	OpenLDAP Server のホスト名。
Port	**389**
Version	**3**
Base DN	144 ページの手順 a で指定したベース DN。
Anonymous bind	**はい** (チェック・ボックスを選択)
User DN	**cn=Manager**
Append base DN	**はい** (チェック・ボックスを選択)
Password	145 ページの手順 d で指定したルート DN ユーザー・パスワード。

5. 「**Connect**」をクリックします。

6. 左側のツリーで、「**ou=People**」ノードを展開します。



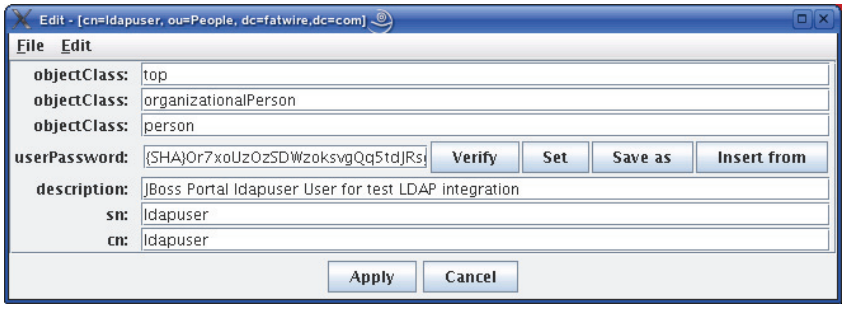
7. パスワードの変更対象となるユーザーをダブルクリックし、**[Ctrl] + [E]** を押します。
8. WebCenter Sites-LDAP インテグレータにより書き込まれた平文パスワードが、「**userPassword**」フィールドに表示されます。「**Set**」をクリックします。



9. ポップアップ・ウィンドウでユーザーのパスワードを入力し、「**Set**」をクリックします。

パスワードは暗号化された形で表示されます。

10. 「**Apply**」をクリックして、新しいパスワードを保存します。



11. パスワード変更の対象ユーザーごとに、手順 7 - 10 を繰り返します。完了したら、WebCenter Sites にログインして統合をテストします。

ldapmodify コマンドを使用したユーザー・パスワードの変更

ldapmodify コマンドは、OpenLDAP サーバーの構成の変更に有効な LDIF 文を入力するためのインタフェースを提供します。この項では、**ldapmodify** および **sldappasswd** コマンドを使用して LDAP ユーザーのパスワードを変更する方法について説明します。

OpenLDAP で ldapmodify コマンドを使用してユーザー・パスワードを変更するには

1. 各ユーザーについて暗号化されたパスワードを生成します。**sldappasswd** コマンドを実行して、暗号化の対象となる平文のパスワードを入力します。このコマンドは、暗号化されたパスワード (ハッシュ) を端末に出力します。次に例を示します。

   ```
   {SSHA}ydUT5RCpBAU80P0PW8gaHnsmYmLlmUL8
   ```

   注意

   多くのユーザーのハッシュを生成する場合は、ハッシュをファイルに保存することをお薦めします。手順 3 でハッシュを簡単に取得できるようになります。この作業を完了したら、ハッシュを保存したファイルは必ず破棄してください。

2. 次のように **ldapmodify** コマンドを実行します。

   ```
   ldapmodify -D 'cn=Manager,dc=<domain>,dc=<extension>'
      -w <root_dn_password>
   ```

   ここで、

   - <domain> と <extension> は、144 ページの手順 a で指定した値です。
   - <root_dn_password> は、145 ページの手順 d で指定したルート DN ユーザーのパスワードです。

   このコマンドから空の行が返されたら、LDIF 文の入力準備は完了です。

3. ユーザーのパスワードを変更します。次のコマンドを実行します。

   a. **dn:cn=<user_name>,ou=People,dc=<domain>,dc=<extension>**

      ここで、user_name はパスワード変更の対象ユーザーのユーザー名、<domain> および <extension> は 144 ページの手順 a で指定した値です。

   b. **changetype:modify**

   c. **replace:userPassword**

   d. **userpassword:<password_hash>**

      ここで、<password_hash> は、この手順の手順 1 にある **sldappasswd** コマンドで生成されたハッシュです。

   e. **[Ctrl] + [D]** を押します。

   f. パスワード変更の対象ユーザーごとに、手順 a - e を繰り返します。終了したら、**[Ctrl] + [C]** を押して、**ldapmodify** コマンドを終了します。

第 11 章

WebLogic 10.3.5 組込み LDAP サーバーのセットアップ

この章では、現在サポートされている WebLogic 組込み LDAP サーバーを、WebCenter Sites で使用できるようにセットアップする手順について説明します。

注意

WebLogic LDAP は、WebCenter Sites-LDAP インテグレータを実行する**前に**セットアップする必要があります。

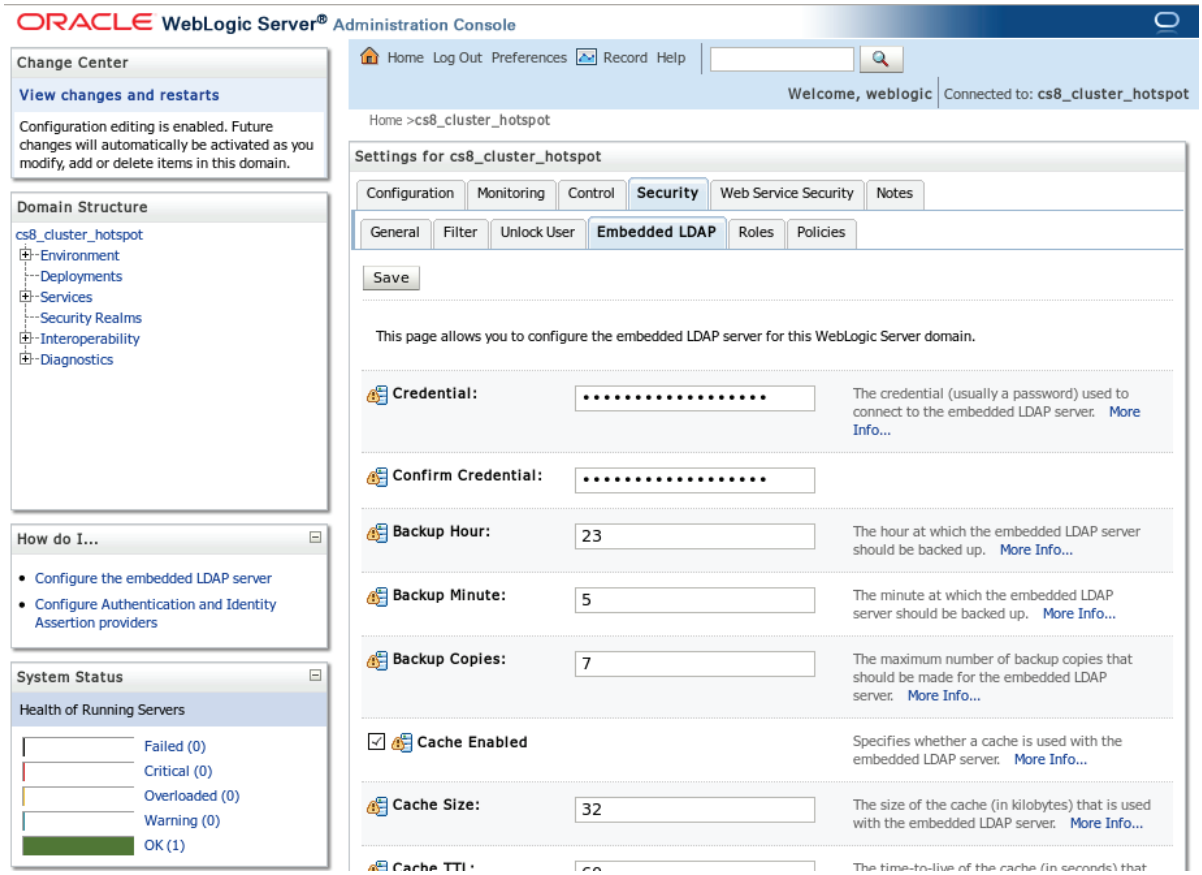
この章は、次の項で構成されています。

WebLogic 組込み LDAP サーバーの有効化

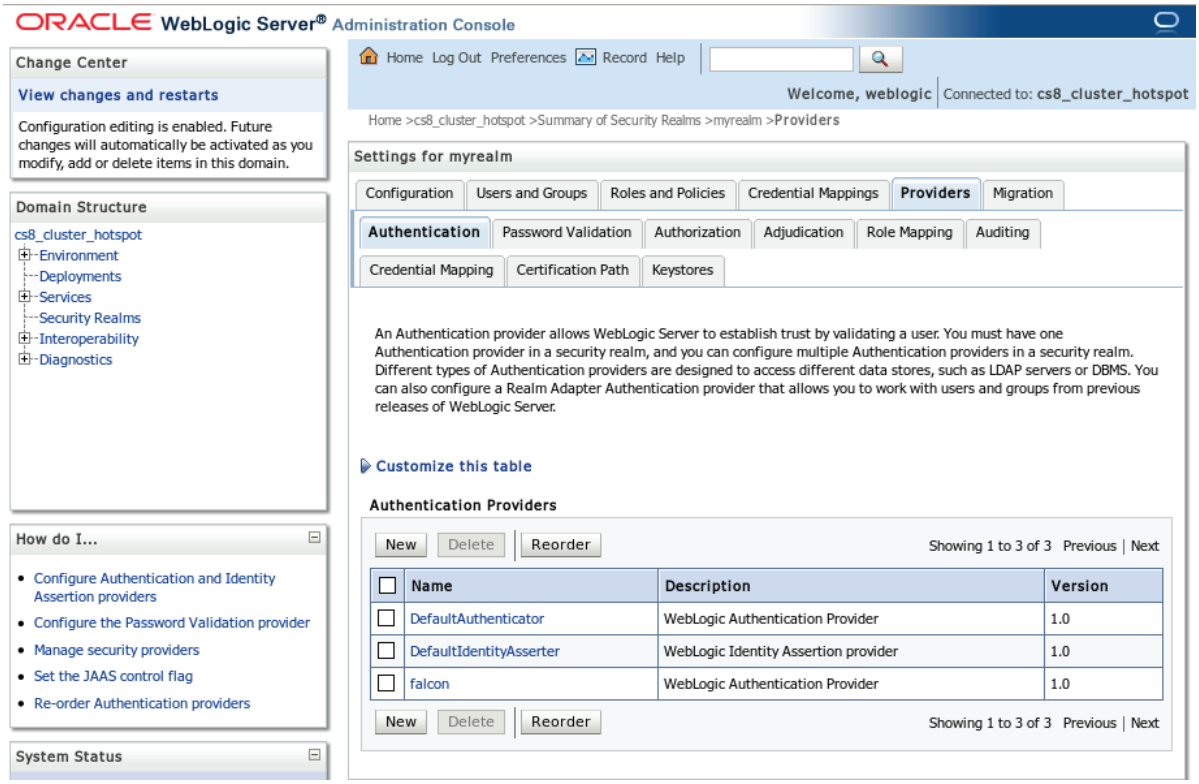
この項では、WebLogic 組込み LDAP サーバーを有効化する方法について説明します。

WebLogic 組込み LDAP サーバーを有効化するには

1. WebLogic Server 管理コンソールにログインします。
2. 左側にある「ドメイン構造」ツリーで、使用している WebLogic ポータル・ドメインをクリックします。
3. 組込み LDAP パスワードを設定します。
   a. ワークスペースで、**「セキュリティ」**タブを選択し、**「組込み LDAP」**サブ・タブを選択します。
   b. 左上にある「チェンジ・センター」ペインで、**「ロックして編集」**をクリックします。
   c. **「資格証明」**フィールドに、目的の組込み LDAP パスワードを入力します。確認のため、**「資格証明の確認」**フィールドに、このパスワードを再入力します。
   d. **「保存」**をクリックします。



4. 組込み LDAP 認証プロバイダを作成します。
   a. 「ドメイン構造」ツリーで**「セキュリティ・レルム」**をクリックします。
   b. ワークスペースで、**「myrealm」**をクリックし、**「プロバイダ」**タブを選択します。



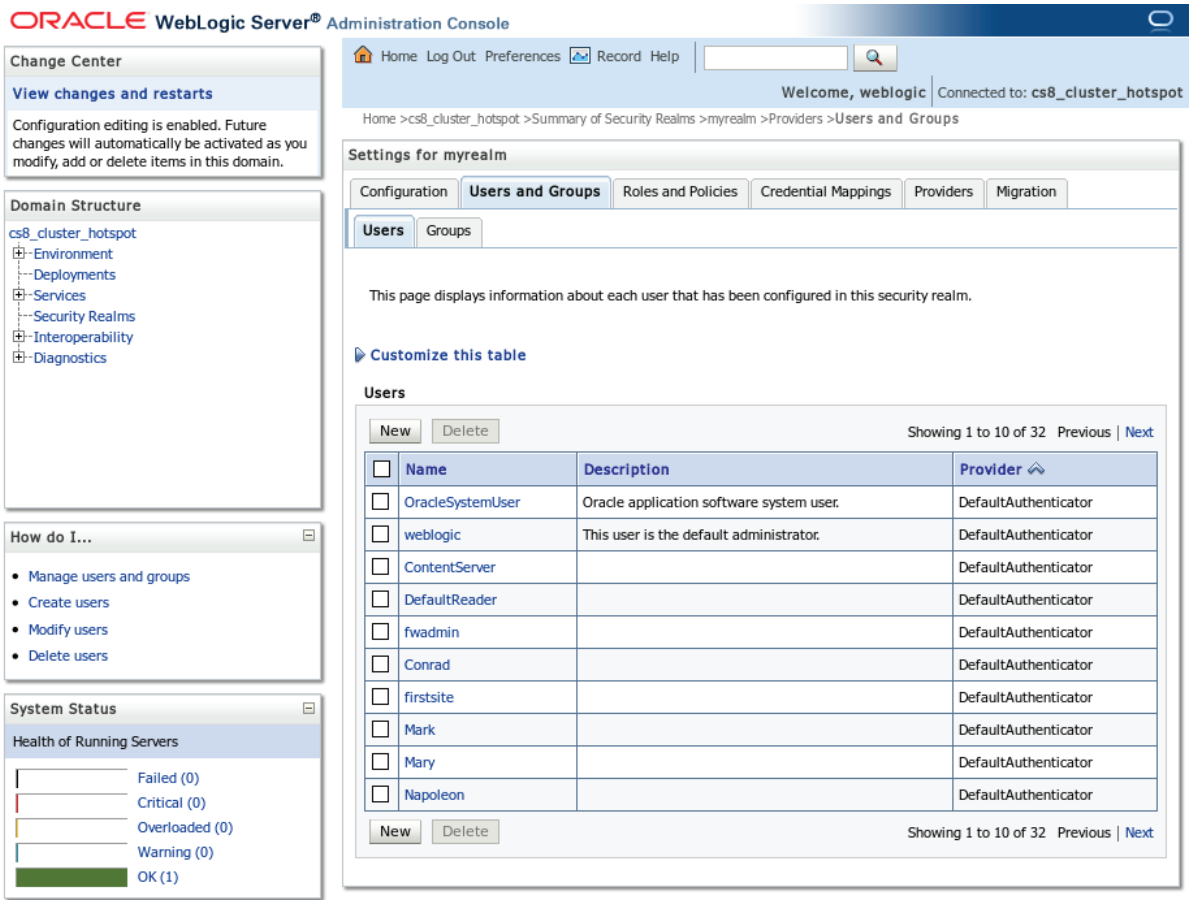
   c. **「新規」**をクリックします。
   d. **「名前」**フィールドに、認証プロバイダの名前を入力します。
   e. 「タイプ」ドロップダウン・リストで、**「DefaultAuthenticator」**を選択します。
   f. **「OK」**をクリックします。新しい認証プロバイダが、プロバイダのリストに表示されます。
5. 「チェンジ・センター」で、**「変更のアクティブ化」**をクリックします。
6. 管理サーバーを停止します。

ユーザー・パスワードの変更

この項では、WebLogic LDAP サーバーでユーザー・パスワードを変更する方法について説明します。

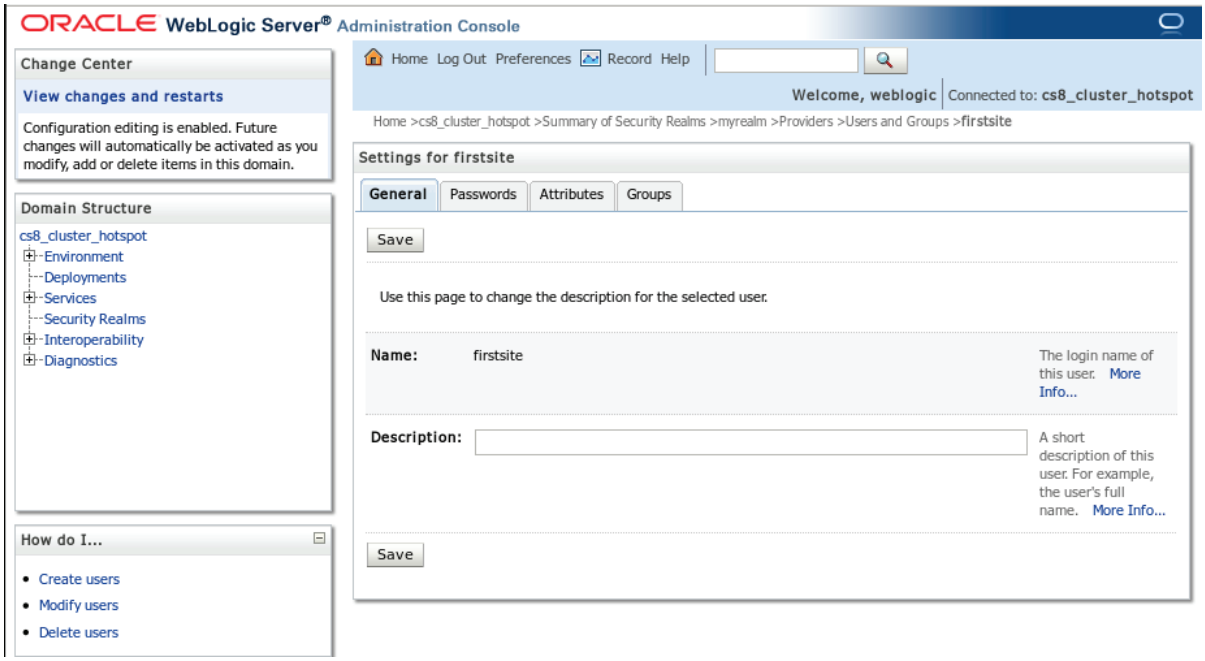
WebLogic LDAP サーバーでユーザー・パスワードを変更するには

1. WebLogic Server 管理コンソールにログインします。
2. 「ドメイン構造」ツリーで「**セキュリティ・レルム**」をクリックします。
3. ワークスペースで、「**myrealm**」をクリックし、「**ユーザーとグループ**」タブを選択します。

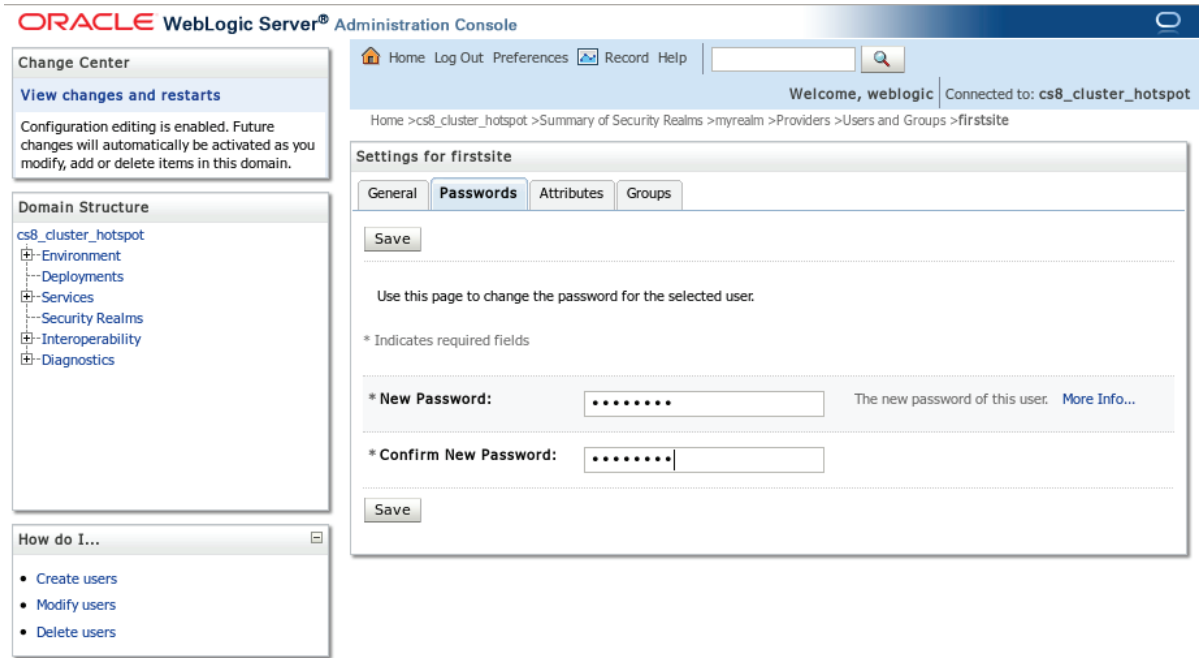


4. パスワード変更の対象となるユーザーをクリックします。

ワークスペースに、「ユーザー名の設定」画面が表示されます。



5. 「パスワード」タブを選択し、両方のフィールドに新しいパスワードを入力します。



6. 「保存」をクリックします。

第 12 章

Microsoft Active Directory Server 2003 のセットアップ

この章では、現在サポートされている Microsoft Active Directory Server (ADS) を、WebCenter Sites で使用できるようにセットアップする手順について説明します。

注意

ADS は、WebCenter Sites-LDAP インテグレータを実行する**前に**セットアップする必要があります。

この章は、次の項で構成されています。

Microsoft Active Directory Server のインストール

この項では、WebCenter Sites で使用できるように、Microsoft Active Directory Server 2003 をインストールする方法について説明します。

この作業は、次の手順から構成されています。

A. オペレーティング・システムのインストール

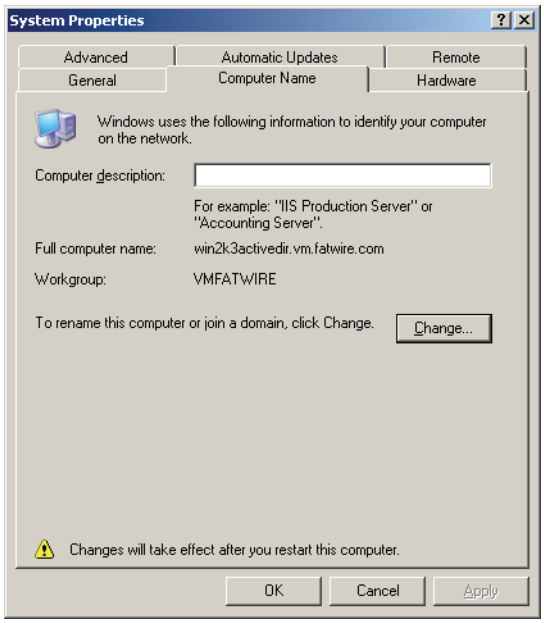
ターゲット・マシンに Windows Server 2003 (Web Edition 以外のタイプ) をインストールします。

インストールが完了しても、インストール・ディスクはドライブに入れたままにしてください。ADS のインストールを完了するには、このディスクが必要です。

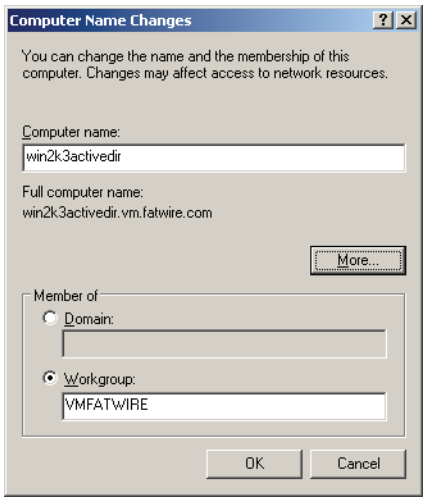
B. マシンの名前およびサフィックスの設定

1. 「システムのプロパティ」ダイアログを開きます。

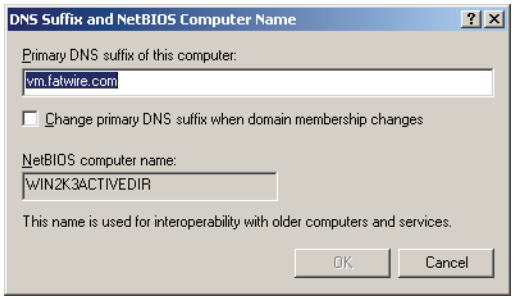
   これには数通りの方法があります。最も早い方法は、デスクトップの**「マイコンピュータ」**アイコンを右クリックし、コンテキスト・メニューから**「プロパティ」**を選択することです。
2. **「コンピュータ名」**タブを選択します。
3. **「変更」**をクリックします。



4. ポップアップ・ウィンドウが表示されたら、次の操作を行います。
   a. マシンに付ける名前を入力します。この名前を記録します。
   b. **「ワークグループ」**ラジオ・ボタンを選択し、**一意の**ワークグループ名を入力します。この名前を記録します。



   c. **「詳細」**をクリックします。
   d. 2 つめのポップアップ・ウィンドウが表示されたら、マシンの DNS サフィックスを入力します。このサフィックスを記録します。



   e. **「ドメインのメンバシップが変更されるときにプライマリ DNS サフィックスを変更する」**チェック・ボックスが**選択されていない**ことを確認します。
   f. **「OK」**をクリックして、「DNS サフィックスと NetBIOS コンピュータ名」ポップアップ・ウィンドウを閉じます。
5. **「OK」**をクリックして、「コンピュータ名の変更」ポップアップ・ウィンドウを閉じます。
6. 「システムのプロパティ」ダイアログ・ボックスで、**「OK」**をクリックします。
7. マシンを再起動します。

C. マシンのネットワーク設定の構成

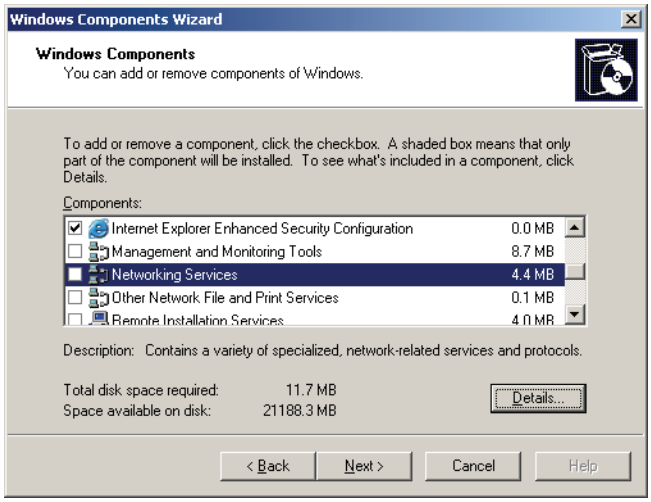
次のようにマシンのネットワーク設定を構成します。

1. IP アドレスに、未使用の静的 IP アドレスを設定します。
2. マシンの IP アドレスに、目的の DNS サーバーを設定します。
3. マシンのネットワーク・インタフェースで、**「TCP/IP プロトコル」**プロパティの**「DNS」**設定にある**「詳細設定」**タブで、**「プライマリおよび接続専用の DNS サフィックスを追加する」**チェック・ボックスが選択されていることを確認します。
4. **「プライマリ DNS サフィックスの親サフィックスを追加する」**チェック・ボックスが選択されていることを確認します。

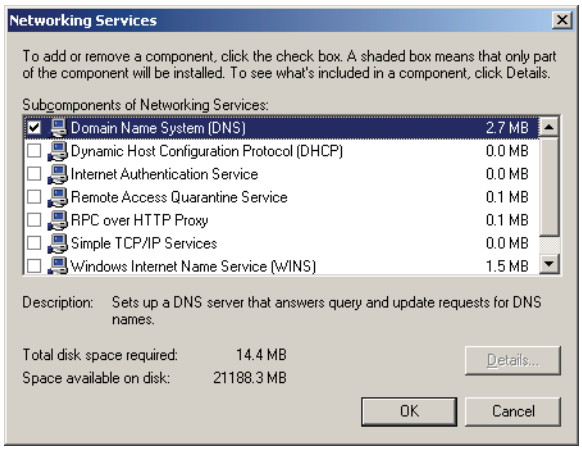
マシンのネットワーク設定の構成手順については、Windows Server 2003 のドキュメントを参照してください。

D. ローカル DNS サーバーのインストール

1. 「コントロール パネル」を開き、**「プログラムの追加と削除」**をダブルクリックします。
2. **「Windows コンポーネントの追加と削除」**をクリックします。
3. 「Windows コンポーネント ウィザード」ポップアップ・ウィンドウで、**「ネットワーク サービス」**項目 (チェック・ボックス**ではない**) を選択し、**「詳細」**をクリックします。



4. 表示されたポップアップ・ウィンドウで、「**ドメイン ネーム システム (DNS)**」を選択し、「**OK**」をクリックします。ポップアップ・ウィンドウが閉じます。

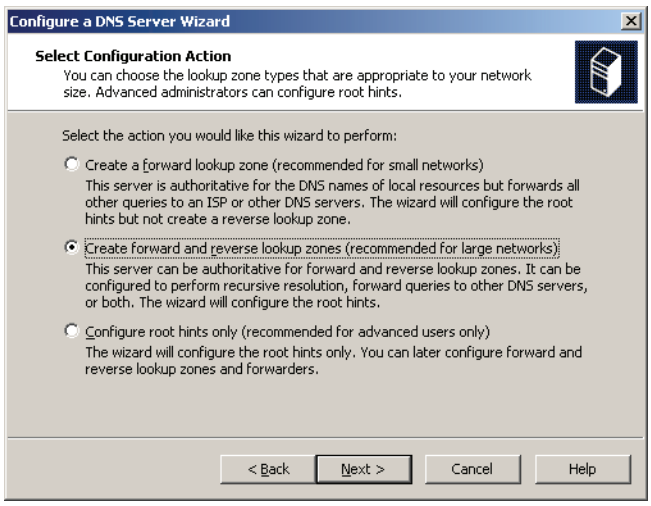


5. 「Windows コンポーネント ウィザード」画面で「**次へ**」をクリックします。
6. インストールが正常に完了したら、「**完了**」をクリックします。

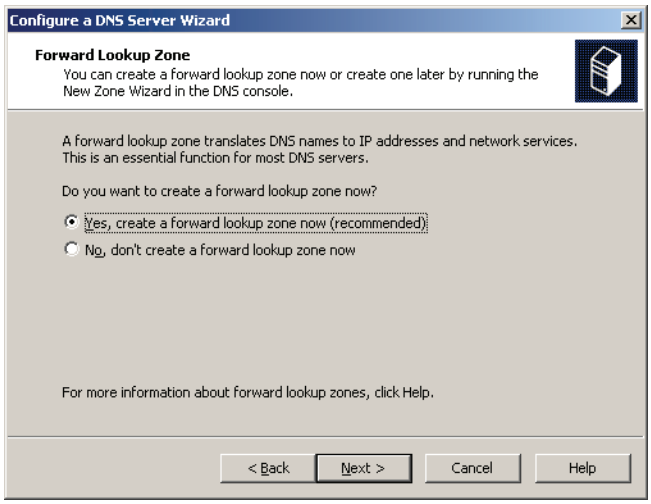
E. ローカル DNS サーバーの構成

1. 「コントロール パネル」で、**「管理ツール」**アイコンをダブルクリックします。
2. **「DNS」**アイコンをダブルクリックします。
3. 「dnsmgmt コンソール」に、161 ページの手順 4 で入力したマシン名を入力します。
4. マシン名を右クリックし、コンテキスト・メニューから**「DNS サーバーの構成」**を選択します。
5. 「DNS サーバーの構成ウィザード」ポップアップ・ウィンドウが表示されるので、**「次へ」**をクリックします。

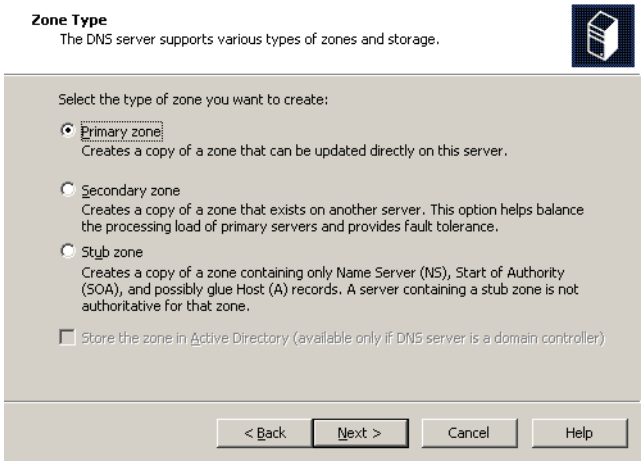
6. 「構成動作の選択」画面で、**「前方および逆引き参照ゾーンを作成する」**ラジオ・ボタンを選択し、**「次へ」**をクリックします。



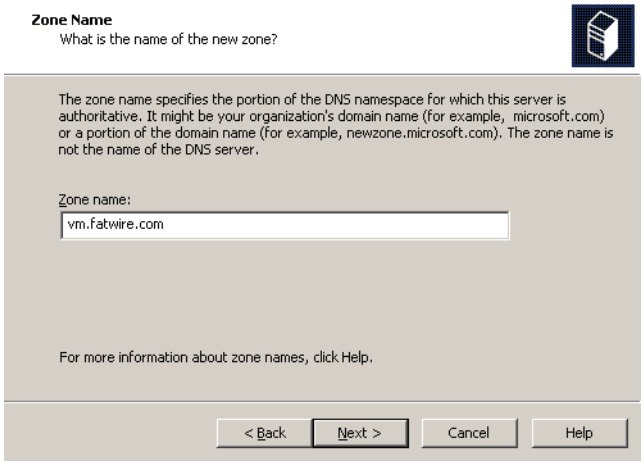
7. 「前方参照ゾーン」画面で、**「今すぐ前方参照ゾーンを作成する (推奨)」**ラジオ・ボタンを選択し、**「次へ」**をクリックします。



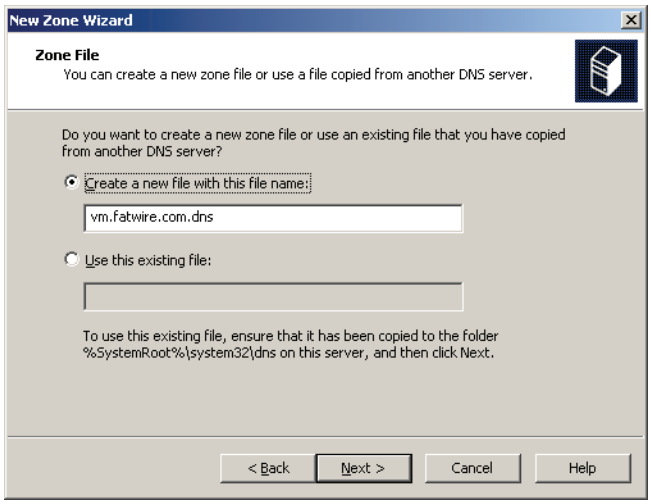
8. 「ゾーンの種類」画面で、**「プライマリ ゾーン」**ラジオ・ボタンを選択し、**「次へ」**をクリックします。



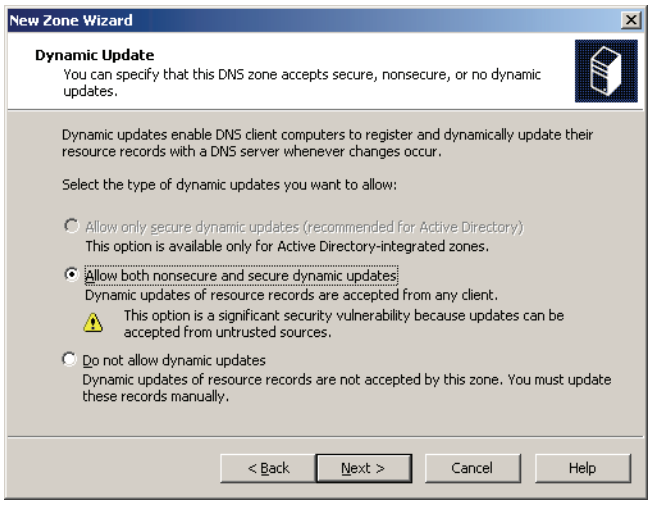
9. 「ゾーン名」画面に、作成しているゾーンの名前を入力します。ゾーン名は 161 ページの手順 d で入力したドメイン・サフィックスです。「**次へ**」をクリックします。



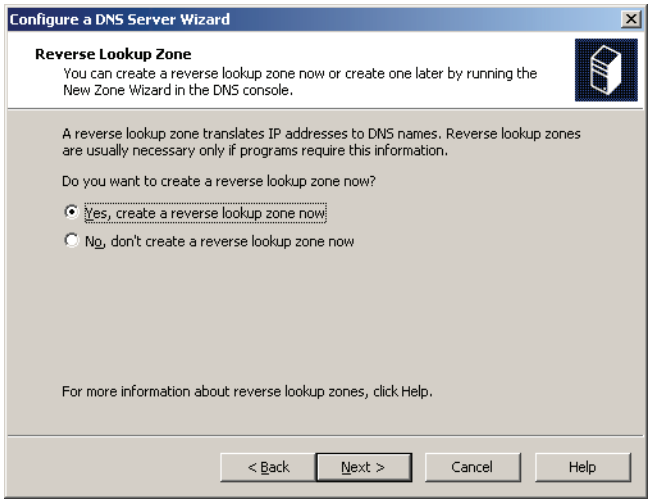
10. 「ゾーン ファイル」画面では、デフォルトのゾーン・ファイル名をそのままにして、「**次へ**」をクリックします。



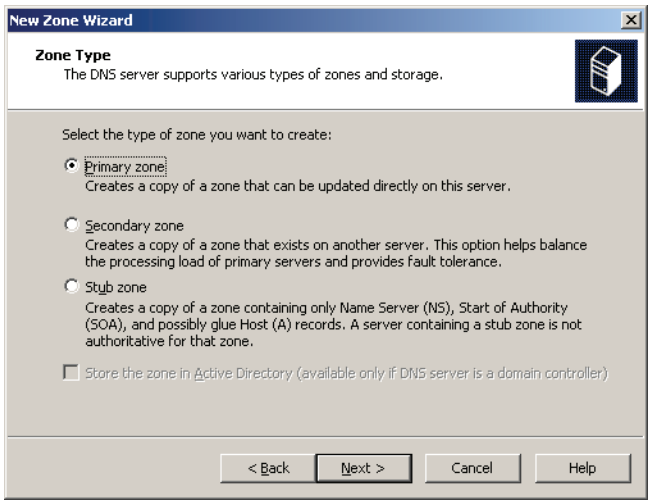
11. 「動的更新」画面で、**「非セキュリティ保護およびセキュリティ保護の両方による動的更新を許可する」**ラジオ・ボタンを選択し、**「次へ」**をクリックします。



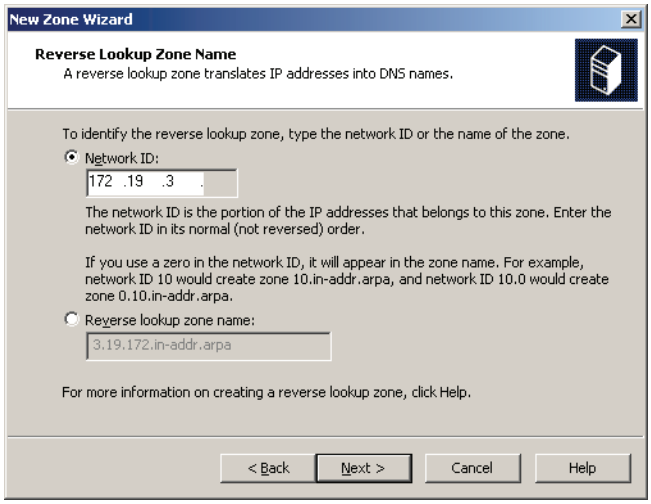
12. 「逆引き参照ゾーン」画面で、**「今すぐ逆引き参照ゾーンを作成する」**ラジオ・ボタンを選択し、**「次へ」**をクリックします。



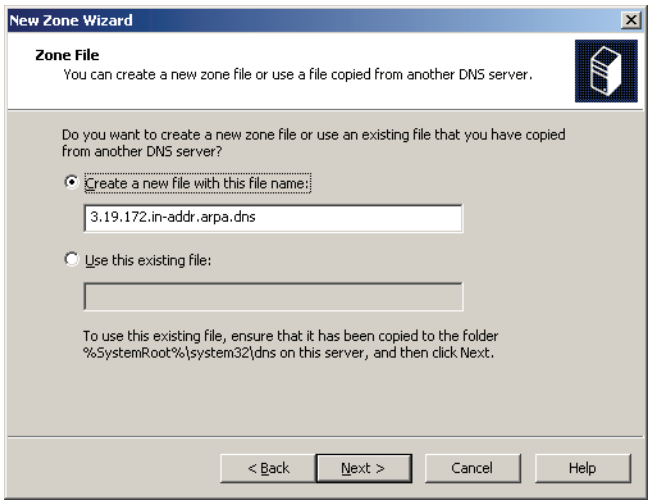
13. 「ゾーンの種類」画面で、「**プライマリ ゾーン**」ラジオ・ボタンを選択し、「**次へ**」をクリックします。



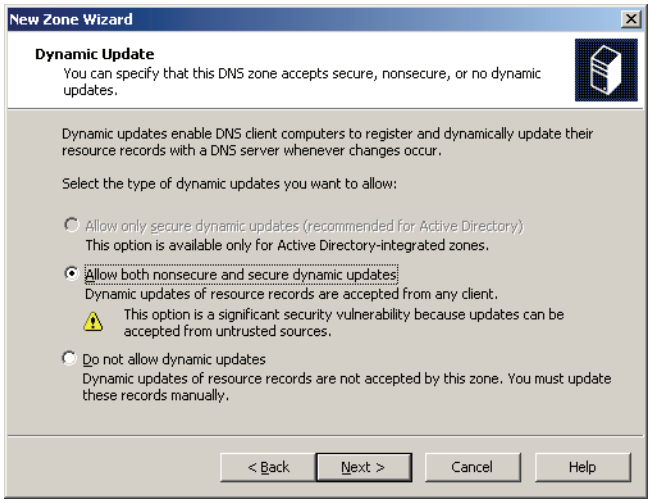
14. 「逆引き参照ゾーン名」画面で、「**ネットワーク ID**」ラジオ・ボタンを選択し、マシンの IP アドレス (162 ページの手順 1 で設定したもの) の先頭 3 オクテットを入力して、「**次へ**」をクリックします。



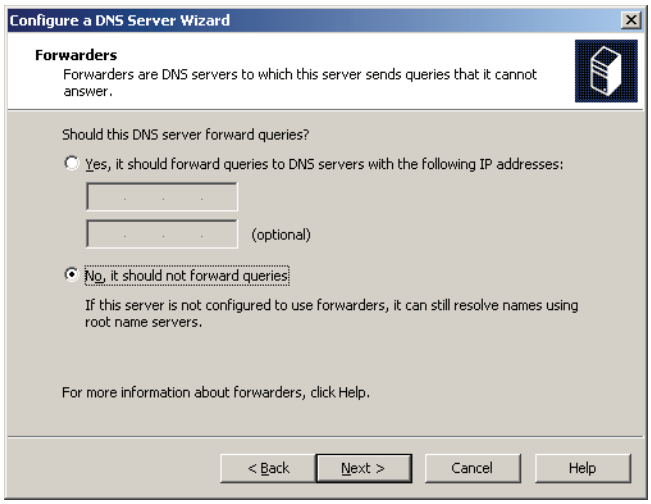
15. 「ゾーン ファイル」画面では、デフォルトのゾーン・ファイル名をそのままにして、**「次へ」**をクリックします。



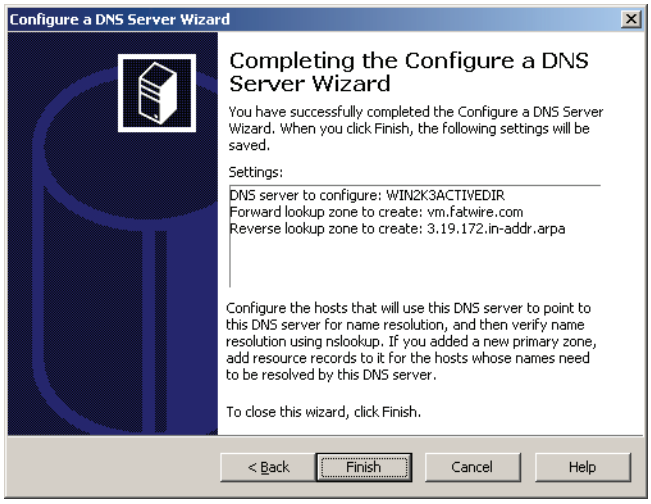
16. 「動的更新」画面で、**「非セキュリティ保護およびセキュリティ保護の両方による動的更新を許可する」**ラジオ・ボタンを選択し、**「次へ」**をクリックします。



17. 「フォワーダ」画面で、**「いいえ、クエリを転送しません」**ラジオ・ボタンを選択し、**「次へ」**をクリックします。



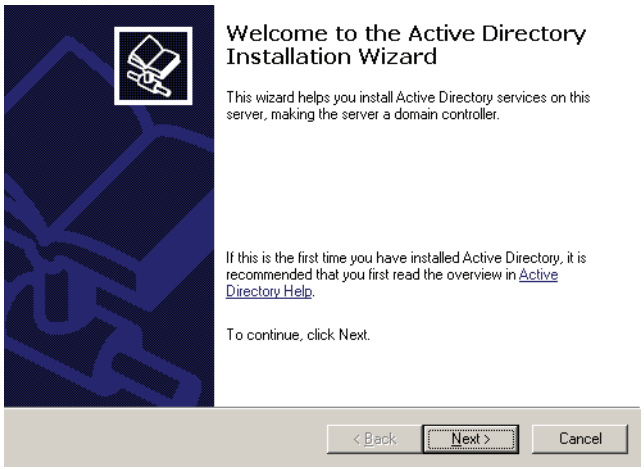
18. 「DNS サーバーの構成ウィザードの完了」画面で、**「完了」**をクリックします。



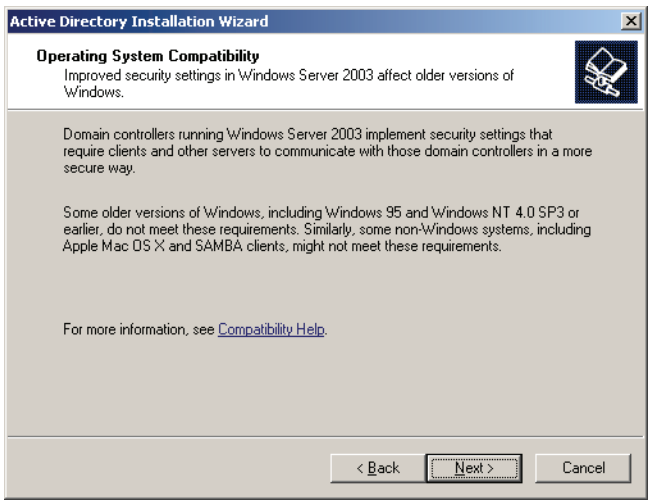
19. DNS サーバー・ウィンドウを閉じるか、最小化します。

F. Microsoft Active Directory Server 2003 のインストール

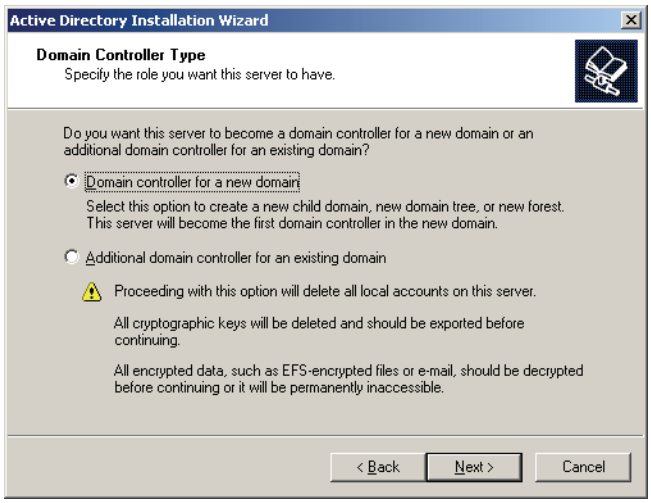
1. 「スタート」、「ファイル名を指定して実行」の順にクリックし、「ファイル名を指定して実行」ダイアログ・ボックスに **dcpromo** と入力します。
2. 「Active Directory のインストール ウィザードの開始」で「次へ」をクリックします。



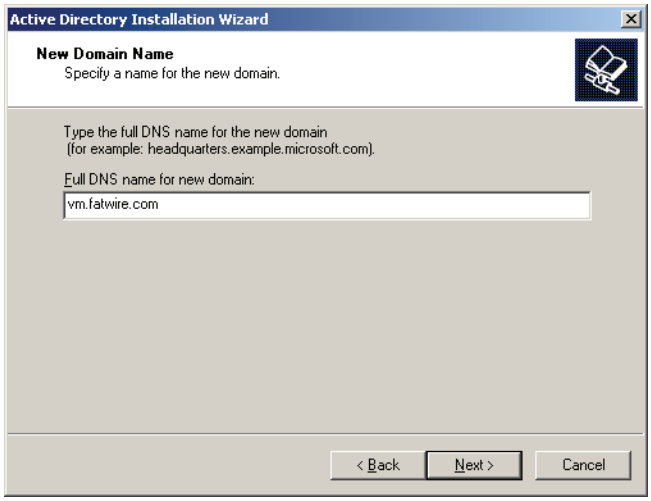
3. 「オペレーティング システムの互換性」画面で、「次へ」をクリックします。



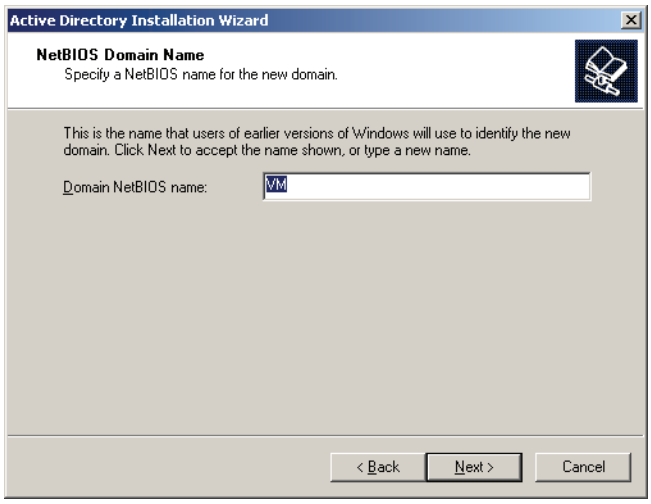
4. 「ドメイン コントローラの種類」画面で、**「新しいドメインのドメイン コントローラ」**ラジオ・ボタンを選択し、**「次へ」**をクリックします。



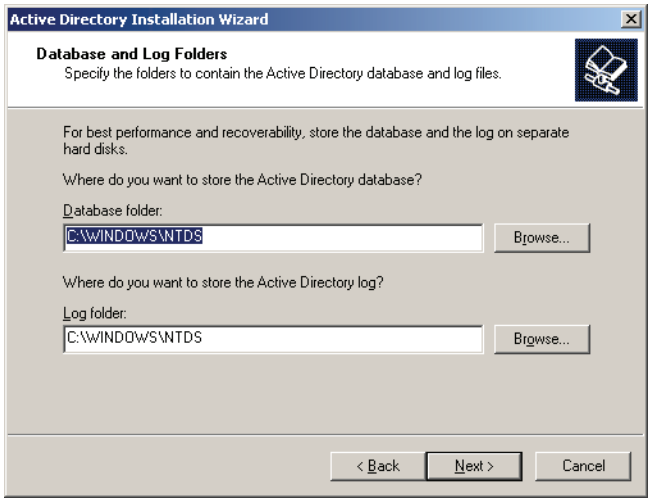
5. 「新しいドメインの作成」画面で、**「新しいフォレストのドメイン」**ラジオ・ボタンを選択し、**「次へ」**をクリックします。
6. 「新しいドメイン名」画面に、166 ページの手順 9 で入力した DNS 名を入力し、**「次へ」**をクリックします。



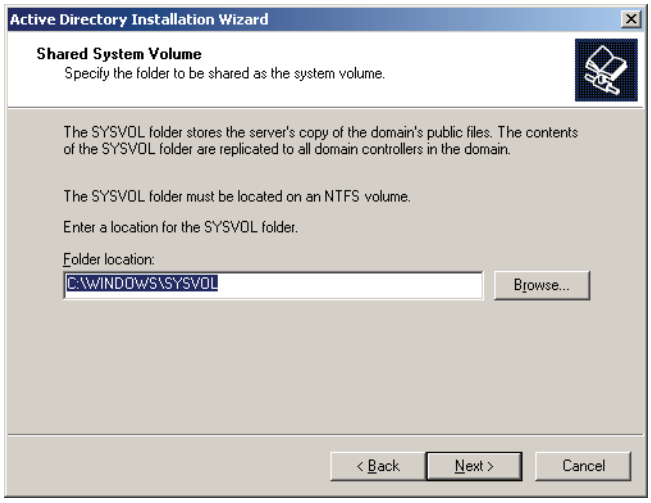
7. 「NetBIOS ドメイン名」画面で、デフォルト値をそのまま残し、「**次へ**」をクリックします。この値を記録します。



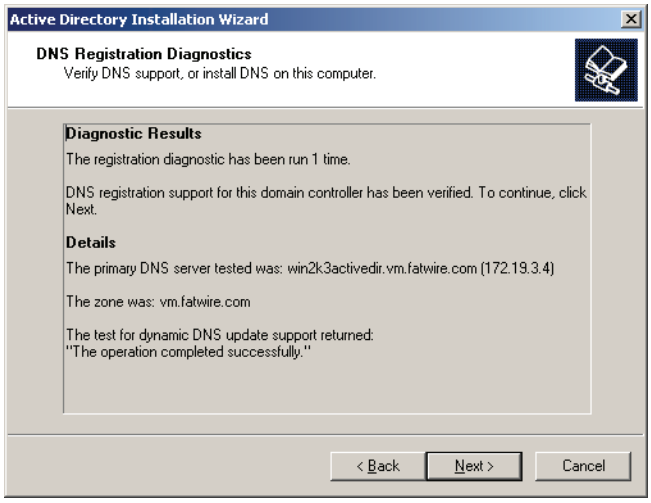
8. 「データベースとログのフォルダ」画面で「**次へ**」をクリックします。



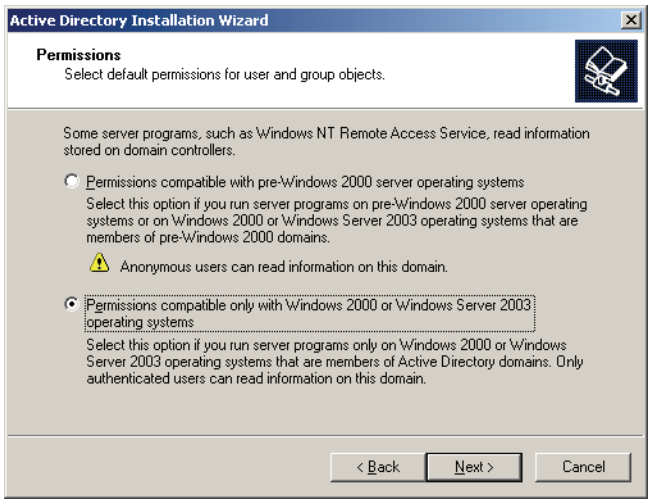
9. 「共有システム ボリューム」画面で、「次へ」をクリックします。



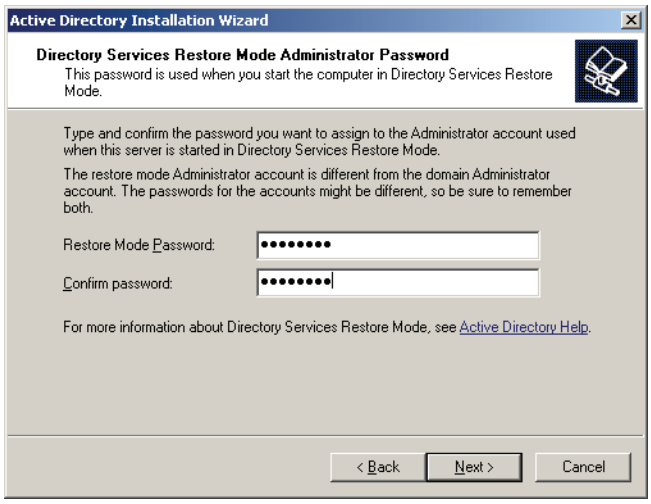
10. 「診断結果」画面で、診断が正常に終了していることを確認し、「次へ」をクリックします。診断に失敗した場合は、指摘された問題を修正し、「戻る」をクリックしてから「次へ」をクリックして診断を再度実行します。



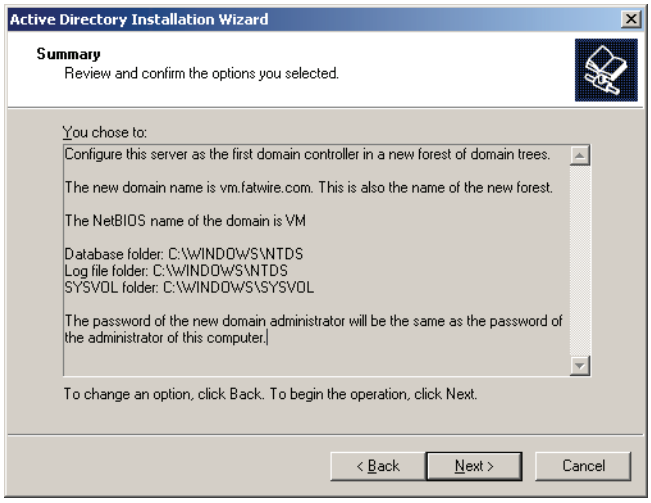
11. 「アクセス許可」画面で「**Windows 2000 または Windows Server 2003 OS とのみ互換性があるアクセス許可**」を選択し、「**次へ**」をクリックします。



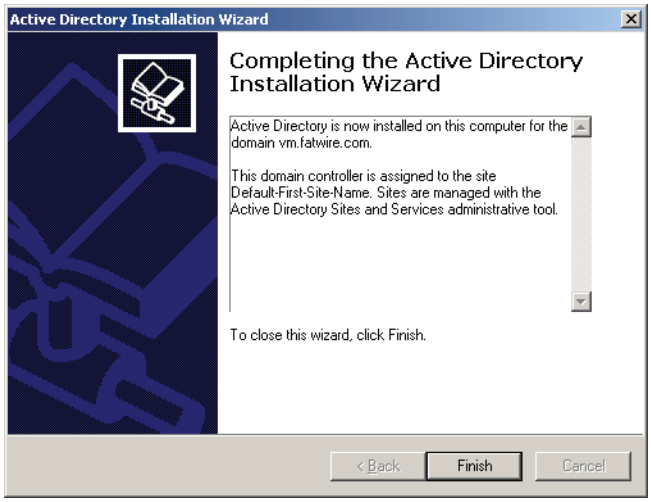
12. 「ディレクトリ サービス復元モード Administrator パスワード」画面にパスワードを入力し、「**次へ**」をクリックします。このパスワードを記録しておきます。



13.「概要」画面で「**次へ**」をクリックします。



14.「Active Directory のインストール ウィザードの完了」画面で「**次へ**」をクリックします。



15. ポップアップ・ダイアログが表示されたら、「**再起動する**」をクリックし、マシンが再起動されるのを待ちます。

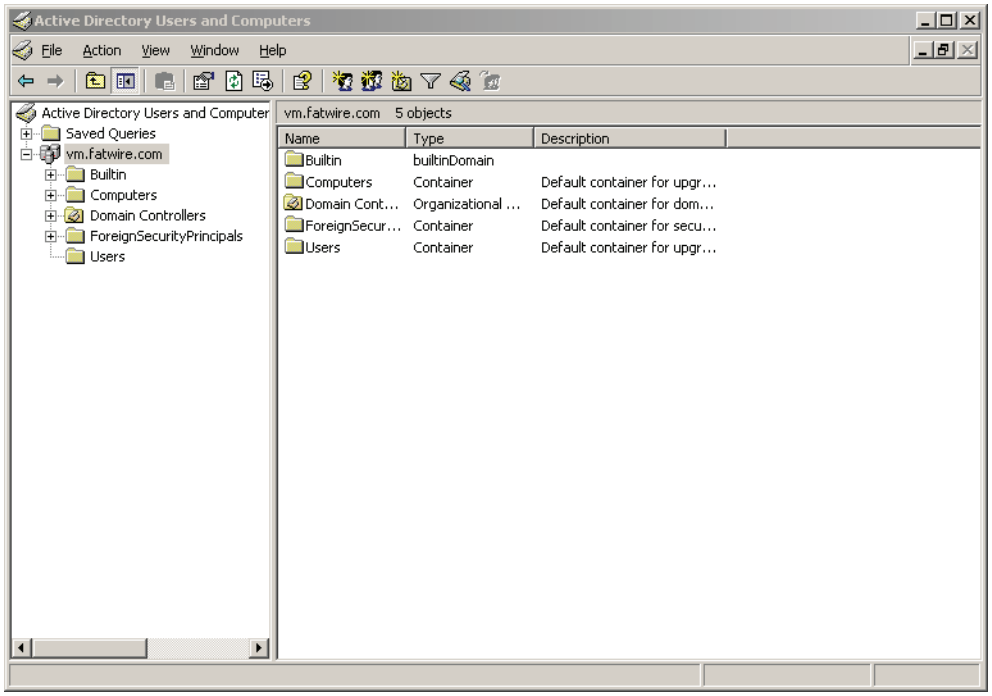
これで、Active Directory Server がインストールされ、使用できるようになりました。

「Active Directory ユーザーとコンピュータ」コンソールへのアクセス

「Active Directory ユーザーとコンピュータ」コンソールは、Active Directory Server 構成の管理に使用します。このコンソールにアクセスするには、次の手順を実行します。

1. **「スタート」**、**「ファイル名を指定して実行」**の順にクリックし、「ファイル名を指定して実行」ダイアログ・ボックスを開きます。
2. 「ファイル名を指定して実行」ダイアログ・ボックスに、**`dsa.msc`** と入力します。
3. **「OK」**をクリックします。

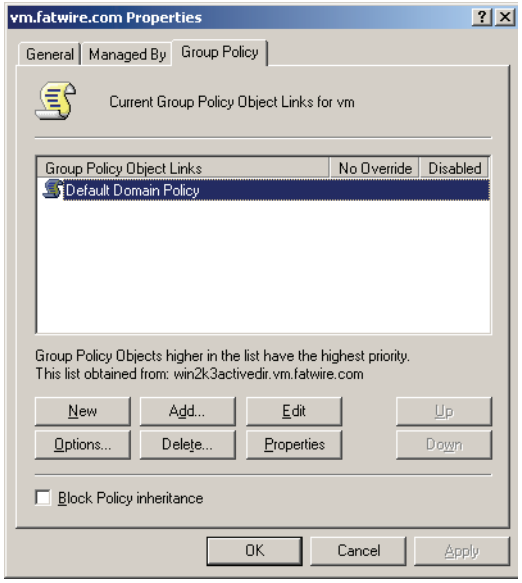
   「Active Directory ユーザーとコンピュータ」コンソールがロードされます。



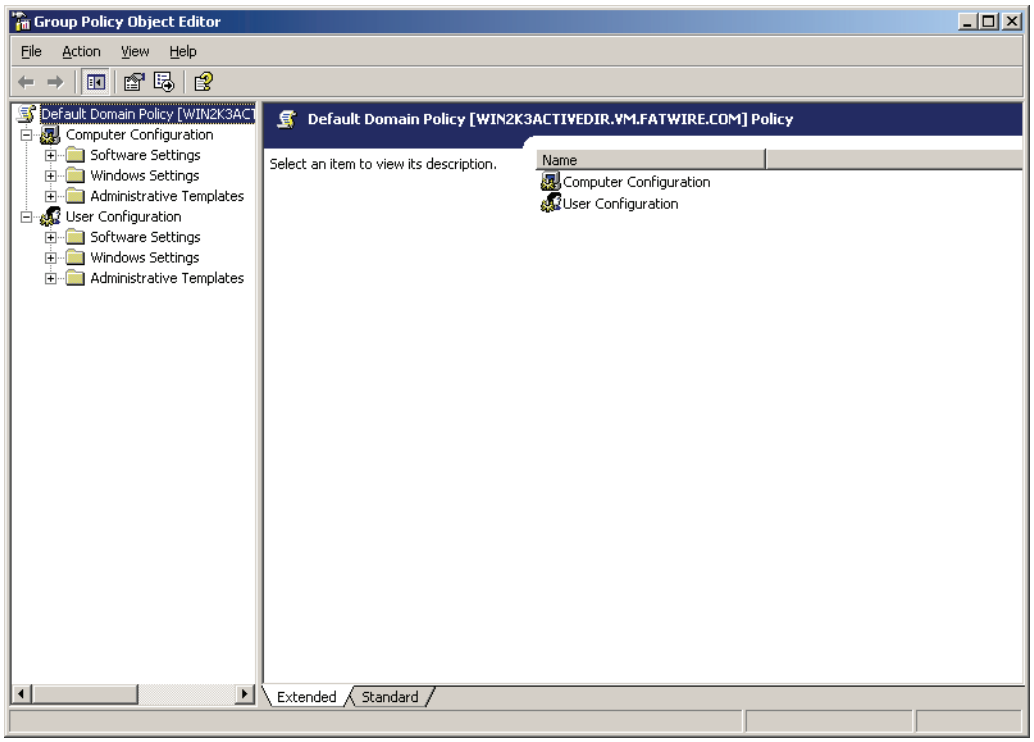
WebCenter Sites に対する ADS パスワードのセキュリティの構成

この項では、Active Directory Server に、WebCenter Sites の要件を満たすパスワード・セキュリティを構成する方法について説明します。

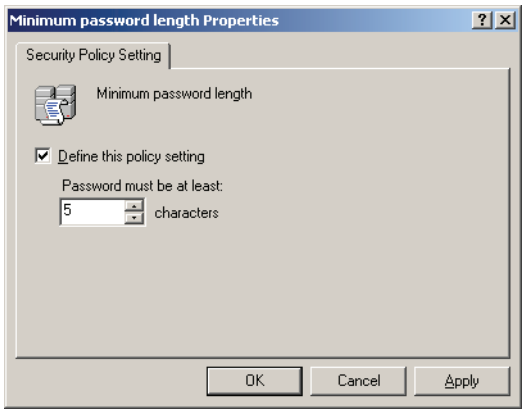
1. 「Active Directory ユーザーとコンピュータ」コンソールを開きます。
2. 左側のツリーで、目的のドメインを右クリックし、コンテキスト・メニューから「**プロパティ**」を選択します。
3. 表示されるダイアログで、「**グループ ポリシー**」タブを選択します。



4. 「グループ ポリシー オブジェクト エディター」が開き、選択したグループ・ポリシーが表示されます。



5. 左側のツリーで、**「コンピュータの構成」→「Windows の設定」→「セキュリティの設定」→「アカウント ポリシー」**の順に展開し、**「パスワードのポリシー」**を選択します。
6. メイン ペインで、**「パスワードの長さ」**項目をダブルクリックします。
7. ポップアップ・ダイアログが表示されたら、値に 4 を入力し、**「OK」**をクリックします。



8. **「複雑さの要件を満たす必要があるパスワード」**項目をダブルクリックします。

9. ポップアップ・ウィンドウが表示されたら、「**無効**」ラジオ・ボタンを選択し、「**OK**」をクリックします。
10. 「**ファイル**」メニューから「**終了**」を選択し、「**OK**」をクリックします。
11. 「ファイル名を指定して実行」ダイアログを開き、**gpudate** と入力して、「**OK**」をクリックします。

ユーザー・パスワードの変更

この項では、Active Directory Server でユーザーのパスワードを変更する方法について説明します。

1. 「Active Directory ユーザーとコンピュータ」コンソールを開きます。
2. 左側のツリーで「**ユーザー**」を選択します。
3. メイン・ペインで、パスワードを変更するユーザーを選択します。
4. 目的のユーザー名を右クリックし、コンテキスト・メニューから「**パスワードのリセット**」を選択します。
5. 表示されたダイアログで、変更後のパスワードを入力および再入力し、「**OK**」をクリックします。

ユーザーの削除

この項では、Active Directory Server でユーザーを削除する方法について説明します。

1. 「Active Directory ユーザーとコンピュータ」コンソールを開きます。
2. 左側のツリーで「**ユーザー**」を選択します。
3. メイン・ペインで、パスワードを変更するユーザーを選択します。
4. 目的のユーザー名を右クリックし、コンテキスト・メニューから「**削除**」を選択します。
5. ポップアップ・ダイアログが表示されるので、「**はい**」をクリックします。

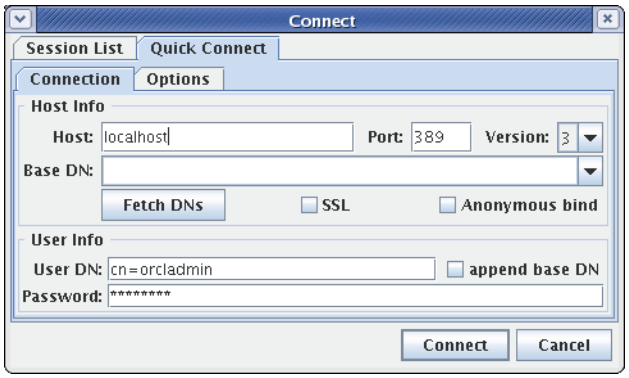
LDAP ブラウザを使用した ADS への接続

この項では、LDAP ブラウザを使用して Active Directory Server に接続する方法を示します。

注意

LDAP ブラウザでは、グループの追加、パスワードの設定およびアカウントの有効化はできません。

1. LDAP ブラウザを開きます。
2. 「**Quick Connect**」タブを選択します。
3. 次の情報を入力します。
   - **Host:** `localhost` (リモートで接続している場合は、実際のホスト名を入力します)
   - **Base DN:** `<DNS_suffix>` (DNS 名のホスト名に続く部分)
   - **Anonymous bind:** 選択解除
   - **User DN:** `administrator@<DNS_suffix>`
   - **Append base DN:** 選択解除
   - **Password:** `<ADS_password>` (175 ページの手順 12 で作成したパスワード)



4. 「**Connect**」をクリックします。

第 4 部

認証サービスのインストールおよび構成

WebCenter Sites は、認証サービスおよびシングル・サインオンを提供している、サポートされたサード・パーティ・アプリケーションと統合できます。

この部は、次の章で構成されています。

- 第 13 章「Central Authentication Service アプリケーションのクラスタ化」
- 第 14 章「Oracle Access Manager との統合のセットアップ」

第 13 章

Central Authentication Service アプリケーションのクラスタ化

WebCenter Sites では、認証およびシングル・サインオンのために、Central Authentication Service (CAS) Web アプリケーションが使用されます。また、CAS をクラスタ化して、WebCenter Sites のユーザー認証の負荷を分散することもできます。CAS Web アプリケーションは、WebCenter Sites のインストール中にデプロイされます。インストール・プロセスでは、プライマリ・クラスタ・メンバーのみが構成およびデプロイされます。追加のクラスタ・メンバーは、手動で構成およびデプロイする必要があります。

この章は、次の項で構成されています。

セカンダリ CAS クラスタ・メンバーのデプロイ

WebCenter Sites のインストーラは、プライマリ WebCenter Sites クラスタ・メンバー上にのみ CAS をデプロイするように構成されています。ユーザー認証の負荷を分散するために CAS をクラスタ化する場合は、セカンダリ CAS クラスタ・メンバーを手動で構成およびデプロイする必要があります。

開始する前に、次の点を確認してください。

- CAS クラスタリングをサポートするように、アプリケーション・サーバーが構成されていること。
- WebCenter Sites および CAS が、プライマリ・クラスタ・メンバー上に正常にインストールされていること。

これらの手順のどちらか 1 つが完了していない場合は、使用しているアプリケーション・サーバーに対応した Oracle WebCenter Sites のインストール・ガイドを参照してください。

セカンダリ CAS クラスタ・メンバーを構成してデプロイするには

1. プライマリ・メンバーの `<cs_install_dir>/bin` ディレクトリから、セカンダリ・メンバーの `<cs_install_dir>/bin` に次の構成ファイルをコピーします。
   - `cas.properties`
   - `host.properties`
   - `jbossTicketCacheReplicationConfig.xml`
2. `host.properties` ファイルで、次のプロパティを更新します。

   ```
   host.name=cas-<host name of server where cluster member will
      be deployed>-<cluster member number>
   ```

注意

各クラスタ・メンバーについて、ホスト名およびメンバー名は一意にする必要があります。たとえば、プライマリ・メンバーとセカンダリ・メンバーでは、プロパティは次のように異なります。

```
host.name=cas-10.120.12.123-1
host.name=cas-10.120.12.127-2
```

3. 次のようにして、jbossTicketCacheReplicationConfig.xml ファイルを更新します。
   - ClusterName 属性で、*TreeCache-Cluster* を一意の名前に置き換えます。

     ```
     <attribute name="ClusterName">TreeCache-Cluster
        </attribute>
     ```

     注意

     すべてのクラスタ・メンバーで、この名前を同じにする必要があります。複数の CAS クラスタを使用している場合は、必ずクラスタごとに異なる名前を使用してください。

   - ClusterConfig 属性で、次のパラメータを更新します。

     ```
     <UDP mcast_addr=multicast address
          mcast_port=multicast port
          bind_addr=host name of server where cluster member
              will be deployed
         ip_ttl=number of network hops between cluster members
          ... />
     ```

     注意

     デフォルトでは、mcast_addr パラメータは 239.555.0.0、mcast_port パラメータは 48866 に設定されています。これらの値はすべてのクラスタ・メンバーで同じである必要があるため、1 つのメンバーの値を変更した場合は、その他すべてのメンバーの値も必ず変更してください。

     デフォルトでは、ip_ttl パラメータは 0 に設定されています。クラスタ・メンバーが同じホストに存在する場合は、このデフォルト値のままにします。しかし、クラスタ・メンバーが同じサブネットに存在する場合は ip_ttl を 1 に、同じサイトに存在する場合は ip_ttl を 32 に設定します。

4. セカンダリ・クラスタ・メンバーのアプリケーション・サーバーで、CLASSPATH 環境変数に <cs_install_dir>/bin を追加します。クラス・パスが適切に設定されていない場合、CAS は起動しません。

5. プライマリ・メンバー用に生成された cas.war ファイルは、クラスタ化された汎用バージョンの CAS です。この cas.war ファイルを、セカンダリ・クラスタ・メンバーのアプリケーション・サーバーにデプロイします。

注意

WebLogic アプリケーション・サーバーを使用している場合は、セカンダリ CAS クラスタ・メンバーをデプロイする前に、(cas/WEB-INF にある) weblogic.xml ファイルの <weblogic-web-app> タグに次の行を追加します。

```
<session-descriptor>
   <persistent-store-type>replicated
   </persistent-store-type>
   <url-rewriting-enabled>true
   </url-rewriting-enabled>
</session-descriptor>
```

6. このプロセスを追加のクラスタ・メンバーごとに繰り返します。
7. WebCenter Sites メンバーの間で、CAS チケットを同期できるようにします。クラスタ・メンバーそれぞれについて、ファイル WEB-INF/classes/cas-cache.xml を次のように編集します。
   a. 行 multicastGroupPort=4666、timeToLive=0 を見つけます。
      - 各 WebCenter Sites クラスタで、ポートが一意であることを確認します (すべてのメンバーは同じポートを使用する必要があります)。
      - クラスタ・メンバーが異なる物理サーバーに常駐している場合は、timeToLive を 1 に変更します。
   b. 更新後のファイルを保存します。

新しいサーバーでの CAS の再デプロイ

注意

この項は、非クラスタ化 CAS、またはプライマリ CAS クラスタ・メンバーを対象にしています。

インストール・プロセス中、インストーラは次のファイルに CAS デプロイメント情報を書込み、WebCenter Sites を CAS に接続できるようにします。

- `WEB-INF/classes` の `SSOConfig.xml`
- `<cs_install_dir>/bin` 内の次のファイル :
  - `cas.properties`
  - `host.properties`
  - `jbossTicketCacheReplicationConfig.xml`

インストール・プロセスが完了し、新しいサーバーへの CAS の再デプロイが必要になったら、上記のファイルおよび CAS を手動で次のように再構成する必要があります。

1. CAS を、直前にデプロイされていたサーバーから削除します。
2. 新しいサーバーに `cas.war` (または、`cas.ear`) をデプロイします。CAS をクラスタ化する場合、このサーバーはプライマリ CAS クラスタ・メンバーとして定義されます。
3. `cs.war` ファイルの `WEB-INF/classes` ディレクトリにある `SSOConfig.xml` ファイルで `casURL` プロパティを更新して、WebCenter Sites を再構成し、CAS が検出されるようにします。
   - **非クラスタ CAS の場合**

     ```
     property name=casUrl value=http://<CAS host name>:<CAS
        port number>/cas
     ```

   - **プライマリ CAS クラスタ・メンバーの場合**

     ```
     property name=casUrl value=http://<load balancer host
        name>:<load balancer port number>/cas
     ```

4. 次の CAS 構成ファイルを、`<cs_install_dir>/bin` ディレクトリから新しいサーバーの任意のディレクトリにコピーします。
   - `cas.properties`
   - `host.properties`
   - `jbossTicketCacheReplicationConfig.xml`

5. 次のように CAS 構成ファイルを更新します。
   - **非クラスタ CAS の場合**
     - `cas.properties` ファイルで、次のプロパティを更新します。

       ```
       cas.securityContext.serviceProperties.service=http://
          <CAS host name>:<CAS port number>/cas/services/
          j_acegi_cas_security_check
       cas.securityContext.casProcessingFilterEntryPoint.
          loginUrl=http://<CAS host name>:<CAS port number>/
          cas/login
       cas.securityContext.ticketValidator.casServerUrlPrefix
          =http://<CAS host name>:<CAS port number>/cas
       ```

     - `host.properties` ファイルで、次のプロパティを更新します。

       ```
       host.name=cas.<CAS host name>-1
       ```

     - `jbossTicketCacheReplicationConfig.xml` ファイルで、次の操作を行います。
       - `ClusterName` 属性で、*`TreeCache-Cluster`* を一意の名前に置き換えます。

         ```
         <attribute name="ClusterName">TreeCache-Cluster
            </attribute>
         ```

       - `ClusterConfig` 属性で、次のパラメータを更新します。

         ```
         bind_addr=host name of server where cluster
            member will be deployed
         ```

   - **プライマリ CAS クラスタ・メンバーの場合**

     手順 2 および 187 ページの手順 3 の説明に従って、`host.properties` および `jbossTicketCacheReplicationConfig.xml` ファイルを更新します。
6. 新しいサーバーで、CAS 構成ファイルが保存されているディレクトリを `CLASSPATH` 環境変数に追加します。クラス・パスが適切に設定されていない場合、CAS は起動しません。

第 14 章

Oracle Access Manager との統合のセットアップ

この章では、Oracle WebCenter Sites インストールと Oracle Access Manager (OAM) の統合について説明します。

この章は、次の項で構成されています。

概要

この項は、次のトピックで構成されています。

統合コンポーネント

Oracle Access Manager との統合には、WebCenter Sites アプリケーションのシングル・サインオン (SSO) 認証プラグイン・クラスの交換、および REST クライアント認証のトークン・オーソリティ・サーブレットの追加が必要です。必要に応じて、WebCenter Sites チャレンジ (ログイン) ページもデプロイできます。

注意

コンテンツ管理 (開発) モードで実行されている WebCenter Sites システムと統合する場合、Oracle Access Manager はブラウザおよび REST 認証に使用されます。(配信モードで実行されている) 本番システムでは、OAM は REST 認証のみに使用されます。

これ以降、それぞれのコンポーネントの詳細について説明します。

1. SSO 認証プラグイン・クラスは、WebCenter Sites 製品に含まれる `wem-sso-api-oam-1.2.jar` に入れて配信されます。この JAR には 3 種類のプライマリ・クラスが含まれていますので、起動したときに、これらのクラスが Sites アプリケーションとともにロードされるように構成する必要があります。
   a. `OAMFilter` は、保護されたリソースへのアクセスを許可する前に、(WebLogic Server (WLS) 境界セキュリティまたは REST 資格証明トークンにより) 認証ユーザーを認識します。
   b. `OAMProvider` には、Sites アプリケーションからリソースを要求する前に認証済資格証明を取得するため、REST クライアント・プログラムにより使用される JAVA API が用意されています。これには、REST 資格証明を認証するために OAMFilter によって内部的に使用されるメソッドも含まれています。
   c. `OAMListener` は、セッションに関連したキャッシュ情報のクリーンアップを促進するために、HTTP セッションの作成と終了を監視するセッション・フィルタです。
2. トークン・オーソリティ・サーブレットは `oamtoken.war` ファイルに入れて配信されます。それは、OAM サーバーに対してユーザーを認証するか、または要求に応じて、OAM 認証済セッションが依然として有効であることを確認する OAM AccessGate です。

3. WebCenter Sites チャレンジ・ページはオプションで、`oamlogin.war` ファイルに入れて配信されます。`oamlogin.war` 内のサーブレットは、OAM がユーザーを認証するために資格情報の取得が必要なときに、カスタム・ブランドのチャレンジ・リクエストを提供します。これは、Central Authentication Service (CAS) とともにインストールされる標準 WebCenter Sites ブランドのログイン・ページのかわりとなるものを提供するために用意されています。このページは OAM によって直接呼び出されるもので、WebCenter Sites リソースを保護するために使用される OAM 認証スキーム内で具体的に構成する必要があります。

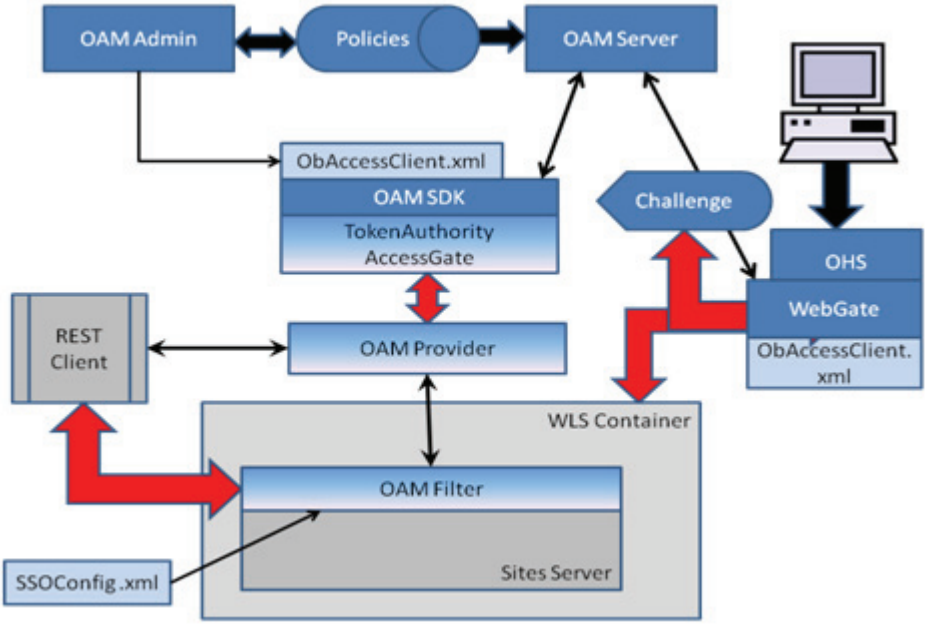
OAM および WebCenter Sites の運用可能な統合を完成させるには、これらのコンポーネントのインストールと Oracle Access Manager の構成が必要です。

OAM 統合の多くは、OAM 自体の要素の構成に関係します。OAM 構成は、主に OAM 管理コンソール内、および複数の Sites サーバー構成ファイルや Oracle HTTP Server (OHS) 構成ファイルにわたって行われます。適切な処理を行うには、ホスト識別子、URL リソース、ドメイン・ポリシーおよび OAM エージェントを適切に構成する必要があります。WebCenter Sites チャレンジ画面は、独立した HTTP サーブレットとして提供されます。WebCenter Sites チャレンジ画面、デフォルトの OAM チャレンジ画面、または構成済ポリシーに付属する認証スキームを通じたカスタム・チャレンジ画面のどれを使用するか選択できます。また、OAM 管理者コンソールを介して、認証および認可で使用されるポリシーすべてをコントロールできるため、広範な構成機能が得られます。

ブラウザ・リクエストのフロー

WebCenter Sites へのログインおよびログアウトに使用される OAM 統合コンポーネントおよびプロセス・フローを図 1 に示します。核となる統合は、OAMFilter クラスと OAMProvider クラスを中心に展開されます。これらのクラスは、Spring 初期化により WebCenter Sites Web アプリケーションに注入され、OAM では必要のない、CAS と同等のサービスに取って代わります。この統合に合わせて、Sites アプリケーションが内部的に変更されることはありません。

図 1: OAM フローチャート



ログイン処理

ブラウザ・アクセスはすべて、標準 OHS Web ゲートを通じ、WLS コンテナの提供する境界セキュリティを使用して行われます。Web ゲートは、リバース・プロキシとして機能し、Access Manager を通じて保護ポリシーを確認します。Web ゲートは、必要に応じてチャレンジ / ログイン・フォームを発行します。リクエストが WLS コンテナに直接渡されることはなく、必ず Web ゲートを通るため、満足のいく認可および認証が確実に行われます。Web ゲートから有効なリクエストを受け取ると、WLS コンテナは、OAM フィルタに ID アサーションを提示します。このアサーションにより、認証ユーザーが識別され、そのユーザーの情報が Sites の `SystemUsers` 表からフェッチされます。ユーザー情報は、Sites アプリケーション内の参照に対する適切な内部アサーションの準備に必要なユーザー ID、名前、および ACL から構成されます。認証を適切に行うには、Sites の `SystemUsers` 表にあるユーザー名と Oracle Internet Directory (または、LDAP ディレクトリ) にあるユーザー名は完全に同一である必要があります。OAM は、認可の保護機能と認証機能を持ちますが、WebCenter Sites は OAM 認証のみを使用し、完全な OAM 認可には依存していません。

OAMFilter がコントロールを受け取ったとき、リクエストは、Web ゲート、および WLS 境界セキュリティにより作成された OAM ID アサーションによりすでに認証されています。このアサーションは、認証ユーザーの名前を提供します。この名前は、Sites の SystemUsers 表からユーザー情報を検索するときに使用されます。したがって、取得された情報は、Sites アプリケーション内で使用される内部アサーションの作成に使用されます。

OAM ID アサーションから変換された内部アサーションは、その後、HTTP セッション・オブジェクトに追加されます。これにより、アプリケーション・セッションの存続期間中、後続のリクエストは、URL (リソース) に直接アクセスできるようになります。しかし、Web ゲートは、有効な OAM セキュリティ・ポリシーに基づいてオーバーライド保護を提供しています。OAM ユーザー・セッション (HTTP セッションとは異なる) の期限が切れた場合、ユーザーの再認証が必要になります。

SSO およびログオフ

Web ゲートは、SSO を制御する OAM Cookie を管理します。これは、Sites の OAM フィルタに対して透過的に行われ、その他の Oracle アプリケーションとのシームレスな統合を実現します。

WebCenter Sites のログオフが要求されたとき、標準の OAM ログオフ機能が OAM ログオフ URL により呼び出されますが、この URL には `end_URL` パラメータが含まれています。`end_URL` パラメータは、OAM がすべてのログオフ・アクティビティを終了した後に必ず表示される次のページを規定します。OAM は、SSO Cookie を削除し、OAM セッションを終了して、登録済のログアウト成功 URL を呼び出します。OAM フィルタは、ログアウト成功 URL を認識し、HTTP セッションを無効化します。OAM ログアウトがすべての作業を完了すると、ブラウザは、`end_URL` パラメータで指定された、WebCenter Sites のようこそ URL にリダイレクトされます。これにより、ログイン資格証明を提供するための新しいチャレンジがユーザーに向けてトリガされます。ログアウト URL の設定は OHS Web ゲート構成で行われます。また、`end_URL` は `SSOConfig.xml` ファイルで定義されます。

REST サービス・フロー

REST 処理は多少異なるフローに従って行われます。これは図 1 でも説明しています。REST クライアントは、OAM プロバイダ API を使用してトークン・オーソリティからサービス・チケットを入手します。このチケットは、Sites サーバーにあるリソースへのアクセス権を付与するための REST リクエストにパラメータとして指定する必要があります。TokenAuthority は OAM アクセス・ゲートとして機能します。これは、REST エンドポイント URL 用に定義されたポリシーと照らし合わせてユーザーを認証します。適切なユーザー名とパスワードで認証に合格すると、REST クライアントに対して、リソースをリクエストするときに使用できるサービス・チケットが発行されます。TokenAuthority は HTTP サーブレットの 1 つですが、SSL で保護することをお薦めします。
TokenAuthority は、次の 3 つのサービスを提供します。

- リクエスト : ユーザー名とパスワードの組合せ、および (リソースとして) エンドポイント URL を使用し、OAM SDK を通じて認証します。結果は、リクエストの OAM UserSession になります。関連するセッション・トークンは、この UserSession から抽出され、UUID をキーとするキャッシュに保持されます。この UUID は要求者に返され、この OAM セッションに関連付けられたサービス・リクエスト・チケットとして使用できるようになります。
- 検証 : リクエスト・チケットを与えると、関連するセッション・トークンがキャッシュから取得され、認証済ユーザー名が返されます。OAM UserSession をチェックし、有効性が維持されていることを確認します。このセッションが有効でなくなっている場合、またはチケットに関連付けられて

いるユーザーがもうログインしていない場合、「403 ステータス (認可されていません)」が返されます。

- 無効化 : リクエスト・チケットを与えると、関連するセッション・トークンがキャッシュから取得され、削除されて、OAM UserSession オブジェクトに変換されます。このオブジェクトは即座に終了します。これは、この OAM セッションを無効化するサービスで、リクエスト・チケットの使用後に発生します。

REST リクエストを受け取る際、OAM フィルタには常にリクエスト・チケットを提供するパラメータが必要です。このチケットは、リソースへのアクセス権が付与される前に、OAM プロバイダを通じて検証されます (SSO プロバイダはトークン・オーソリティを呼び出します)。通常のチケット・リクエストの使用は 1 回のみで、最長存続期間は OAM セッション・タイムアウトによって決まります。有効なチケットについて、OAM ユーザー・セッションがただちに無効化され、リソースへのアクセスが 1 回のみ許可されます。複数回有効のチケットも同様に処理されますが、このチケットはローカルにキャッシュされるため、限られた期間内、REST クライアントにより再利用される可能性があります。

公開済 REST API は変化しません。この統合により REST クライアント・プログラミングが影響を受けることはなく、CAS プロバイダの場合と同様に動作します。内部的には、API は、使用される認証プロバイダに応じて必要なクラスを動的にインスタンス化します。リモート REST クライアント・プログラムは JAVA で記述されており、コンパイルと実行のために `wem-sso-api-oam-1.2.jar` を必要とします。

図 1 に示すように、REST クライアントは直接、Sites サーバーに向かいます。このクライアントにはエンドポイントの選択肢が 2 つあります。図に示すとおり、Sites アプリケーションに直接進むこともできますし、OHS Web ゲートを経由することもできます。後者の場合、このエンドポイントの使用を許可するポリシーが定義されています。どちらのエンドポイントを使用するかの判断は、パフォーマンス、またはセキュリティ、もしくはこの両方を考慮して行います。

OAM 統合の前提条件

この項は、次のトピックで構成されています。

- OAM コンポーネントのインストール
- 統合に向けた OAM の準備

OAM コンポーネントのインストール

Oracle Access Manager 統合をセットアップする前に、環境のサポートに必要な Oracle コンポーネントをインストールし、正常に動作させる必要があります。OAM がすでに *Oracle WebCenter Sites の動作保証マトリックス*および本書で指定されたサポート・レベルでインストールおよび実行されている場合は、この項を無視して 203 ページの「OAM と Oracle WebCenter Sites の統合」に進んでください。それ以外の場合は、次の手順を続行します。

注意

次にリストするシステム・コンポーネントを記載されている順にインストールします。ここに示した手順は包括的なものではありません。ガイドラインとして使用してください。

適切なバージョンが使用されているかどうか注意してください。各パッケージの Oracle インストーラは、システムに特定バージョンの関連コンポーネントがインストールされていることを要件としています。バージョン要件が守られていない場合、インストーラはその特定のインストールを継続できません。リストされている各パッケージには、追加ドキュメントへのリンクが 1 つ以上含まれています。

リストされているコンポーネントはすべて、Oracle E-Delivery のサイトからダウンロードできます。これらのコンポーネントはすべてインストールされますが、OAM 統合で動作している必要があるコンポーネントは、Oracle Internet Directory Server、Oracle HTTP Server、および Oracle Access Manager Server のみです。

次の Oracle コンポーネントを掲載されている順にインストールします。

1. Oracle Database 11g バージョン 11.2.0
2. Oracle Fusion Middleware Repository Creation Utility 11g (11.1.1.5.x)
3. Oracle WebLogic Server (10.3.5) Generic および Coherence
4. Oracle Identity Management 11g (11.1.1.5.x)
5. Oracle Identity Management および Access Management 11g (11.1.1.5.0)
6. Oracle Fusion Middleware Web Tier Utilities 11g (11.1.1.2.0)
7. Oracle Access Manager WebGates (11.1.1.5.x)

Oracle Database 11*g* バージョン 11.2.0

1. Oracle Database 11*g* バージョン 11.2.0 をインストールします。

   ```
   http://docs.oracle.com/cd/E11882_01/install.112/e24321/
   toc.htm
   ```

2. Oracle 11*g* データベースを作成および構成します。具体的な手順については、第 1 章「Oracle 11g データベースの作成および構成」 *を参照して*ください。
3. 新しく作成されたデータベースで使用できるプロセスとオープン・カーソルの最大数を増やすために、sqlplus で次のコマンドを実行し、データベースを再起動します。

   ```
   alter system set processes=500 scope=spfile;
   alter system set open_cursors=800 scope=both;
   ```

Oracle Fusion Middleware Repository Creation Utility 11*g* (11.1.1.5.x)

1. 使用するデータベースが Repository Creation Utility の要件を満たしていることを確認します。

   `http://docs.oracle.com/html/E18558_01/fusion_requirements.htm#CHDJGECA`

2. Repository Creation Utility を使用してスキーマを作成します。

   `http://docs.oracle.com/cd/E12839_01/doc.1111/e14259/rcu.htm#CHDGJCGJ`

   すべてのコンポーネントを選択します。

Oracle WebLogic Server (10.3.5) Generic および Coherence

WebLogic Server をインストールします。

`http://docs.oracle.com/cd/E21764_01/doc.1111/e14142/toc.htm`

後で作成するため、ここではドメインは作成しません。

Oracle Identity Management 11*g* (11.1.1.5.x)

これには、Oracle Identity Management (11.1.1.2.0) および Oracle Identity Management 11*g* Patch Set 4 (11.1.1.5.0) が必要です。

`http://docs.oracle.com/cd/E21764_01/install.1111/e12002/instps2.htm#BGBDGICJ`

1. Oracle Identity Management 11*g* (11.1.1.2.0) をインストールします。

   構成はパッチの適用後に行う必要があるため、**「ソフトウェアのインストール - 構成なし」**を選択します。

2. Oracle Identity Management 11*g* Patch Set 4 (11.1.1.5.0) をインストールします。

3. Oracle Identity Management (11.1.1.5.0) を構成します。

   `http://docs.oracle.com/cd/E21764_01/install.1111/e12002/oid.htm#BABGDJFC`

   a. `<ORACLE_HOME>/bin/config.sh` を実行します。

      次に例を示します。

      `/u01/software/Apps/OraMiddleware/Oracle_IDM1/bin/config.sh`

   b. 「ドメインの選択」画面で**新規ドメインの作成**を選択し、構成データを提供します。

   c. 「スキーマ・データベースの指定」画面で、**「既存のスキーマの使用」**を選択し、Repository Creation Utility により作成されたスキーマが入っているデータベースの情報を含む接続文字列を入力します。

      次に例を示します。

      `localhost:1521:oamdb`

Oracle Identity Management および Access Management 11*g* (11.1.1.5.0)

1. Oracle Identity Management および Access Management 11*g* をインストールします。

   `http://docs.oracle.com/cd/E21764_01/install.1111/e10033/configtwo.htm#CEGFJHDF`

   Repository Creation Utility により作成された既存のスキーマと、198 ページの「Oracle Identity Management 11g (11.1.1.5.x)」のインストールの手順 b で作成した WebLogic ドメインを使用します。

2. 既存のドメインを拡張します。

   a. `<WL_HOME>/common/bin/config.sh` を実行します。

      次に例を示します。

      `/u01/software/Apps/OraMiddleware/wlserver_10.3/common/bin/config.sh`

   b. **「拡張」**および既存の WebLogic ドメインを選択します。

      198 ページの「Oracle Identity Management 11g (11.1.1.5.x)」のインストールの手順 b で作成したドメインを選択します。

   c. 次の製品が選択されていることを確認し、**「次へ」**をクリックします。

      Basic WebLogic Server Domain: 10.3.4.0 [wlserver_10.3]*

      Oracle Enterprise Manager: 11.1.1.0 [oracle_common]

      Oracle Access Manager with Database Policy Store: 11.1.1.3.0 [Oracle_IDM2]

      Oracle Identity Management: 11.1.1.2.0 [Oracle_IDM1]

      Oracle JRF: 11.1.1.0 [oracle_common]

   d. すべての構成が完了していることを確認します。

Oracle Fusion Middleware Web Tier Utilities 11*g* (11.1.1.2.0)

これには、Oracle Fusion Middleware Web Tier Utilities 11*g* (11.1.1.2.0) および Oracle Fusion Middleware Web Tier Utilities Patch Set 4 (11.1.1.5.0) が必要です。

1. Oracle Fusion Middleware Web Tier Utilities 11*g* (11.1.1.2.0) をインストールします。

   `http://docs.oracle.com/cd/E12839_01/doc.1111/e14260/install.htm#CHDHCJEC`

   構成はパッチの適用後に行う必要があるため、**「ソフトウェアのインストール - 構成なし」**を選択します。

2. Oracle Fusion Middleware Web Tier Utilities Patch Set 4 (11.1.1.5.0) をインストールします。

3. Oracle Fusion Middleware Web Tier Utilities 11*g* (11.1.1.5.0) を構成します。

   `http://docs.oracle.com/cd/E12839_01/doc.1111/e14260/install.htm#autoId14`

   a. `<WEB_TIER_ORACLE_HOME>/bin/config.sh` を実行します。

次に例を示します。

```
/u01/software/Apps/OraMiddleware/Oracle_WT1/bin/config.sh
```

b. 「コンポーネントの構成」画面で、**「Oracle HTTP Server」**、**「Oracle Web Cache」**および**「選択されたコンポーネントと WebLogic ドメインの関連付け」**を選択し、構成データを提供します。

c. WebLogic ドメインの指定画面で、198 ページの「Oracle Identity Management 11g (11.1.1.5.x)」のインストールの手順 b で作成したドメインを選択します。

Oracle Access Manager WebGates (11.1.1.5.x)

OAM Access Manager Web ゲートのドキュメントは、次の場所にあります。

```
http://docs.oracle.com/cd/E21764_01/install.1111/e12002/
webgate.htm
```

1. サード・パーティの GCC ライブラリをインストールします。

   a. 64 ビット・システムで Oracle Access Manager WebGates をインストールするには、あらかじめ、システムの任意のディレクトリに `libgcc_s.so.1` および `libstdc++.so.6` バージョン 3.4.6 の 64 ビット・ライブラリを入れておく必要があります。

   b. 次のコマンドを実行し、出力が常に 0 より大きいことを確認します。

   ```
   strings -a libgcc_s.so.1 | grep -c "GCC_3.0"
   strings  -a libgcc_s.so.1  | grep -v "GCC_3.3.1" | grep -c
      "GCC_3.3"
   strings -a libgcc_s.so.1 | grep -c "GCC_4.2.0"
   file  libgcc_s.so.1 | grep "64-bit" | grep -c "x86-64"
   file  libstdc++.so.6  |  grep "64-bit" | grep -c "x86-64"
   ```

2. Oracle Access Manager WebGates (11.1.1.5.0) をインストールします。

3. OAM Access Manager WebGates のドキュメントの第 20.4 項にあるインストール後の手順を完了します。

   ```
   http://docs.oracle.com/cd/E21764_01/install.1111/e12002/
   webgate.htm#autoId11
   ```

注意

この例では、Oracle Identity Management とともにインストールされている Oracle HTTP Server と Web ゲートが使用されています。

パラメータとその値の例は次のとおりです。

```
<MW_HOME>
/u01/software/Apps/OracleMiddleware


<Webgate_Home> および <Webgate_Oracle_Home>
/u01/software/Apps/OraMiddleware/Oracle_OAMWebGate1


<Webgate_Instance_Directory>
/u01/software/Apps/OraMiddleware/asinst_1/config/OHS/ohs1


<Oracle_Home_for_Oracle_HTTP_Server>
/u01/software/Apps/OraMiddleware/Oracle_IDM1
```

統合に向けた OAM の準備

1. WebLogic 管理サーバーを起動します。

   ```
   <domain_home>/bin/startWebLogic.sh
   ```

   次に例を示します。

   ```
   /u01/software/Apps/OraMiddleware/user_projects/domains/
      OAMDomain/bin/startWebLogic.sh
   ```

2. WebLogic ノード・マネージャを起動します。

   ```
   <weblogic_home>/server/bin/startNodeManager.sh
   ```

   次に例を示します。

   ```
   /u01/software/Apps/OraMiddleware/wlserver_10.3/server/bin/
      startNodeManager.sh
   ```

3. Enterprise Manager のファーム・アプリケーションを表示します。

   a. ブラウザで次の URL に移動します。

      ```
      http://<weblogic_admin_host>:<weblogic_admin_port>/em
      ```

   b. WebLogic Server の資格証明を使用してログインします。

   c. Farm_<your_domain> で、「WebLogic ドメイン」、<your_domain> の順に開きます。

      AdminServer、oam_server1、wls_ods1 および wls_oif1 が表示されます。これは、WebLogic 管理サーバー、Oracle Access Manager Server Web アプリケーション、Oracle Directory Server Web アプリケーション、および Oracle Identity Federation Server Web アプリケーションです。

d. 「Identity and Access」を開きます。

OAM、oid1 および ovd1 が表示されます。

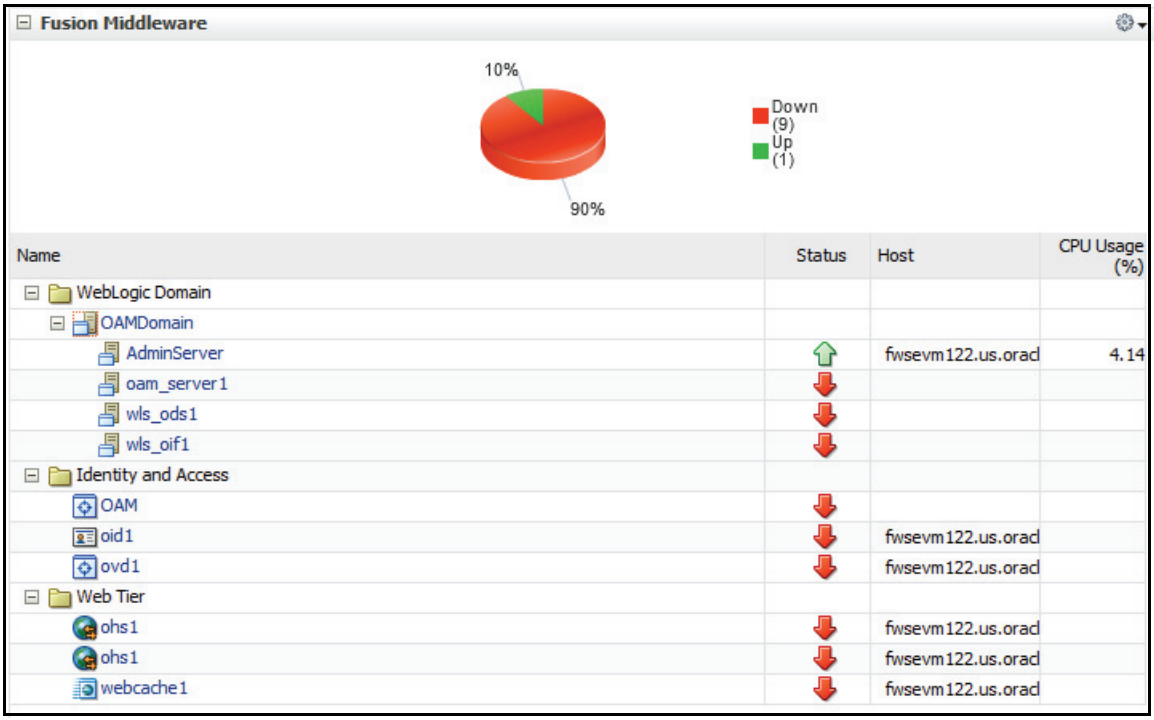
これは、Oracle Access Manager Server、Oracle Internet Directory Server、および Oracle Virtual Directory Server です。

e. 「Web 層」を開きます。

ohs1、ohs1 および webcache1 が表示されます。

これは、Web 層とともにインストールされている Oracle HTTP Server、Identity Management とともにインストールされている Oracle HTTP Server、および Web キャッシュ・サーバーです。

f. 右側には、Fusion Middleware の下に、各アプリケーションおよびサーバーのステータスが表示されます。現在、AdminServer のみ実行中と表示されています。



4. Oracle Access Manager を起動します。

a. ファーム・アプリケーションから次の操作を実行します。

1) Fusion Middleware の下の「**oam_server1**」をクリックします。

2) oam_server1 の下にある「**WebLogic Server**」をクリックします。ドロップダウン・メニューが表示されます。

3) 「**コントロール**」の上にカーソルを重ねて、「**起動**」をクリックします。

4) 起動が完了すると、ステータス矢印が緑色に変わります。

b. WebLogic 管理コンソールから次の操作を実行します。

1) 「**サーバー**」をクリックします。

2) 「**コントロール**」タブをクリックします。

3) 「**oam_server1**」チェック・ボックスを選択して、「**起動**」をクリックします。

4) 起動の完了後、「**サーバー**」をもう一度クリックすると、「状態」に「実行中」と表示されます。

c. OAM コンソールに移動します。

1) ブラウザで次の URL に移動します。

```
http://<weblogic_host>:<weblogic_admin_port>/oamconsole
```

2) WebLogic Server の資格証明を使用してログインします。

3) 統合には OAM コンソールへのアクセスが必要です。

OAM と Oracle WebCenter Sites の統合

この項は、次のトピックで構成されています。

開始する前に

WebCenter Sites と OAM 認証の統合では、考慮しなければならない重要な点がいくつかあります。

- この章ではこれまで、OAM と Oracle WebCenter Sites の統合に必要な必須ソフトウェアと関連コンポーネントについて説明してきました。この章をレビューしておらず、また必須コンポーネントがインストールされ、適切にセットアップされていることを確認していない場合は、このドキュメントを読み直してください。
- WebCenter Sites がインストールされ、デフォルトの CAS で適切に動作している必要があります。

> **注意**
>
> WebCenter Sites のロールを格納するために LDAP サーバーの使用を計画している場合は、OAM 統合の前に、この構成を完了する必要があります。
>
> ユーザーの重複が問題である場合は、WebCenter Sites と OAM に同じ LDAP サーバーを使用できます。

- OAM 統合には、Oracle HTTP Server、Oracle Internet Directory Server および Oracle Access Manager Server の実行が必要です。

- セットアップ・アクティビティの大半では、Oracle Access Manager 管理コンソール (OAMCONSOLE) アプリケーションが必要です。この機能を使用する権限を持っていることを確認してください。

この章の残りの部分では統合プロセスについて説明します。統合プロセスは複数の手動による手順から構成されており、これらの手順を記述されているとおりに実行する必要があります。

統合手順

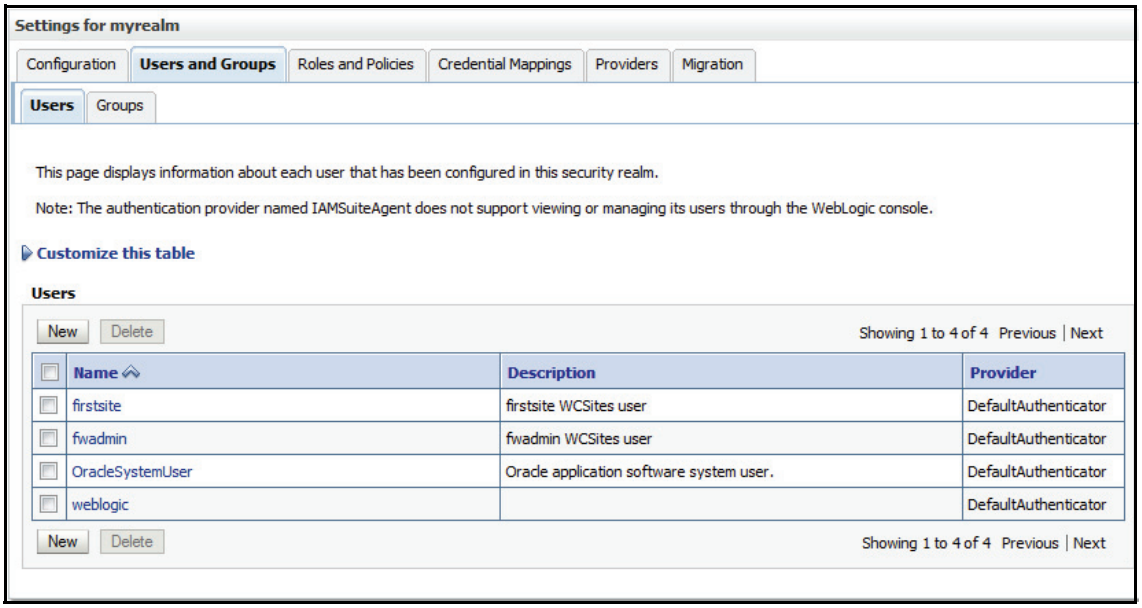
1. OAM ユーザー・アイデンティティ・ストアで Sites ユーザーを定義します。

> **注意**
>
> OAM は認証にのみ使用されます。OAM 認可には依存しません。Oracle Internet Directory および Oracle Directory Server などもユーザー・アイデンティティ・ストアとして使用できますが、デフォルトは Oracle WebLogic Embedded LDAP で、この章の残りの部分でユーザー・アイデンティティ・ストアとして使用されます。ユーザー名は、Sites の `SystemUsers` 表にあるユーザー名と一致する必要があります。

OAM では、認証ポリシーおよび認可ポリシーが強制されます。WebCenter Sites は、リソースの保護に認証ポリシーのみを使用します。WebCenter Sites は独自の認可ポリシーを使用しています。

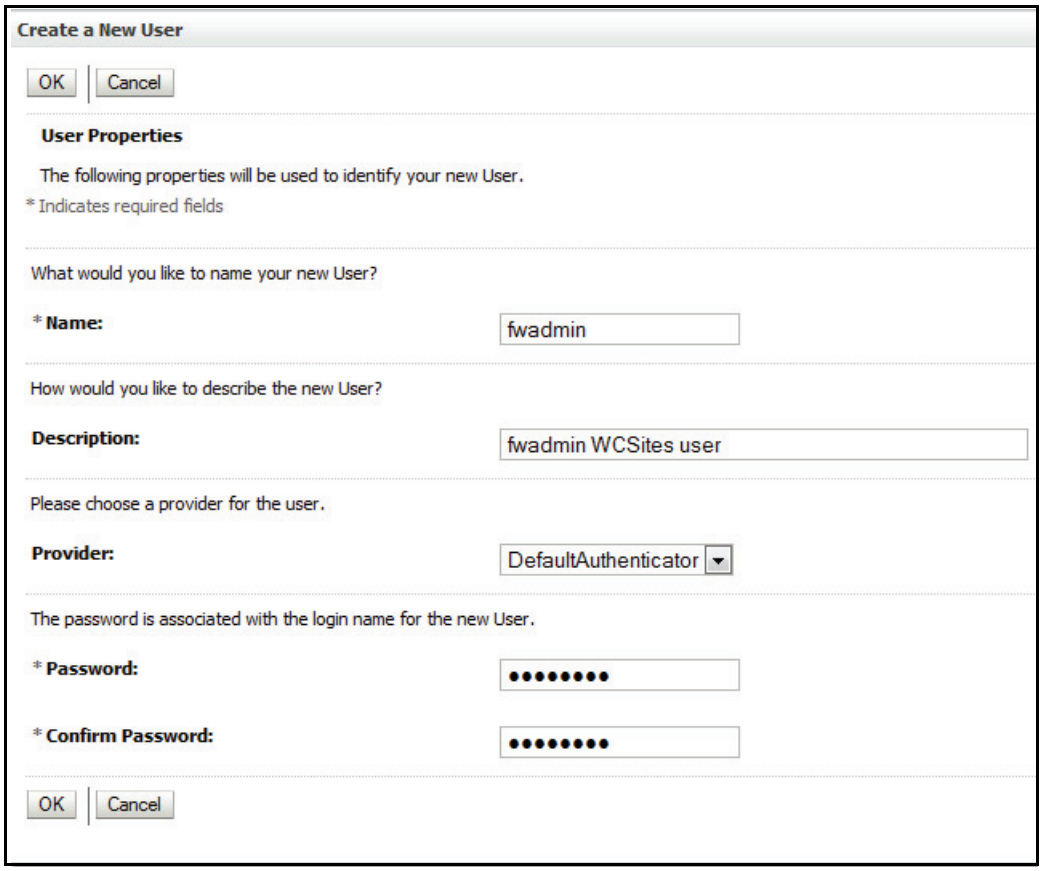
Oracle WebLogic Embedded LDAP のユーザー名は、WebCenter Sites の `SystemUsers` 表にあるユーザー名と一致する必要があります。WebLogic 組込み LDAP にユーザーを追加する手順は、次のとおりです。

a. WebLogic 管理コンソールにログインします。
b. 「**セキュリティ・レルム**」をクリックします。
c. 「**myrealm**」をクリックします。
d. 「**ユーザーとグループ**」タブを選択します。



追加されるユーザーごとに、次の手順を完了します。

1) 「**新規**」をクリックします。
2) ユーザー名を入力します。
3) ユーザーの説明を入力します。
4) プロバイダの **DefaultAuthenticator** を選択します。
5) ユーザーのパスワードを入力します。
6) ユーザーのパスワードをもう一度入力します。
7) 「**OK**」をクリックします。

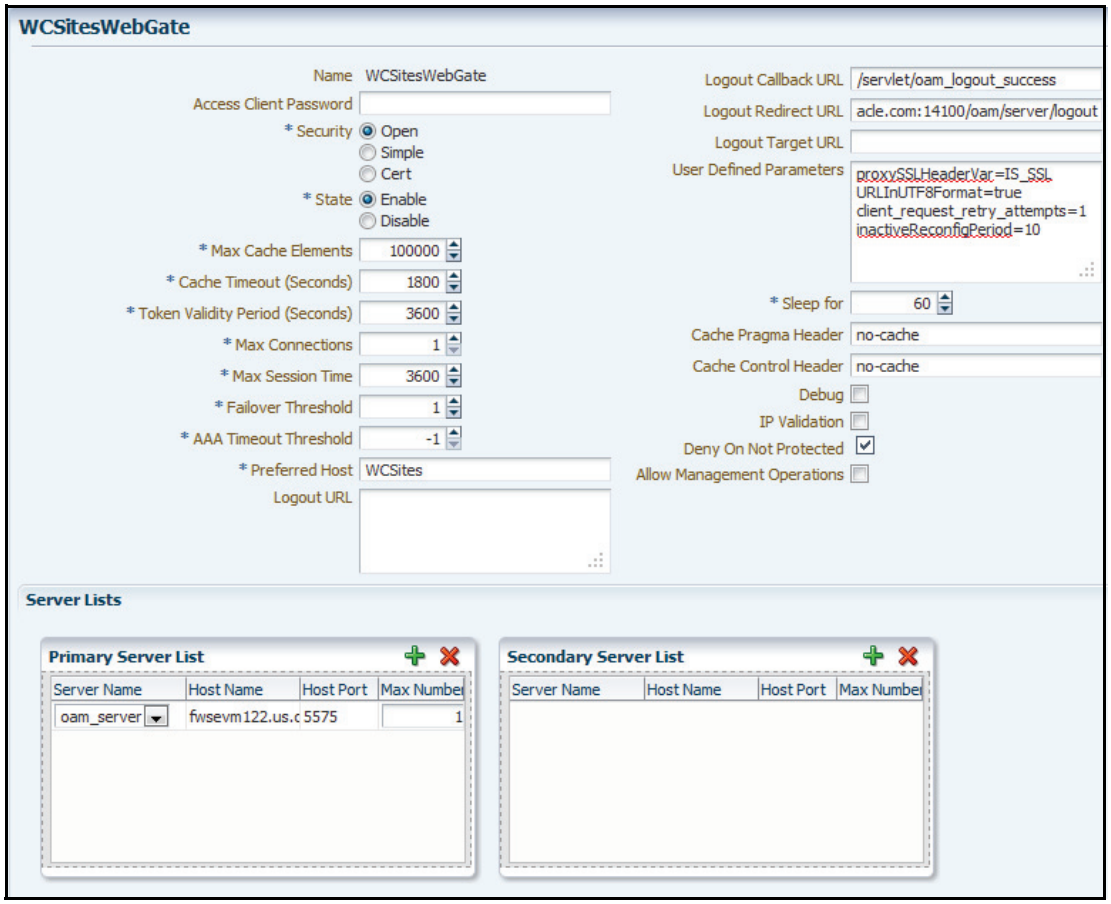


2. OHS でのデプロイメント用に OAM Web ゲート・エージェントを作成します。
   a. OAM コンソール・アプリケーションにログインします。
      `http://<weblogic_host>:<weblogic_admin_port>/oamconsole`
   b. **「システム構成」**タブを選択します。
   c. 「SSO エージェント」の**「新規 OAM 11g Web ゲート」**をクリックします。
   d. 「名前」に、`WCSitesWebGate` と入力し、**「適用」**をクリックします。
   e. 「優先ホスト」に、`WCSites` と入力します。
   f. 「ログアウト・コールバック URL」に、`/<sites context root>/oam_logout_success` と入力します。
   g. 「ログアウト・リダイレクト URL」に、`http://<weblogic_host>:<oam_server_port>/oam/server/logout` と入力します。
   h. **「適用」**をクリックします。
   i. 新しく作成した Web ゲート構成ファイル (ObAccessClient.xml および cwallet.sso) を OHS 構成にコピーします。
      `cp <domain_home>/output/WCSitesWebGate/*`

```
<ohs_instance_home>/config/OHS/ohs1/webgate/config
```

次に例を示します。

```
cp /u01/software/Apps/OraMiddleware/user_projects/domains/
   OAMDomain/output/WCSitesWebGate/*
/u01/software/Apps/OraMiddleware/asinst_1/config/OHS/ohs1/
   webgate/config
```

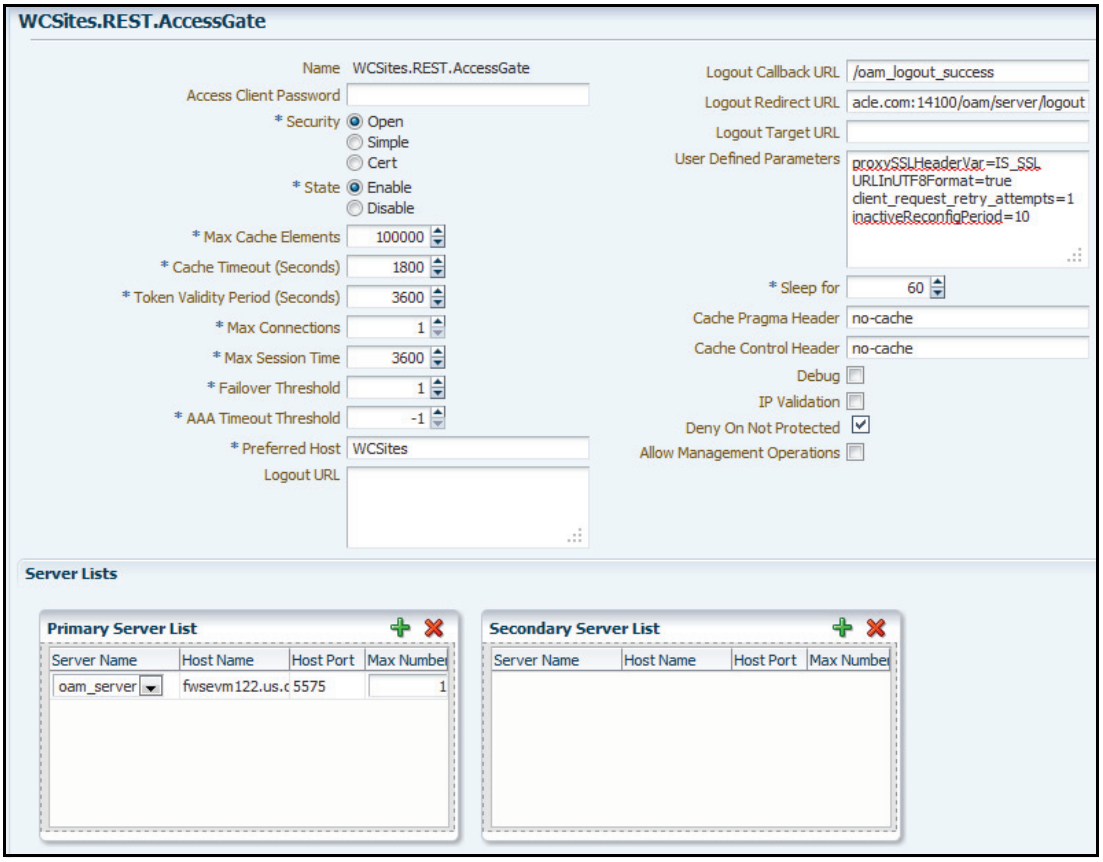


3. oamtoken Web アプリケーションでのデプロイメント用に OAM Web ゲート・エージェントを作成します。
   a. OAM コンソール・アプリケーションにログインします。
      `http://<weblogic_host>:<weblogic_admin_port>/oamconsole`
   b. **「システム構成」**タブをクリックします。
   c. 「SSO エージェント」の**「新規 OAM 11g Web ゲート」**をクリックします。
   d. 「名前」に、`WCSites.REST.AccessGate` と入力し、**「適用」**をクリックします。
   e. 「優先ホスト」に、`WCSites` と入力します。
   f. 「ログアウト・コールバック URL」に、`/oam_logout_success` と入力します。

g. 「ログアウト・リダイレクト URL」に、`http://<weblogic_host>:<oam_server_port>/oam/server/logout` と入力します。

h. **「適用」**をクリックします。

Web ゲート構成ファイルは、手順 5 でコピーされます。



4. WebCenter Sites 用ホスト識別子を作成します。

a. 「ホスト識別子」で、WCSites をチェックします。WCSites が存在する場合は、**「WCSites」**をダブルクリックし、手順 e に進みます。それ以外の場合は、手順 b に進みます。

b. **「ホスト識別子」**をクリックします。

c. **「作成」**アイコンをクリックします。

d. 「名前」に、WCSites と入力します。

e. 「説明」に、「これは WebCenter Sites のホスト識別子です。」と入力します。

f. 操作パネルで、**「追加」**(+) アイコンをクリックし、「ホスト名」に WCSites と入力します。

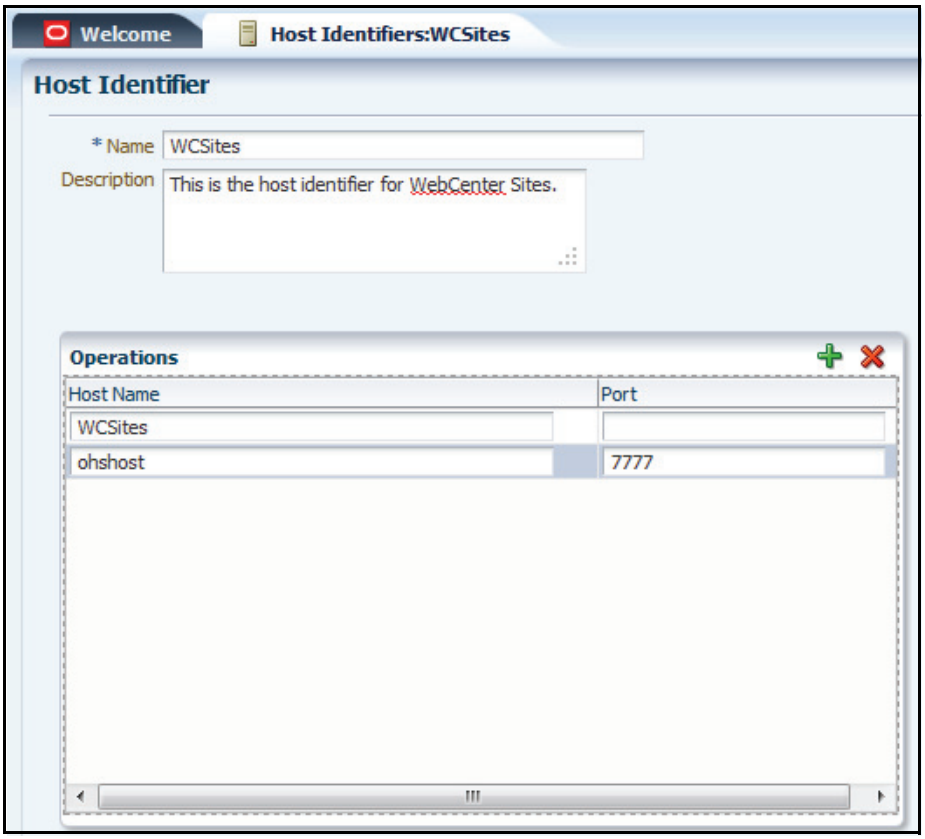
注意

ここで指定したホスト名は、Web ゲートで指定された優先ホストと一致する必要があります。

g. 「追加」(+) アイコンをもう一度クリックし、「ホスト名」に OHS サーバーのホスト名、「ポート」に OHS サーバーのポートを入力します。

ロード・バランシング配置で複数のホストを使用している場合、OHS インスタンスそれぞれについて、この手順を繰り返します。

h. 「適用」をクリックします。



5. `oamtoken.war` ファイルをデプロイします。

a. `oamtoken.war` ファイルのデプロイ元となるディレクトリを作成し、このディレクトリへ、Sites インストーラの `wem` ディレクトリから `oamtoken.war` ファイルを展開します。

次に例を示します。

```
mkdir /u01/software/Apps/Weblogic1035/user_projects/domains/
   OAMCSDomain/applications/oamtoken


cd /u01/software/Apps/Weblogic1035/user_projects/domains/
   OAMCSDomain/applications/oamtoken
```

```
jar -xvf /u01/CS/installation_files/ContentServer/wem/
   oamtoken.war
```

b. 手順 2 で作成した Web ゲート構成ファイルを、展開した oamtoken Web アプリケーションの `WEB-INF/oblix/lib` ディレクトリにコピーします。既存のファイルはすべて上書きします。

Web ゲート構成ファイルは、OAM がデプロイされているシステムの `<domain_home>/output/ WCSites.REST.AccessGate/ ObAccessClient.xml` にあります。

c. 下の xml を使用して、展開した oamtoken Web アプリケーションの `WEB-INF/classes` ディレクトリに、`tokenauthority.xml` という名前のファイルを作成します。展開した oamtoken Web アプリケーションの `WEB-INF` ディレクトリの場所をポイントするように、`oblixPath` プロパティの値を変更します。oamtoken Web アプリケーションを別の場所にデプロイする場合は、新しいデプロイ先を反映するように `oblixPath` プロパティを変更する必要があります。

次に例を示します。

```
/u01/software/Apps/Weblogic1035/user_projects/domains/
   OAMCSDomain/applications/oamtoken/WEB-INF
```

```
   tokenauthority.xml:
<?xml version="1.0" encoding="UTF-8"?>

<beans xsi:schemaLocation="http://www.springframework.org/
   schema/beans http://www.springframework.org/schema/beans/
   spring-beans-2.0.xsd" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance" xmlns="http://www.springframework.org/
   schema/beans">

   <bean class="com.fatwire.wem.sso.oam.token.TokenConfig"
   id="configuration">

     <property value="{path_to_oamtoken_WEB-INF_directory}"
   name="oblixPath"/>

   </bean>

 </beans>
```

d. 展開済の oamtoken Web アプリケーションをデプロイします。

注意

WebLogic で、現在の場所からデプロイメントにアクセスできるようにします。

oamwebtoken Web アプリケーションに含まれるサーブレットは、表示可能なユーザー名とパスワード資格証明を使用して呼び出すことができます。このアプリケーションは、SSL を使用して保護された Web アプリケーションとしてデプロイすることをお薦めします。

6. oamlogin.war ファイルをデプロイします。

この Web アプリケーションには、WebCenter Sites チャレンジ・ページが含まれます。

注意

この手順はオプションです。デフォルトの OAM フォームまたは別のカスタム・ログイン・フォームを使用している場合は省略できます。

a. oamlogin.war ファイルのデプロイ元となるディレクトリを作成し、このディレクトリへ、Sites インストーラの wem ディレクトリから oamlogin.war ファイルを展開します。

次に例を示します。

```
mkdir /u01/software/Apps/Weblogic1035/user_projects/domains/
   OAMCSDomain/applications/oamlogin


cd /u01/software/Apps/Weblogic1035/user_projects/domains/
   OAMCSDomain/applications/oamlogin


jar -xvf /u01/CS/installation_files/ContentServer/wem/
   oamlogin.war
```

b. 下のコードを使用して、展開した oamlogin Web アプリケーションの WEB-INF/classes ディレクトリに、wemsites_settings.properties という名前のファイルを作成します。< > で囲まれている変数を、使用している環境に適した値で置き換えます。

```
oamredirect=http://<weblogic_host>:<oam_server_port>/oam/
   server/auth_cred_submit
oamlogout=http://<weblogic_host>:<oam_server_port>/oam/
   server/logout

forgotpassword=<email_account>@<email_domain>
```

注意

oamredirect プロパティが正しく設定されていない場合、ユーザー名とパスワードの認証は失敗します。

c. 展開済の oamlogin Web アプリケーションをデプロイします。

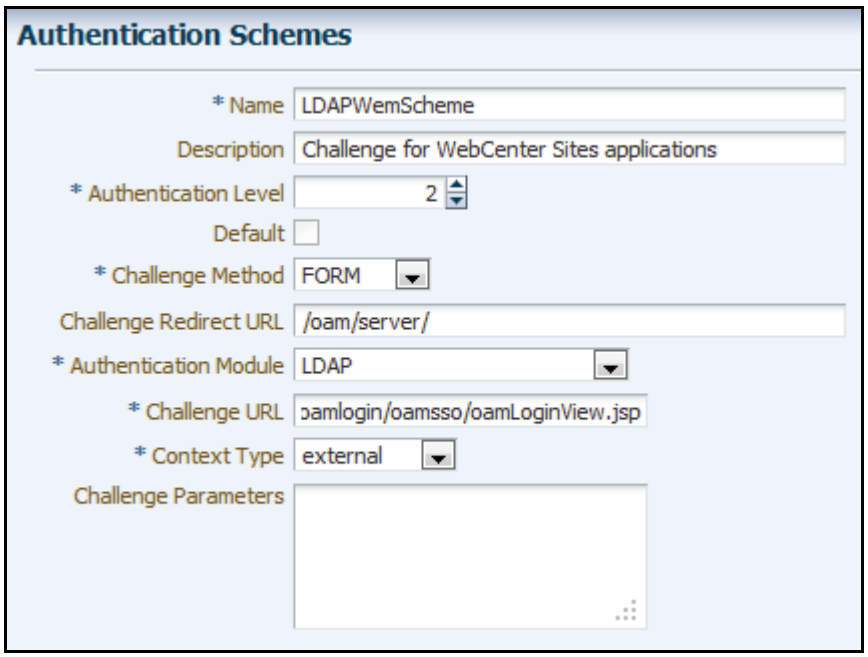
注意

WebLogic で、現在の場所からデプロイメントにアクセスできるようにします。

7. WebCenter Sites チャレンジ・ページにリダイレクトする認証スキームを作成します。

> **注意**
>
> この手順はオプションです。デフォルトの OAM フォームまたは別のカスタム・ログイン・フォームを使用している場合は省略できます。

   a. OAM コンソール・アプリケーションにログインします。
      `http://<weblogic_host>:<weblogic_admin_port>/oamconsole`
   b. **「認証スキーム」**をクリックし、**「作成」**をクリックします。
   c. 認証スキームの名前を入力します。
   d. 説明として、「WebCenter Sites アプリケーション用チャレンジ」と入力します。
   e. 「認証レベル」に 2 を入力します。
   f. 「チャレンジ・メソッド」で**「FORM」**を選択します。
   g. 「チャレンジ・リダイレクト URL」に `/oam/server/` と入力します。
   h. 「認証モジュール」で**「LDAP」**を選択します。
   i. 「チャレンジ URL」に `http://<oamlogin_app_server_host>:<oamlogin_port>/oamlogin/oamsso/oamLoginView.jsp` と入力します。
   j. 「コンテキスト・タイプ」で**「外部」**を選択します。
   k. **「適用」**をクリックします。



8. mod_wl_ohs.conf OHS 構成ファイルをセットアップします。

このファイルは、前述の手順で使用した OHS インスタンスの ohs1 ディレクトリに入っています。

次に例を示します。

```
/u01/software/Apps/OraMiddleware/asinst_1/config/OHS/ohs1/
   mod_wl_ohs.conf
```

後述のように、このファイルに、/oamlogin コンテキスト・ルート (Sites チャレンジ・ページを使用する場合のみ必須) および Sites コンテキスト・ルートに対する別のエントリを追加する必要があります。WebLogicHost および WebLogicPort の値は、指定された Web アプリケーションが常駐しているアプリケーション・サーバーのホスト名およびポートです。

```
# NOTE : This is a template to configure mod_weblogic.
LoadModule weblogic_module   "${ORACLE_HOME}/ohs/modules/
   mod_wl_ohs.so"
# This empty block is needed to save mod_wl related
   configuration from EM to this file when changes are made at
   the Base Virtual Host Level
<IfModule weblogic_module>
#      WebLogicHost {WEBLOGIC_HOST}
#      WebLogicPort {WEBLOGIC_PORT}
#      Debug ON
#      WLLogFile /tmp/weblogic.log
#      MatchExpression *.jsp
</IfModule>
<IfModule weblogic_module>
 <location /oamlogin>
  SetHandler weblogic-handler
  WebLogicHost {name|IP of WebLogic server where Sites is
   deployed}
  WebLogicPort 7002
 </location>
</IfModule>
<IfModule weblogic_module>
 <location /servlet>
  SetHandler weblogic-handler
  WebLogicHost {hostname|IP of WebLogic server where Sites is
   deployed}
  WebLogicPort 7001
 </location>
</IfModule>
# <Location /weblogic>
#      SetHandler weblogic-handler
#      PathTrim /weblogic
#      ErrorPage  http:/WEBLOGIC_HOME:WEBLOGIC_PORT/
#  </Location>
```

注意

http.conf ファイルに、mod_wl_ohs.conf ファイルのインクルード文が存在することを確認します。

次に例を示します。

```
include "/u01/software/Apps/OraMiddleware/asinst_1/
config/
   OHS/ohs1/mod_wl_ohs.conf"
```

9. HTTP サーバー、Internet Directory サーバーおよび仮想ディレクトリ・サーバーを起動します。

注意

これは Oracle Identity Management とともにインストールされ、このガイド全体で使用されている HTTP サーバーです。

   a. 次のコマンドを入力します。

      1) `export ORACLE_INSTANCE=/u01/software/Apps/OraMiddleware/asinst_1`

      2) `/u01/software/Apps/OraMiddleware/Oracle_IDM1/opmn/bin/opmnctl startall`

   b. Enterprise Manager のファーム・アプリケーションからは、Oracle Internet Directory Server (oid1)、Oracle Virtual Directory Server (ovd1)、および Oracle Identity Management とともにインストールされた OHS (ohs1) が起動されたことがわかります。

10. この手順では、WebCenter Sites デプロイメントの SSOConfig.xml ファイルを変更します。このファイルは、ロードされる認証クラスを制御するとともに、それらのクラスで必要とされる様々なプロパティを制御します。

   a. デプロイされた WebCenter Sites アプリケーションのデプロイされた WEB-INF/classes ディレクトリにある SSOConfig.xml ファイルのバックアップを作成します。

      次に例を示します。

      ```
      /u01/software/Apps/Weblogic1035/user_projects/domains/
         OAMCSDomain/applications/CS/WEB-INF/classes/SSOConfig.xml
      ```

   b. SSOConfig.xml を次のファイルのように変更します。

注意

次のファイルでは、serviceUrl、ticketUrl、signoutURL、dbUsername および dbPassword プロパティを設定します。

signoutUrl プロパティでは、WebCenter Sites ログアウトを呼び出すときに使用する URL を指定します。この URL には、OAM によるログアウト処理がすべて完了した後でブラウザが復帰する、エンコードされた URL を含めます。

dbUsername および dbPassword プロパティには、WebCenter Sites 全体管理者の資格証明を入力できます (デフォルトは fwadmin および xceladmin です)。これらのプロパティの値は、WebCenter Sites アプリケーションの起動時に暗号化されます。

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:context="http://www.springframework.org/schema/
   context"
    xsi:schemaLocation="
        http://www.springframework.org/schema/beans http://
   www.springframework.org/schema/beans/spring-beans-2.5.xsd
        http://www.springframework.org/schema/context http://
   www.springframework.org/schema/context/spring-context-
   2.5.xsd">
  <!-- Single Sign On provider -->
  <bean id="ssoprovider"
class="com.fatwire.wem.sso.oam.OAMProvider">
  <property name="config" ref="ssoconfig" />
  </bean>
  <!-- Single Sign On filter -->
  <bean id="ssofilter"
class="com.fatwire.wem.sso.oam.filter.OAMFilter">
  <property name="config" ref="ssoconfig" />
  <property name="provider" ref="ssoprovider" />
  </bean>
  <!-- Single Sign On listener -->
  <bean id="ssolistener"
class="com.fatwire.wem.sso.oam.listener.OAMListener">
  </bean>
  <!-- Single Sign On configuration -->
  <bean id="ssoconfig"
class="com.fatwire.wem.sso.oam.conf.OAMConfig">

  <!-- URL prefix for REST service endpoint -->
   <property name="serviceUrl" value="http://
{OHS_host}:{OHS_port}/{Sites_context_root}/REST" />

  <!-- URL prefix for Token Service servlet -->
   <property name="ticketUrl" value="http://
{oamtoken_app_server_host}:{oamtoken_port}/oamtoken" />
```

```
  <!-- URL to be called when WEM logout is required. -->
   <property name="signoutUrl" value="http://
{weblogic_host}:{oam_server_port}/oam/server/
logout?end_url=http%3A%2F%2F{OHS_host}%3A{OHS_port}%2F{Sites_co
ntext_root}%2Fwem%2Ffatwire%2Fwem%2FWelcome />

        <!-- Do not proxy tickets, tt's the last server in the
call chain -->
    <property name="proxyTickets" value="false" />

    <!-- Database Credentials needed by user lookup in
OAMFilter -->
    <property name="dbUsername" value="{user with authority to
read the WebCenter Sites SystemUser table}" />

    <property name="dbPassword" value="{above users password}"
/>

     <!-- Your application protected resources (relative to
applicationUrl) -->
    <property name="protectedMappingIncludes">
      <list>
               <value>wem/fatwire/**</value>
               <value>/faces/jspx/**</value>
               <value>/ContentServer?[pagename=OpenMarket/
   Xcelerate/UIFramework/LoginPage|OpenMarket/Xcelerate/
   UIFramework/ShowMainFrames|fatwire/getAllUserGroups|fatwire/
   getAllSecurityConfigs|rest/asset,#]</value>
               <value>Satellite?[pagename=fatwire/
   insitetemplating/request|OpenMarket/Xcelerate/ControlPanel/
   Request|OpenMarket/Xcelerate/ControlPanel/EditPanel|fatwire/
   wem/ui/Ping|fatwire/wem/sso/validateMultiticket|OpenMarket/
   Xcelerate/UIFramework/ShowPreviewFrames,#]</value>
      </list>
    </property>
        <property name="protectedMappingStatelessIncludes">
      <list>
               <value>/REST/**</value>
      </list>
    </property>
    <!-- Your application protected resources excludes
(relative to applicationUrl) -->
    <property name="protectedMappingExcludes">
      <list>
               <value>/wem/fatwire/wem/ui/SysLocStrSvc</value>
      </list>
    </property>
  </bean>

</beans>
```

11. wem-sso-api-oam-1.2.jar ファイルを WebCenter Sites デプロイメントにコピーします。

    このファイルは Sites インストーラの wem ディレクトリにあります。これを、デプロイされた Sites アプリケーションの WEB-INF/lib ディレクトリにコピーする必要があります。

    次に例を示します。

    ```
    cp /u01/CS/installation_files/ContentServer/wem/wem-sso-api-
       oam-1.2.jar /u01/software/Apps/Weblogic1035/user_projects/
       domains/OAMCSDomain/applications/CS/WEB-INF/lib
    ```

残りの手順では、WebCenter Sites アプリケーションを保護するために必要なポリシー構成を Oracle Access Manager コンソールから行います。

12. WebCenter Sites 用アプリケーション・ドメインを作成します。
    a. **「アプリケーション・ドメイン」**をクリックし、**「作成」**アイコンをクリックします。
    b. 「名前」に、WebCenterSites と入力します。
    c. 「説明」に、「これは WebCenter Sites のアプリケーション・ドメインです。ここにすべてのリソースおよびポリシーが保存されています。」と入力します。
    d. **「適用」**をクリックします。

手順手順 13 - 15 では、WebCenter Sites アプリケーション・ドメインの認証ポリシーを作成します。

次の認証ポリシーを作成する必要があります。

- ブラウザ用の保護済リソース・ポリシー
- REST クライアント用の保護済リソース・ポリシー
- 保護されていないパブリック・リソース・ポリシー

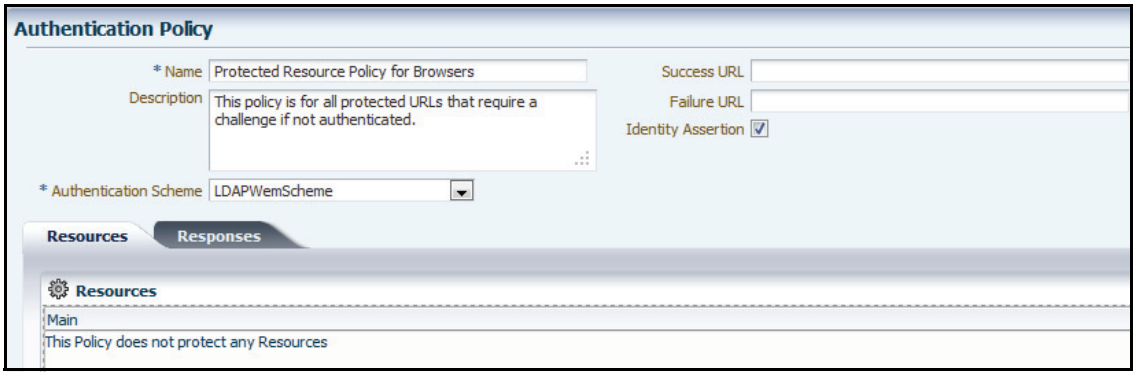
これらのポリシーは Web ゲートにより強制されます。最初の 2 つのポリシーは、アクセスの対象であり、まだ認証されていない場合はチャレンジを必要とするリソースすべてに適用されます。3 つめのポリシーは、認証を必要としないリソースすべてに適用されます。3 つめのポリシーで定義されるリソースは認証を必要としませんが、特定のポリシー・ディレクティブに従っています。認証を必要としないオブジェクト (たとえば、グラフィカル・イメージ、アニメーション、一般に公開されているページ) は、Web ゲートには無視されますが、リバース・プロキシで適切に機能させるには宣言が必要です。

注意

認証ポリシーはリソースなしで作成されます。リソースは後半の手順で追加されます。

13. ブラウザ用の保護済リソース・ポリシーを作成します。
    a. 217 ページの手順 12 で作成した WebCenterSites アプリケーション・ドメインを展開します。
    b. **「認証ポリシー」**をクリックします。
    c. **「作成」**アイコンをクリックします。
    d. 「名前」に、「ブラウザ用保護済リソース・ポリシー」と入力します。
    e. 「説明」に、「このポリシーは、認証されていない場合にチャレンジを要求される保護済 URL すべてで使用されます。」と入力します。
    f. 「認証スキーム」には、WebCenter Sites チャレンジ・ページを使用している場合は**「LDAPWemScheme」**を選択します。デフォルトの OAM ログイン・フォームを使用している場合は**「LDAPScheme」**を、他のカスタム・ログイン・フォームを使用している場合は別のスキームを選択します。

       LDAPWemScheme は、212 ページの手順 7 で作成した認証スキームです。
    g. **「ID アサーション」**チェック・ボックスを選択します。



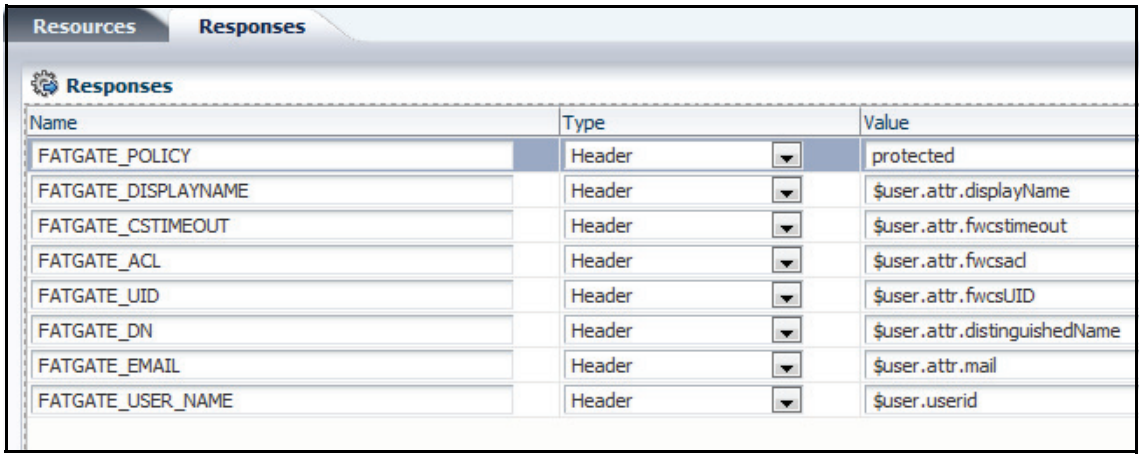
認証ポリシーが満たされると、レスポンスを作成できるようになります。このレスポンスは、WebCenter Sites HTTP フィルタが LDAP 属性を認識し、認証されたユーザーに関する情報を提供するために必要です。これ以降の手順では、**「レスポンス」**タブにレスポンスを追加します。

    h. **「レスポンス」**タブをクリックします。
    i. **「追加」**(+) アイコンをクリックします。
    j. 「名前」を入力し、「タイプ」を選択して「値」を入力します。

       エントリ FATGATE_POLICY および FATGATE_EMAIL について、手順 i および j を繰り返します。

注意

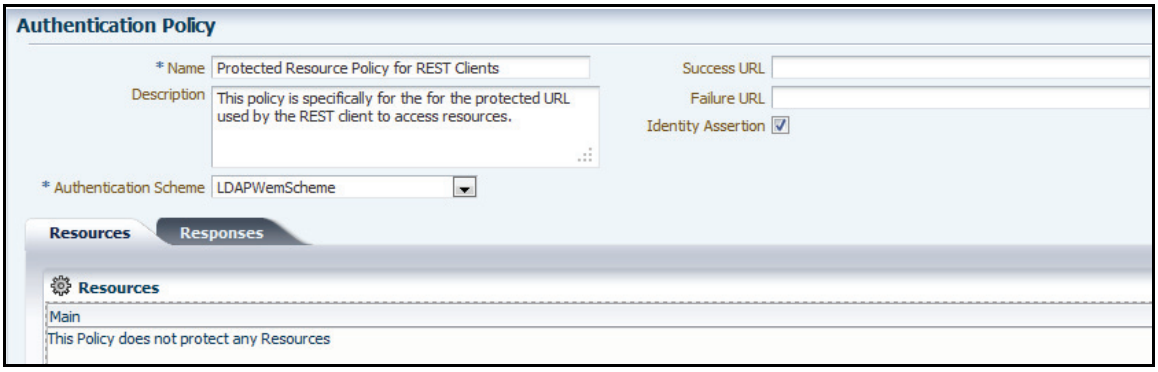
必要なレスポンスは FATGATE_POLICY および FATGATE_EMAIL のみです。残りのレスポンスはオプションです。



k. **「適用」**をクリックします。

14. REST クライアント用の保護済リソース・ポリシーを作成します。
    a. **「認証ポリシー」**をクリックします。
    b. **「作成」**アイコンをクリックします。
    c. 「名前」に、「REST クライアント用保護済リソース・ポリシー」と入力します。
    d. 「説明」に、「このポリシーは、REST クライアントによってリソースへのアクセスに使用される保護済 URL 専用です。」と入力します。
    e. 「認証スキーム」には、WebCenter Sites チャレンジ・ページを使用している場合は**「LDAPWemScheme」**を選択します。デフォルトの OAM ログイン・フォームを使用している場合は**「LDAPScheme」**を、他のカスタム・ログイン・フォームを使用している場合は別のスキームを選択します。

       LDAPWemScheme は、212 ページの手順 7 で作成した認証スキームです。
    f. **「ID アサーション」**チェック・ボックスを選択します。

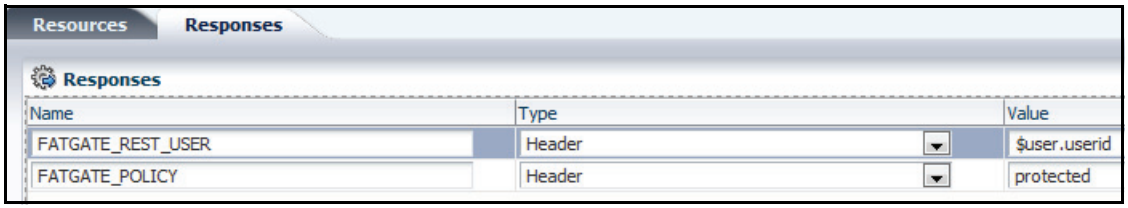


g. 「レスポンス」タブをクリックします。

h. 「追加」(+) アイコンをクリックします。

i. 「名前」を入力し、「タイプ」を選択して「値」を入力します。

エントリ FATGATE_REST_USER および FATGATE_POLICY について、手順 h および i を繰り返します。レスポンスは両方とも必要です。



j. 「適用」をクリックします。

15. 非保護リソース・ポリシーを作成します。

a. 「認証ポリシー」をクリックします。

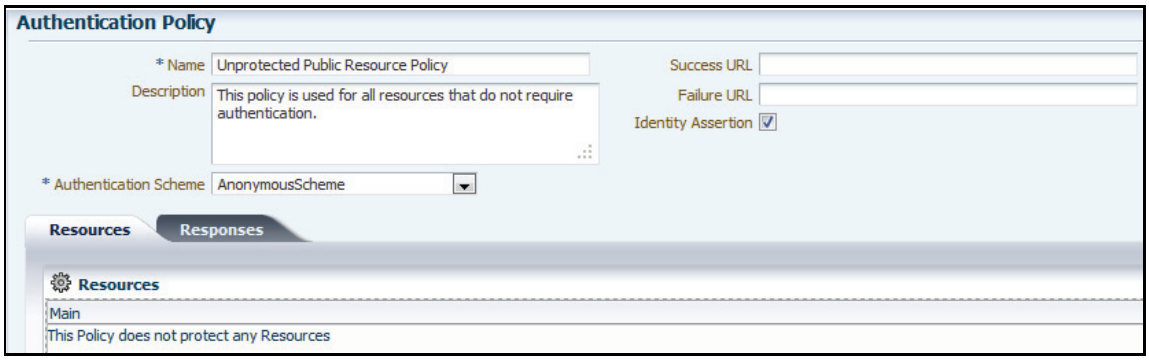
b. 「作成」アイコンをクリックします。

c. 「名前」に、「非保護パブリック・リソース・ポリシー」と入力します。

d. 「説明」に、「このポリシーは、認証を必要としないリソースすべてで使用されます。」と入力します。

e. 「認証スキーム」で「**AnonymousScheme**」を選択します。

f. 「ID アサーション」チェック・ボックスを選択します。

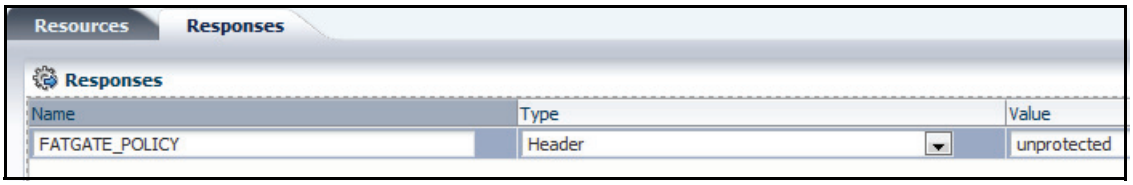


g. 「レスポンス」タブをクリックします。

h. 「追加」(+) アイコンをクリックします。

i. 「名前」を入力し、「タイプ」を選択して「値」を入力します。

エントリ FATGATE_POLICY について、手順 h および i を完了します。



j. 「適用」をクリックします。

16. WebCenter Sites アプリケーション・ドメイン用の認証ポリシーを作成します。

この認証ポリシーは、認証がデータベース設定に基づいて Sites アプリケーションにより内部的に行われたときに、すべての WebCenter Sites リソースに適用されます。ただし、暗黙の制約を使用して認証ポリシーを定義し、Web ゲートが Sites アプリケーションにリソース・リクエストを渡すようにする必要があります。

a. 「認可ポリシー」をクリックします。

b. 「作成」アイコンをクリックします。

c. 「名前」に、「すべてのリソースは認可されています」と入力します。

d. 「説明」に、「このポリシーにより、すべてのリソースは制約なしに完全に認可されます。」と入力します。

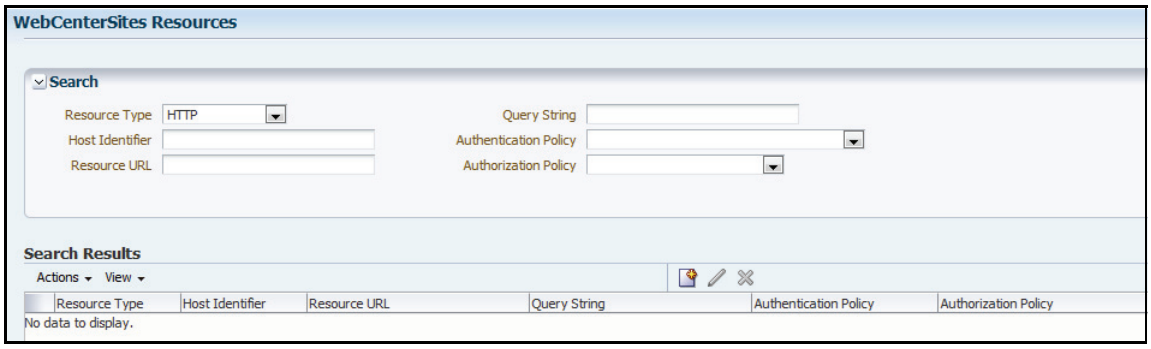
e. 「暗黙的な制約の使用」チェック・ボックスが選択されていることを確認します。

f. 「適用」をクリックします。

17. WebCenter Sites アプリケーション・ドメイン用のリソース定義を作成します。

a. 「リソース」をダブルクリックします。

このパネルには、検索条件に一致するリソースのみが表示されます。新しいリソースが追加されるたびに、「検索」ボタンをクリックして、このリソースを「検索結果」リストに表示する必要があります。



b. **「新規リソース」**をクリックして、「リソースの作成」パネルを開きます。

c. 「タイプ」を選択します。
すべてのリソースのタイプは HTTP です。

d. 「ホスト識別子」を選択します。
すべてのリソースは、ホスト識別子に WCSites を使用します。

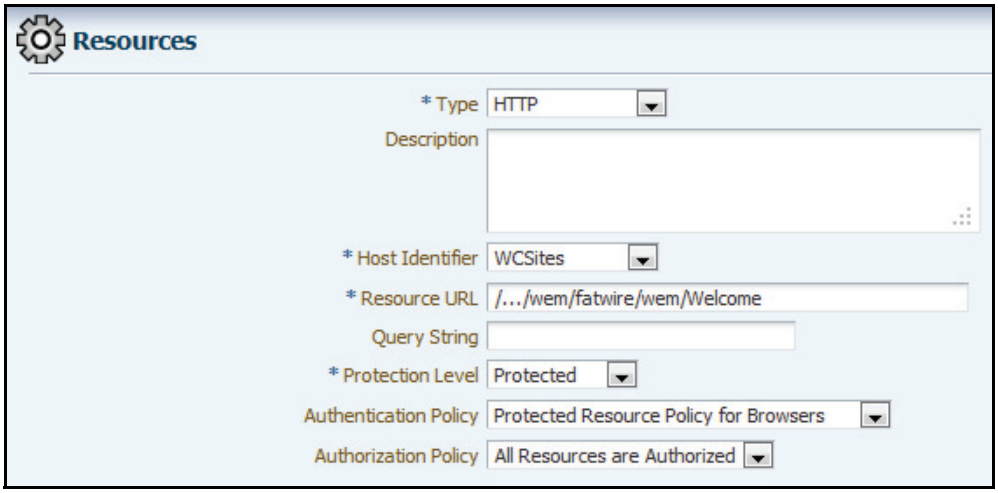
e. 「リソース URL」を入力します。

f. 「保護レベル」を選択します。
「除外」を選択した場合、手順 g および h は省略します。

g. 「認証ポリシー」を選択します。

h. 「認可ポリシー」を選択します。

i. **「適用」**をクリックします。



j. 次のリソース・リストを使用して、手順 b - i を繰り返します。

注意

「非保護」のリソースは /.../* のみです。
ポリシーを持つリソースはすべて「保護」です。
残りのリソースは「除外」です。

表 5: リソース

リソース URL	保護レベル	認証	認可
/.../*.jpg	除外		
/.../*.css	除外		
/.../*.png	除外		
/.../*.swf	除外		
/.../*.html	除外		
/.../*.jar	除外		
/.../*.gif	除外		
/.../*.jsp	除外		
/.../*.jspx	除外		
/.../faces/jspx/logout.jspx	除外		
/oamlogin/oamsso/*	除外		
/index.html	除外		
/.../home	除外		
/.../*	非保護	パブリック	すべて許可
/.../wem/fatwire/wem/Welcome	保護	ブラウザ	すべて許可
/oamlogin/test	保護	ブラウザ	すべて許可
/.../REST/*	保護	REST	すべて許可
/.../wem/fatwire/*	保護	ブラウザ	すべて許可
/.../faces/jspx/*	保護	ブラウザ	すべて許可
/.../ContentServer/*	保護	ブラウザ	すべて許可
/.../Satellite/*	保護	ブラウザ	すべて許可

k. リソースをすべて追加したら、定義済リソースのリストと「表 5: リソース」を比較して、すべてのポリシーが適切に定義されていることを確認します。先頭の「/.../」にピリオドが 3 つ含まれていることを確認します。入力されたリソース URL で大文字小文字が正しく使い分けられていることを確認します。これらのポリシーが正確に入力されていないと、Sites アプリケーションは正しく動作しません。

18. これで構成は完了です。WebCenter Sites コンテンツ管理および開発インストールのユーザー認証に OAM が使用されるようになります。

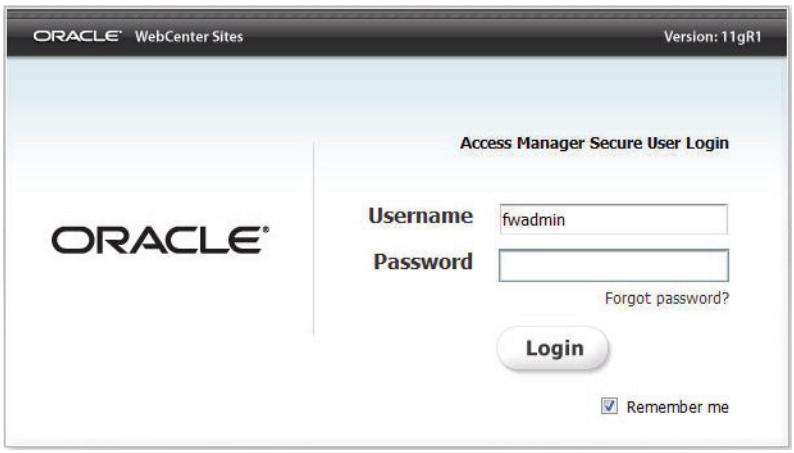
OHS サーバーを含むすべてのアプリケーションをいったん停止し、再び再起動して、変更内容を有効にします。

19. この手順はオプションで、`oamlogin.war` ファイルをデプロイした場合のみ実行できます。

    a. 任意のブラウザに次の URL を入力します。

    `http(s)://<OHS_host>:<OHS_port>/oamlogin/test`

    システムが適切に動作している場合は、WebCenter Sites チャレンジ・フォームが表示されます。



    b. ユーザー名とパスワードを入力して、**「ログイン」**をクリックします。パスワードは Sites データベースではなく、LDAP で定義されていることに注意してください。

    c. システムが適切に動作している場合、テスト・ページが開かれ、Web ゲートから提供された情報がすべて表示されます。これには、作成したポリシーで指定されたレスポンスが含まれます。このページをリフレッシュすると、更新後の情報が再表示されます。

    d. テスト・フォームで**「ログオフ」**をクリックします。標準の OAM ログオフを確認するフォームが表示されます。

    e. URL を再入力し、カスタム・チャレンジ・フォームを表示します。

    構成を慎重にレビューして、期待どおりの結果であることを確認します。

OAM と Oracle WebCenter Sites: Satellite Server の統合

Oracle Access Manager 統合用 Satellite Serve の構成は、WebCenter Sites 用の場合よりも手順が簡単です。この項では、Satellite Server を 1 つ構成するための手順について概説しますが、複数の Satellite Servers を構成する場合でも手順は同じです。

この項は、次のトピックで構成されています。

開始する前に

Satellite Server を統合する前に、次のアクションが完了していることを確認してください。

- Oracle Access Manager のインストールおよび実行
- WebCenter Sites と OAM の統合
- Satellite Server のインストール

統合手順

この手順では、WebCenter Sites デプロイメントの `SSOConfig.xml` ファイルを変更します。このファイルは、ロードされる認証クラスを制御するとともに、それらのクラスで必要とされる様々なプロパティを制御します。

1. デプロイされた WebCenter Sites アプリケーションのデプロイされた `WEB-INF/classes` ディレクトリにある `SSOConfig.xml` ファイルのバックアップを作成します。

   次に例を示します。

   ```
   /u01/software/Apps/Weblogic1035/user_projects/domains/
      OAMCSDomain/applications/SS/WEB-INF/classes/SSOConfig.xml
   ```

2. `SSOConfig.xml` を次のファイルのように変更します。

   注意

   次のファイルでは、`serviceUrl`、`ticketUrl` および `signoutURL` プロパティを設定します。

   `signoutUrl` プロパティでは、WebCenter Sites ログアウトを呼び出すときに使用する URL を指定します。この URL には、OAM によるログアウト処理がすべて完了した後でブラウザが復帰する、エンコードされた URL を含めます。

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
    xmlns:context="http://www.springframework.org/schema/
   context"
    xsi:schemaLocation="
        http://www.springframework.org/schema/beans http://
   www.springframework.org/schema/beans/spring-beans-2.5.xsd
        http://www.springframework.org/schema/context http://
   www.springframework.org/schema/context/spring-context-
   2.5.xsd">
  <!-- Single Sign On provider -->
  <bean id="ssoprovider"
class="com.fatwire.wem.sso.oam.OAMProvider">
  <property name="config" ref="ssoconfig" />
  </bean>
  <!-- Single Sign On filter -->
  <bean id="ssofilter"
class="com.fatwire.wem.sso.oam.filter.OAMFilter">
  <property name="config" ref="ssoconfig" />
  <property name="provider" ref="ssoprovider" />
  </bean>
  <!-- Single Sign On listener -->
  <bean id="ssolistener"
class="com.fatwire.wem.sso.oam.listener.OAMListener">
  </bean>
  <!-- Single Sign On configuration -->
  <bean id="ssoconfig"
class="com.fatwire.wem.sso.oam.conf.OAMConfig">

  <!-- URL prefix for REST service endpoint -->
   <property name="serviceUrl" value="http://
{OHS_host}:{OHS_port}/{Sites_context_root}/REST" />

  <!-- URL prefix for Token Service servlet -->
   <property name="ticketUrl" value="http://
{oamtoken_app_server_host}:{oamtoken_port}/oamtoken" />

  <!-- URL to be called when WEM logout is required. -->
    <property name="signoutUrl" value="http://
{weblogic_host}:{oam_server_port}/oam/server/
logout?end_url=http%3A%2F%2F{OHS_host}%3A{OHS_port}%2F{Sites_co
ntext_root}%2Fwem%2Ffatwire%2Fwem%2FWelcome" />

  <!-- Proxy tickets, tt's the last server in the
call chain -->
    <property name="proxyTickets" value="true" />

  <!-- Your application protected resources (relative to
   applicationUrl) -->
  <!-- For Oracle Access Manager these URLs are not used and
   are defined as OAM Authentication Policy resources -->
    <property name="protectedMappingIncludes">
      <list>
      </list>
```

```
    </property>
    <property name="protectedMappingStatelessIncludes">
      <list>
         <value>/REST/**</value>
      </list>
    </property>
    <!-- Your application protected resources excludes
   (relative to applicationUrl) -->
    <property name="protectedMappingExcludes">
      <list>
      </list>
    </property>
  </bean>

</beans>
```

`proxyTickets` パラメータが `true` に設定されていることを確認します。Satellite Server が、REST クライアント・プログラムにより割り当てられた認証チケットを WebCenter Sites に渡すようにするには、この設定が必要です。

REST エンドポイントの場所 (`serviceUrl` プロパティで定義されたもの) は Satellite Server の場所によって異なります。ファイアウォールの内部にある場合は、WebCenter Sites を直接参照すると、セキュリティを危険にさらさずに最高のパフォーマンスを達成できます。Satellite Server が別の場所にある場合、またはインターネットに直接公開されている場合は、WebCenter Sites を保護するため、エンドポイントはすべてのリクエストを OHS 経由で送信します。

Satellite Server の前面で OHS を使用する拡張構成は、WebCenter Sites 構成を保護するための代替手段です。この構成は WebCenter Sites にアクセスします。