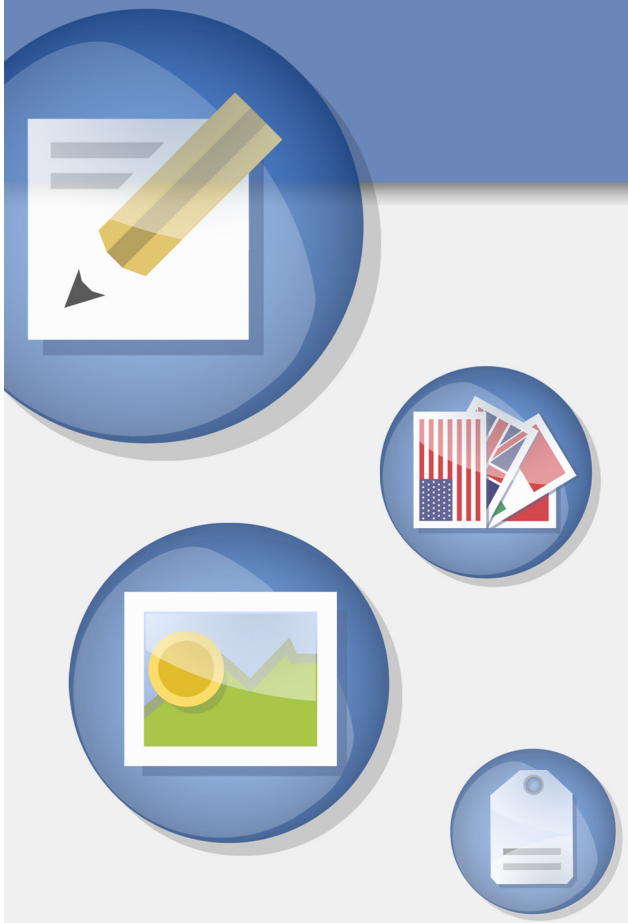
FatWire | Content Server 7

Version 7.5 Patch 2



Configuring Third-Party Software

Document Revision Date: Aug. 20, 2009

FatWire® SOFTWARE

Configuring Third-Party Software
Document Revision Date: Aug. 20, 2009
Product Version: 7.5 Patch 2

FatWire Technical Support
www.fatwire.com/Support

FatWire Headquarters
FatWire Corporation
330 Old Country Road
Suite 207
Mineola, NY 11501
www.fatwire.com

Table of

Contents

Part 2. Installing a Web Server

Part 3. Installing and Configuring LDAP

About This Guide

This guide contains information about installing and configuring third-party software specifically for use by FatWire Content Server. You will use the information in this guide along with the CS installation guide for your platform, (and with the CS-LDAP integration guide, if you choose to integrate with LDAP).

How This Guide is Organized

The guide is divided into the following parts:

- Part 1, "Creating and Configuring a Database" shows you how to create and configure the supported databases before you install Content Server. (Supplements the Content Server installation guides.)
- Part 2, "Installing a Web Server" shows you how to install and configure the supported web servers, if you choose to use one. (Supplements the Content Server installation guides.)
- Part 3, "Installing and Configuring LDAP" shows you how to set up the supported LDAP server for integration with Content Server. (Supplements the CS-LDAP integration guide.)
- Part 4, "Virtualization" shows you how to create and configure virtual machines.

Who Should Use This Guide

This guide is for installation engineers who have experience installing and configuring enterprise-level software, including databases, database drivers, application servers, portal servers, and LDAP servers.

Graphics in This Guide

Graphics in this guide are screen captures of dialog boxes and similar windows that you will interact with during the installation or configuration process. These graphics are presented to help you follow the installation and configuration processes. They are not intended to be sources of information such as parameter values, options to select, and product version numbers.

Technical Support

Help is available from FatWire Technical Support at the following website:

`http://www.fatwire.com/Support`

Part 1

Creating and Configuring a Database

Content Server requires access to a supported database that is configured specifically for Content Server. Instructions for creating and configuring supported databases are given in the following chapters:

- Chapter 1, "Creating and Configuring an Oracle 10g Database"
- Chapter 2, "Creating and Configuring an Oracle 11g Database"
- Chapter 3, "Creating and Configuring an MS SQL Server Database"
- Chapter 4, "Creating and Configuring an IBM DB2 8.x Database"
- Chapter 5, "Creating and Configuring an IBM DB2 9.1 Database"

The databases listed above are not configured for production; they are set up with full permissions. In practice, the permissions can be restricted for the user that Content Server will use to access a database. However, the following rights must exist: ability to create, modify, and delete tables and indexes.

If you need instructions on installing a supported database, refer to the product documentation. For instructions on creating and configuring a supported database refer to the chapters listed above. (Note that database configuration is identical across different application servers.)

Chapter 1

Creating and Configuring an Oracle 10*g* Database

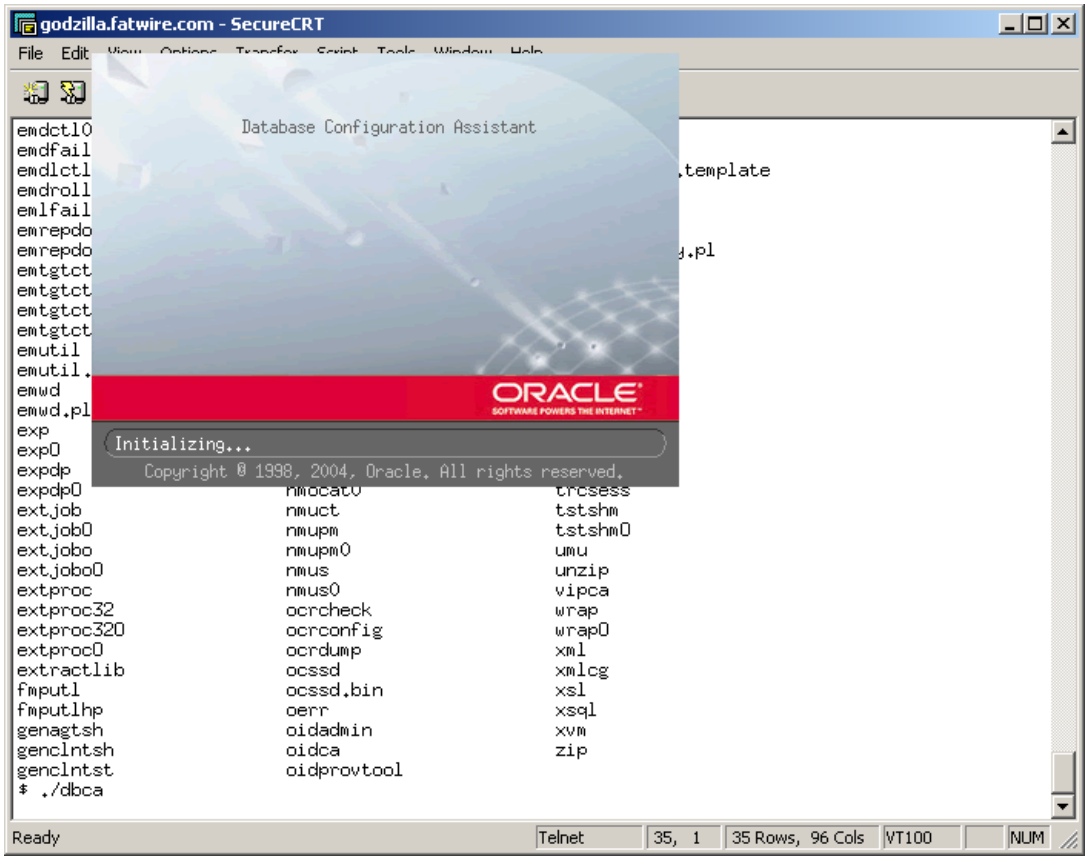
Use this chapter to set up an Oracle 10*g* database for your Content Server installation. For background information regarding database configuration and users' permissions, see Part 1, "Creating and Configuring a Database."

This chapter contains the following sections:

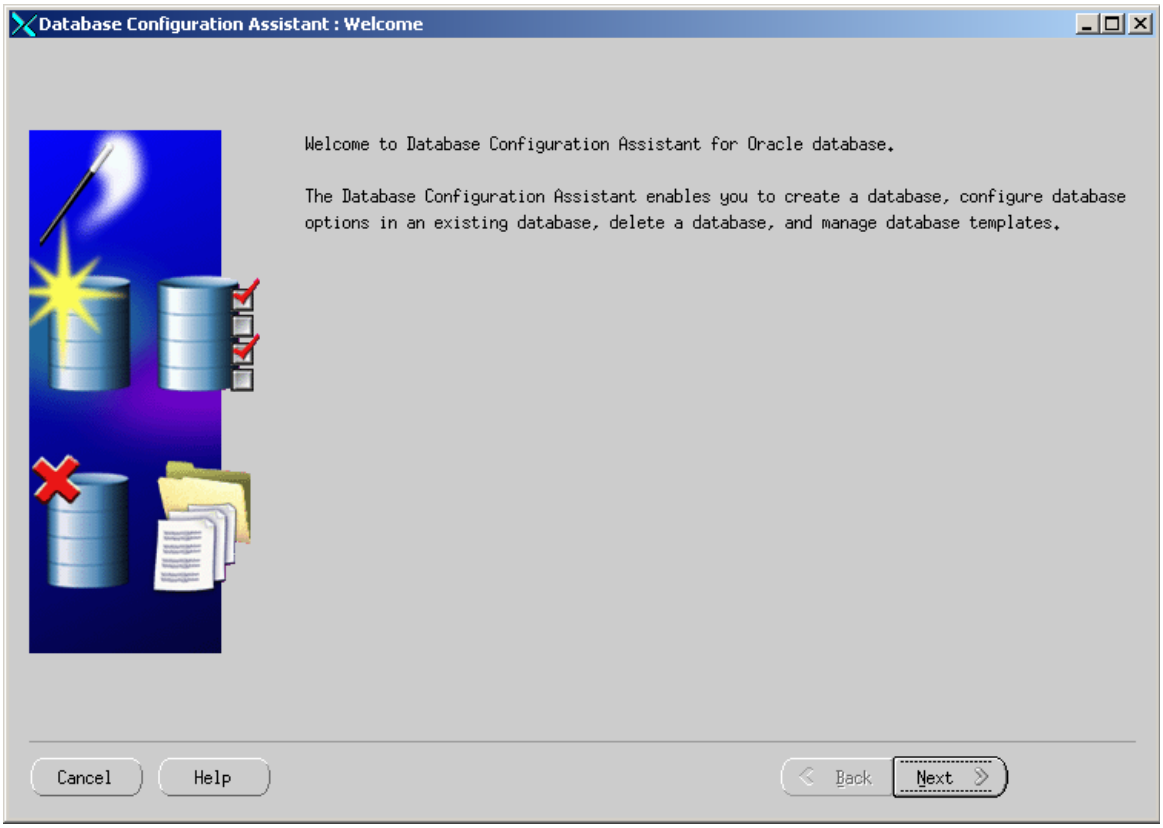
Step I. Create an Oracle 10*g* Database

1. Execute the “Oracle Database Configuration Assistant” by doing one of the following:
   - In Unix, execute the command: **`dbca`**
   - In Windows, go to the “Oracle Programs” group and select **Database Configuration Assistant**.

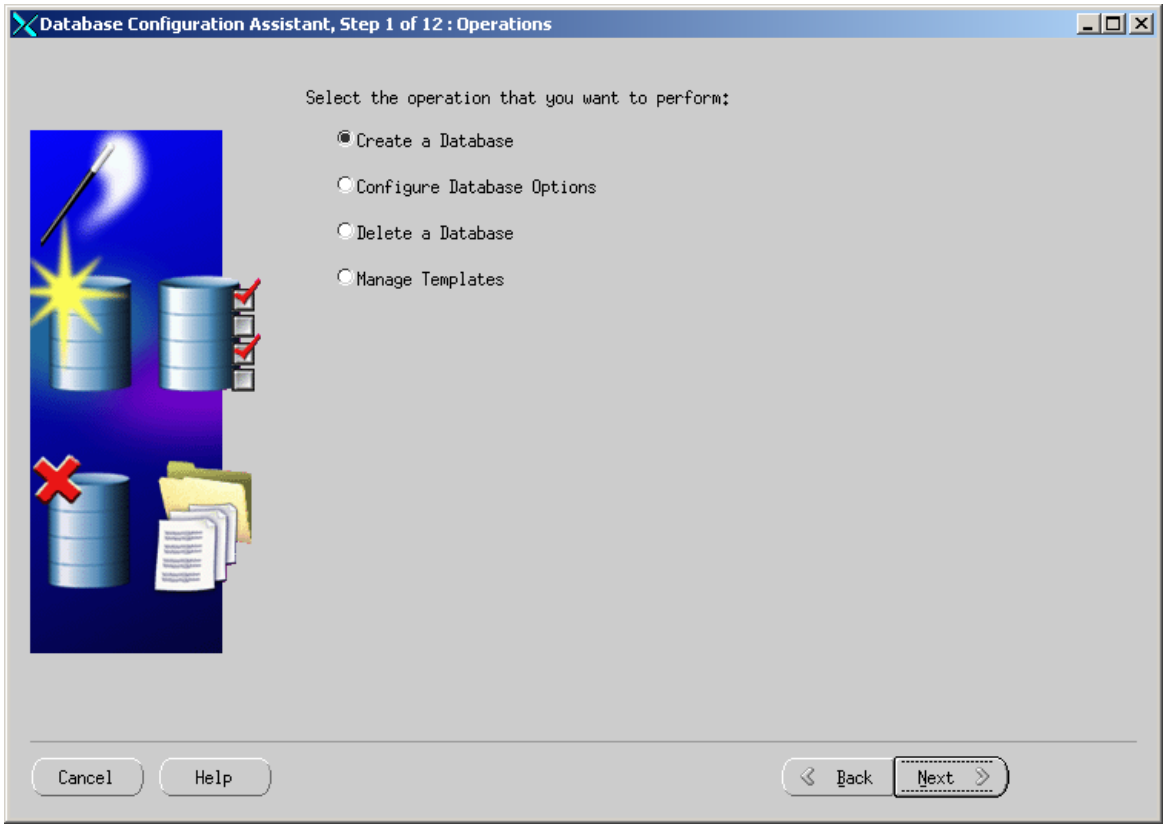
> **Note**
>
> This step displays a load screen that can take some time to complete. Be patient.



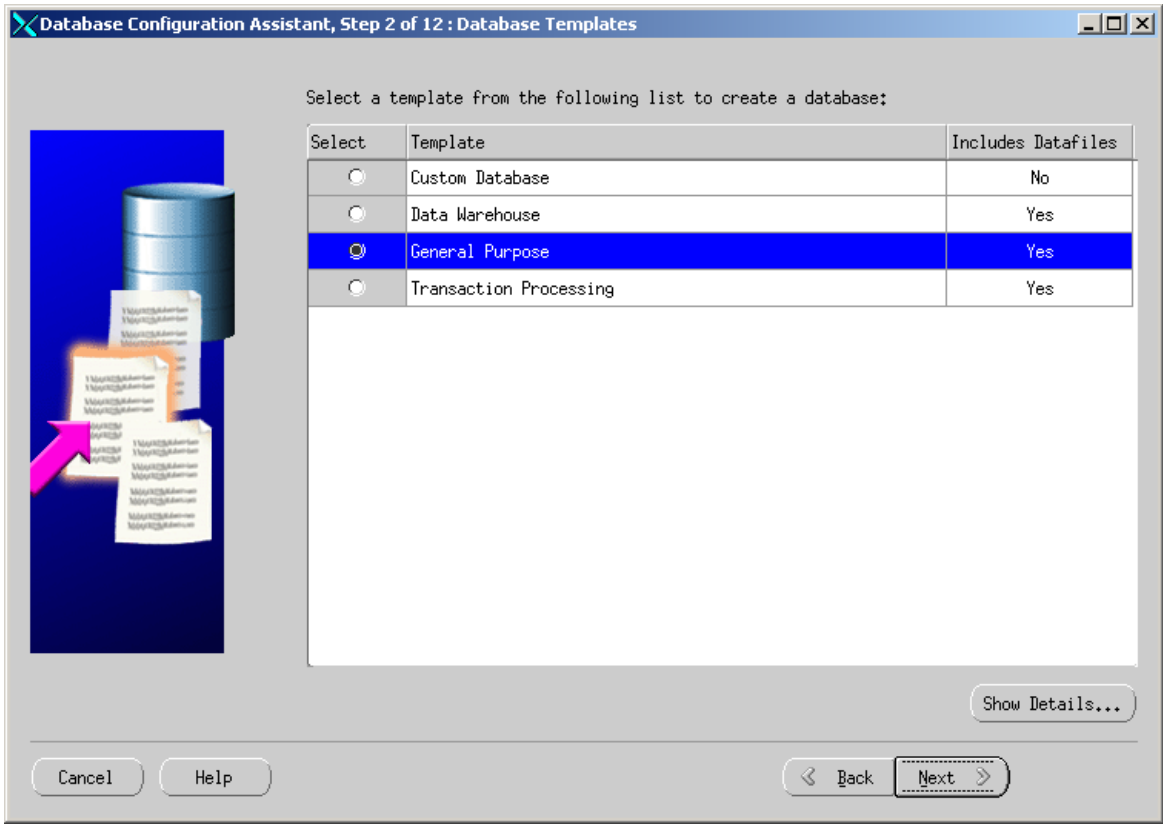
2. On the first screen that is displayed, click **Next**. In the following screen, click **Next**.



3. Select the radio button **Create a Database** and click **Next**.



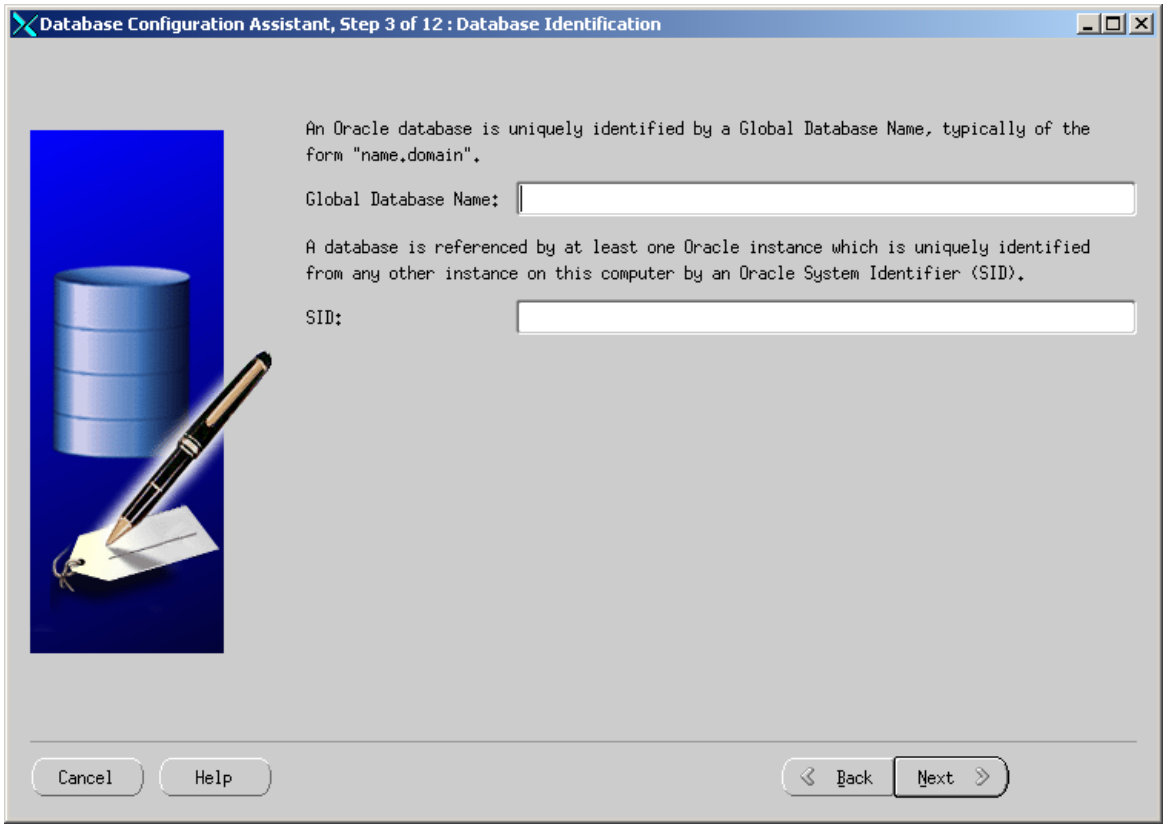
4. Select the radio button **General Purpose** and click **Next**.



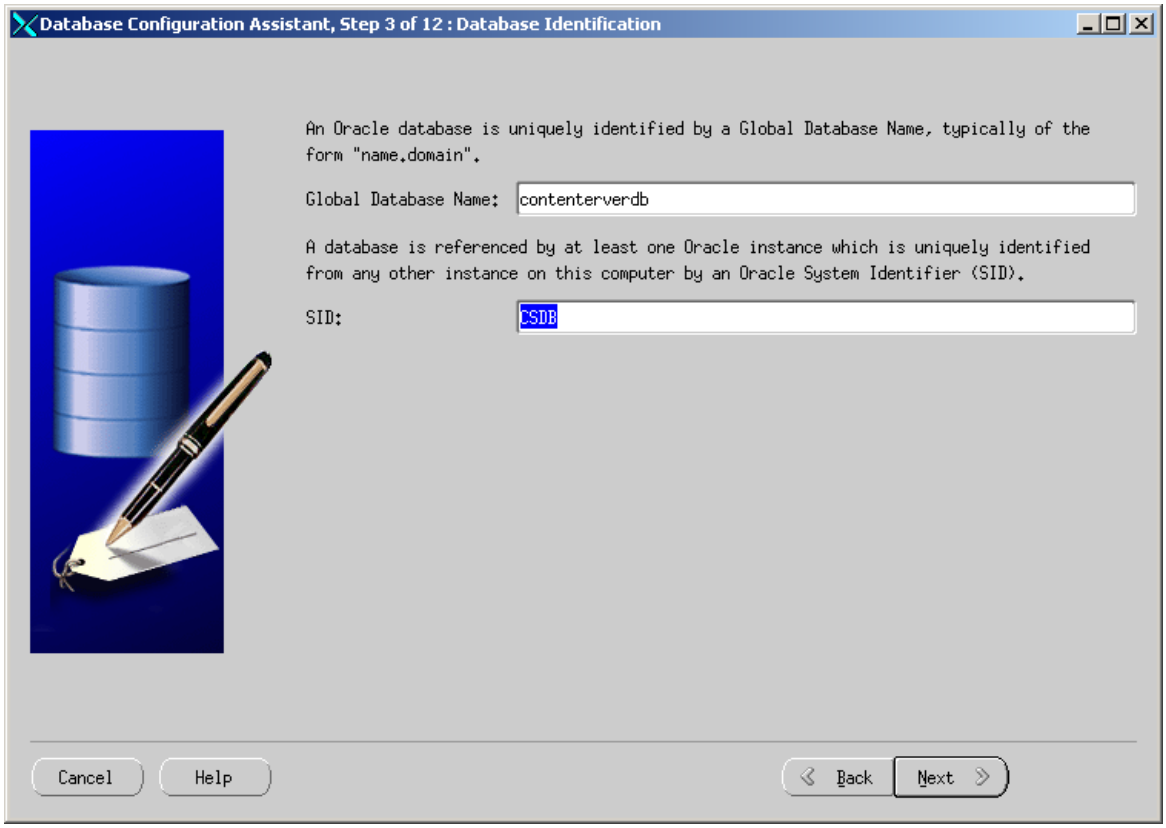
Note

Database block size **must** be at least `4096` bytes. Selecting the **General Purpose** option automatically sets the block size to `8192` bytes.

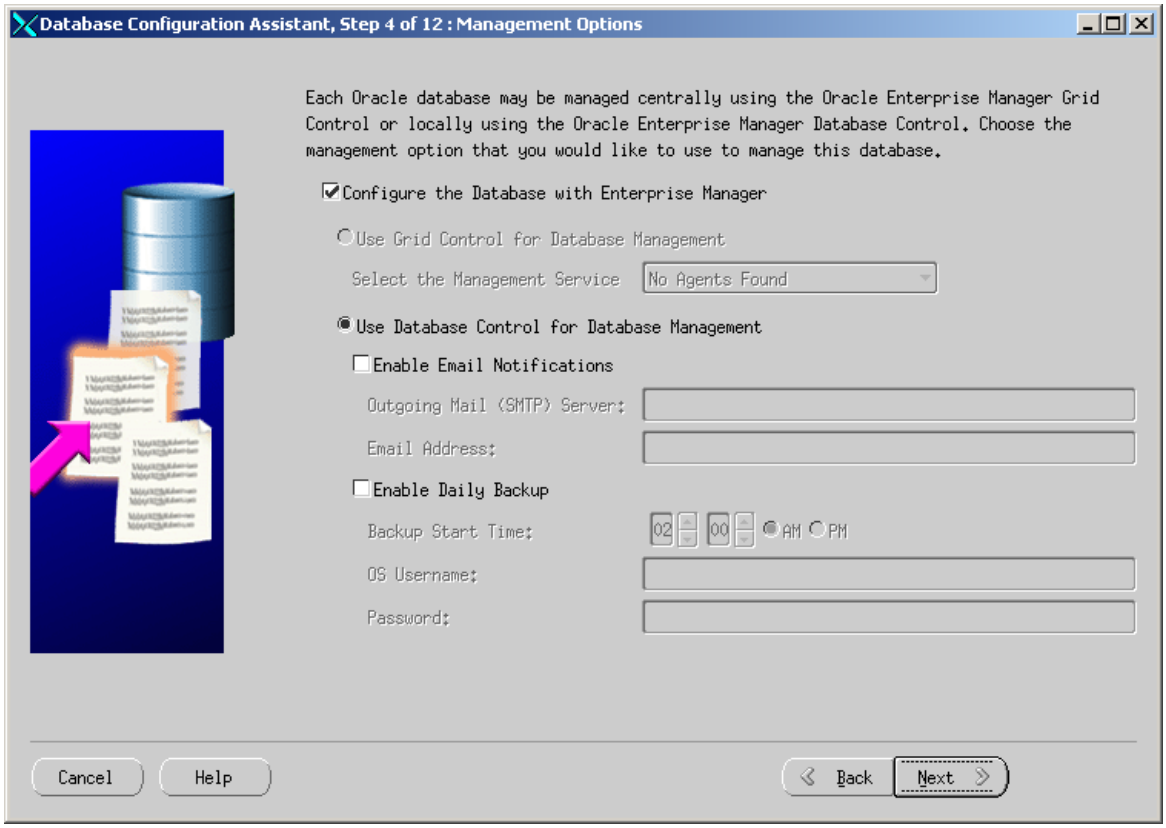
5. Enter a unique global database name and SID (in this example the global database name is `contentserverdb`. The SID is `CSDB`). Click **Next**.



6. Do not change any options. Click **Next**.

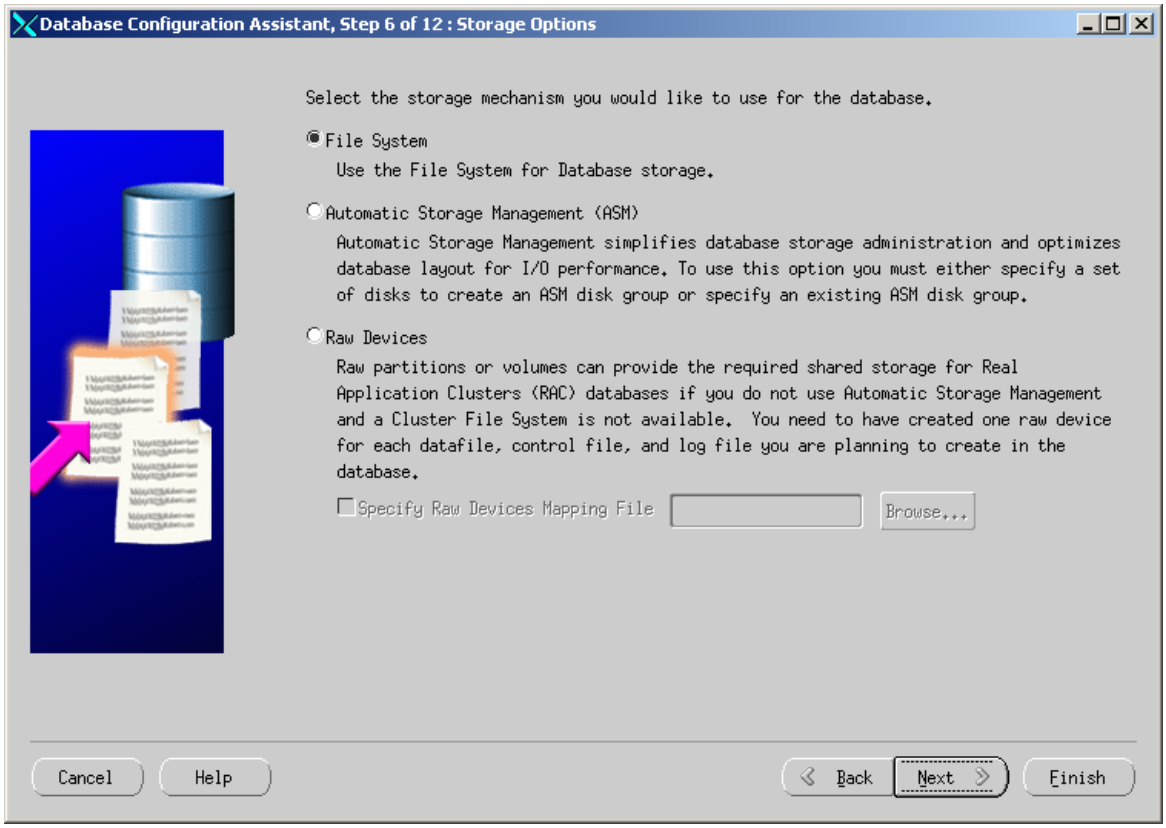


7. Do not change any options. Click **Next**.

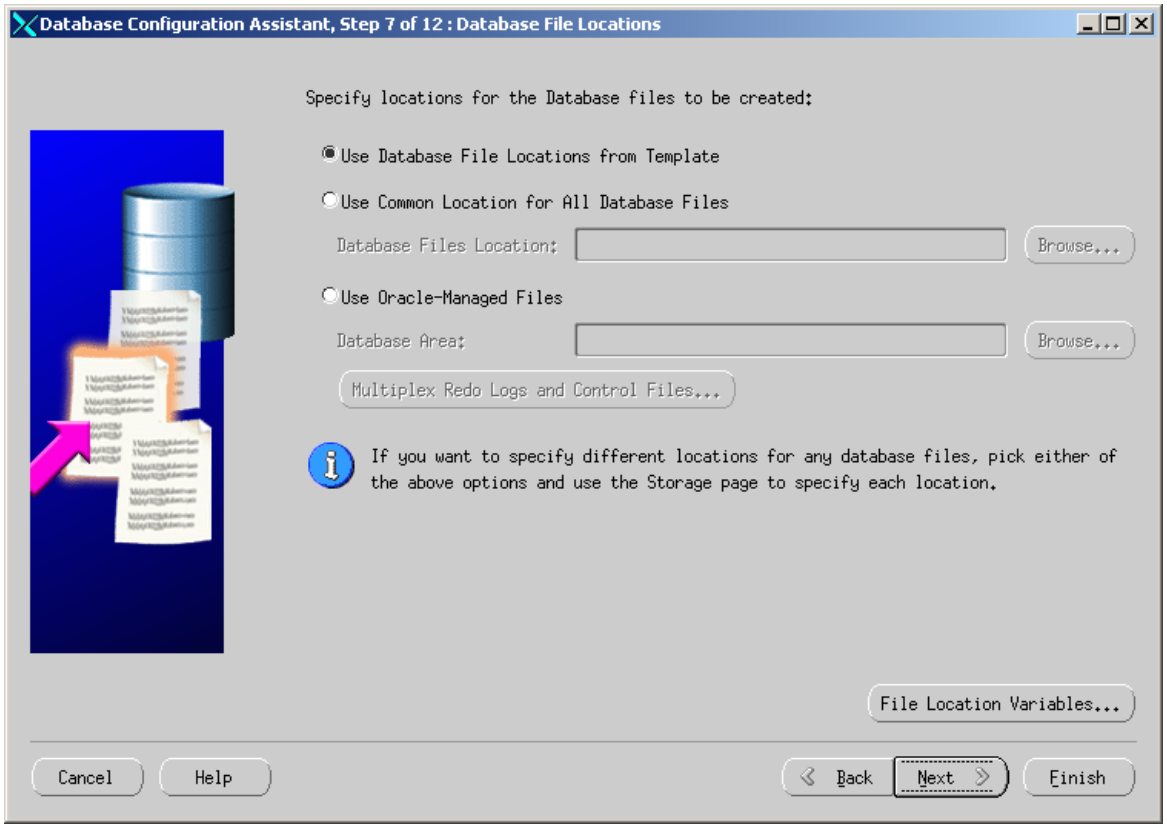


8. Enter a password, re-enter the same password in the "Confirm Password" field and click **Next**.
9. For enhanced security select the radio button **Use Different Passwords** and enter a unique password for each of the given users.

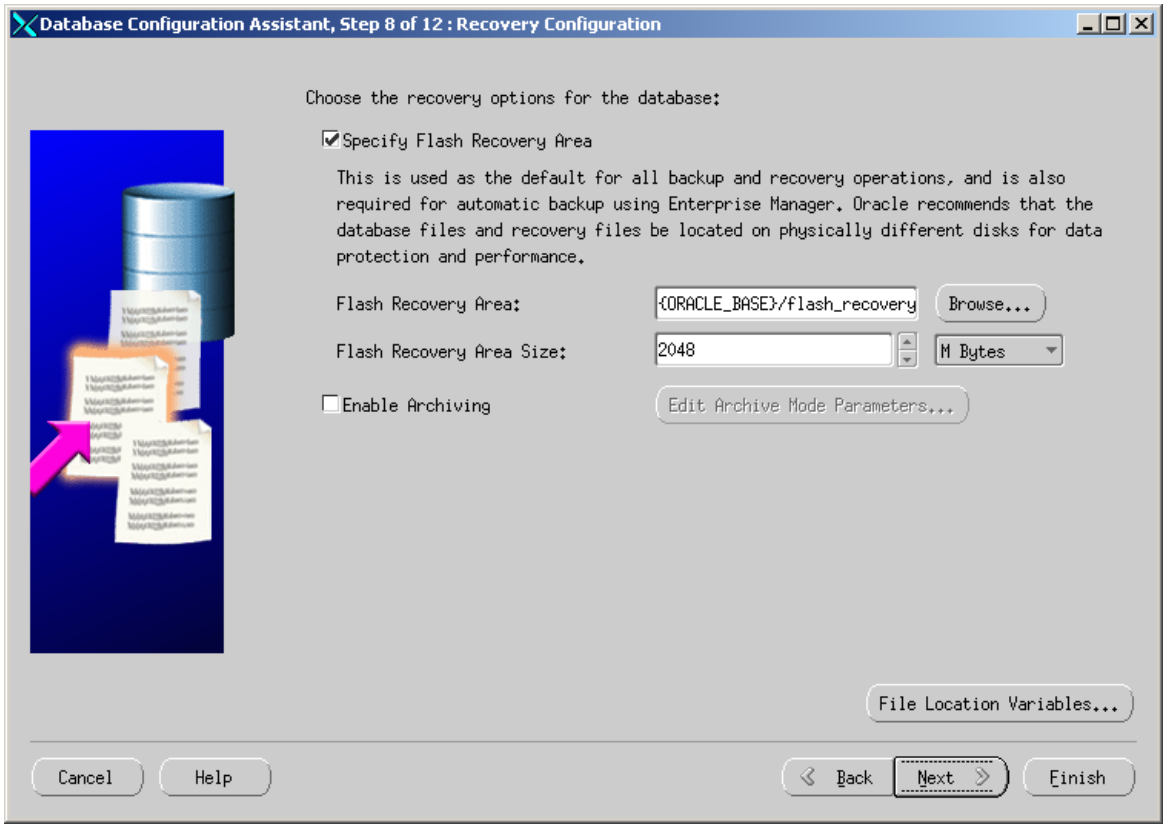
10. Do not change any options. Click **Next**.



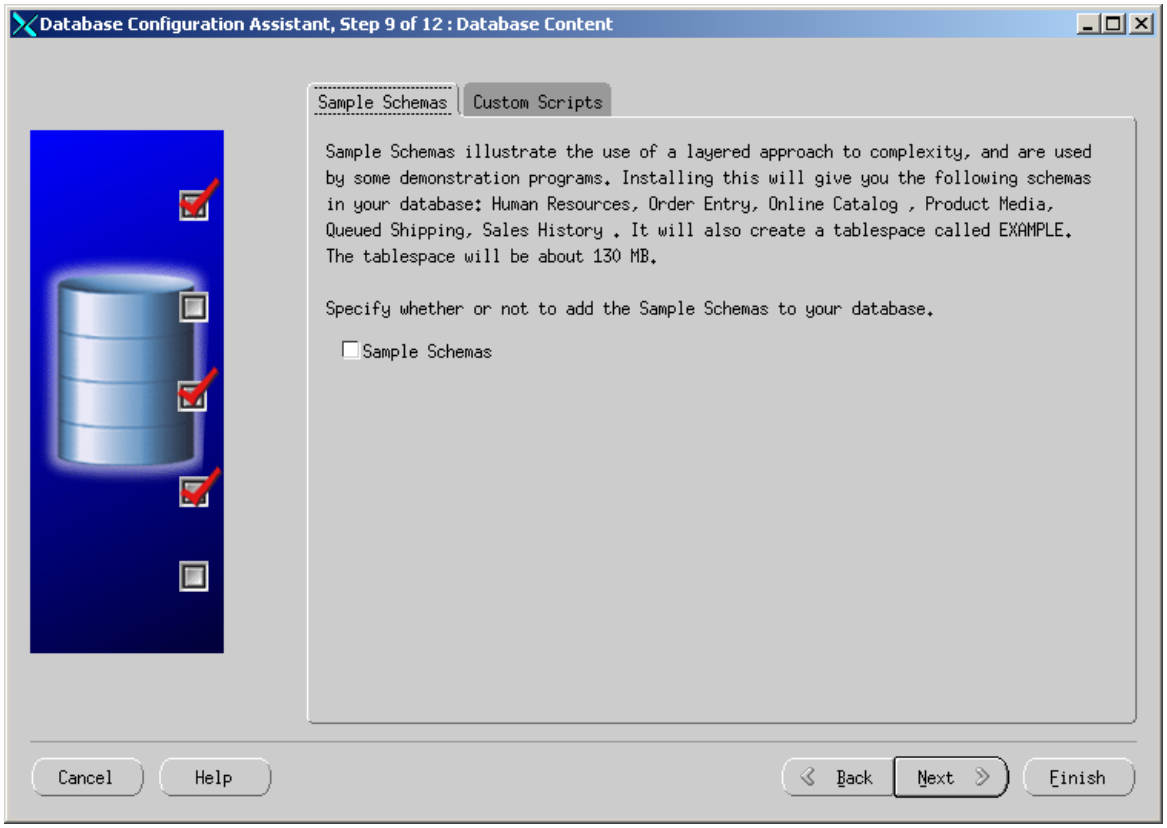
11. Do not change any options. Click **Next**.



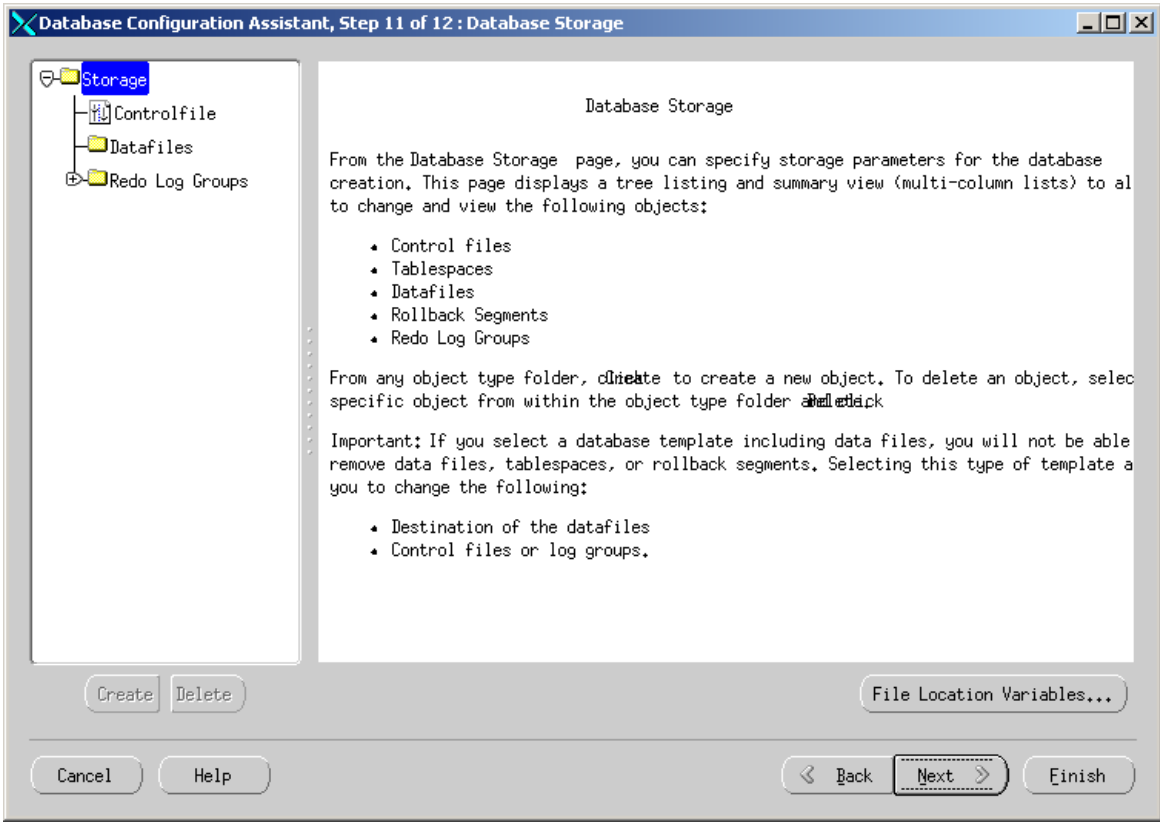
12. Do not change any options. Click **Next**.



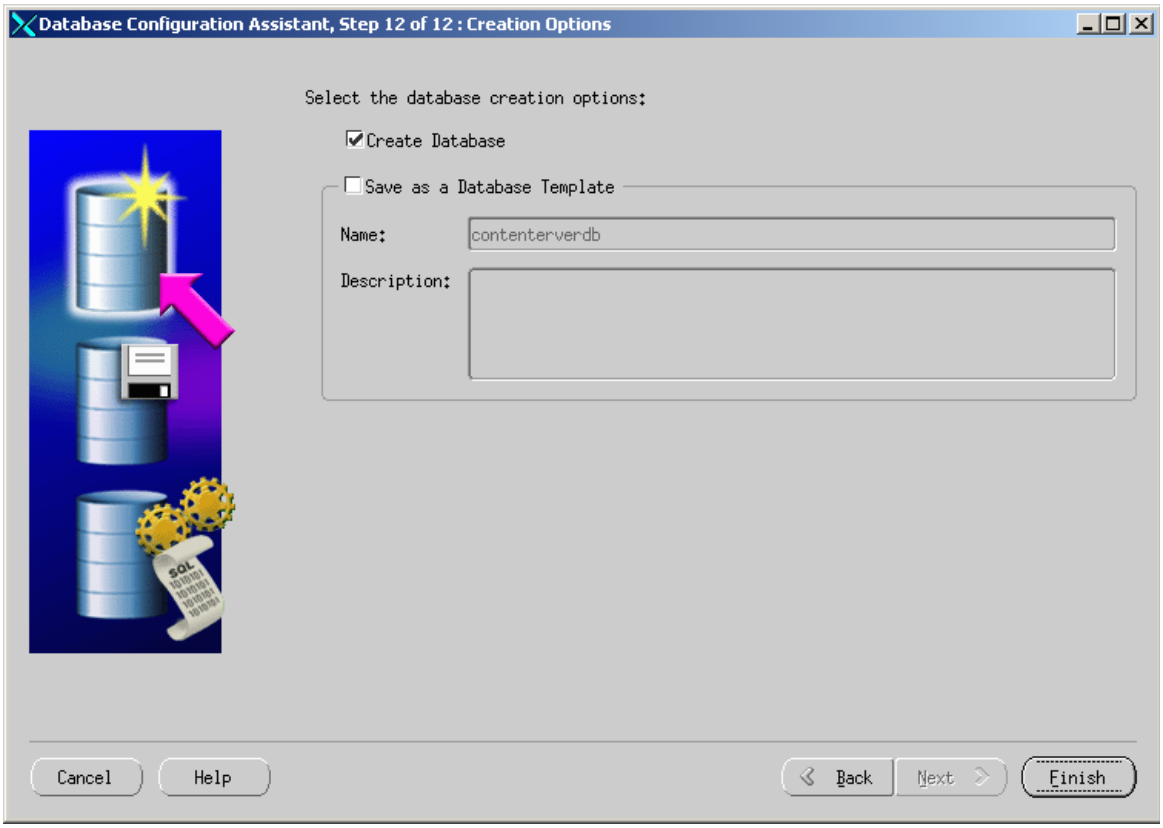
13. Do not change any options. Click **Next**.



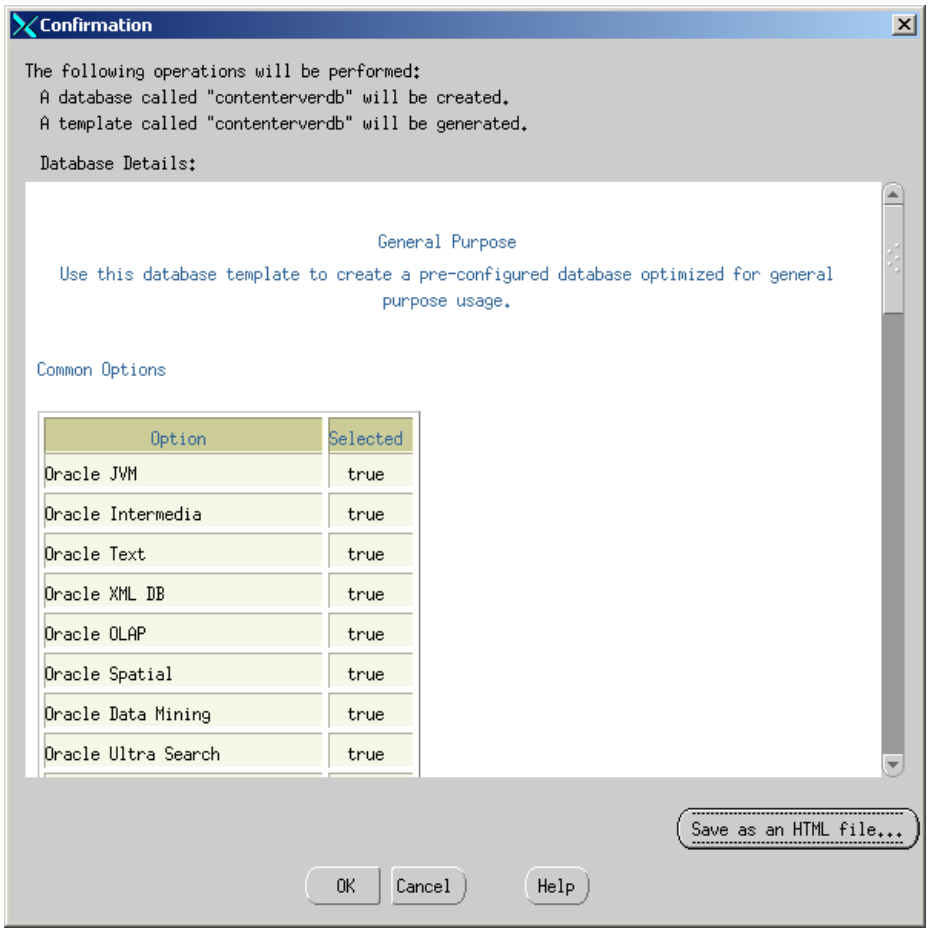
14. Click the **Character Sets** tab and do the following:
    a. Select **Choose from the list of character sets** and select **UTF-8** from the drop-down menu.
    b. Click the **National Character Set** drop down-menu and select **UTF8**.
15. Leave all other options on the different tabs as is and click **Next**.
16. For database storage, no options need to be changed. However, if you wish to change the location of the database from the default of `oradata` located under the Oracle installation, you can do so on this page. Click **Next**.



17. Do not change any options. Click **Finish**.



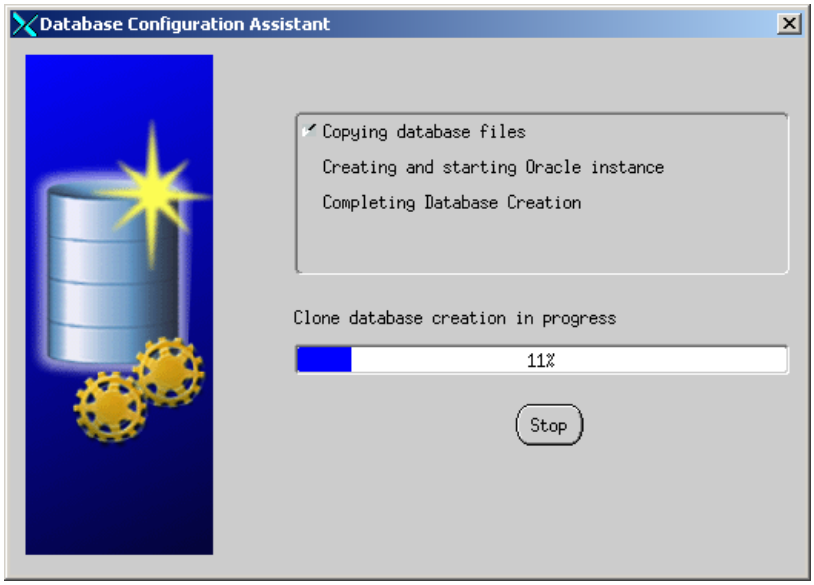
18. In the “Configuration” window, review the choices that you made on the previous screens. If you need to modify your choices, click **Cancel** and make the modifications. Otherwise, click **OK** to continue.



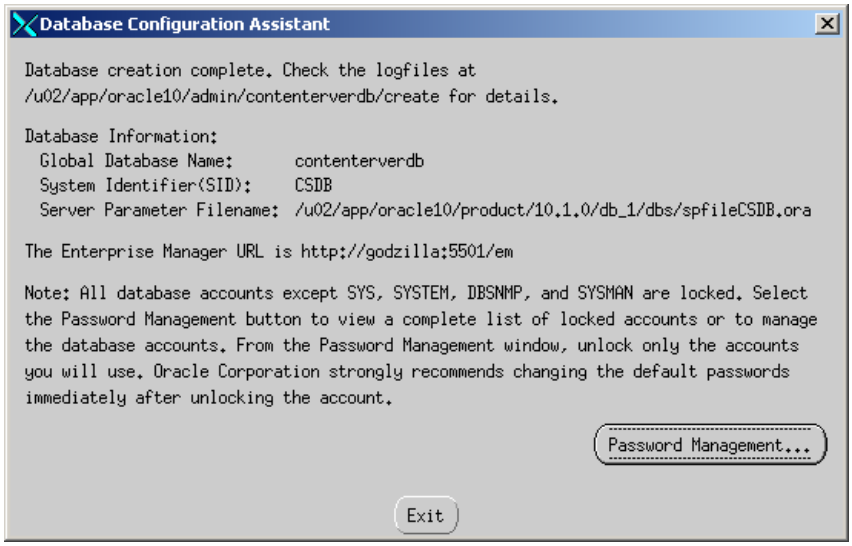
Note

If you are planning to use internationalization, for Content Server the key value is: `National Character Set: UTF8`

19. The following window shows the progress of the database creation. This step can take time to complete.



20. When database creation is completed, click **Exit**.



Step II. Create a New User for Content Server

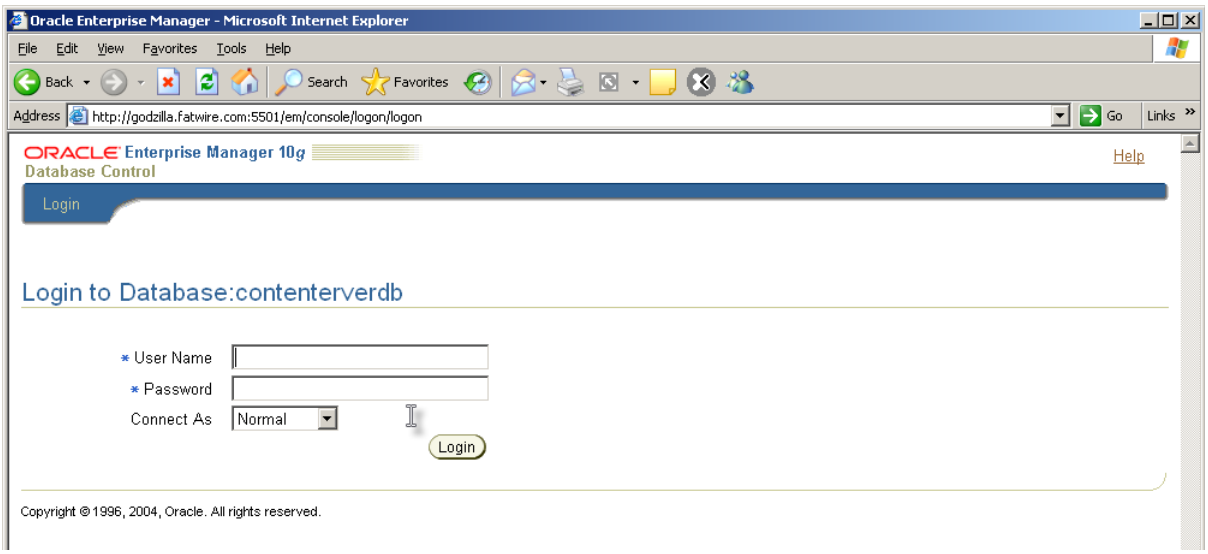
1. Locate the file `emoms.properties` (in `<oracle home>/<server name>_<SID>/sysman/config/`).
   a. Find the line: `oracle.sysman.emSDK.svlt.ConsoleServerPort`
   b. The port after the line in step a is important. Make a note of it.
2. Run the command: **`emctl status dbconsole`**

   The command should return an output similar to the following:

```
Oracle Enterprise Manager 10g Database Control Release
     10.1.0.2.0
Copyright (c) 1996, 2004 Oracle Corporation. All rights
     reserved.
http://godzilla:5500/em/console/aboutApplication
     Oracle Enterprise Manager 10g is running.
------------------------------------------------------------
Logs are generated in directory /u02/app/oracle10/product/
     10.1.0/db_1/godzilla_orcl10so/sysman/log
```

> **Note**
>
> If the command returns the message that the Oracle Enterprise Manager is not running, start Oracle Enterprise Manager with the command: **`emctl start dbconsole`**

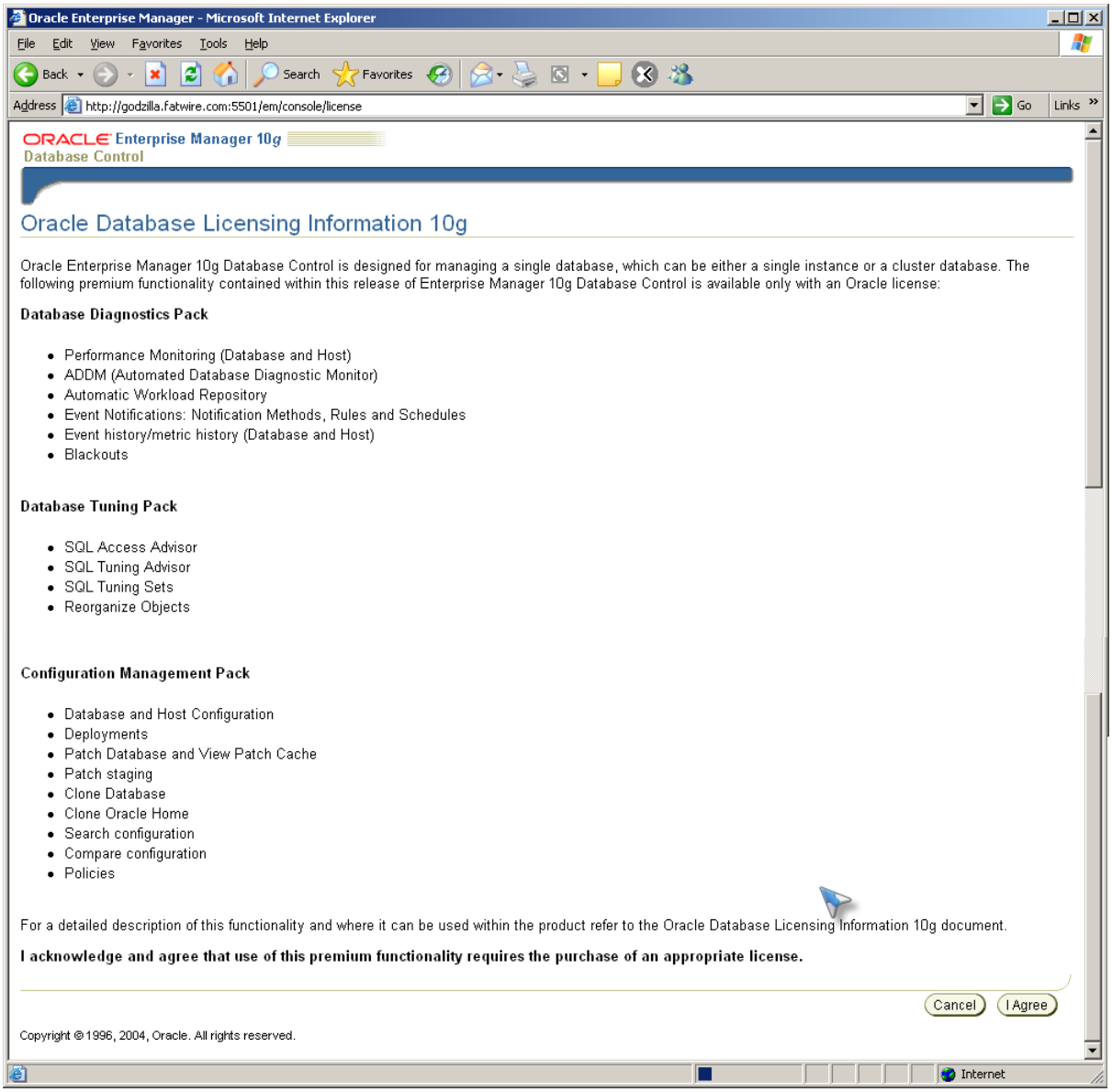
3. Open a browser and do the following:
   a. Browse to the URL `http://<hostname>:<port>/em` (from step 2).



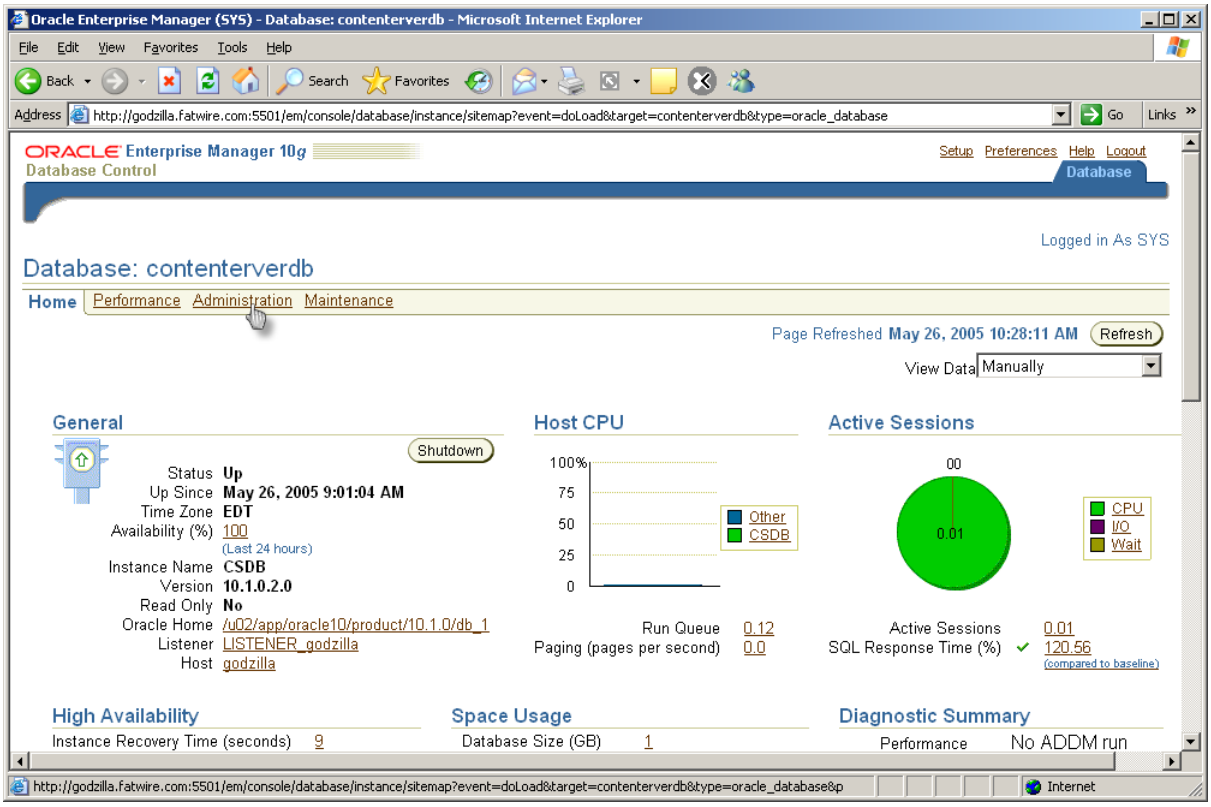
b. Log in to the browser, using the following field values:

Field Name	Field Value
User name	`sys`
Password	`<password entered when creating the db>`
Connect As	`SYSDBA`

c. As this is the first time you are using the Oracle Enterprise Manager, a license page is displayed. Click **I Agree**.



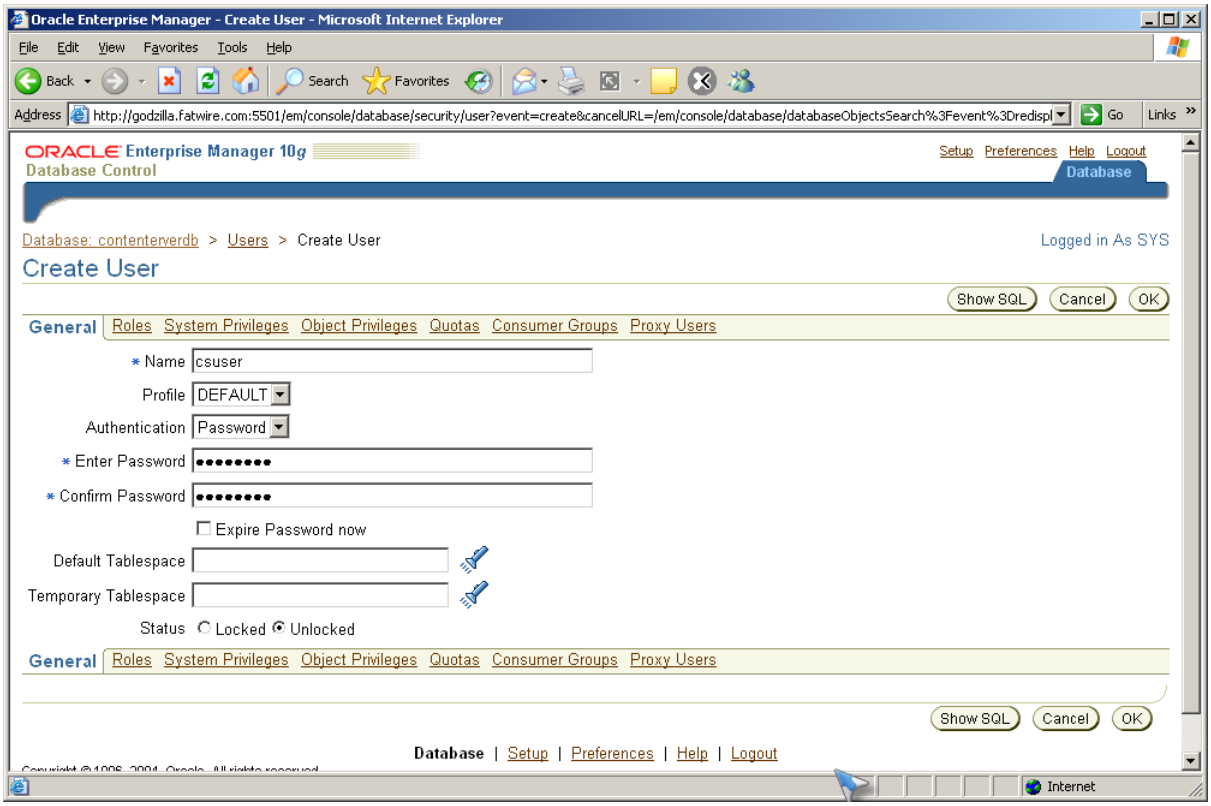
4. Click the **Administration** tab.



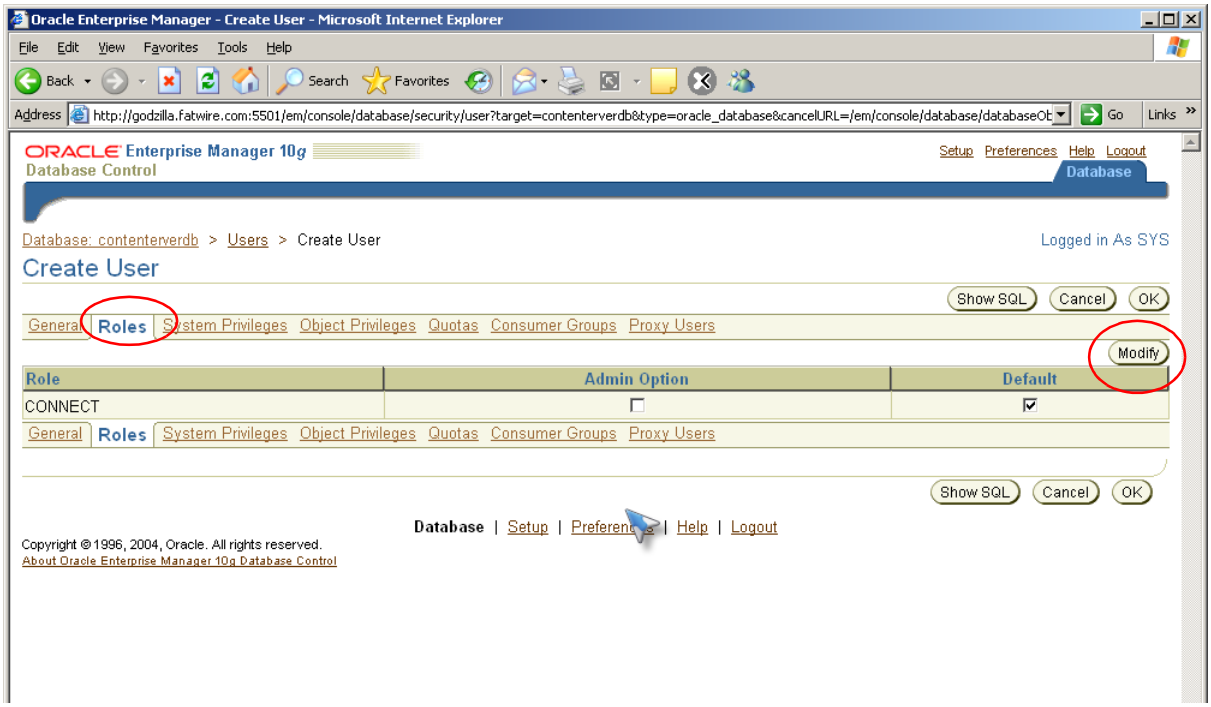
a. From the **Security** menu, select **Users**. Click the **Create** button.

b. In the "Create User" screen, fill in required fields with the values that are listed in the following table:

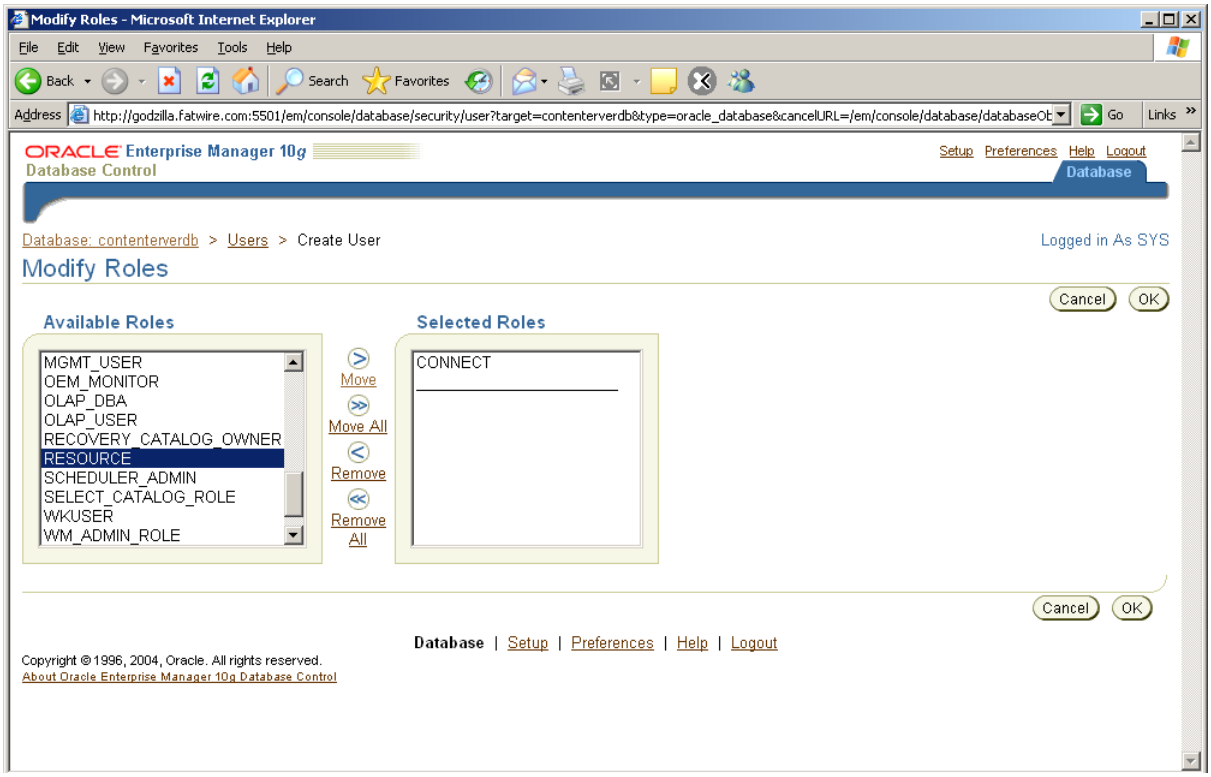
Field Name	Field Value
Name	`csuser`
Enter Password	`<your choice>`
Confirm Password	`<same password>`



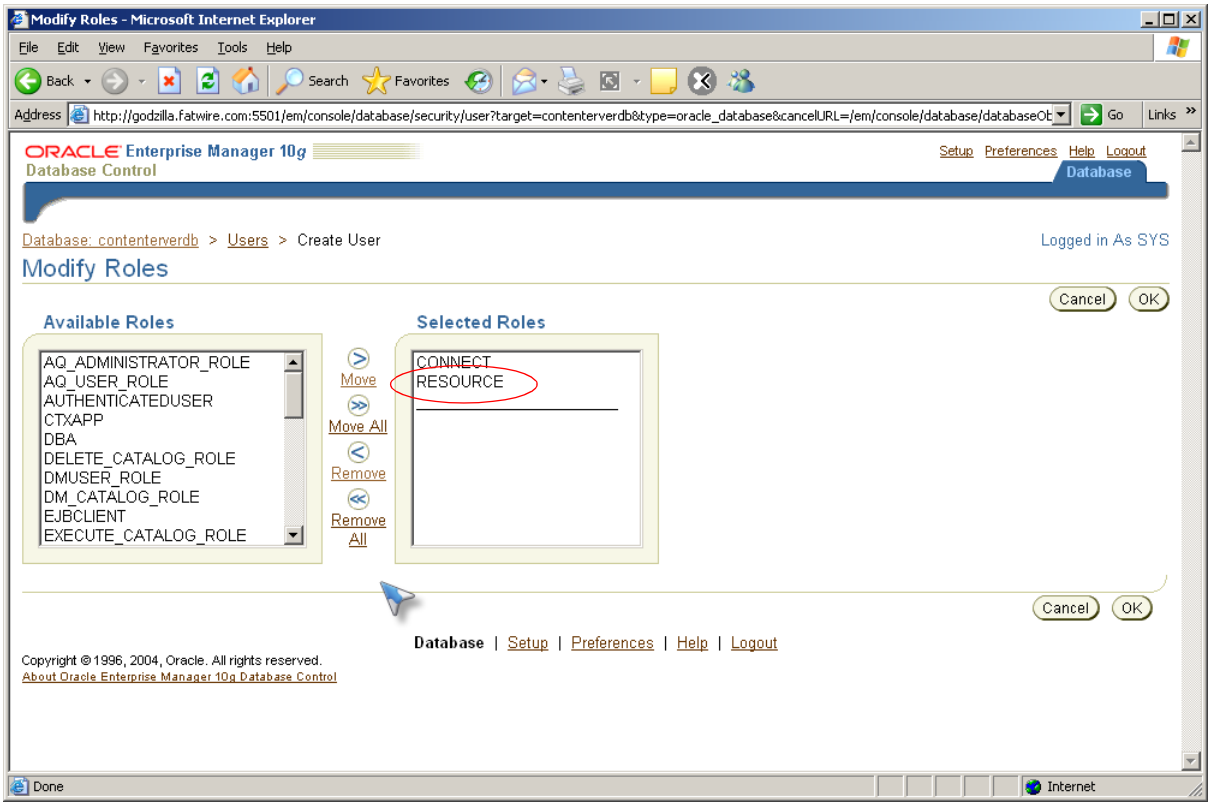
5. Click the **Roles** tab.
   a. Click the **Modify** button.



   b. From the list of "Available Roles" (left side), select **Resource** and click the **Move** button.

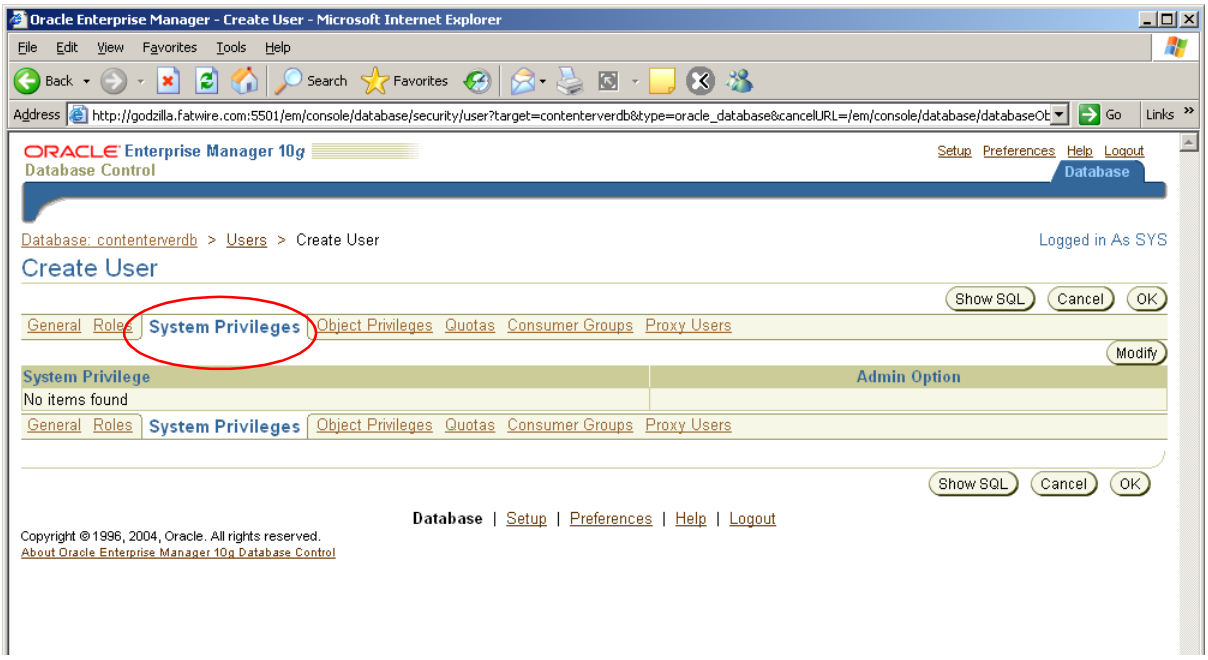


Resource is moved to the “Selected Roles” list.

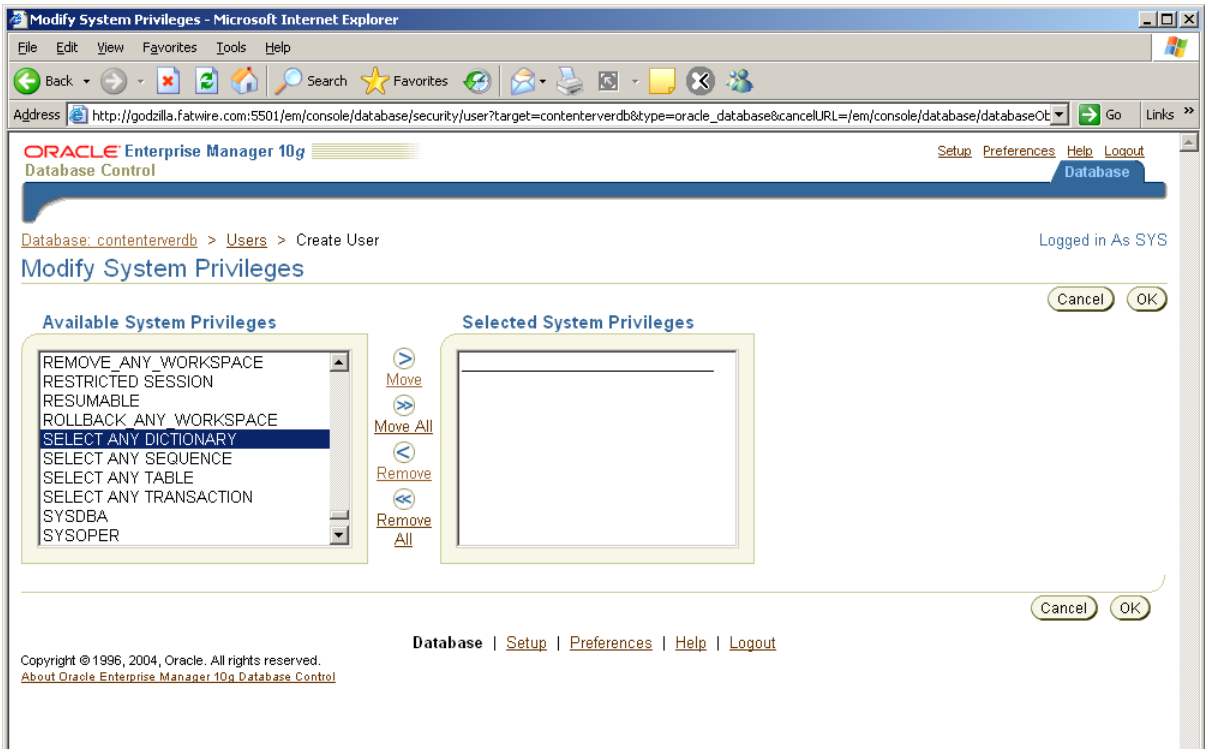


c. Click **OK**.

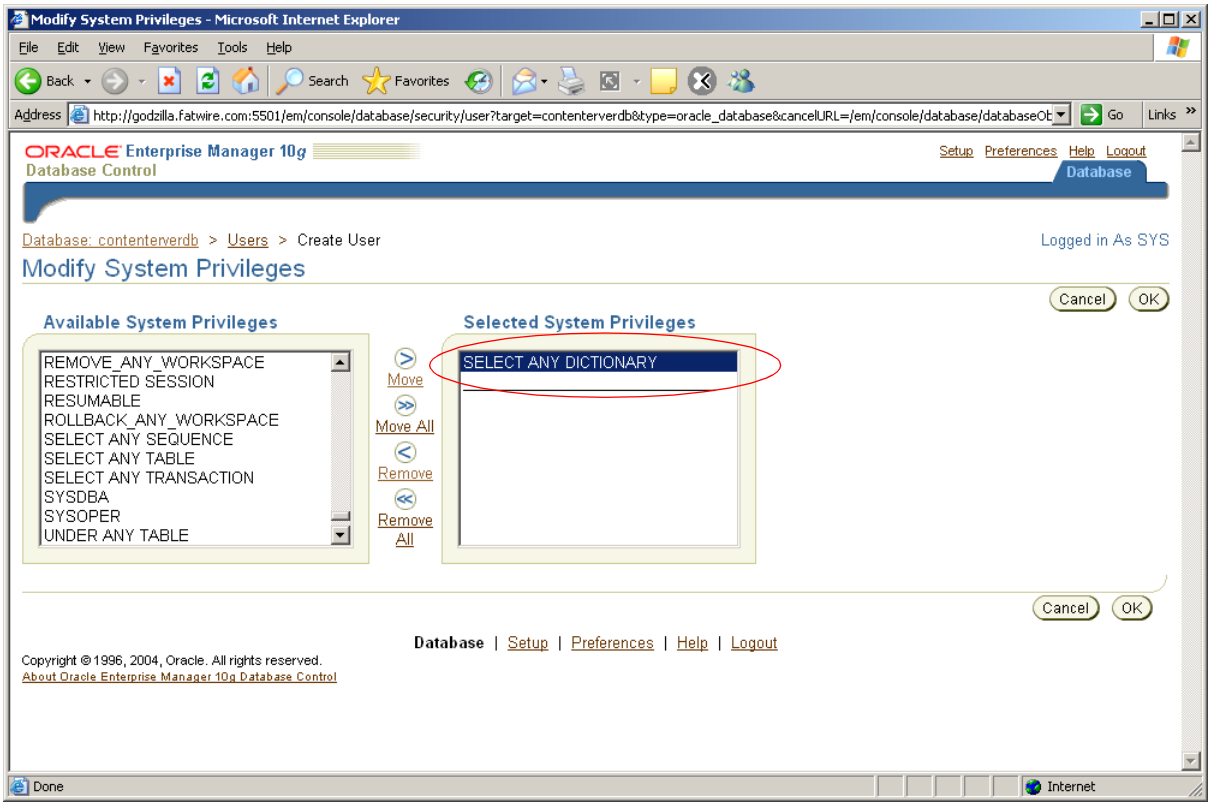
6. Click the **System Privileges** tab.
   a. Click the **Modify** button.



   b. From the list of "Available System Privileges" (left side), choose **Select Any Dictionary** and click the **Move** button.



Select Any Dictionary is moved to the “Selected System Privileges” list.



   c. (Optional) If you are creating a portal installation on WebLogic, also add the **Create View** privilege (by repeating step b).

   d. Click **OK**.

   The database is now ready for Content Server.

7. In the upper right-hand corner, click **Logout**.
8. The database is ready for Content Server. You can now create and configure the data source.

Next Step

You are now ready to create and configure the data source. For instructions, refer to your Content Server installation guide.

Chapter 2

Creating and Configuring an Oracle 11*g* Database

Use this chapter to set up an Oracle 11*g* database for your Content Server installation. For background information regarding database configuration and users' permissions, see Part 1, "Creating and Configuring a Database."

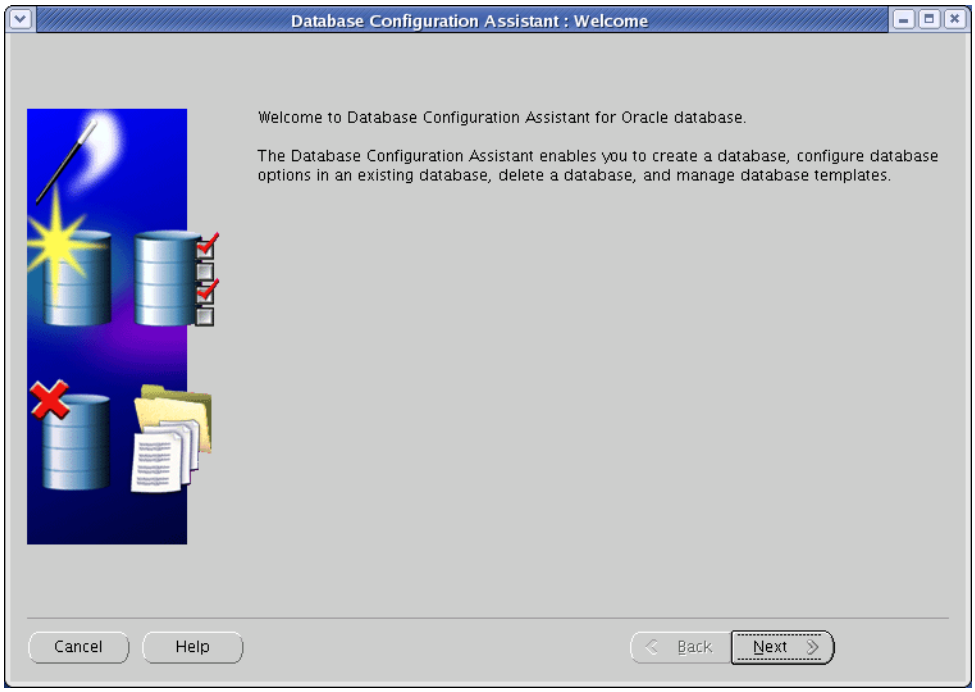
This chapter contains the following sections:

Step I. Create an Oracle 11*g* Database

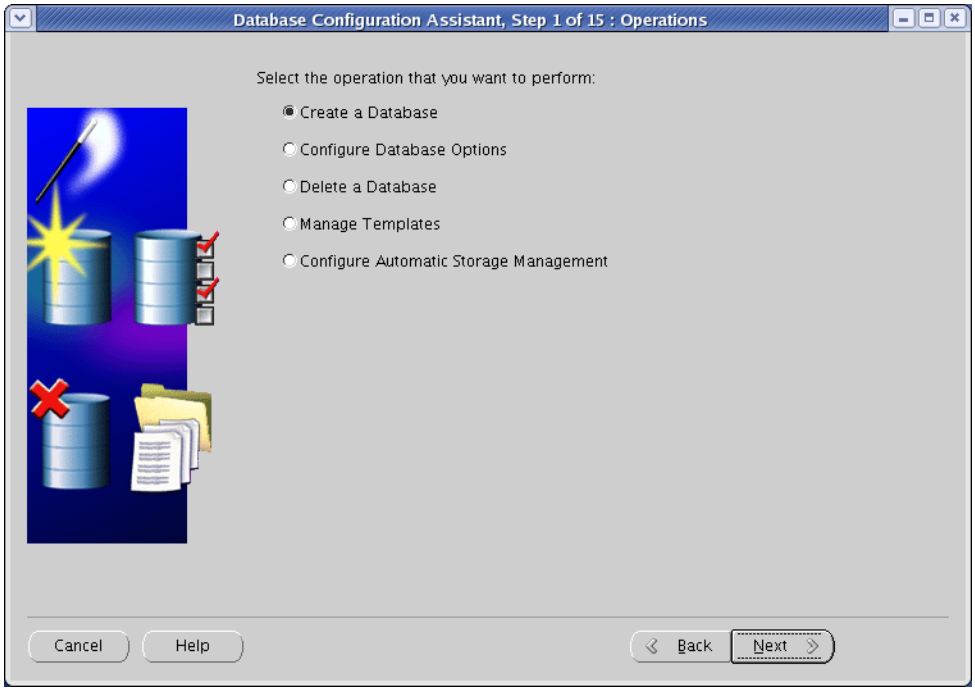
1. Launch the Oracle Database Configuration Assistant by executing the following command:

   ```
   <ora_home>/bin/dbca
   ```

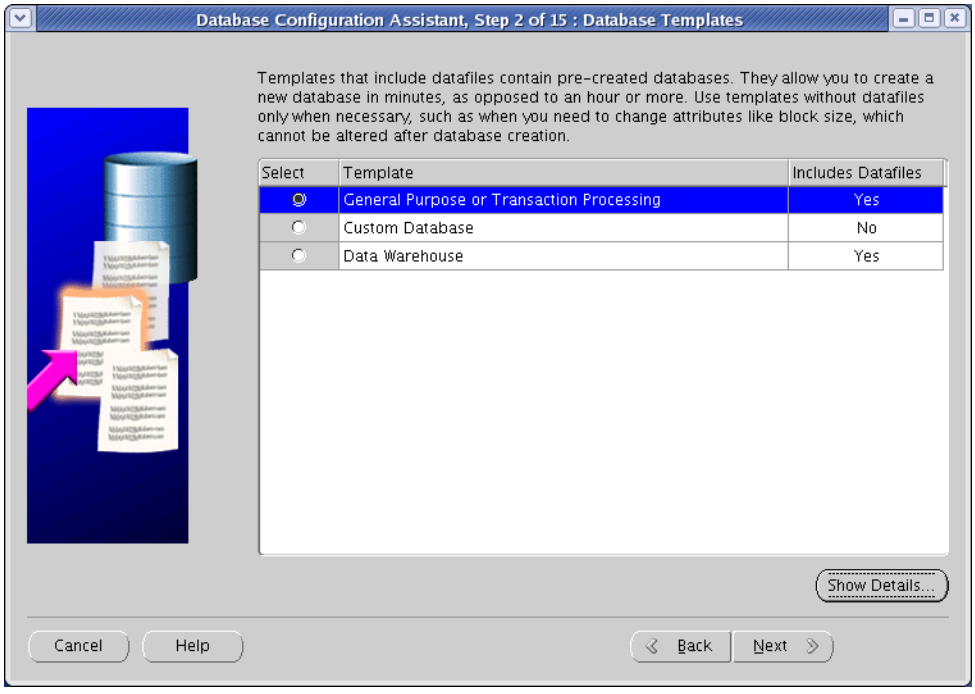
2. In the "Welcome" screen, click **Next**.



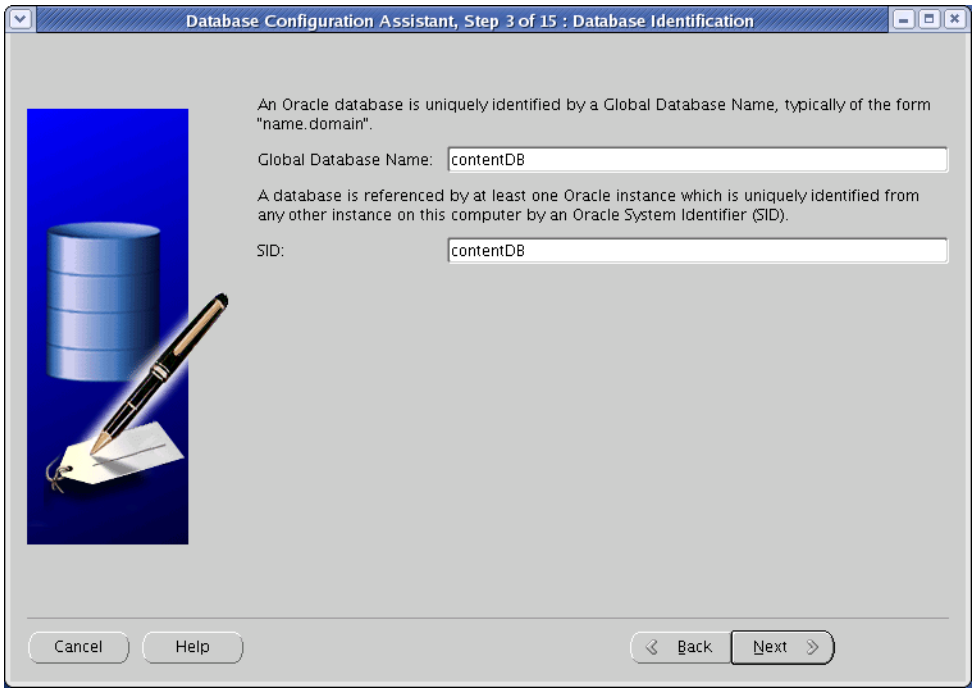
3. In the “Operations” screen, select **Create a Database** and click **Next**.



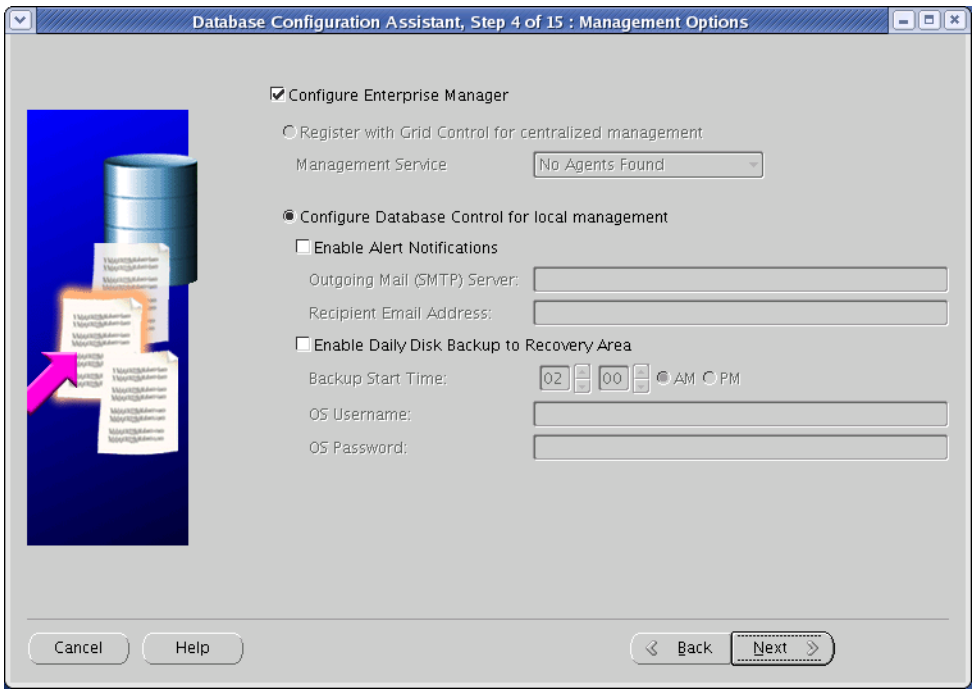
4. In the “Database Templates” screen, select **General Purpose or Transaction Processing** and click **Next**.



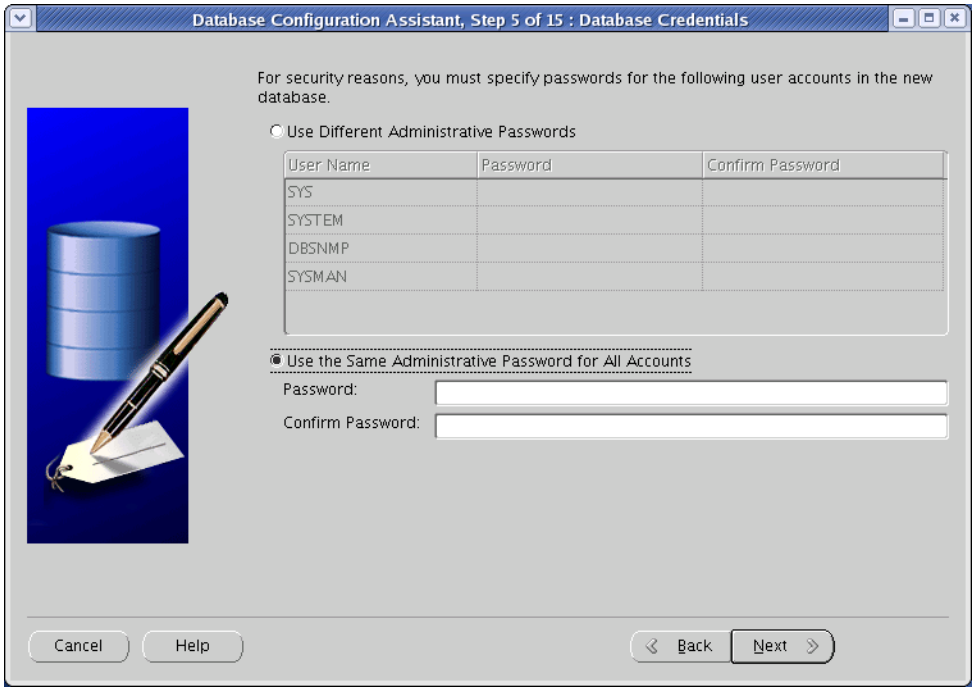
5. In the “Database Identification” screen, enter the global database name and the SID. (FatWire recommends using the same value for both; in our example, we are using `contentDB`.) When you are finished, click **Next**.



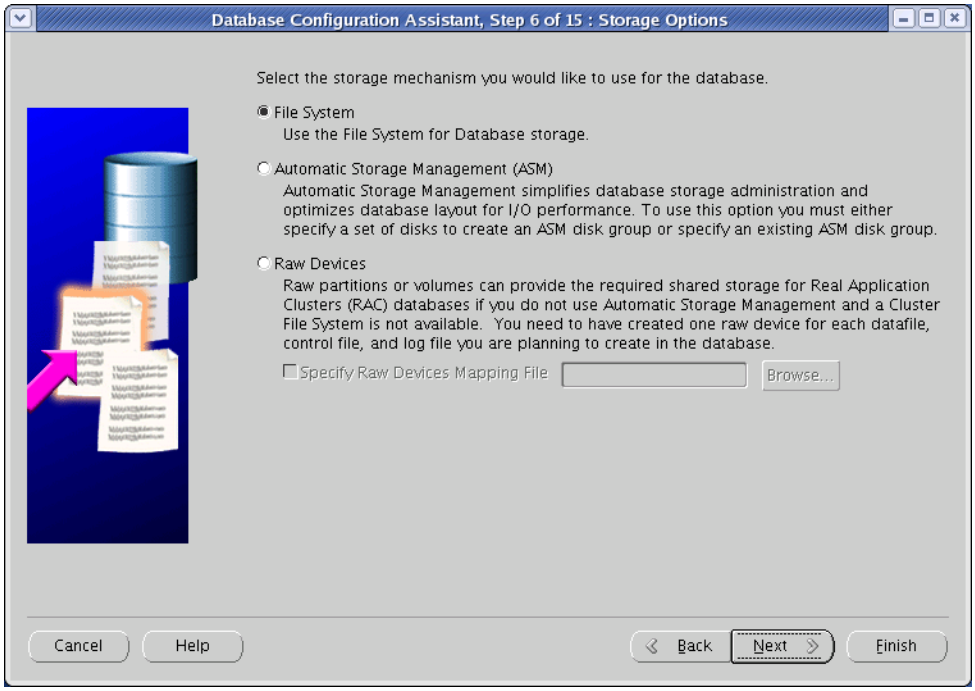
6. In the “Management Options” screen, select the **Configure Enterprise Manager** check box. Select other options as desired. When you are finished, click **Next**.



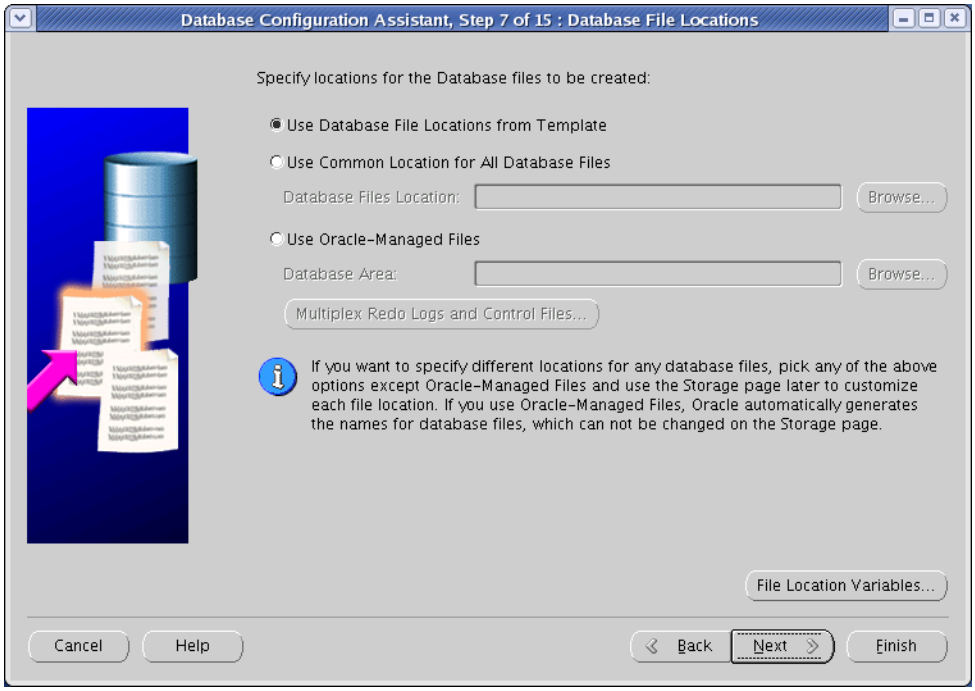
7. In the “Database Credentials” screen, do one of the following:
   - If you are installing a production system, select **Use Different Administrative Passwords**, enter a unique password for each database user shown in the table, and click **Next**.
   - If you are installing a non-production system, select **Use the Same Administrative Password for All Accounts**, enter and re-enter a password, and click **Next**.



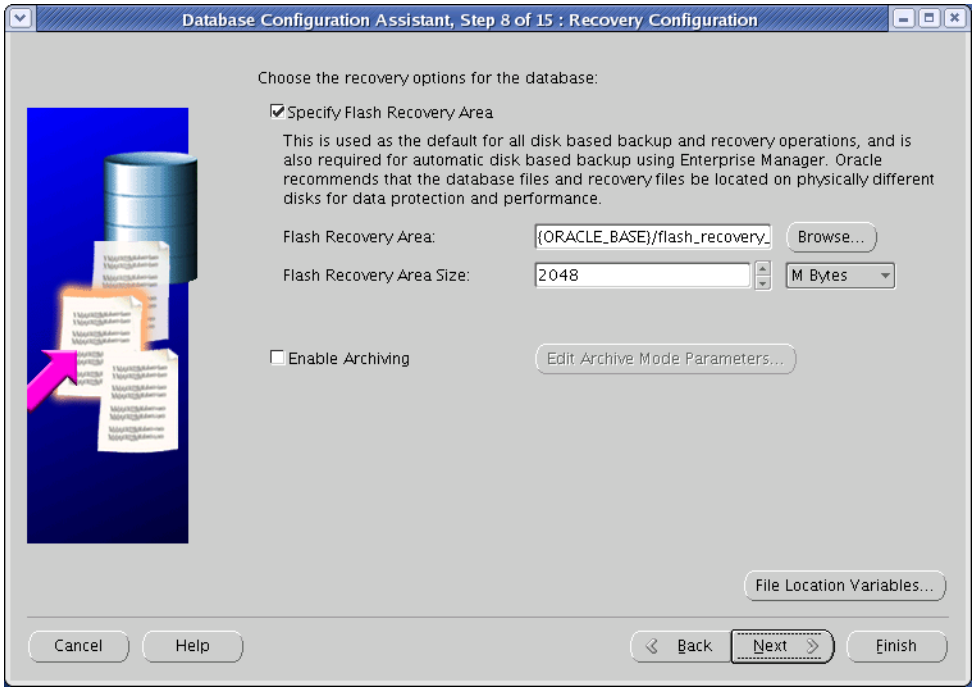
8. In the "Storage Options" screen, select **File System** and click **Next**.



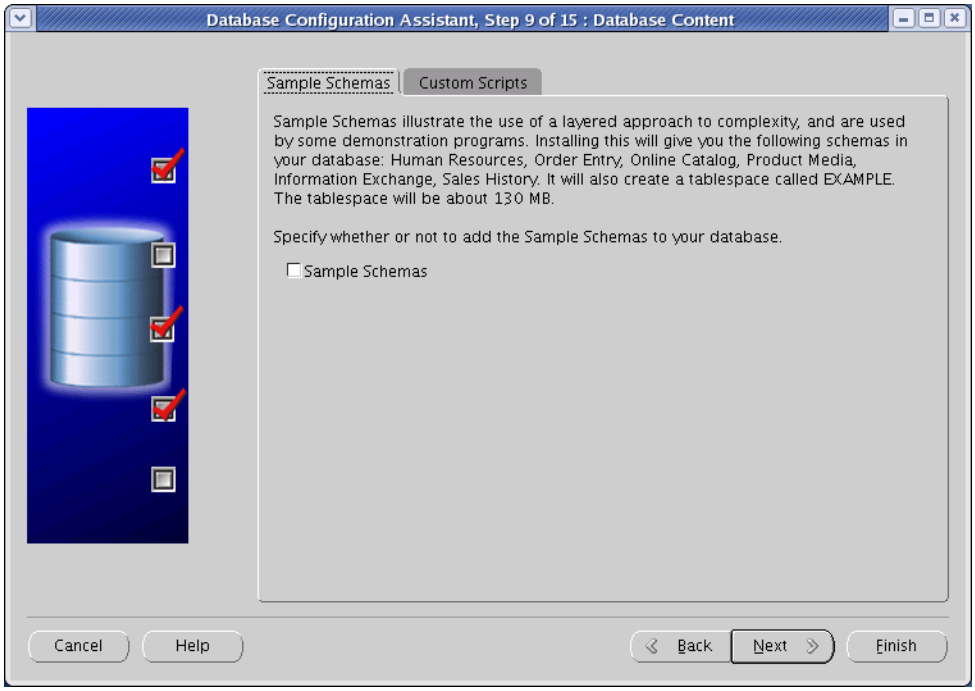
9. In the "Database File Locations" screen, select **Use Database File Locations from Template** (unless you want to use custom file names and locations) and click **Next**.



10. In the “Recovery Configuration” screen, leave the default values and click **Next**.

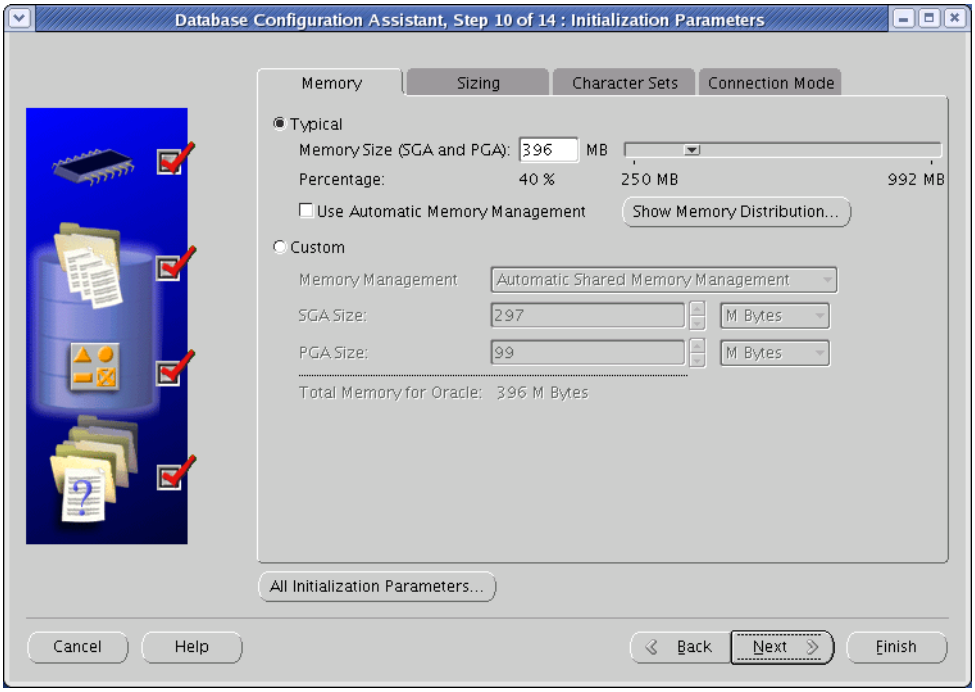


11. In the “Database Content” screen, click **Next**.



12. In the "Initialization Parameters" screen, do the following:

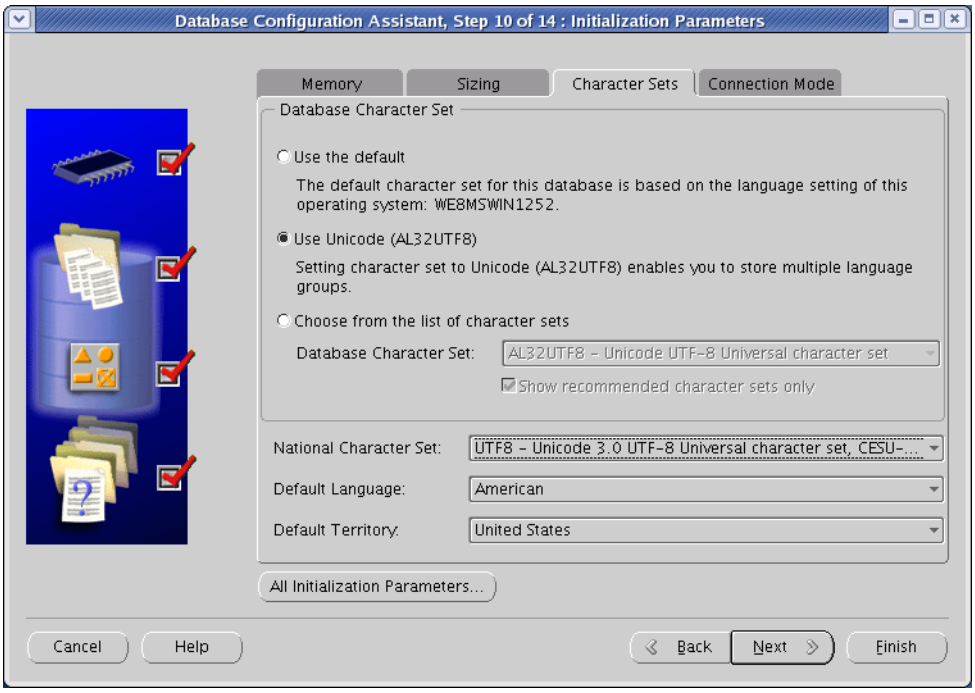
a. In the **Memory** tab, set the preferred memory size for your database. The value you enter here will depend on the size and contents of your database. FatWire recommends a minimum of 384MB.



b. In the **Character Sets** tab, do the following:

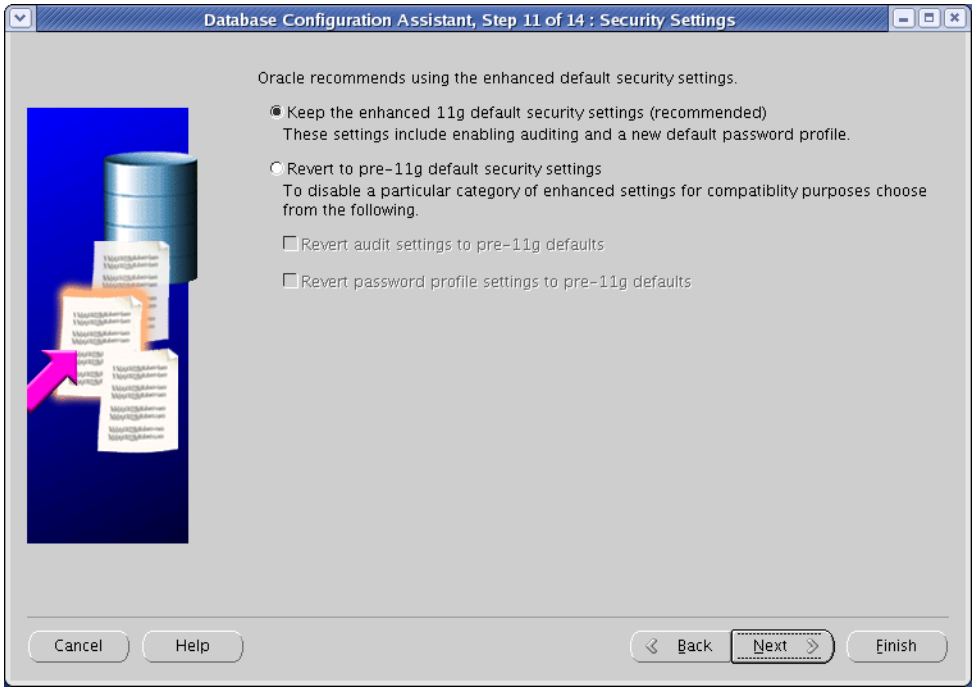
1) Select the **Use Unicode (AL32UTF8)** radio button.

2) In the "National Character Set" drop-down list, select **UTF-8 - Unicode 3.0 UTF-8 Universal Character Set**.

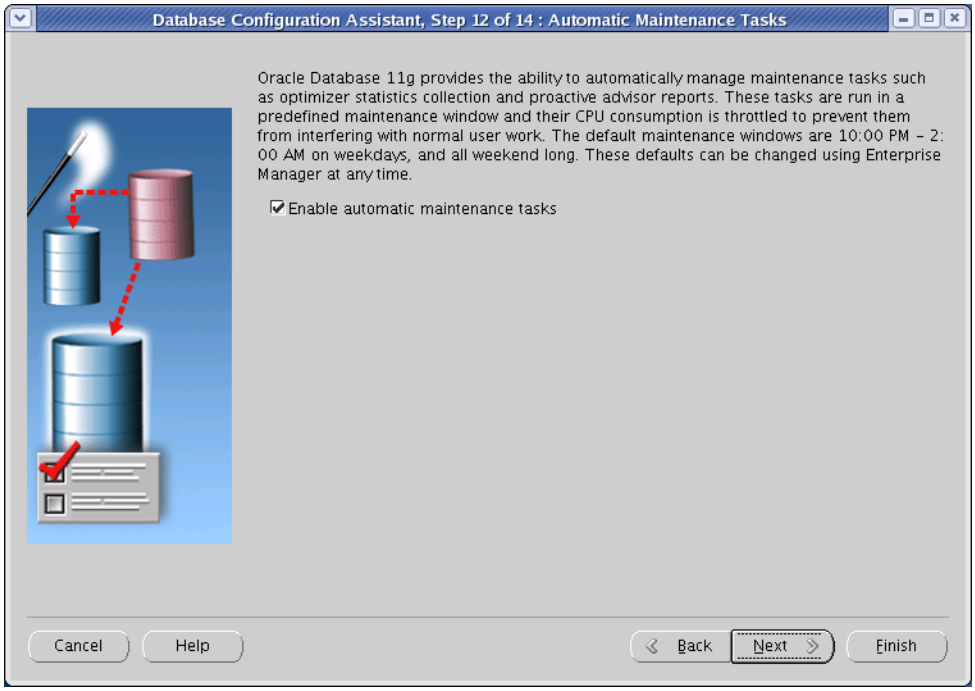


c. Click **Next**.

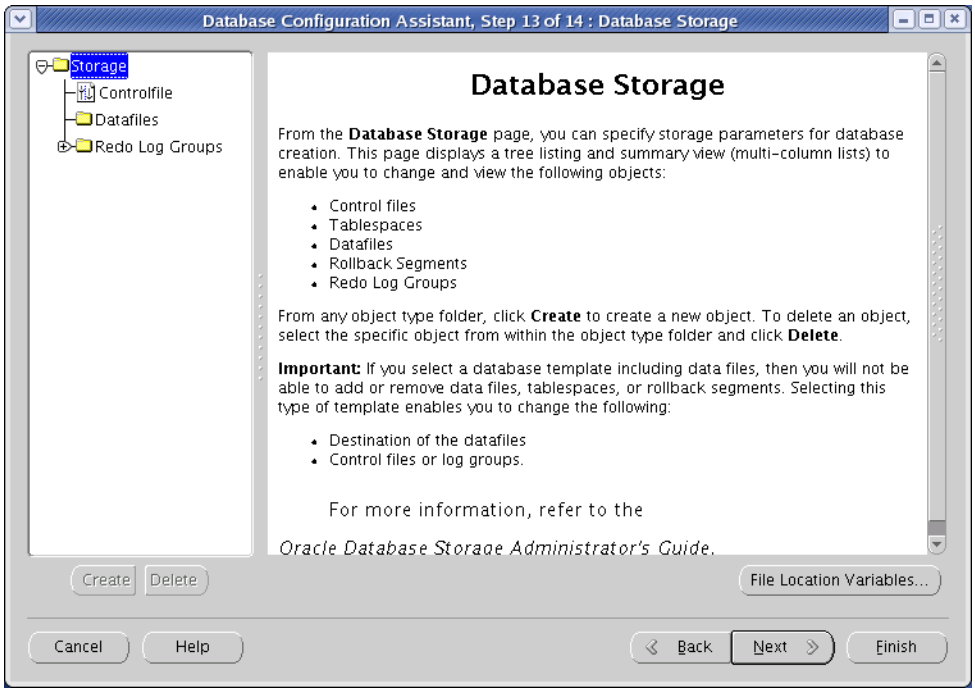
13. In the “Security Settings” screen, click **Next**.



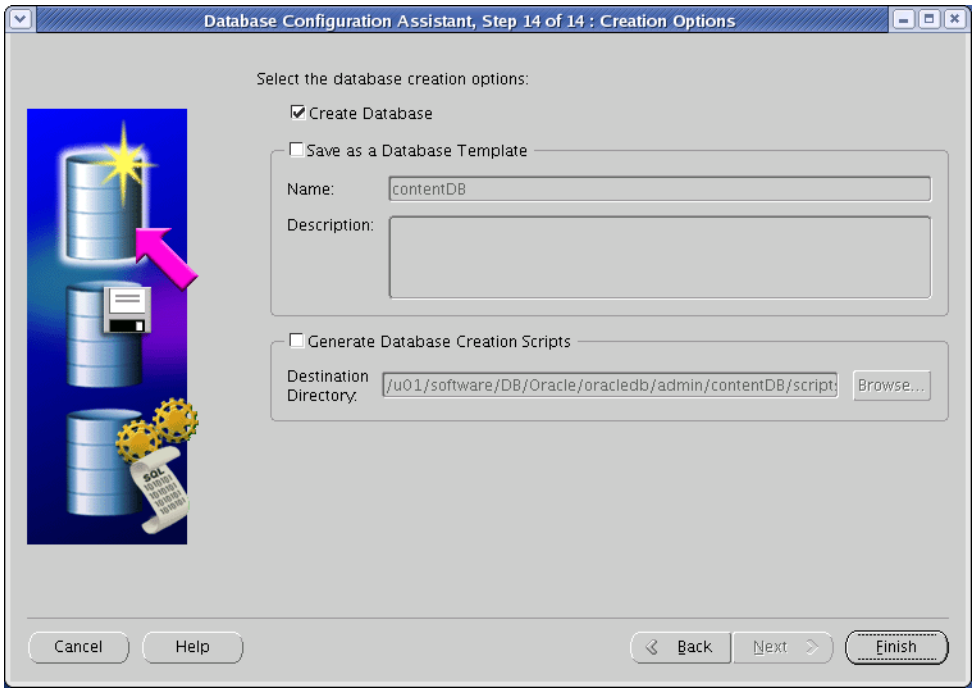
14. In the “Automatic Maintenance Tasks” screen, click **Next**.



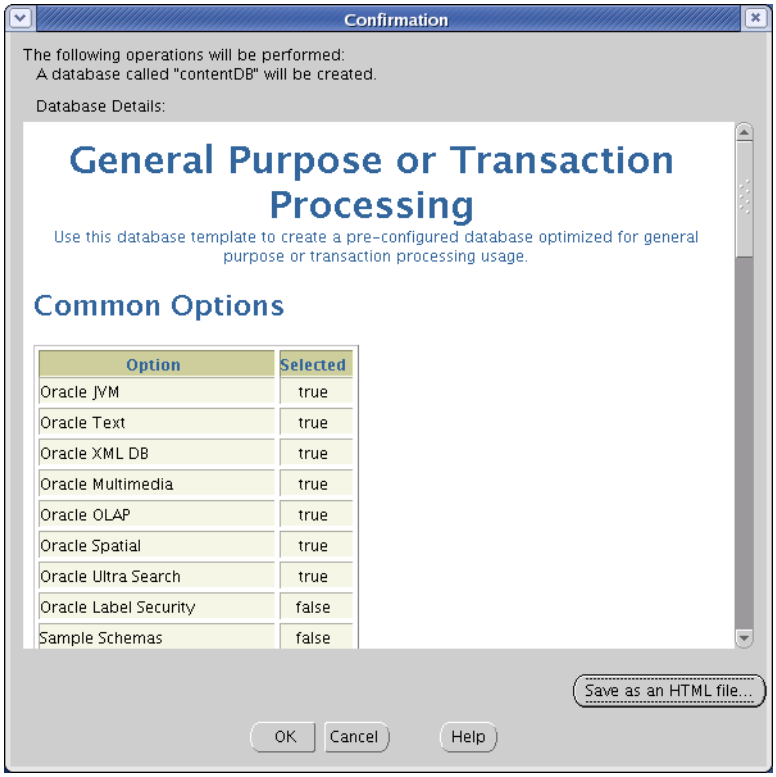
15. In the "Database Storage" screen, review the selected file locations. (If you need to make changes, click **File Location Variables**.) Click **Next**.



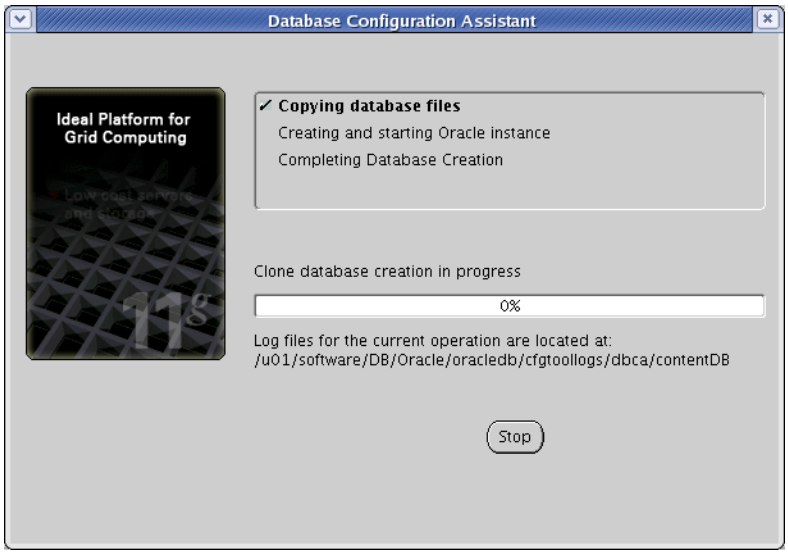
16. In the "Creation Options" screen, click **Finish**.



17. In the "Confirmation" screen, review the selected options, then click **OK**.



18. Allow the database creation tasks to complete. If any one of the tasks fails, remedy the problem before continuing.



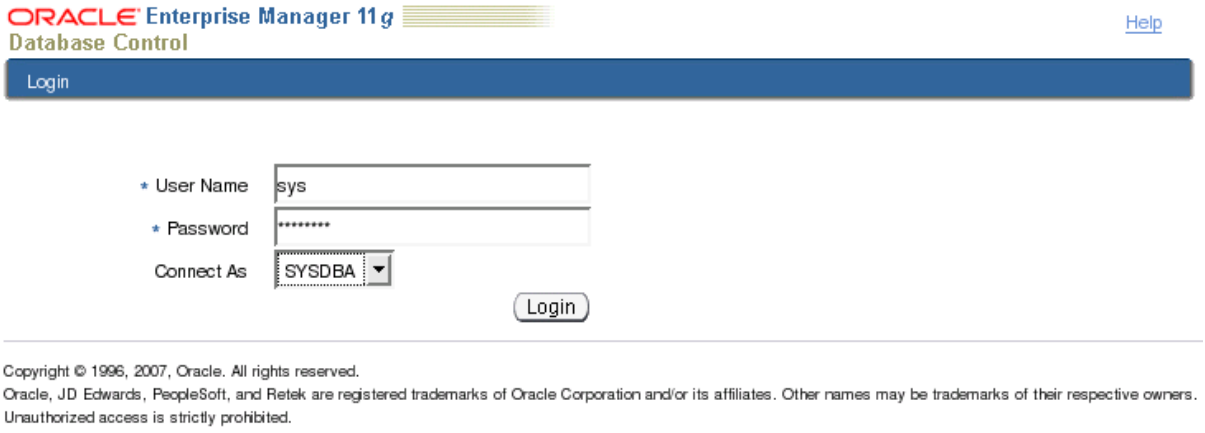
19. At the summary screen, make a record of the database SID and the database control URL, then click **Exit**.

Step II. Create a New User for Content Server

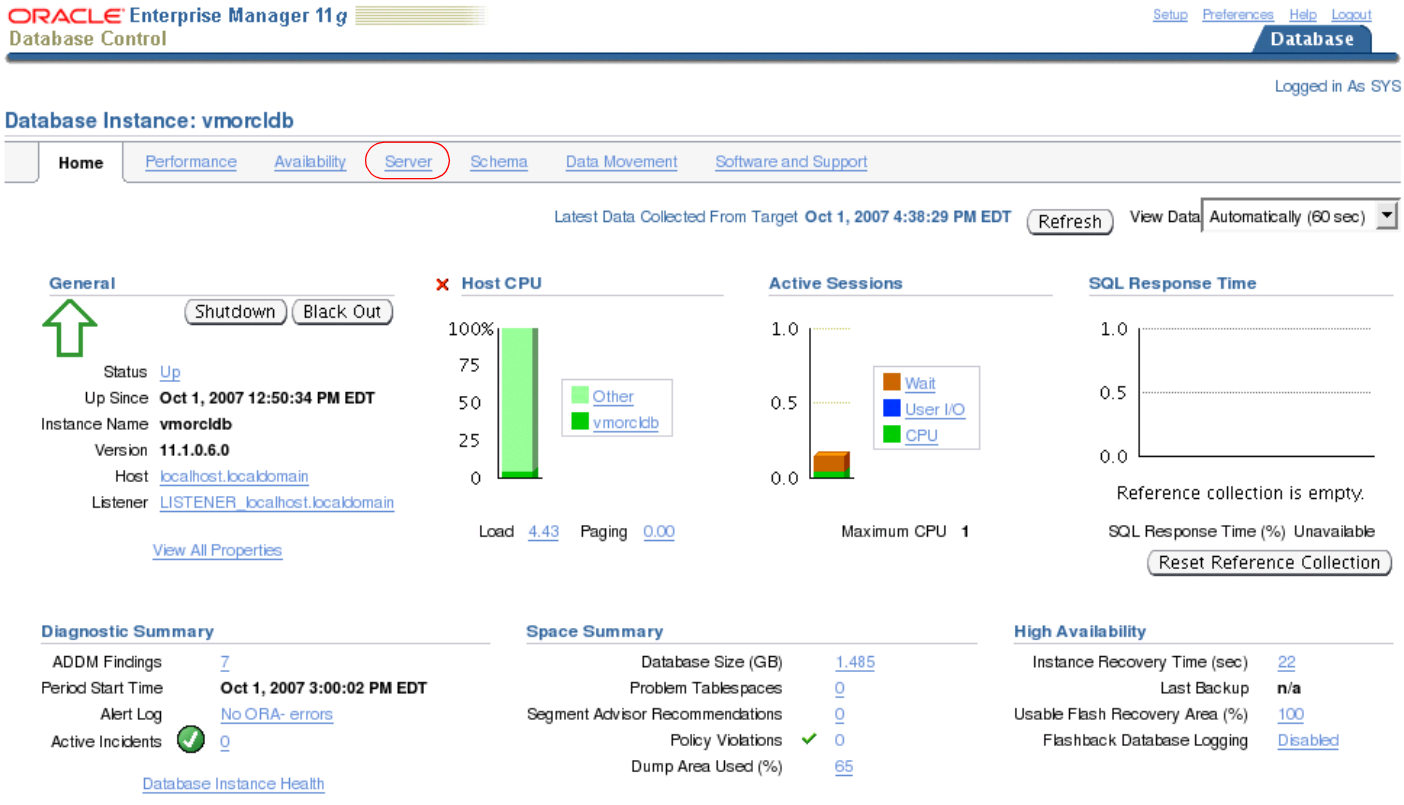
1. Determine the Console Server port:
   a. Open the `emoms.properties` file in a text editor. The file is located in:
      `<ora_home>/<servername>_<SID>/sysman/config/`
   b. Find the line,
      `oracle.sysman.emSDK.svlt.ConsoleServerPort`
      and make a record of the port number value at the end of the line.
2. Log in to the Oracle Enterprise Manager console:
   a. Execute the following command: **`emctl status dbconsole`**
      The command should return an output similar to the following:

```
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. Open a browser and go to the URL highlighted in bold in step a above. If you see a “Security Mismatch” error, ignore it (the error appears if you are using a self-signed certificate).
   c. Log in as the `sys` user (you specified a password for this user in step 7 on page 41) connecting as **SYSDBA**.

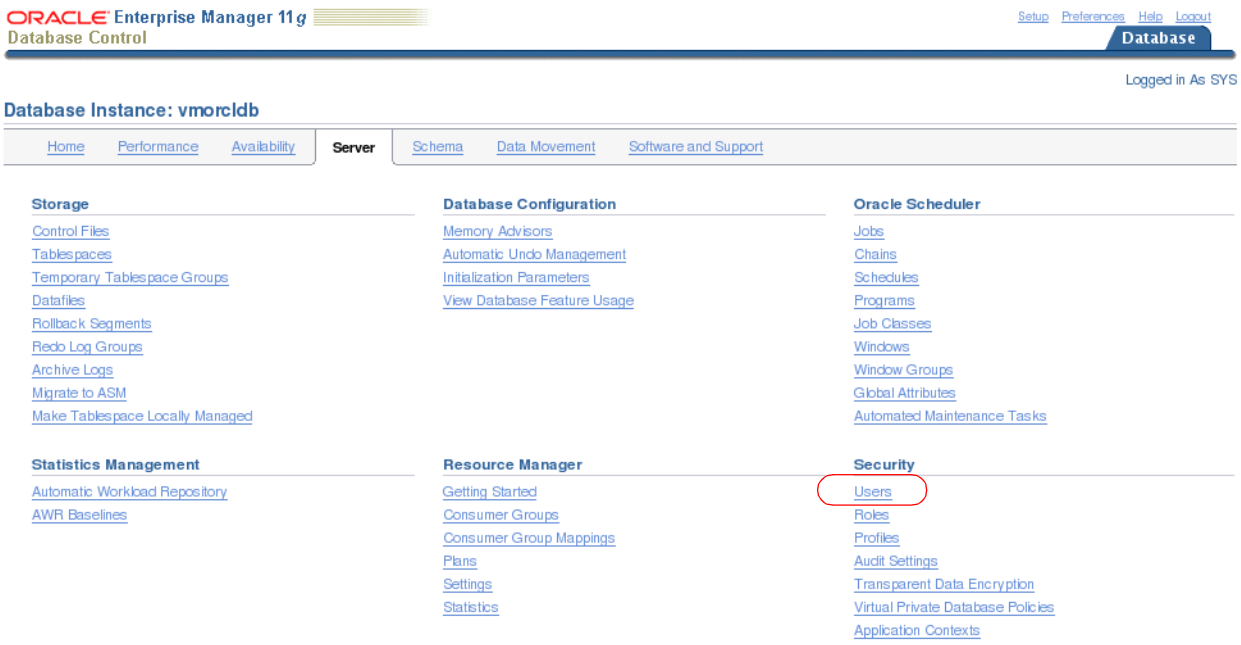


3. In the tab bar, click **Server**.

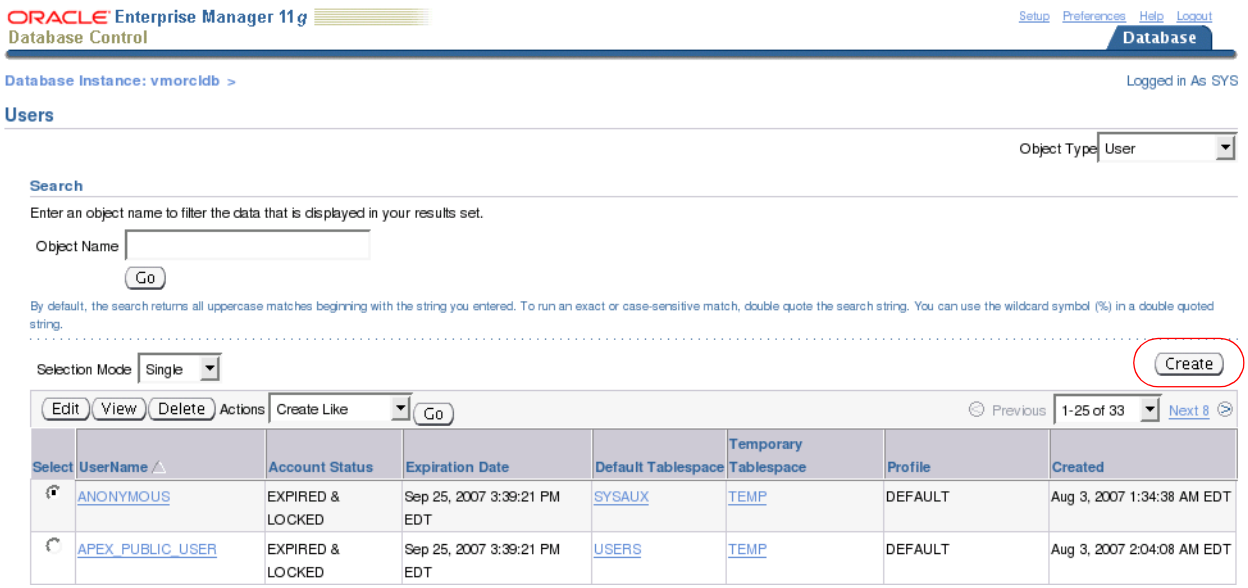


4. Create the new user. Do the following:

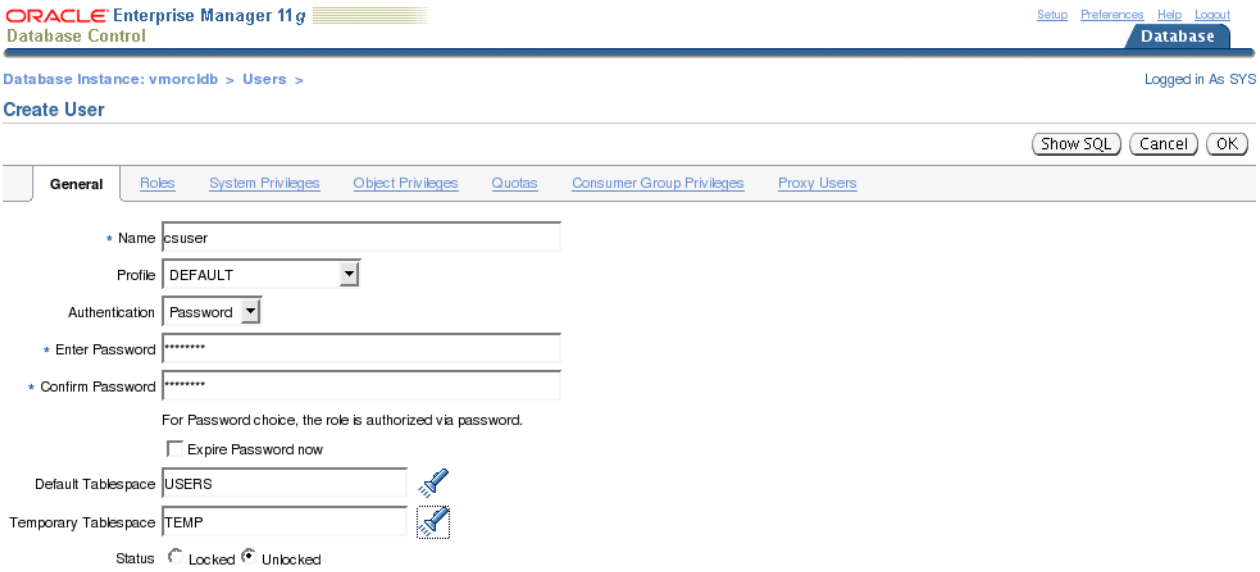
   a. In the "Security" section of the page, click **Users**.



   b. Click **Create** near the top right corner of the user list.



c. In the "Create User" form, fill in all required fields (marked with an asterisk). Fill in all other fields as necessary.



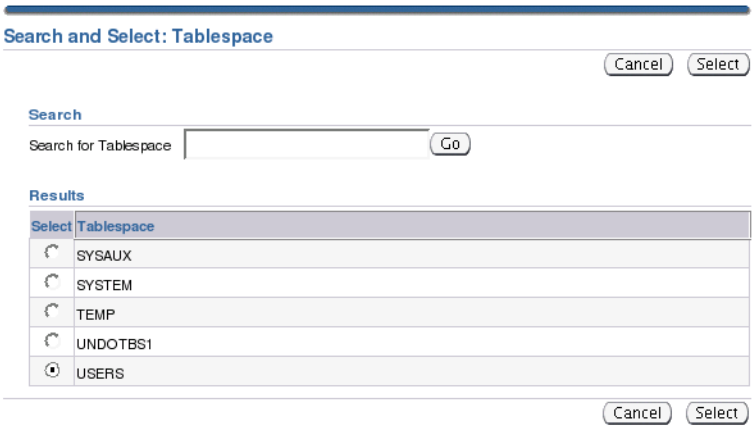
5. Select the default and temporary tablespaces for the new user. Do the following:

a. Select the default tablespace:

1) In the "Create User" form, click the **flashlight** button next to the **Default Tablespace** field.

2) In the form that appears, select the **USERS** radio button.

3) Click **Select**.



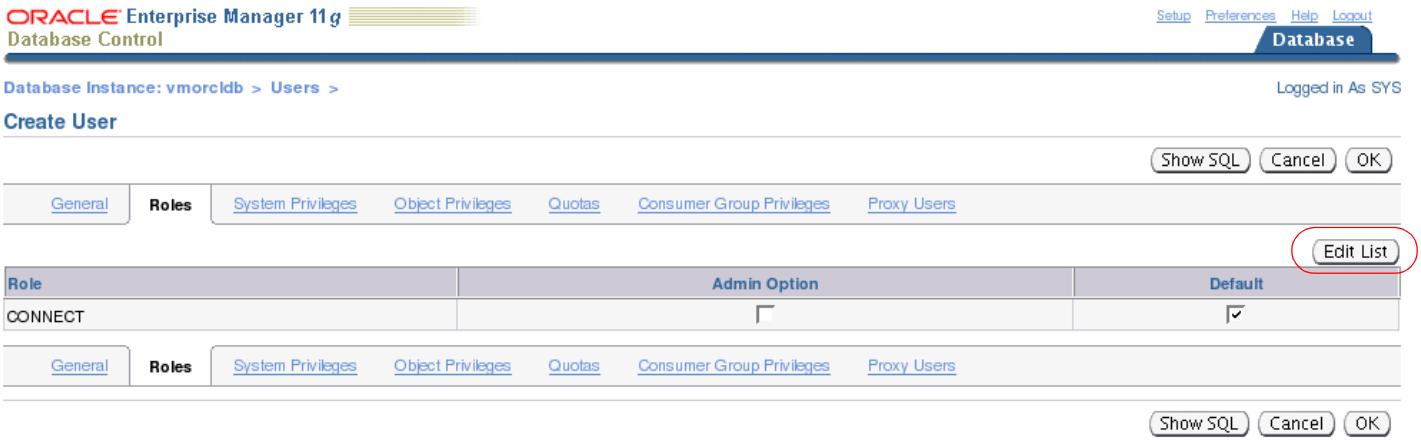
b. Select the temporary tablespace:

1) In the "Create User" form, click the **flashlight** button next to the **Temporary Tablespace** field.

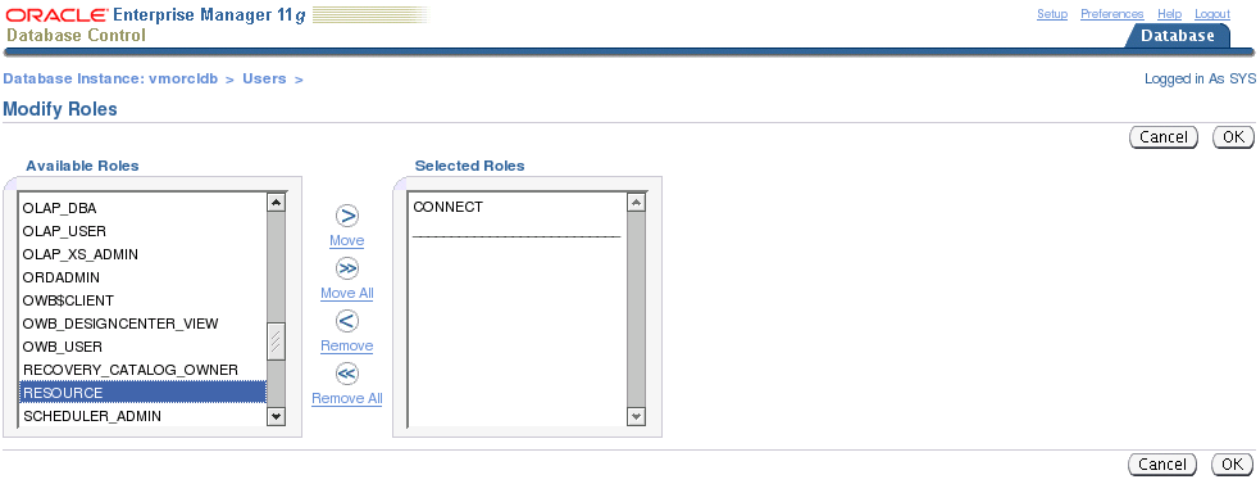
2) In the form that appears, select the **TEMP** radio button.

3) Click **Select**.

6. Assign the “Resource” role to the new user. Do the following:
   a. In the tab bar, click **Roles**.
   b. Click **Edit List** at the top right corner of the list of roles.

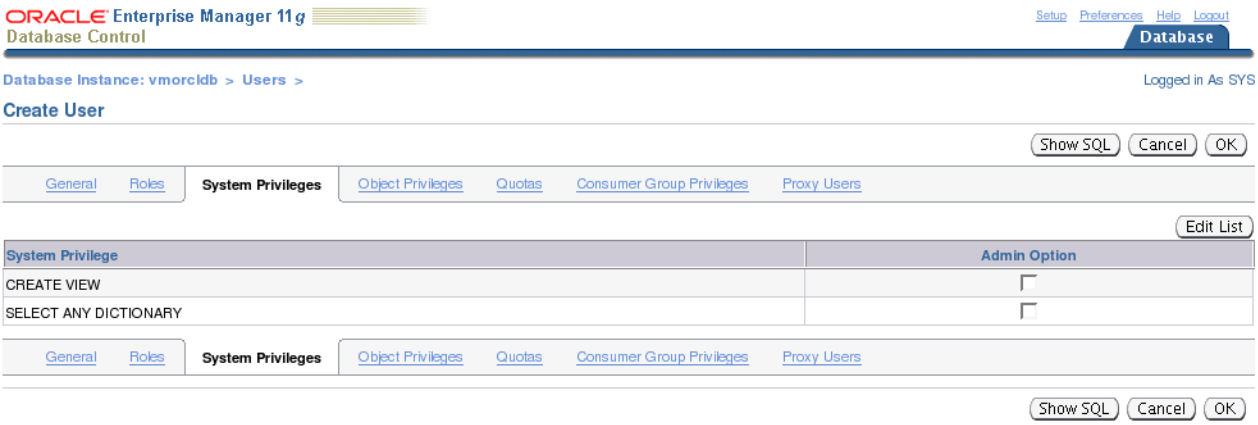


   c. In the “Available Roles” list, select the **RESOURCE** role and click **Move**.
      The role appears in the “Selected Roles” list.
   d. Click **OK**.

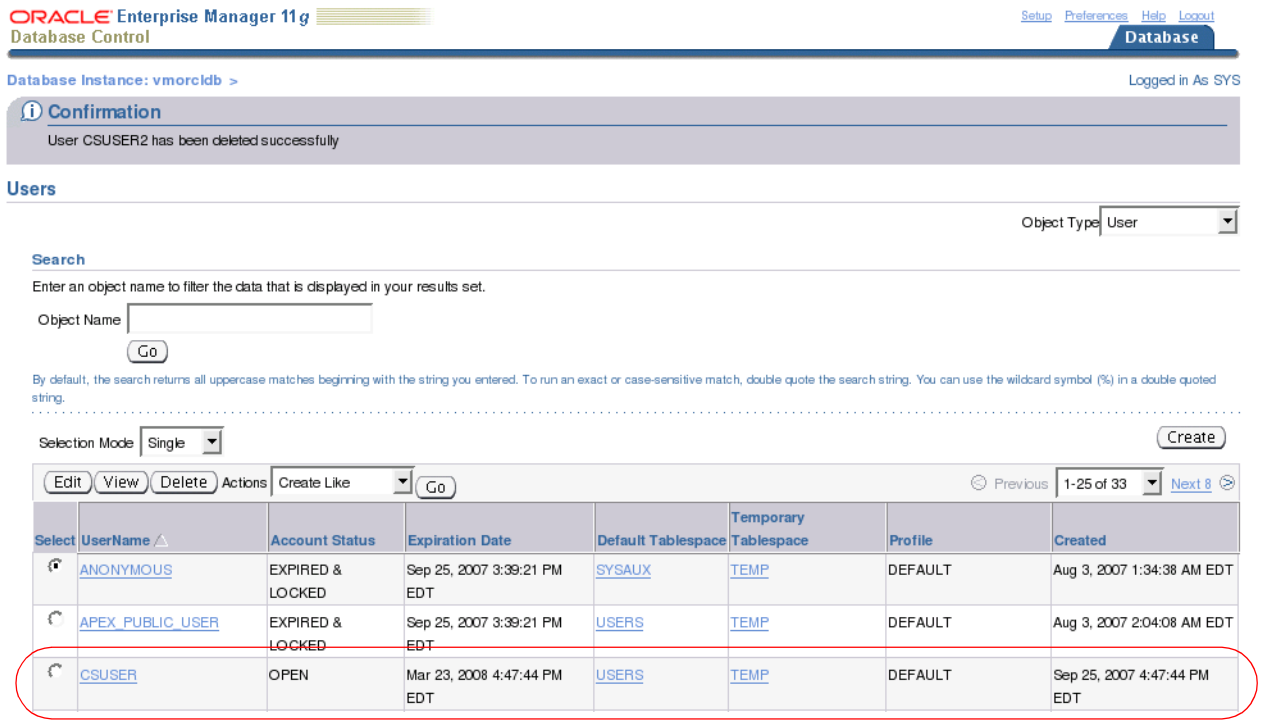


7. Assign system privileges to the new user. Do the following:
   a. In the tab bar, click **System Privileges**.
   b. Click **Edit List** at the top right corner of the list of privileges.
   c. In the “Available System Privileges” list, select **CREATE VIEW** and **SELECT ANY DICTIONARY**, then click **Move**.
      The privileges appear in the “Selected System Privileges” list.

d. Click **OK**.



A message confirming the creation of the new user is displayed. The user appears in the list of users.



Next Step

You are now ready to create and configure the data source. For instructions, refer to your Content Server installation guide.

Chapter 3

Creating and Configuring an MS SQL Server Database

Use this chapter to set up a SQL Server database for your Content Server (Spark) installation. For background information regarding database configuration and users' permissions, see Part 1, "Creating and Configuring a Database."

This chapter contains the following section:

Creating a Database on MS SQL Server 2005

To create and configure a database on MS SQL Server 2005

1. Use the Windows Account Manager to create a new user account for the CS database user (for example, `csuser`), and assign a password to the account.
1. Open SQL Server Manager Studio.
2. Log in to MS SQL Server:
   a. Enter your user name and password (the default user name is `sa`).
   b. Click **Connect**.
3. Create the database:
   a. In the left-hand tree, expand the **Databases** node.
   b. Right-click the **Databases** node and select **New Database** from the pop-up menu.
   c. In the "New Database" window, enter a name for your database and click **OK**.

   Your newly created database appears under the **Databases** node in the tree.
4. In the tree, expand the node representing your newly created database, then expand the **Security** node underneath it.
5. Click the **Users** tab.
6. Right-click within the white space underneath the list of existing users and select **New User** from the pop-up menu.
7. In the "Database User - New" window, enter the user name of the CS database user (which you created in step 1 of this procedure) into the **User name** and **Login name** fields.
8. In the "Owned Schemas" and "Role Members" areas, select the **db_owner** check box.
9. Click **OK**.

Database configuration is complete. You are now ready to create and configure the data source using the user name and password of the CS database user you created in step 1 of this procedure. For instructions, refer to your Content Server (Spark) installation guide.

Chapter 4

Creating and Configuring an IBM DB2 8.*x* Database

Use this chapter to set up a supported IBM DB2 database for your Content Server installation. For background information regarding database configuration and users' permissions, see Part 1, "Creating and Configuring a Database."

This chapter contains the following sections:

Creating and Configuring DB2 8.*x* for Content Server

1. Open DB Control Center (`db2cc`).
2. Browse to the instance under which you want to create the new database.

   If you do not have an existing instance in the left-hand tree, do the following:

   a. Right-click **Instances** and click **Add…**

   b. Fill in the form provided (or click **Discover**) then click **OK**.
3. Right-click **Branch Databases > Create > Database Using Wizard…**
4. In the "Create Database Wizard," fill in the following screens as indicated:

   a. "Database name"
   Enter a unique database name (such as `CSDB2`), then click **Next**.

   b. "Specify how and where to store the user tables."
   Leave the default option **Low maintenance** selected and click **Next**.

   c. "Specify how and where to store the system catalog tables."
   Leave the default option **Low maintenance** selected and click **Next**.

   d. "Specify how and where to store system temporary tables."
   Leave the default option **Low maintenance** selected and click **Next**.

   e. "Tune the performance of this database." Click **Next**.

   f. "Specify the locale for this database."
   Complete the following steps:

      1) In the **Code Set** drop-down list, select **UTF-8**.

      2) Under **Collating Sequence**, leave the default option selected.

      3) Click **Next**.

   g. Review the actions that will take place when you click **Finish**, then click **Finish**.
5. A DB2 message box appears, giving you the option to run the "Configuration Advisor." Click **No**.

   A new database (with the name you provided in step 4) is now available in the left-hand tree.
6. In the left-hand tree, right-click **Buffer Pools > Create**.
7. In the "Create Buffer Pool" dialog box, do the following:

   a. In the "Buffer Pool name" field, add a unique name (such as `CSBUFFER32`).

   b. In the **Page size** drop-down list, select **32**.

   c. Click **OK**.
8. In the left-hand tree, right-click **Table Spaces > Create**.
9. In the "Create Table Space Wizard," fill in the following screens as explained below:

   a. "Specify a name for your table space."
   Enter a unique name (such as `csTableSpace`) in the "Table Space name" field.
   Then click **Next**.

b. "Specify the type of table space you want to create."
Leave the default value and click **Next**.

c. "Specify a buffer pool for your new table space."
Select the buffer pool created in step 7 of this procedure and click **Next**.

d. "Select the space management system that you want to use."
Leave the default option **System-managed space (low maintenance)** selected and click **Next**.

e. "Define containers for this table space."
Click **Add**, then complete the following steps:

1) In the "Define Container" dialog box, enter a unique name for this container (such as `CScontainer`).

2) Under "Current Directory," select a location for this table space (note that you must select a physical location on a mounted disk where you want to place this table space; if you do not have an acceptable location at this point you should create one). Once you have selected a location, click **OK**.

3) Click **Next** in the "Define Container" dialog box.

f. "Specify the extent and prefetch sizes for this table space."
Leave the default options selected and click **Next**.

g. "Select hard drive specifications."
Select the appropriate option for your physical media type from the list and click **Next**.

h. "Specify the dropped table recovery option for your new table space." Click **Next**.

i. Review the actions that will take place when you click **Finish**, then click **Finish**.

10. Repeat step 9 of this procedure to create a temporary table space, making the following adjustments to the procedure:

a. When completing step 9a, indicate in the name that this is a temporary table space.

b. When completing step 9b, select **System Temporary** for the type of table space.

11. In the left-hand tree, select **User and GroupObjects** and right-click **DB Users** > **Add**.

a. In the "Database" tab, do the following:

1) Select a user from the **User** drop-down list.

> **Note**
>
> The drop-down list contains all valid system users. If there are no valid system users, you must create one before continuing.

2) Under "Grant authorities for the Selected User," select all the options.

> **Note**
>
> This is not recommended for a delivery system. Choose the options that are appropriate for your delivery system)

b. Click the **Table Space** tab and do the following:

1) Click **Add Tablespace**. In the "Add Tablespace" dialog box, select the tablespace created in step 9 of this procedure and click **OK**.

2) In the "Table Space" tab, the new table space is now selected, but has a ∅ symbol next to it. Select **Grant** from the **Privileges** drop-down list (located near the bottom of the tab).

c. Repeat step b for the temporary table space created in step 10.

d. Optionally, repeat step b to add the default table space `USERSPACE1`.

> **Note**
>
> The default table space was created with the database. Therefore its location is not under your control.

e. Click **OK**.

12. In the left-hand tree, right-click the database created in step 4 of this procedure and click **Configure Parameters**. In the list that opens, make the following changes:

a. Change `LOCKLIST/100` to `LOCKLIST/1024`

b. Change `LOCKTIMEOUT/None` to `LOCKTIMEOUT/30`

c. Change `APPLHEAPSZ/256` to `APPLHEAPSZ/1024`

13. Database configuration is complete. You are now ready to create and configure the data source. For instructions, refer to your Content Server installation guide.

Chapter 5

Creating and Configuring an IBM DB2 9.1 Database

Use this chapter to set up a supported IBM DB2 database for your Content Server installation. For background information regarding database configuration and users' permissions, see Part 1, "Creating and Configuring a Database."

This chapter contains the following sections:

Installing and Configuring DB2 9.1 for Content Server

To install and configure a DB2 9.1 database, you will complete the following steps:

A. Install DB2

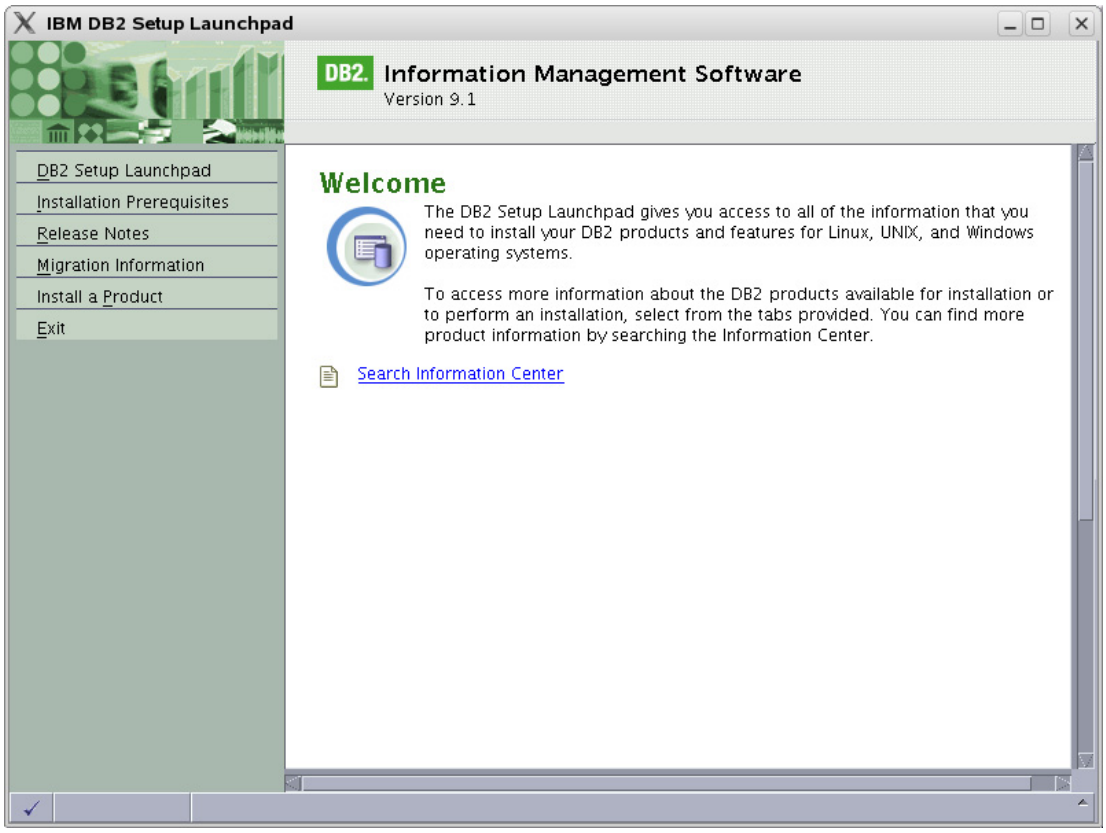
B. Create a New DB2 Database

C. Create a User for the New Database

D. Configure the Database

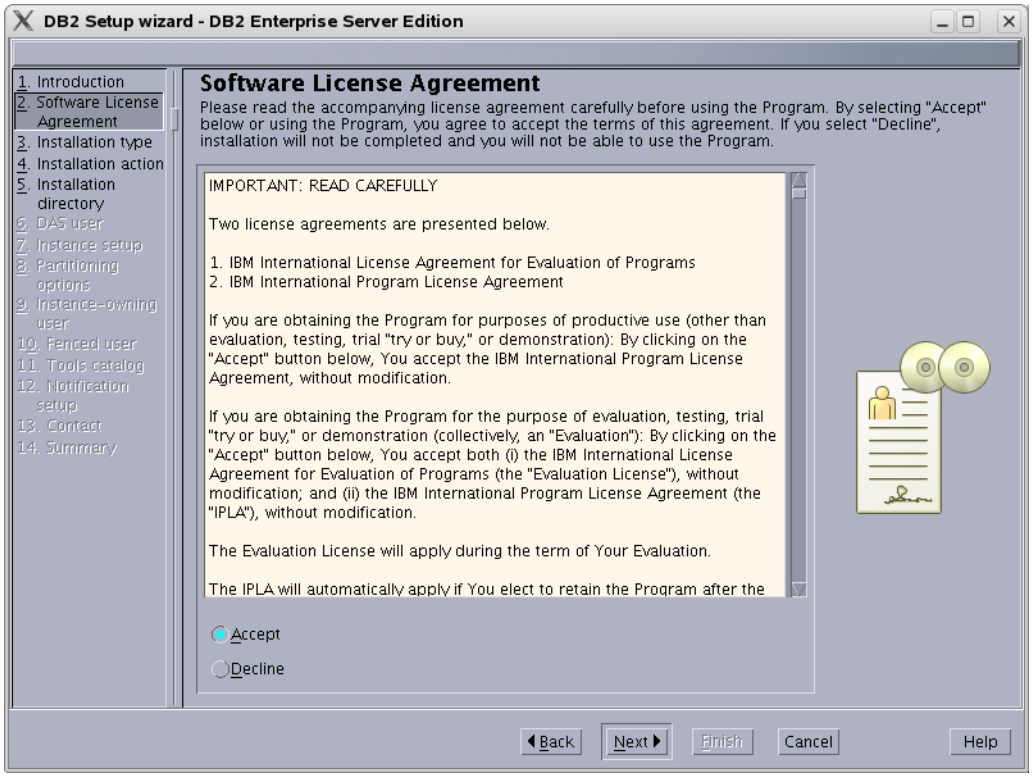
A. Install DB2

1. Uncompress the correct installation file for your distribution.
2. Run `./db2setup`
3. In the "Information Management Software" screen, select **Install a Product**.

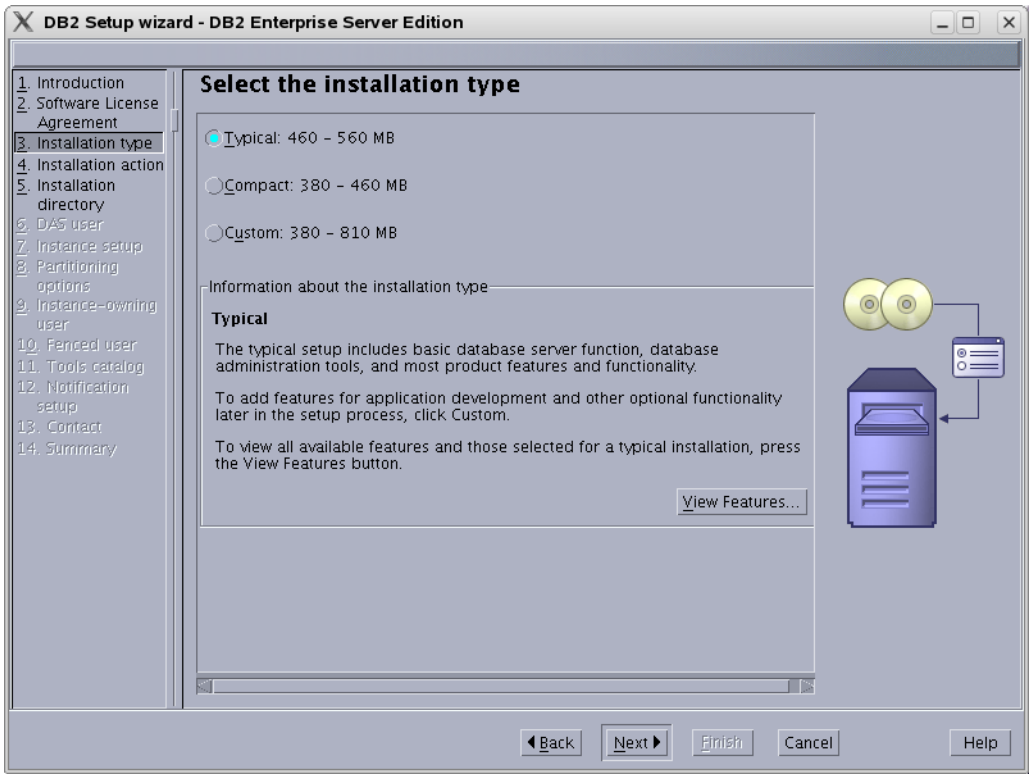


4. Under “DB2 Enterprise Server Edition,” select **Install New**.

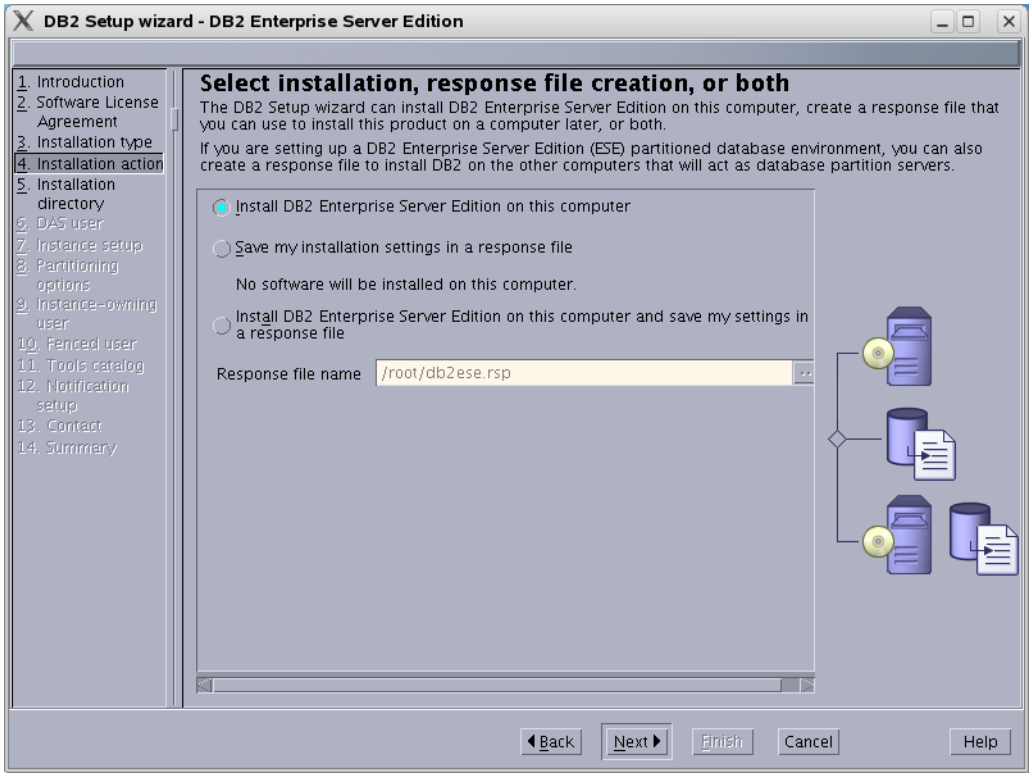
5. In the “Welcome to the DB2 Setup Wizard,” click **Next**.
6. In the “Software License Agreement” screen, click **Accept**, then click **Next**.



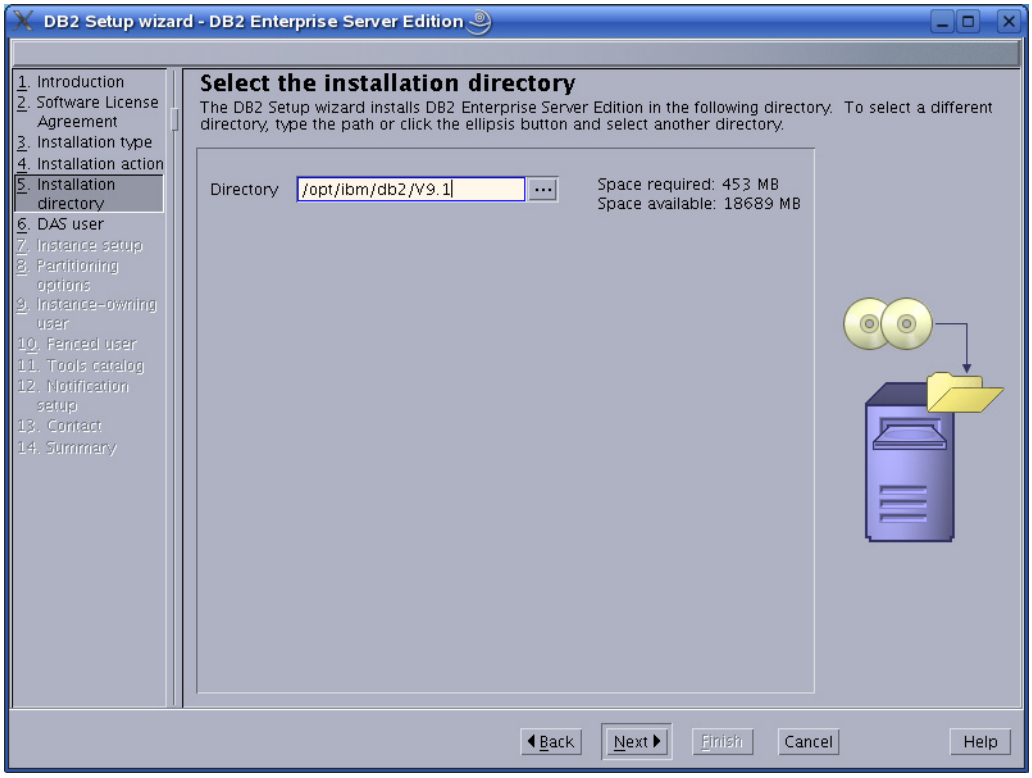
7. In “Select the Installation Type,” select **Typical** and click **Next**.



8. In "Select installation, response file creation, or both," select **Install DB2 Enterprise Server Edition on this Computer** and click **Next**.



9. In “Select the installation directory,” either enter a directory or use the default and click **Next**.

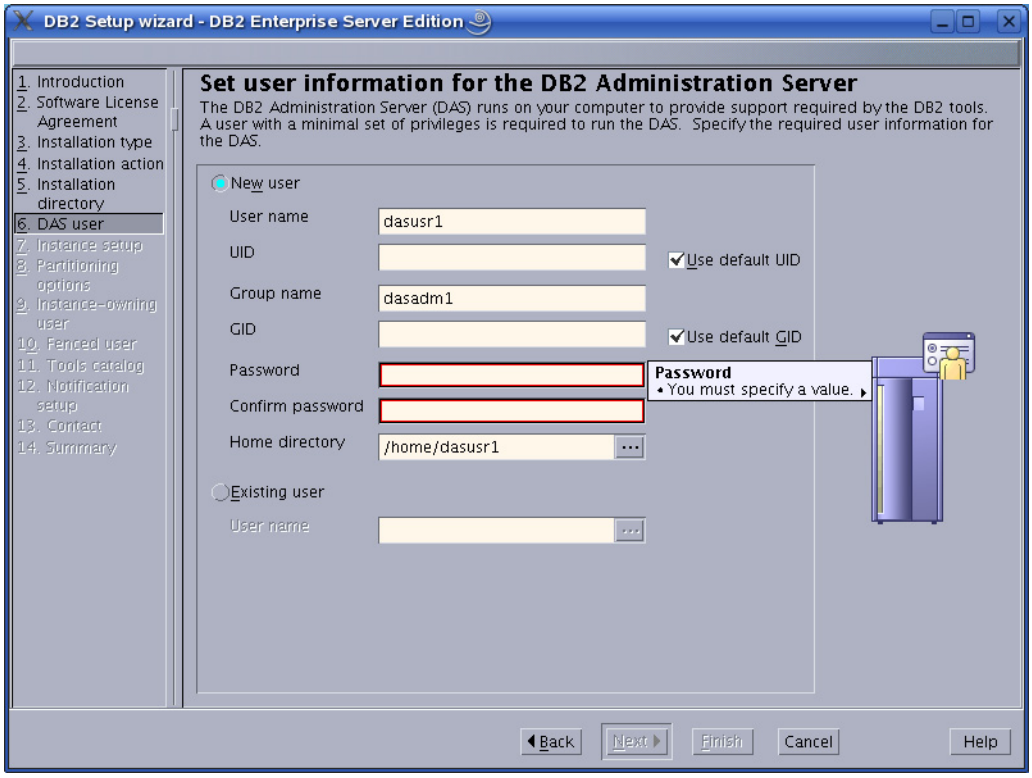


10. In “Set user information for the DB2 Administration Server”:

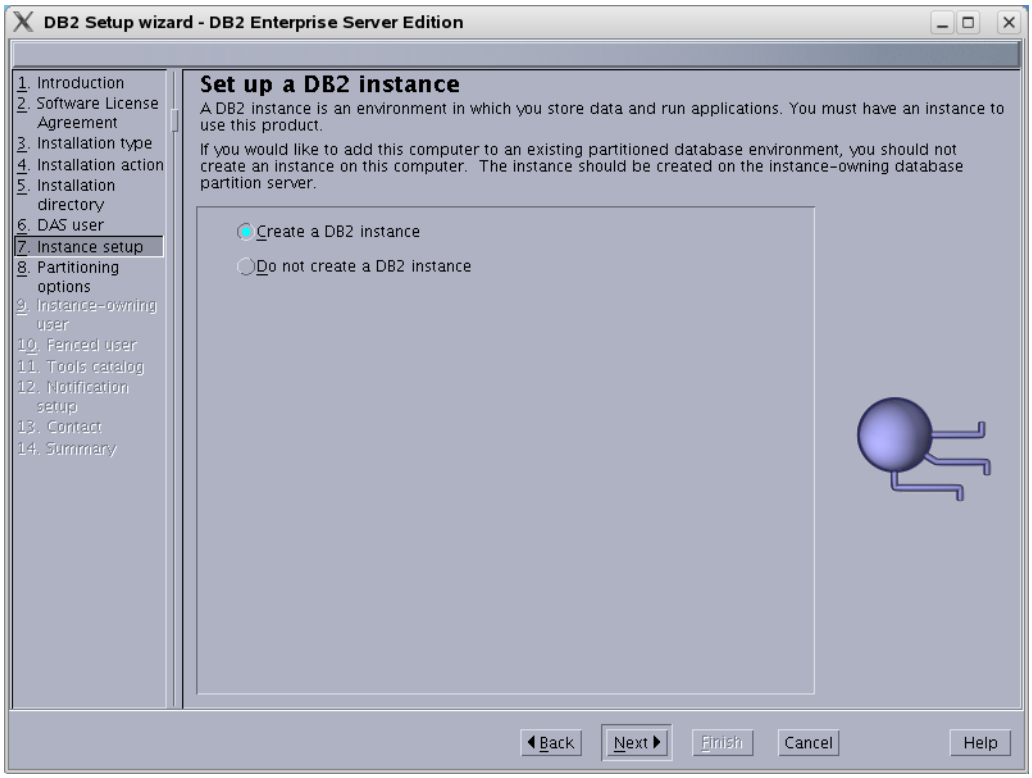
a. Keep the defaults, unless a previous attempt to install DB2 failed.

b. Enter a password.

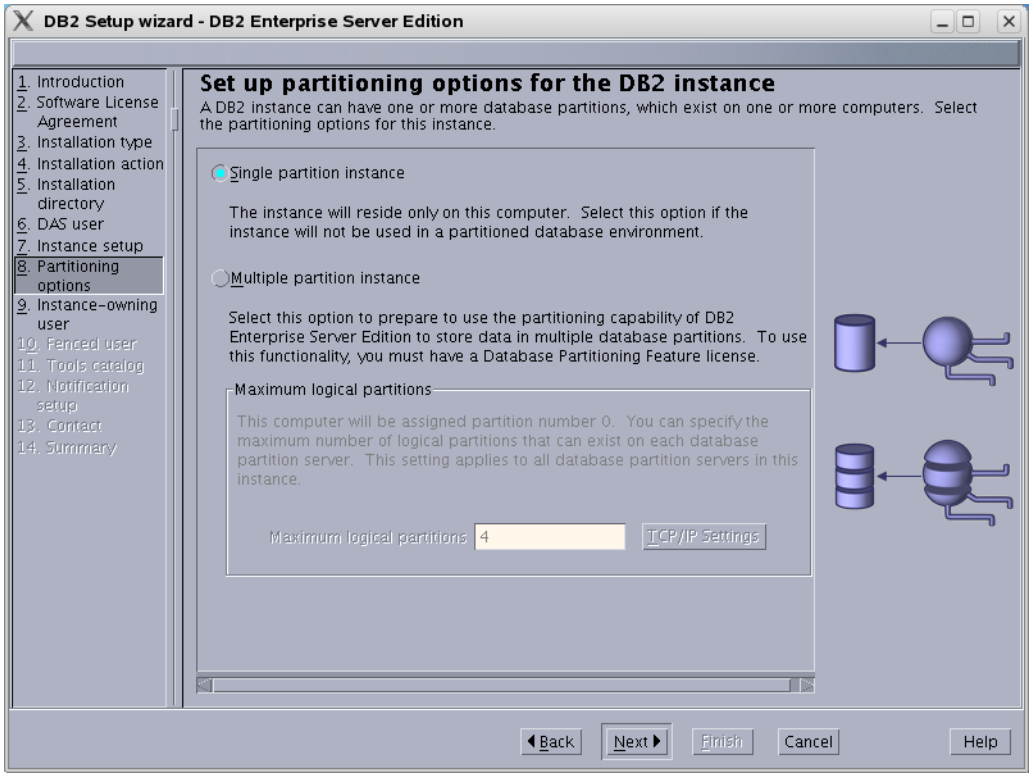
c. Click **Next**.



11. In "Set up a DB2 instance," select **Create a DB2 instance** and click **Next**.



12. In "Set up partitioning options for the DB2 instance," select **Single partition instance** and click **Next**.

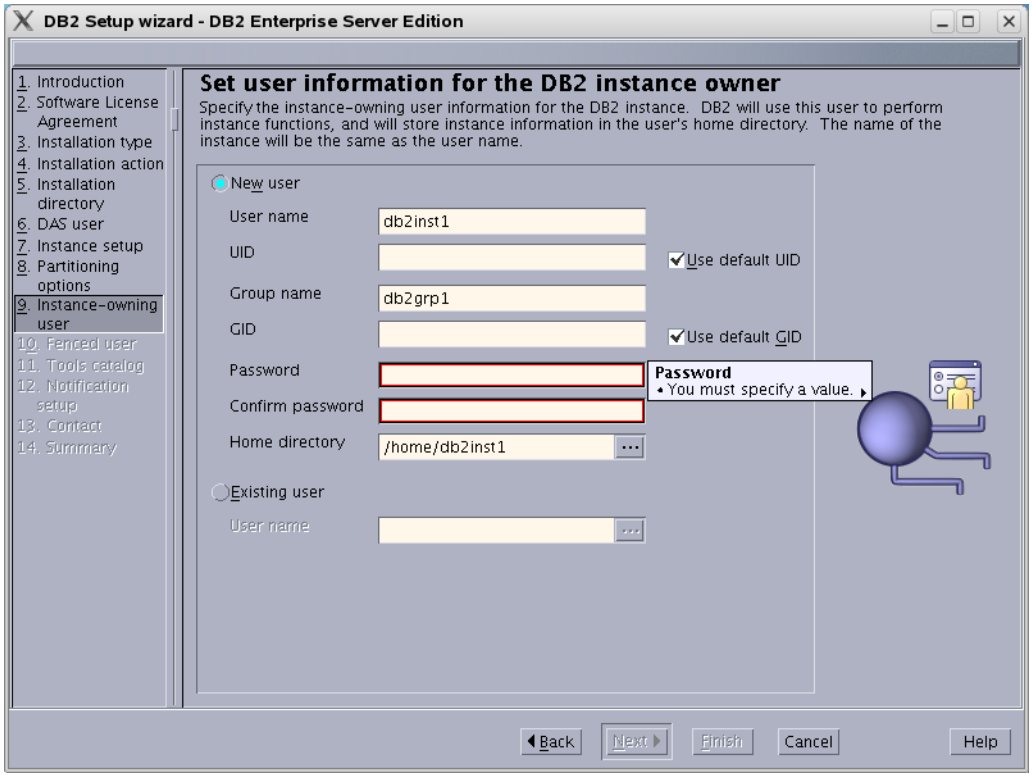


13. In “Set user information for the DB2 instance owner”:

a. Keep the defaults, unless a previous attempt to install DB2 failed.

b. Enter a password.

c. Click **Next**.

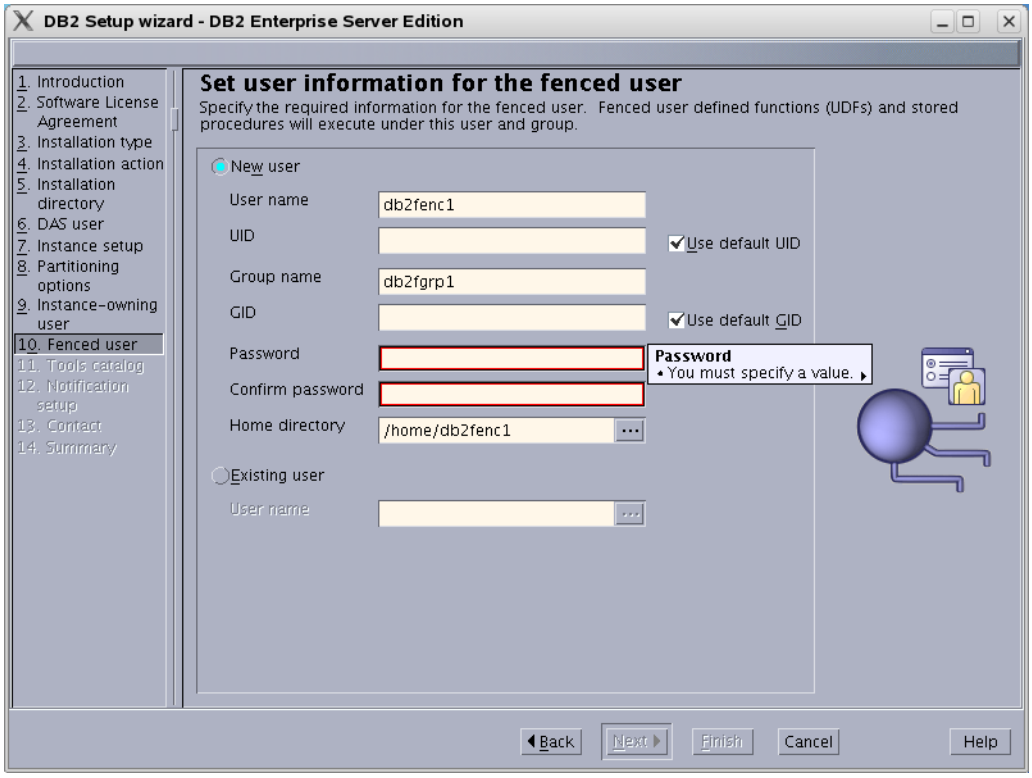


14. In “Set user information for the fenced user”:

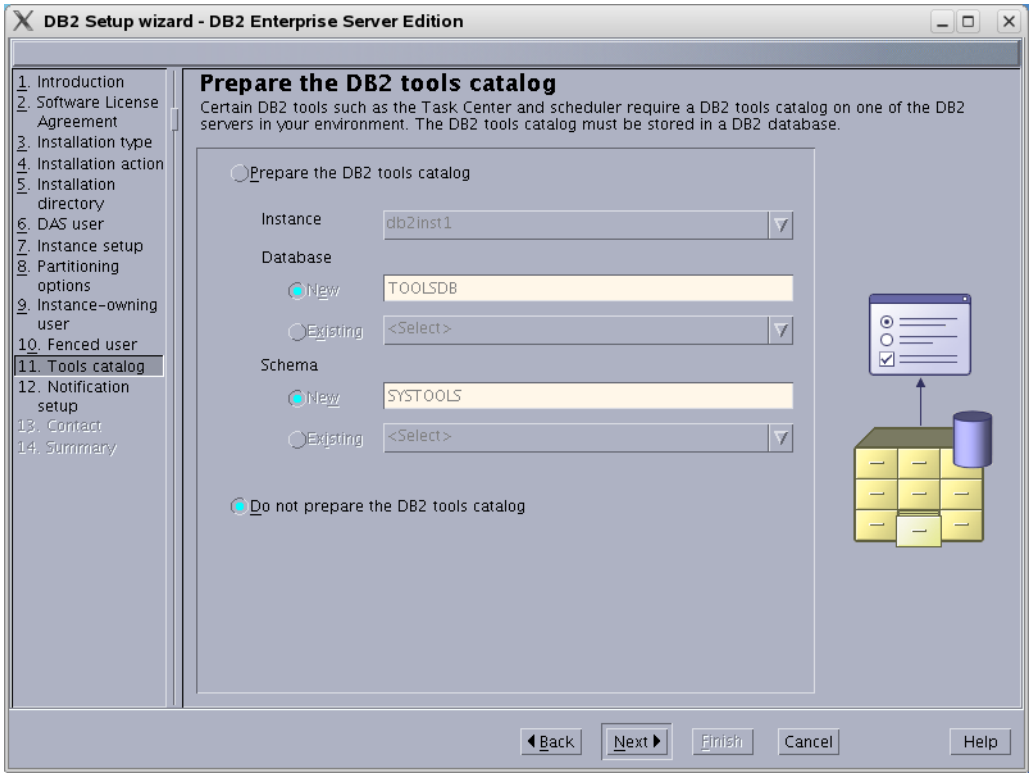
a. Keep the defaults, unless a previous attempt to install DB2 failed.

b. Enter a password.

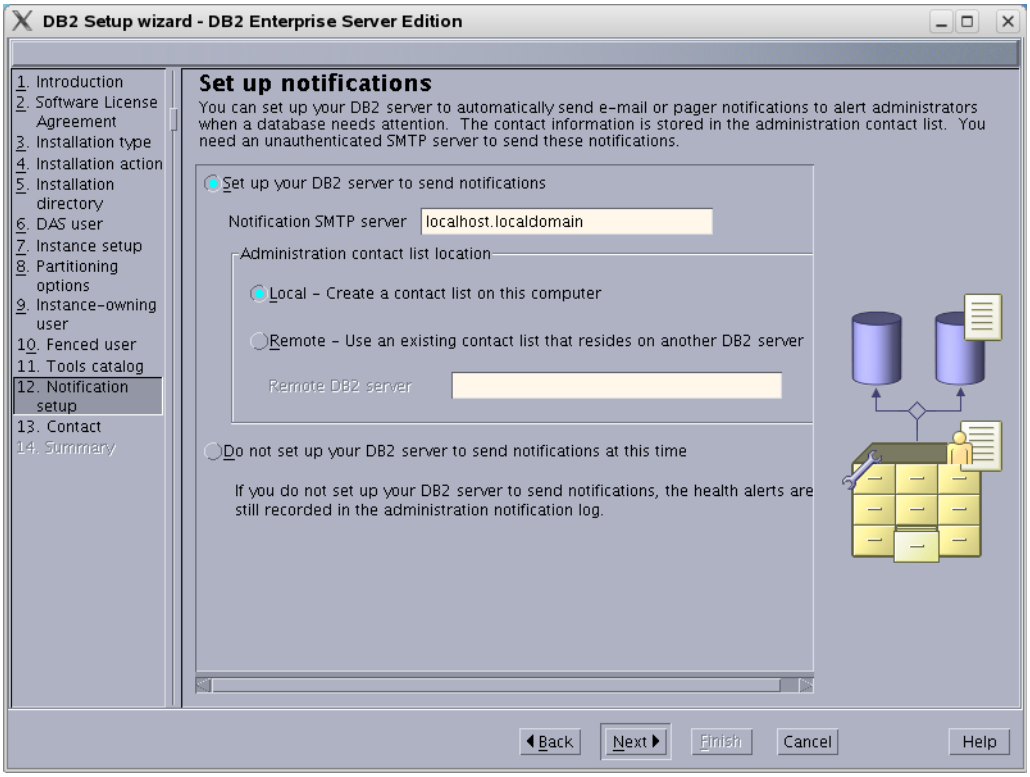
c. Click **Next**.



15. In "Prepare the DB2 tools catalog," select **Do not prepare the DB2 tools catalog** and click **Next**.

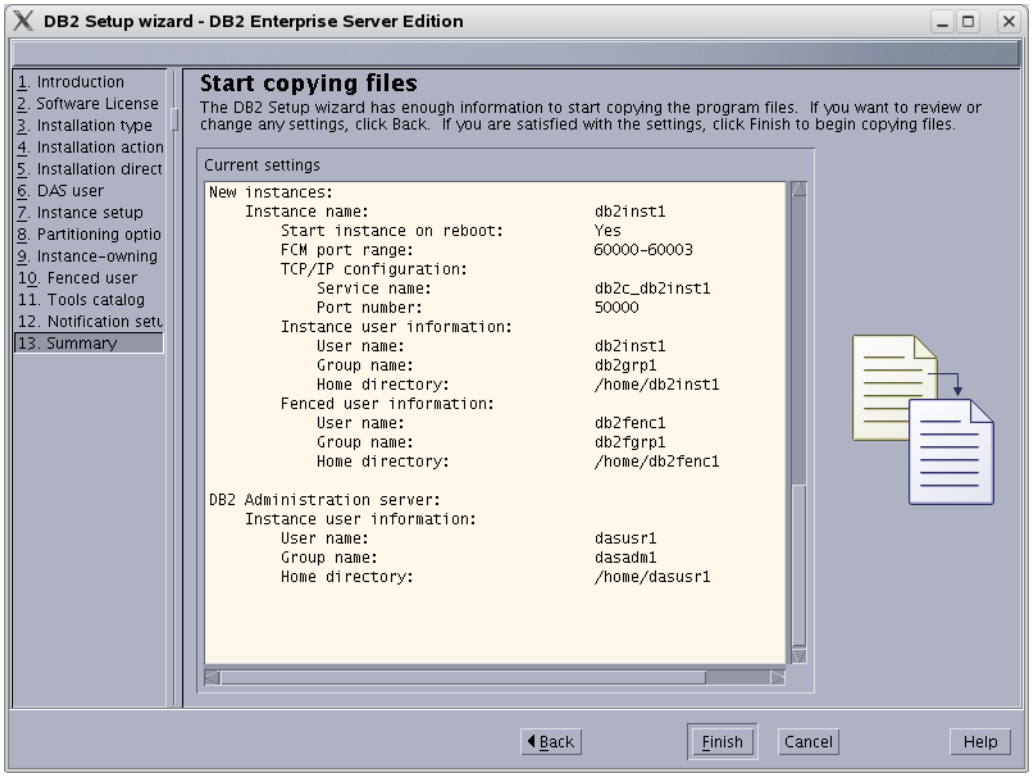


16. In “Set up notifications,” do one of the following:

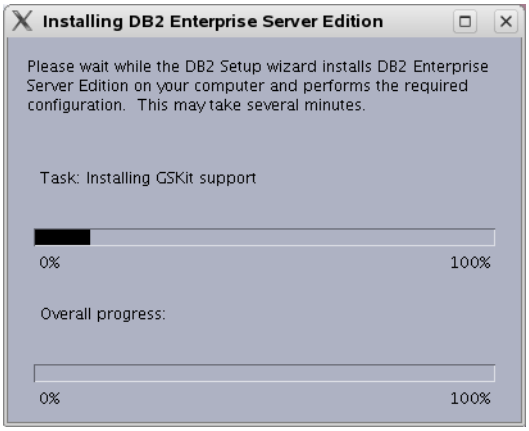


- If your system is a production server, select **Set up your DB2 server to send notifications**, enter a correct address for the local host, and click **Next**.
- If your system is a not a production server, you can select **Do not set up your DB2 server to send notifications at this time**, and click **Next**.

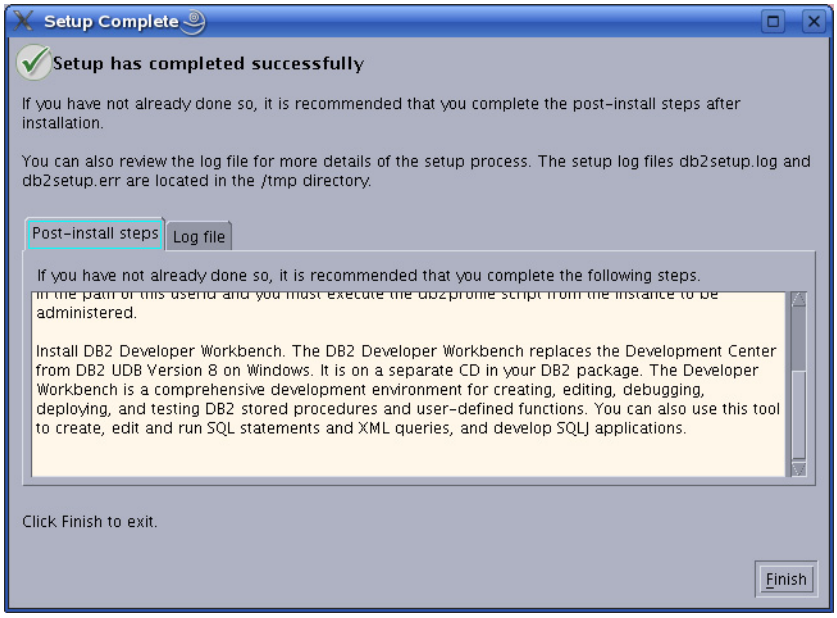
17. In "Start copying files," check that your options are correct and click **Finish**.



18. Allow the installation to proceed.



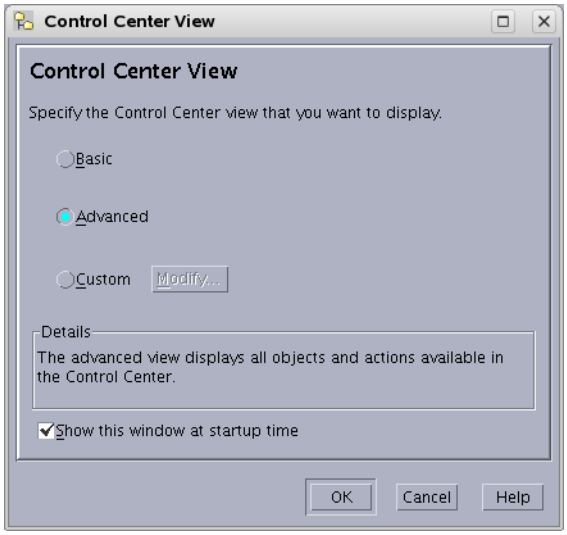
19. In “Setup has completed successfully,” read the notes, check the log tab, and click **Finish**.



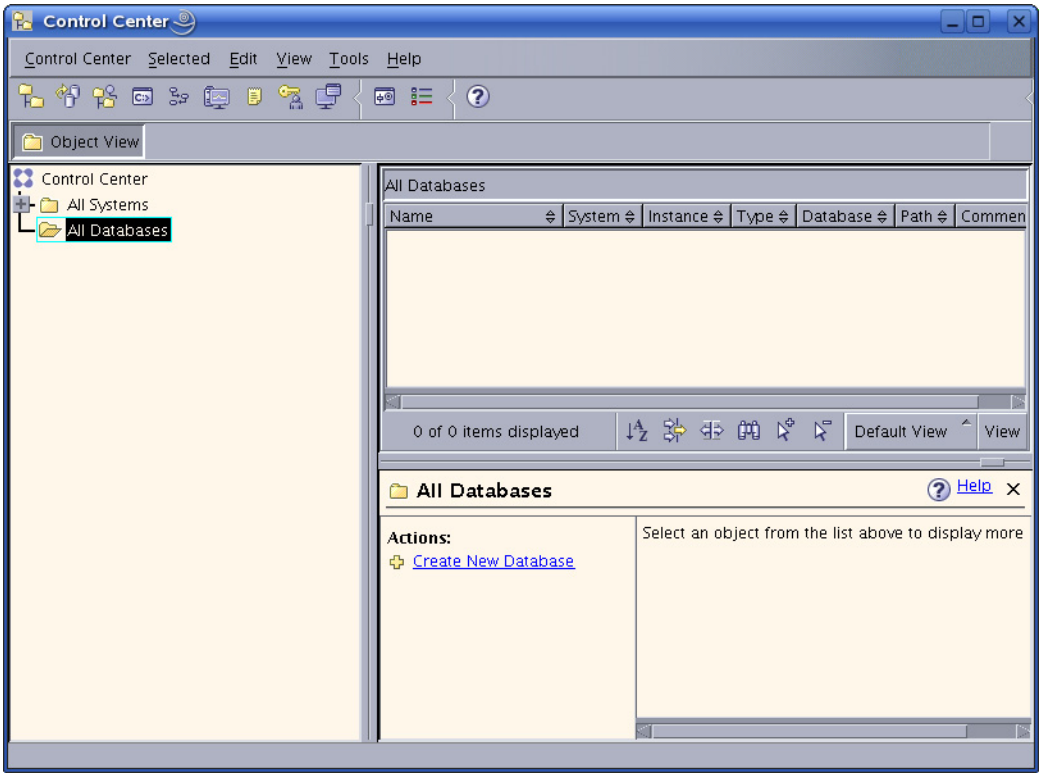
20. The installation of DB2 9.1 is now complete.

B. Create a New DB2 Database

1. Log in as `db2inst1` (or your instance user created during the installation, step 13).
2. Navigate to: `./sqllib/bin and run db2cc`
3. In the “Control Center View” screen, select **Advanced**.

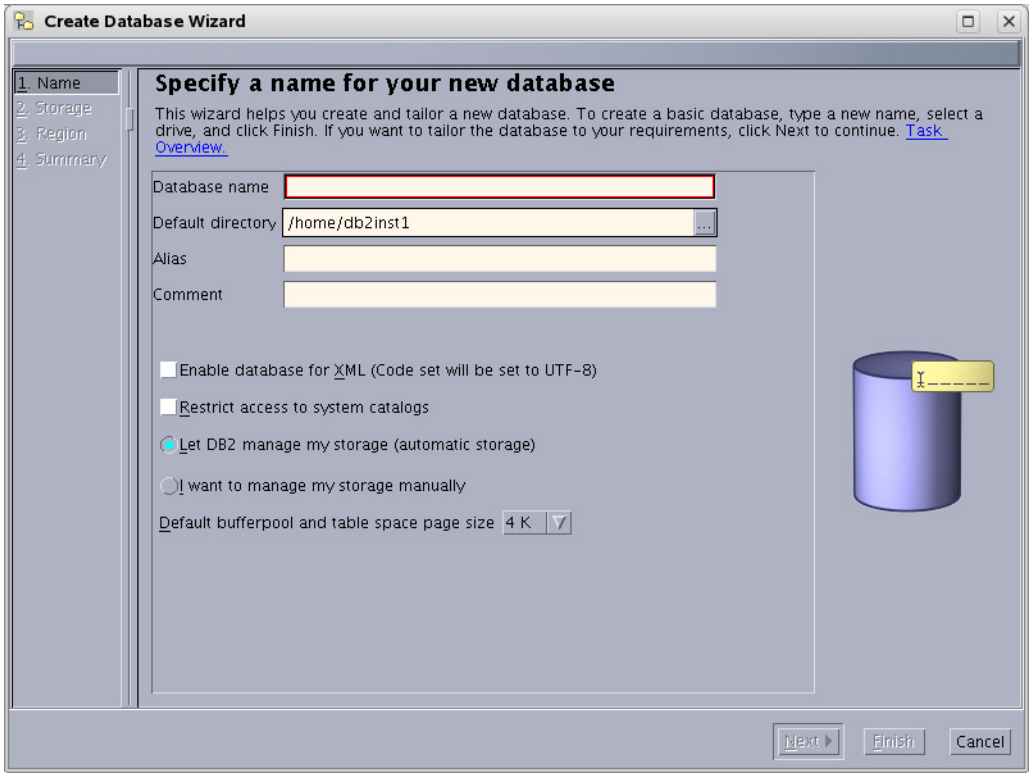


4. In the “Control Center,” open the application for creating a database:
   a. Click the plus sign next to the tree option **All Systems**.

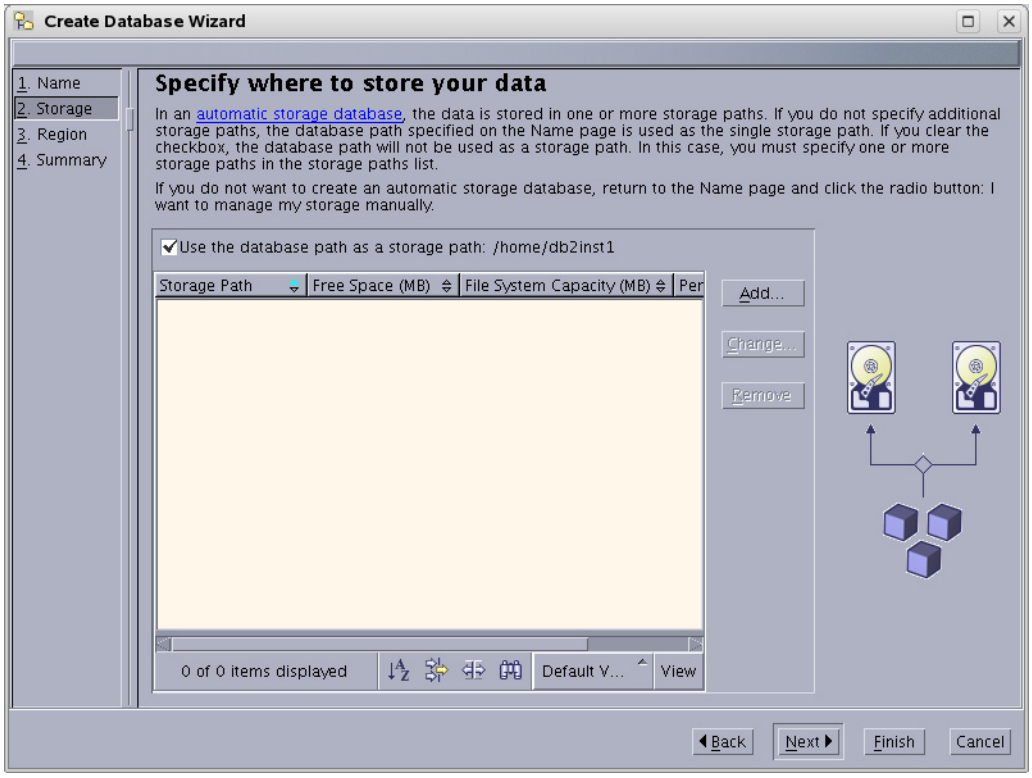


   b. Click the expanded branch **All Databases**. (If you have not created a database previously, this branch is empty.)
   c. Right-click the branch **All Databases** and select **Create Database > Standard**.

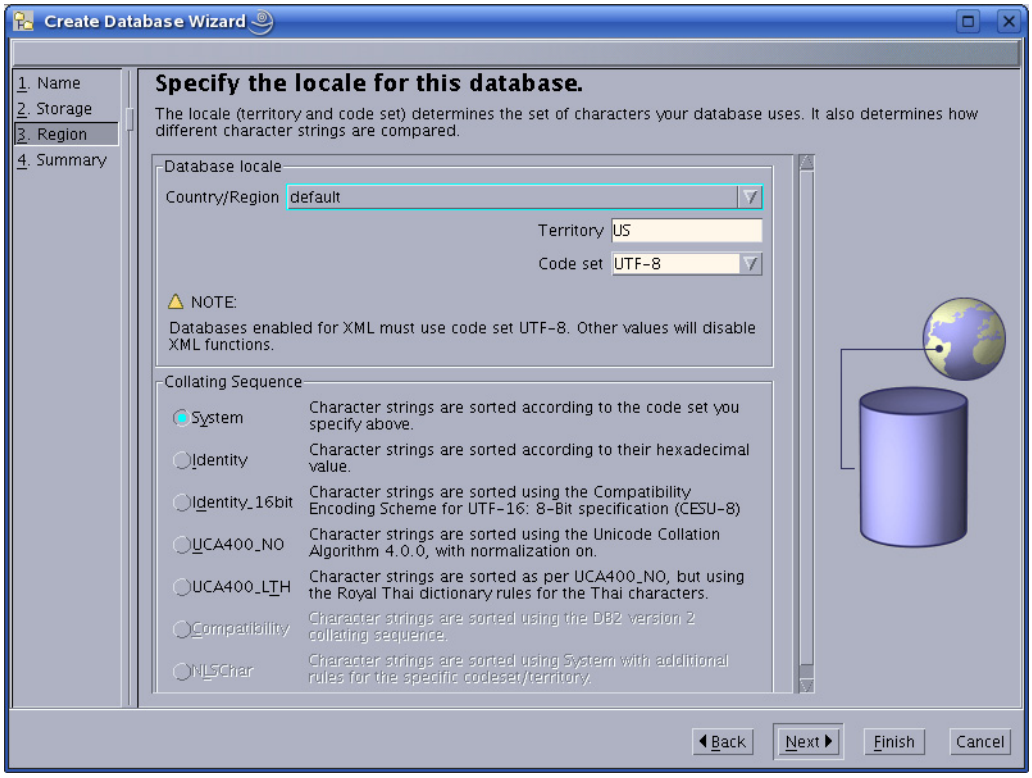
5. In “Specify a name for your new database”:
   a. Enter a name for this database.
   b. Select the check box **Enable database for XML**.
   c. In the drop-down “Default bufferpool and table space page size,” select **32** and click **Next**.



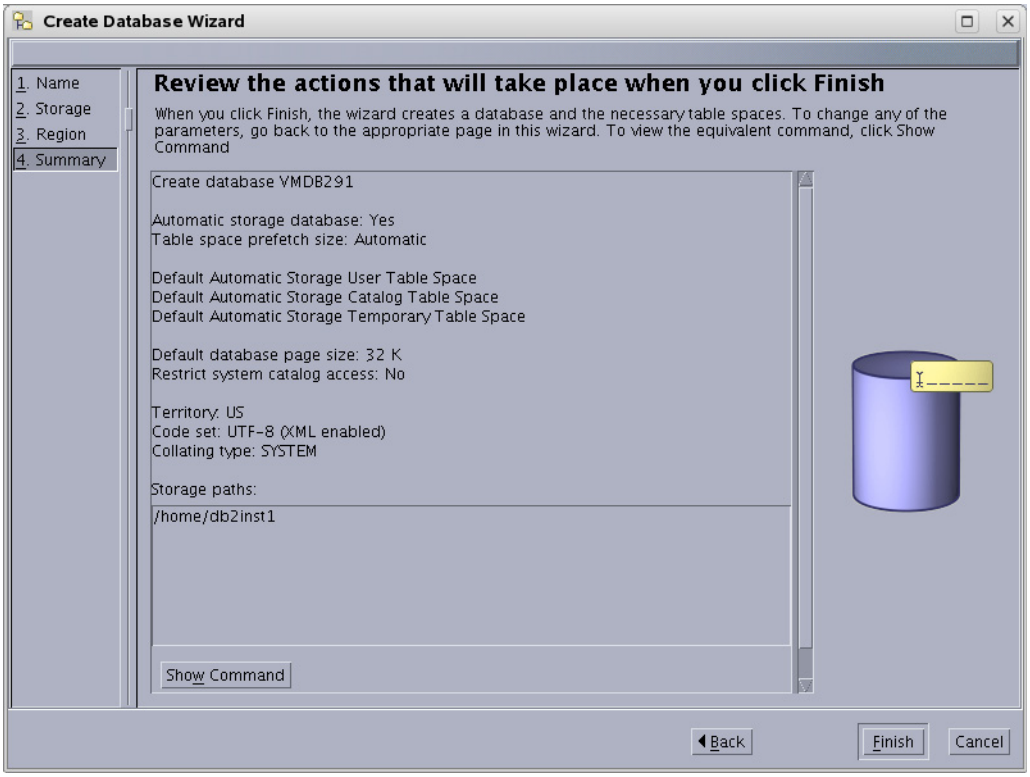
6. In "Specify where to store your data," click **Next** (a value is unnecessary, as we kept the default option of **Let DB2 manage my storage (automatic storage)**, on the previous page).



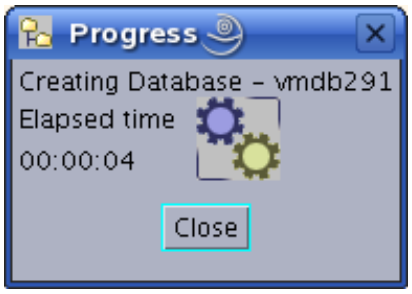
7. In “Specify the locale for this database,” ensure that the drop-down “Code set” displays UTF-8 and click **Next**.



8. In “Review the actions that will take place when you click finish,” confirm that everything looks correct and click **Finish**.

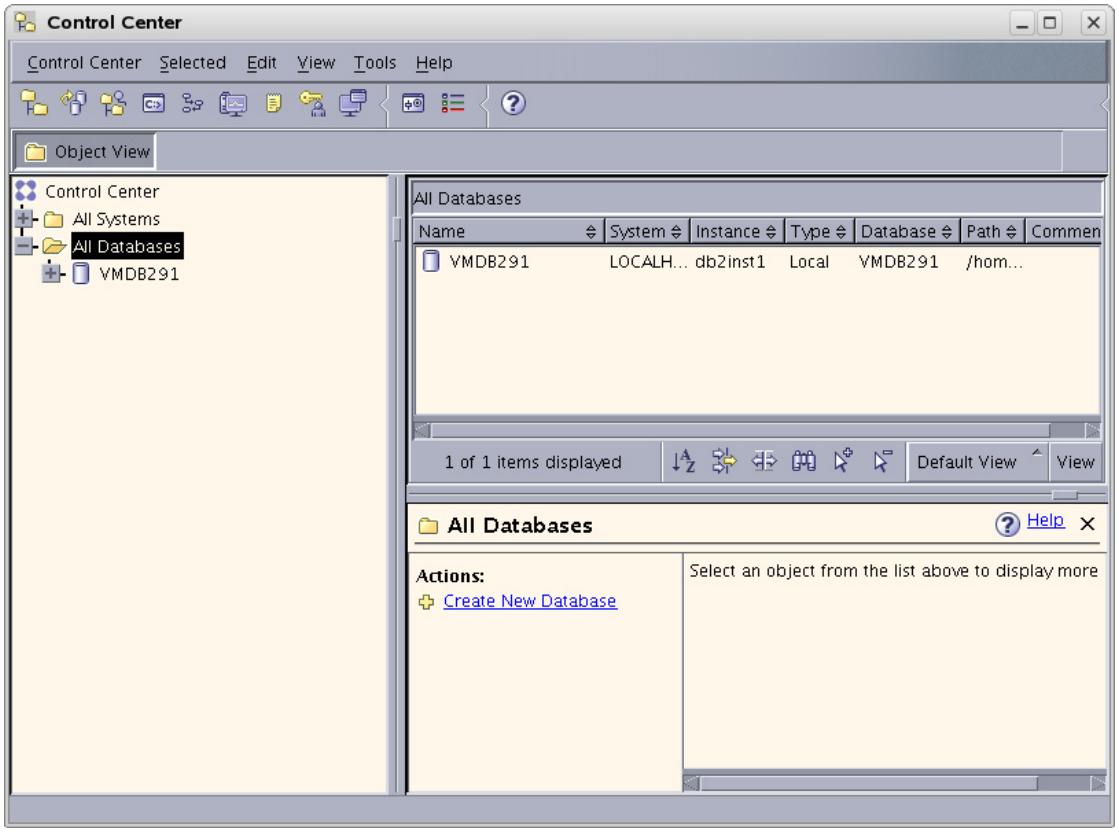


9. Allow the “Progress” window to complete creating the database. The window will close automatically when the database has been created.



10. The database has now been created and is displayed in the control center.

The figure below shows that a single database named `vmdb291` is present in the control center



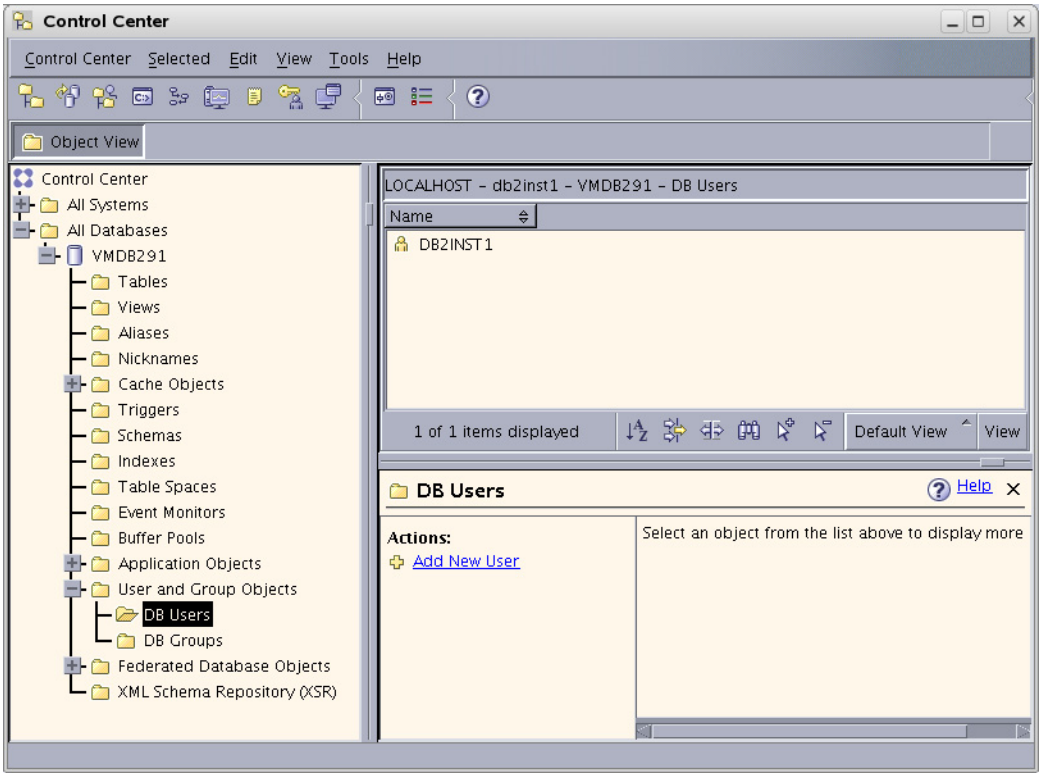
C. Create a User for the New Database

1. Go to the command line. As the system user, create a new user named `csuser` that will be used to access the database from your FatWire product.

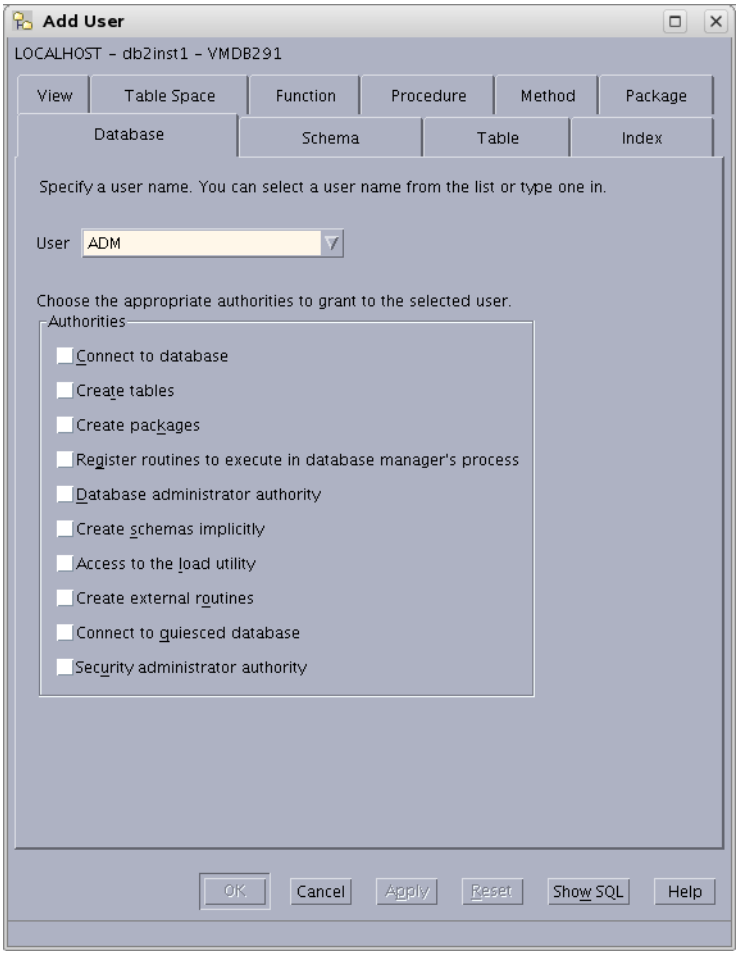
Example of how to create a user named `csuser` on Linux:

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

2. Go back to the “Control Center” and add the user:
   a. Expand the newly created database in the tree by clicking the plus sign, then expanding the branch **User and Group Objects.**
   b. Click **DB Users** to open the right-hand panel.
   c. Right-click the branch **DB Users** and select the **Add** option.



3. In the “Add User” application:
   a. Select the user that was created in step C on page 84.
   b. Under “Authorities,” select all check boxes.
   c. Click **OK**.

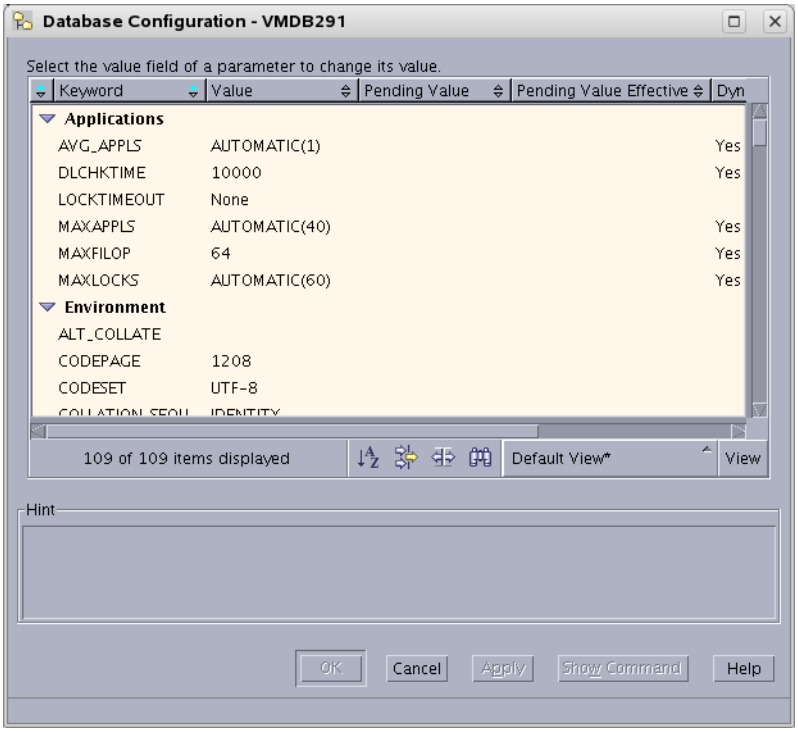


D. Configure the Database

1. Right-click the database that you created (listed in the branch that displays the database icon) and select **Configure Parameters**.
2. In "Database Configuration":
   a. Scroll through the list of options and replace the values of the following parameters with the values shown here:

LOCKTIMEOUT	30
APP_CTL_HEAP_SZ	1024
APPHEAPSZ	1024

   b. Click **OK**.



3. Right-click the database that you created (listed in the branch that displays the database icon) and select **Restart**.

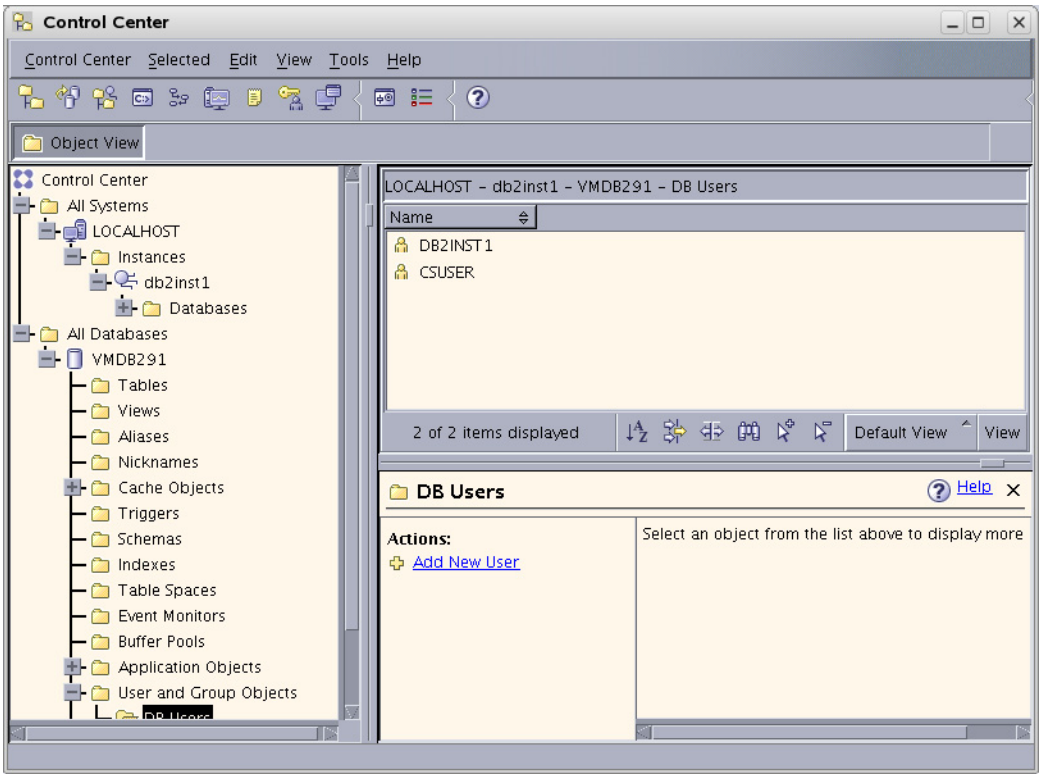
   A status window flashes. ***This does not mean that the operation has been completed.*** Typically, you will need to wait 2 to 3 minutes for the system to restart.

4. Stop the instance:

   a. Expand the following "Control Center" tree branch: **All Systems** > **LOCALHOST** > **Instances** > ***name_of_your_ instance***

   b. Right-click the instance.

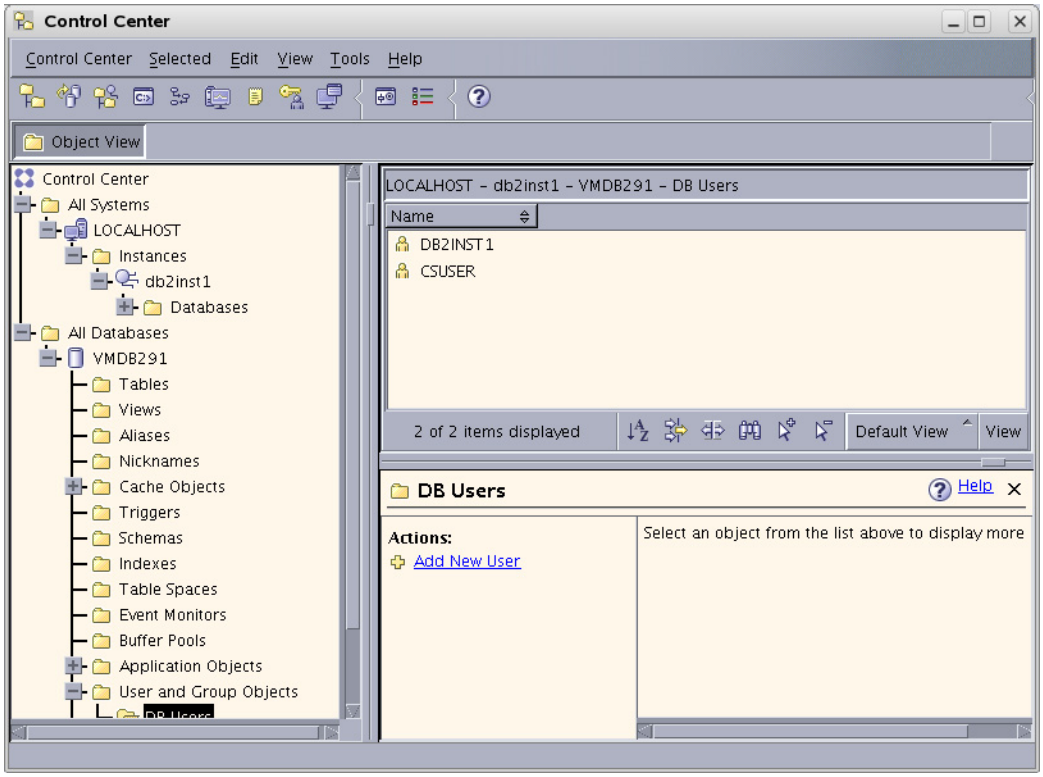
   c. Select **Stop**.



   d. In the "Confirm stop" dialog box, click **OK**.

   e. Wait for the message that the instance has been stopped.

5. Start the instance:
   a. Expand the following “Control Center” tree branch: **All Systems** > **LOCALHOST** > **Instances** > ***name_of_your_ instance***
   b. Right-click the instance.
   c. Select **Start**.



6. Wait for the message that the instance has been started. ***This does not mean that the operation has been completed.*** Typically, you will need to wait 2 to 3 minutes for the system to restart.

   Your database is now ready for use with your FatWire software product.

Part 2

Installing a Web Server

This part describes how to install a web server. It contains the following chapters:

Chapter 6

Worksheets for Documenting the Web Server Installation

This chapter contains worksheets listing the web server parameters that you need to track.

Print this chapter. Then, as you install software, fill in the blank fields in these worksheets with the values of the specified parameters. You will save considerable time by doing this. Additionally, if something fails during the installation, the information in these worksheets will be valuable while you are troubleshooting. Use a separate set of worksheets for each installation so that each installation is fully documented.

The worksheets are constructed as tables that are divided into the following categories:

- Key to Sample Values
- Web Server Parameters

Key to Sample Values

The installation worksheets list parameters along with their sample values. Each sample value is classified as one of the following:

- **Default**: the value is automatically created at the time of the installation.
- **Normal**: the value represents the normal configuration for a simple installation. Do not use a different value unless your system requires it.
- **Option**: the value must be chosen from a preset list of options.
- **Suggested**: the value is recommended for the parameter.

> **Note**
>
> A **Suggested** account name has an Example password value. We strongly recommend that you select a password for this account that is appropriate for the security of your system.

- **Example**: the value is only an example that must be replaced by the value that is appropriate for your installation. The example value is not likely to be valid in your environment.

Web Server Parameters

Table 1: IIS Web Server Parameters

Parameter	Shown As	Comments	Your Value
Web Version	*WebVersion*	Example: Apache 1.3.37	
Web Host Name	*WebHost*	Example: `jeeves`	
Web Host IP Address	*WebIP*	Example: `104.222.111.155`	
Web Server Port	*WebPort*	Default: `80`	
IIS Only: Filter Name (ISAPI plug-in name)	*FilterName*	Suggested: `iisforwardfilter`	
Apache Only: Apache Root Directory	*ApacheRoot*	Example: `/usr/apache`	

Table 2: Apache Web Server Parameters

Parameter	Shown As	Comments	Your Value
Web Version	*WebVersion*	Example: Apache 1.3.37	
Web Host Name	*WebHost*	Example: `jeeves`	
Web Host IP Address	*WebIP*	Example: `104.222.111.155`	
Web Server Port	*WebPort*	Default: `80`	
IIS Only: Filter Name (ISAPI plug-in name)	*FilterName*	Suggested: `iisforwardfilter`	
Apache Only: Apache Root Directory	*ApacheRoot*	Example: `/usr/apache`	

Chapter 7

Installing IBM HTTP Server 6.1

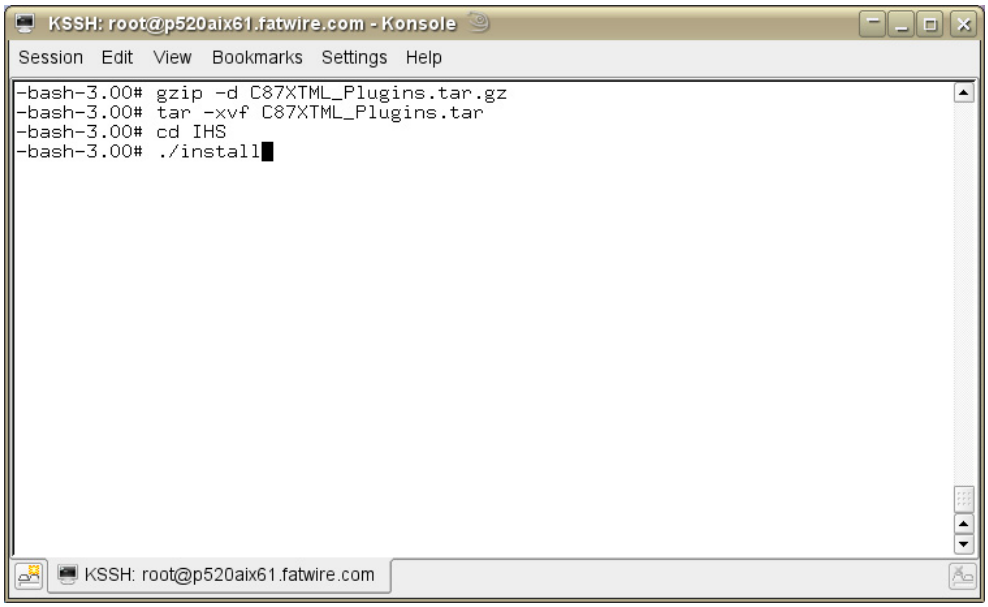
This chapter contains the following sections:

Note

In this guide, IBM HTTP Server is referred to as “IHS.” WebSphere Application Server is referred to as “WAS.”

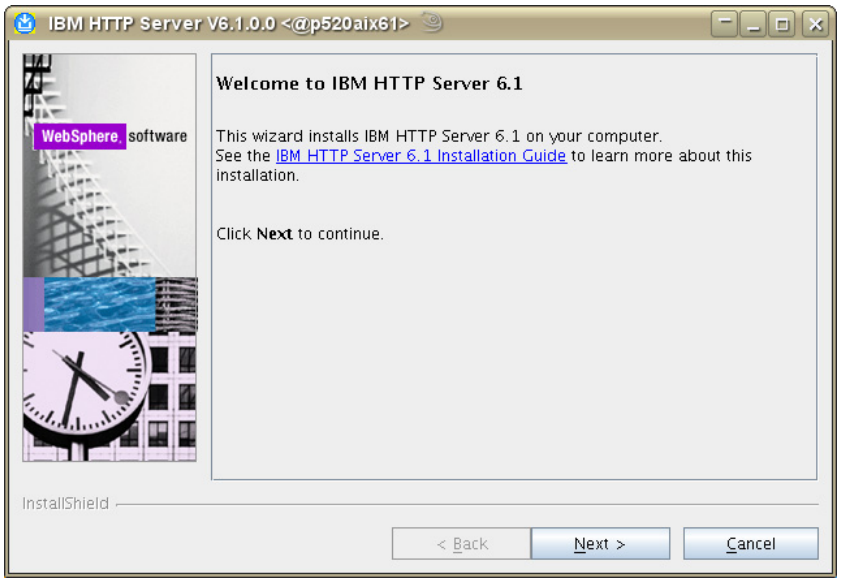
Installation Steps

1. Download the correct file, WebSphere Plugins, for your IBM operating system.
2. Extract the file to a temporary directory.

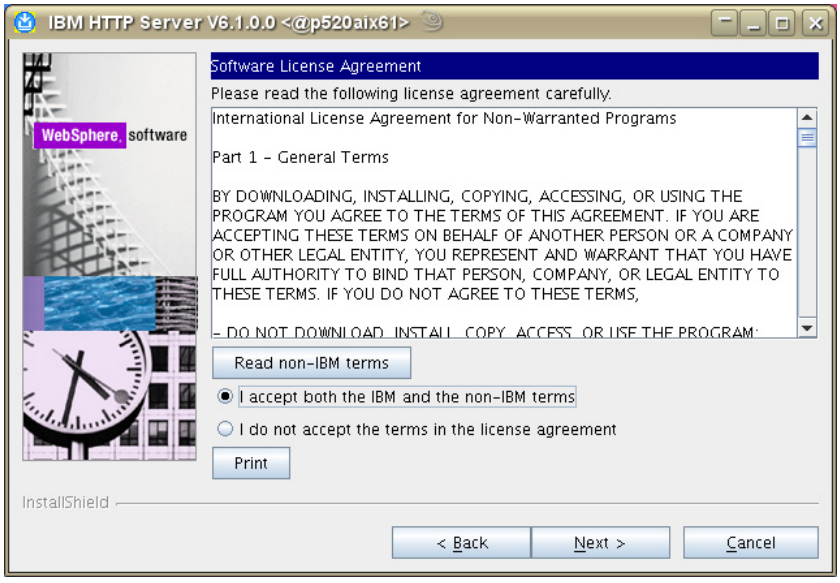


   - On Unix: **`tar -xvf <file name>`**
     For example:
     gzip -d C87XTML_Plugins.tar.gz
     tar -xvf C87XTML_Plugins.tar
   - On Windows: **`unzip <file name>`**
     For example:
     unzip C87XTML_Plugins.zip
3. Change the directory to `IHS/`.
   For example:
   cd IHS/
4. Run the installer:
   - For Unix: `./install`
   - For Windows: `install.exe`

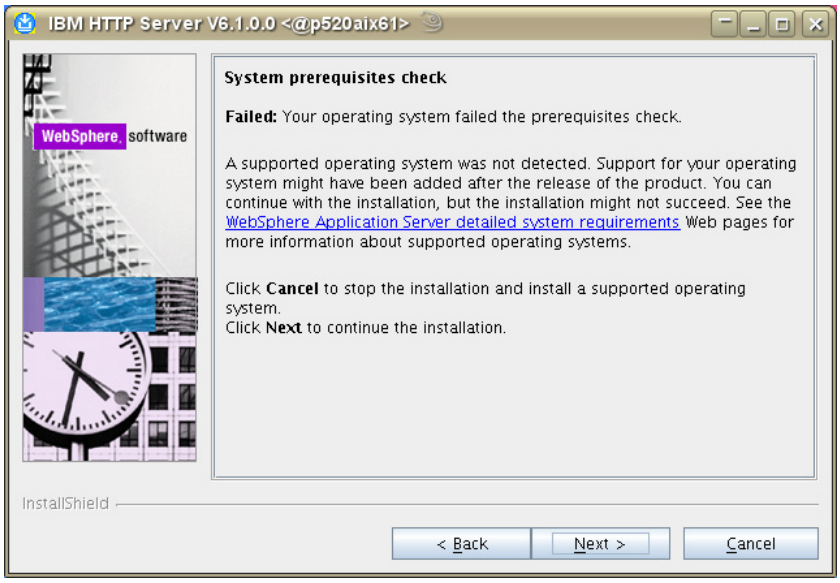
5. The “GUI” installer appears. Click **Next**.



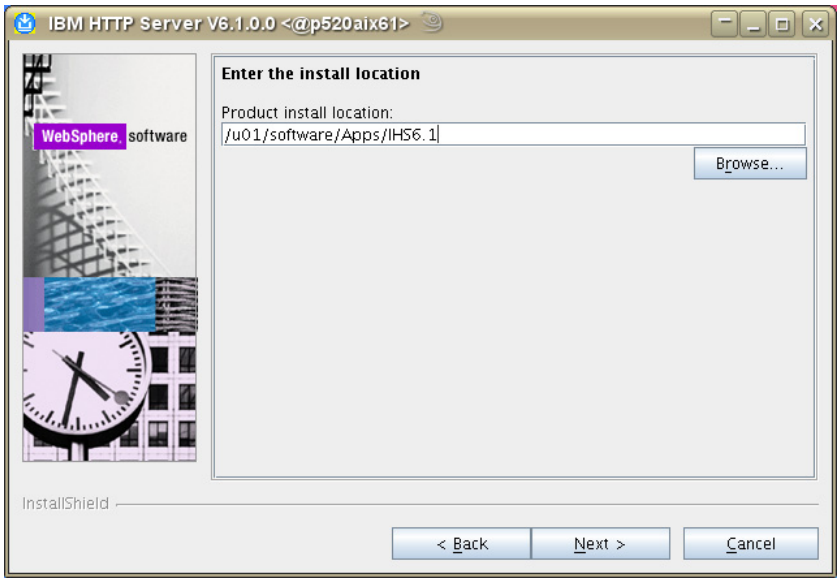
6. Click the radio button **I accept the IBM and non-IBM terms**, to accept the license agreement and click **Next**.



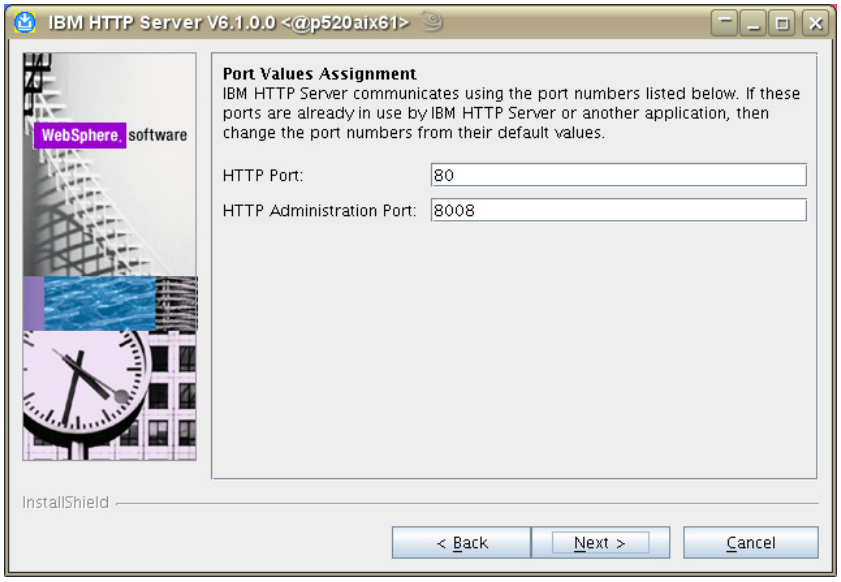
7. In the “System prerequisites check” screen click **Next**.



8. In the “Enter the Install location” screen, select a location to install IHS 6.1 by using the **Browse** button, then click **Next**.



9. In the “Port Values Assignment” screen, enter the ports on which you wish to run IHS. Then click **Next**.



Note

We assume throughout this guide that you are using the default ports: `80` and `8008`. If you have changed them, replace the values given with the ports you have selected.

10. In the “HTTP Administration Server Authentication” screen:

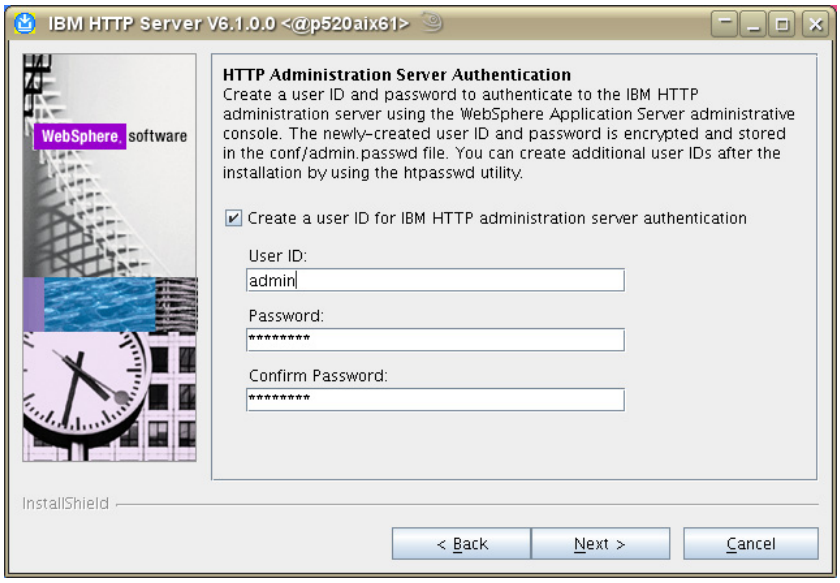
a. Select

- **Create a user ID for IBM administration server authentication**.

b. Fill in the fields:

- **User ID**: `admin`
- **Password**: <enter and confirm>

c. Click **Next**.



11. In the "Setup HTTP Administration Server" screen:

a. Select:

- **Setup IBM HTTP administration server to administer IBM HTTP Server**
- **Create a unique ID and Group for the IBM HTTP Server administration**

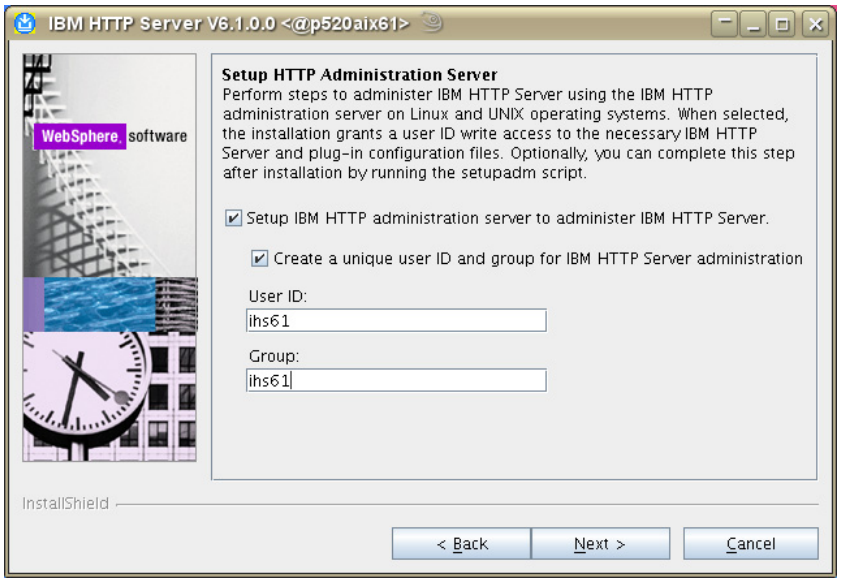
b. Fill in the fields:

- **User ID**: `ihs61`
- **Group**: `ihs61`.

Note

Record the unique name for the User ID and Group. They are needed to integrate with WAS. The User ID and Group can be anything you choose; `ihs61` is only an example.

c. Click **Next**.



12. In the "IBM HTTP Server Plugin for IBM WebSphere Application Server" screen:

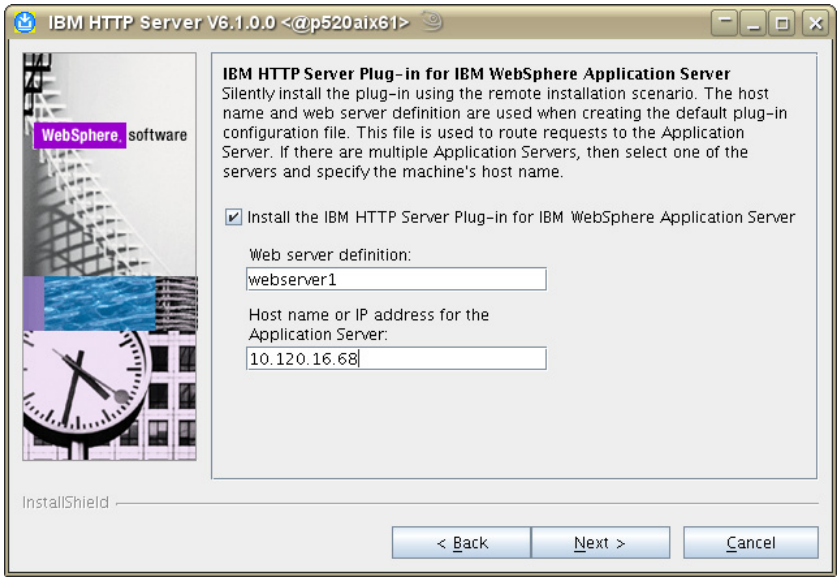
a. Select:

- **Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server**.

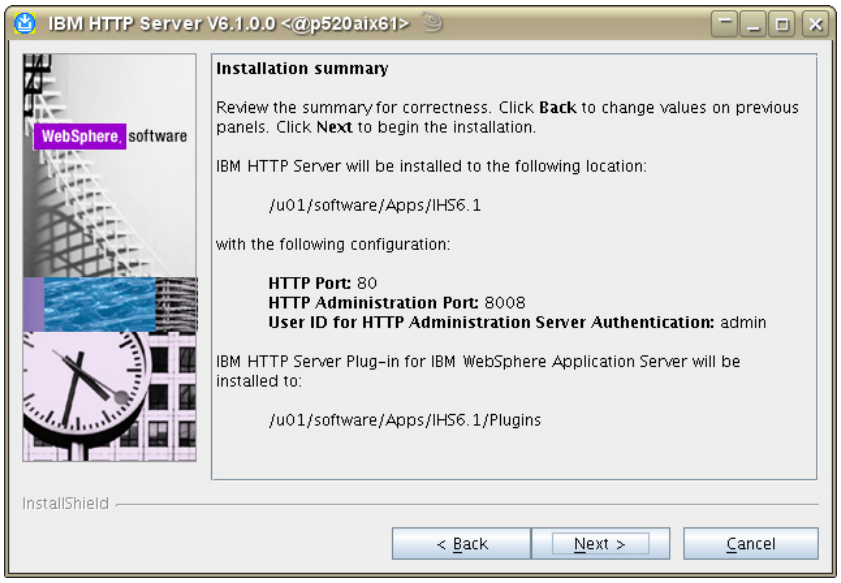
b. Fill in the fields:

- **Web server definition**: `webserver1`
- **Host name**: Enter the hostname on which the application server is found.

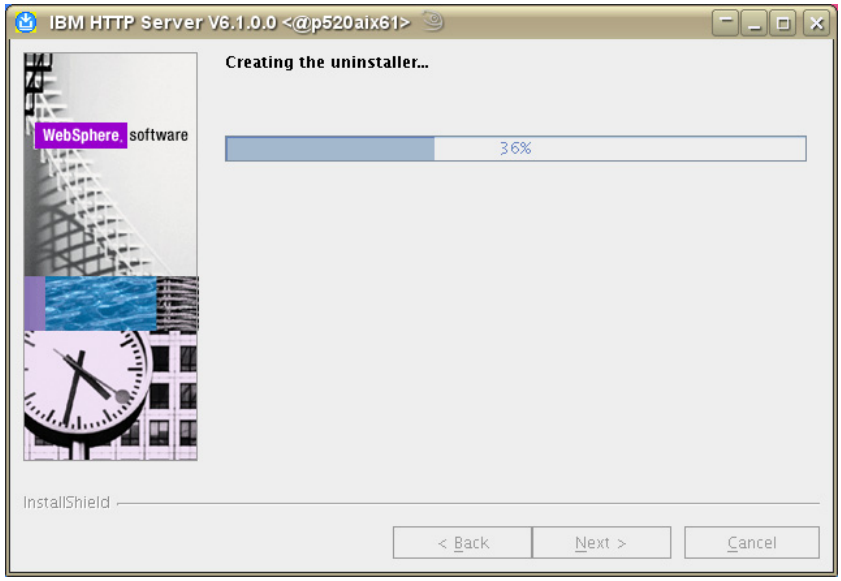
c. Click **Next**.



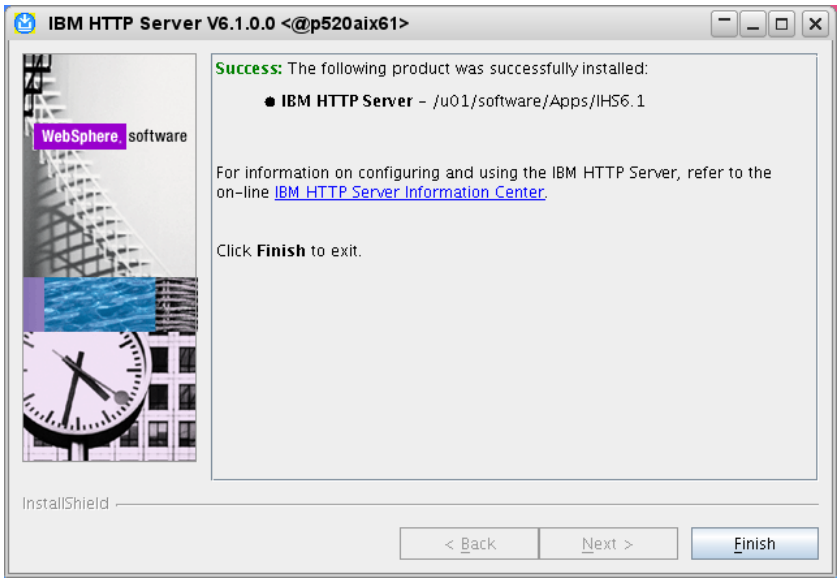
13. In the “Installation summary” screen click **Next**.



14. Allow the installer to finish.



15. When the installation is complete click **Finish**.



Note

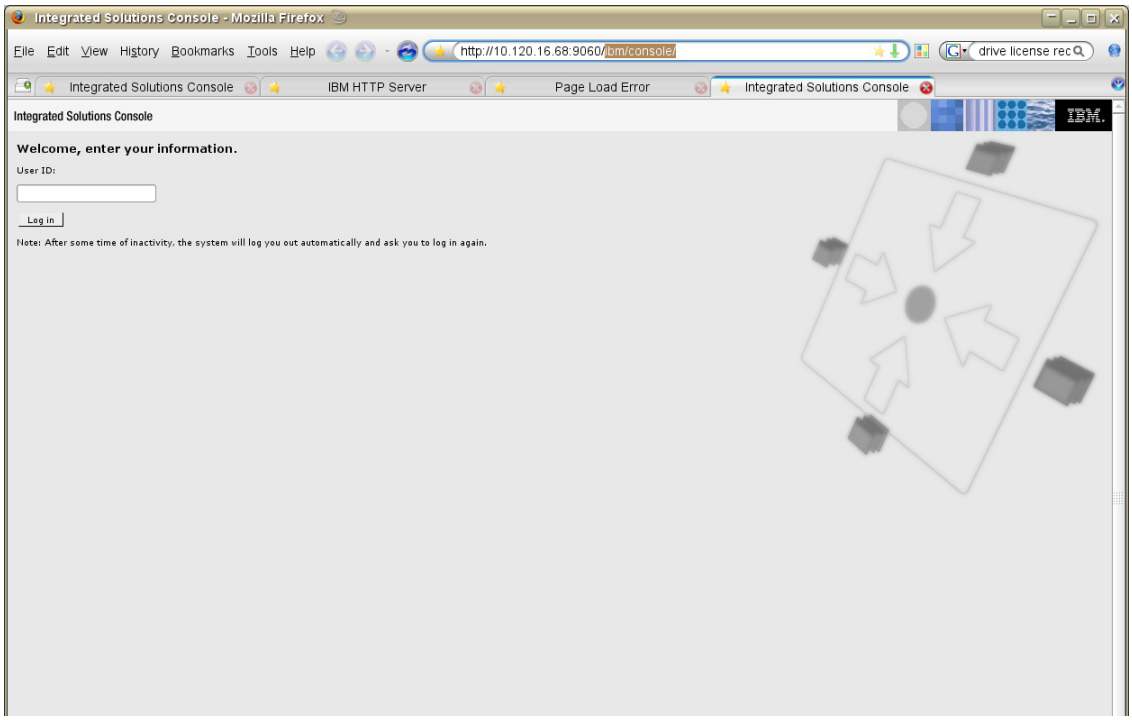
Now, you will need to use the update installer to patch IBM HTTP Server to the same version as WebSphere 6.1. Information on using the update installer can be found on the IBM site when you download updates.You will need to update both the IHS server and the IHS plugins separately. To do so, you will need the WebSphere and the plugin fixpacks.

Installing IHS with WebSphere Application Server on the Local Server

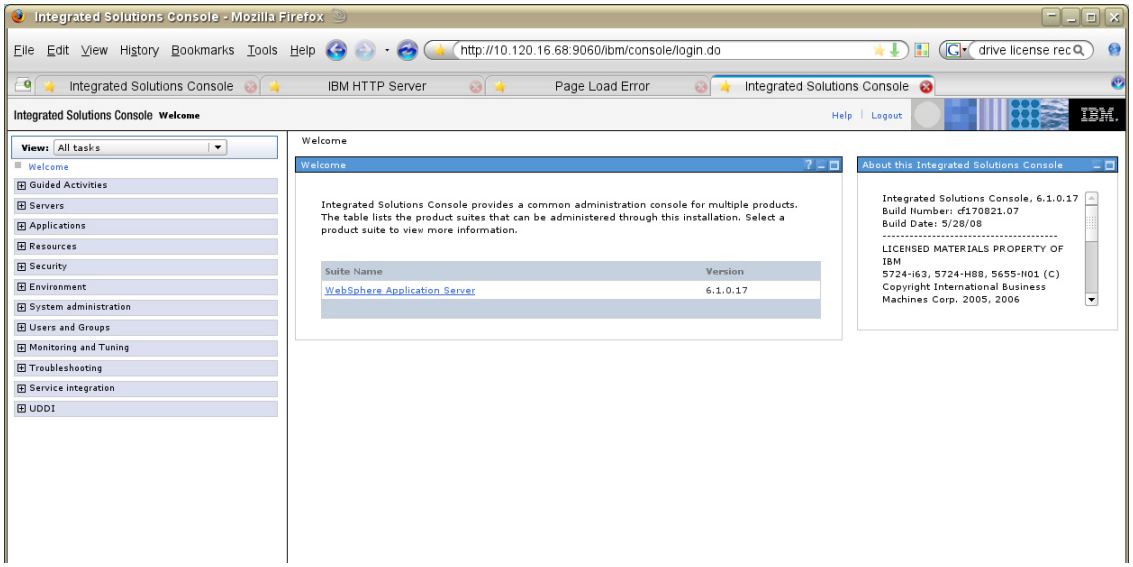
Note

It is preferable to perform this installation after Content Server is already installed. Then the plugin, `cfg.xml`, is automatically updated to include Content Server.

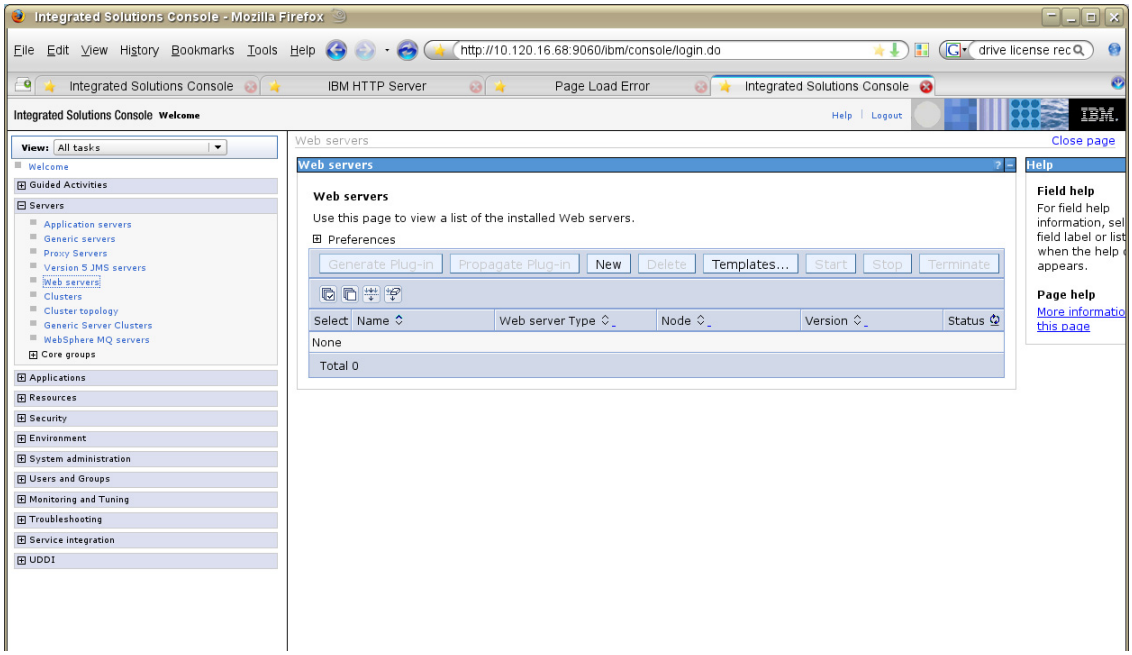
1. Browse to the WAS management console, for example:
   `http://10.120.16.68:9060/ibm/console/`



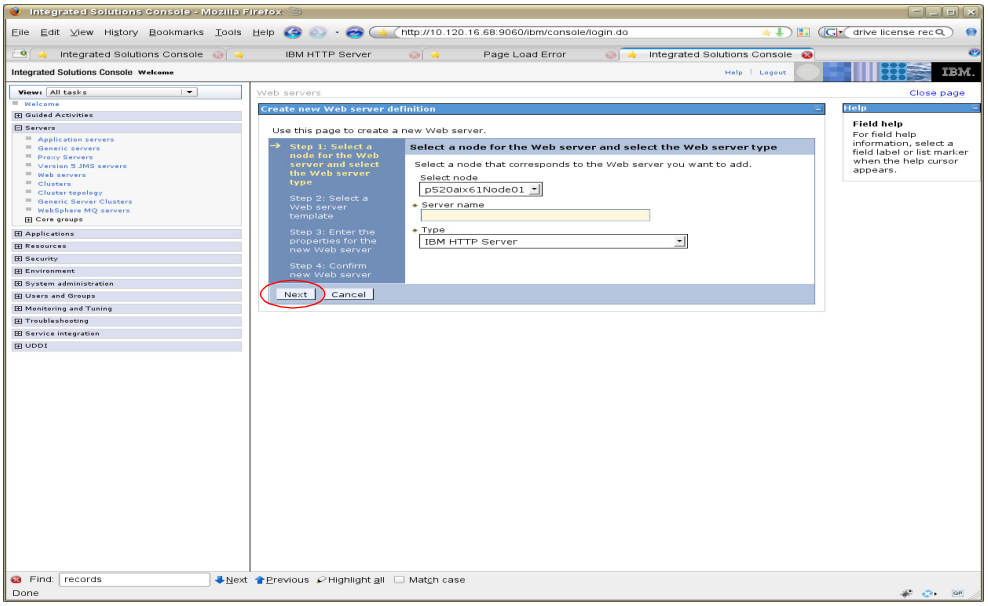
2. Log in to the Admin Site.



3. Select: **Servers** > **Web Servers**.



4. Click **Next**.

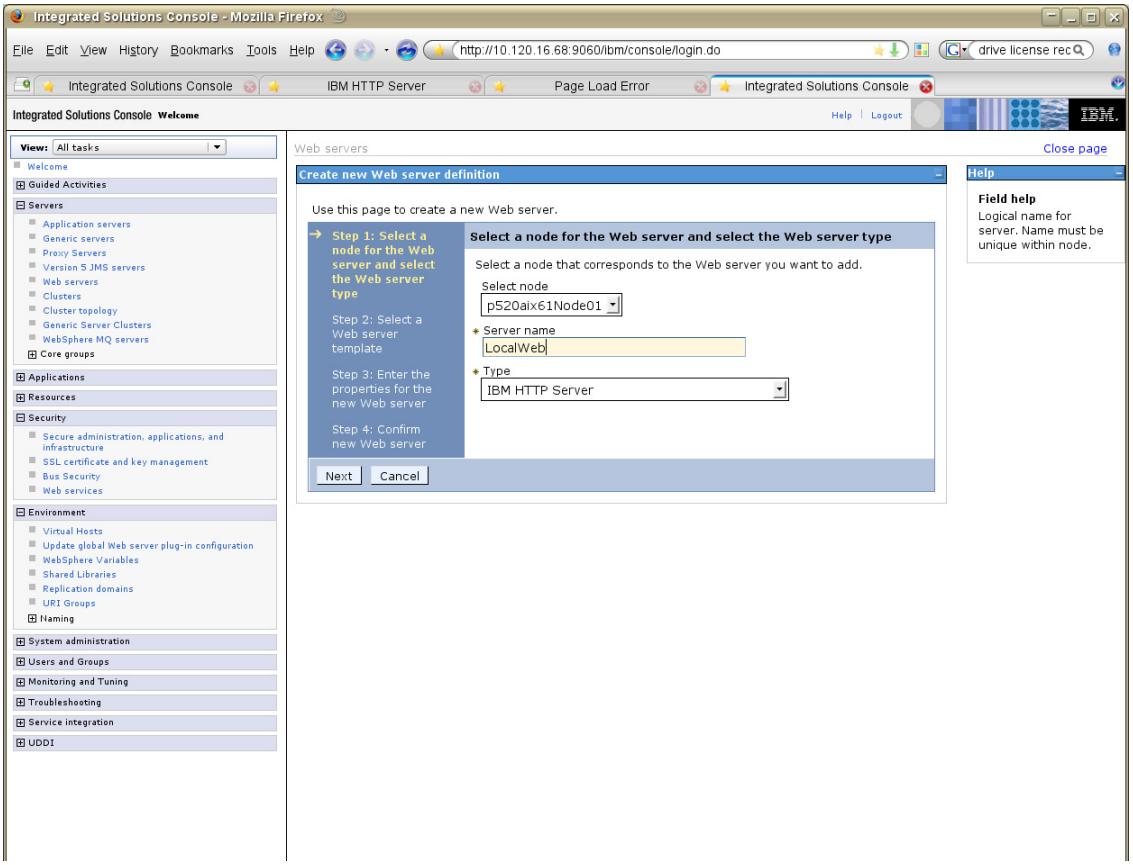

Integrated Solutions Console - Mozilla Firefox
Create new Web server definition
Use this page to create a new Web server.
Step 1: Select a node for the Web server and select the Web server type
Select a node for the Web server and select the Web server type
Select a node that corresponds to the Web server you want to add.
Select node
p520aix61Node01
Server name
Type
IBM HTTP Server
Step 2: Select a Web server template
Step 3: Enter the properties for the new Web server
Step 4: Confirm new Web server
Next
Cancel
Help
Field help
For field help information, select a field label or list marker when the help cursor appears.
Close page

5. To link IHS to WAS:

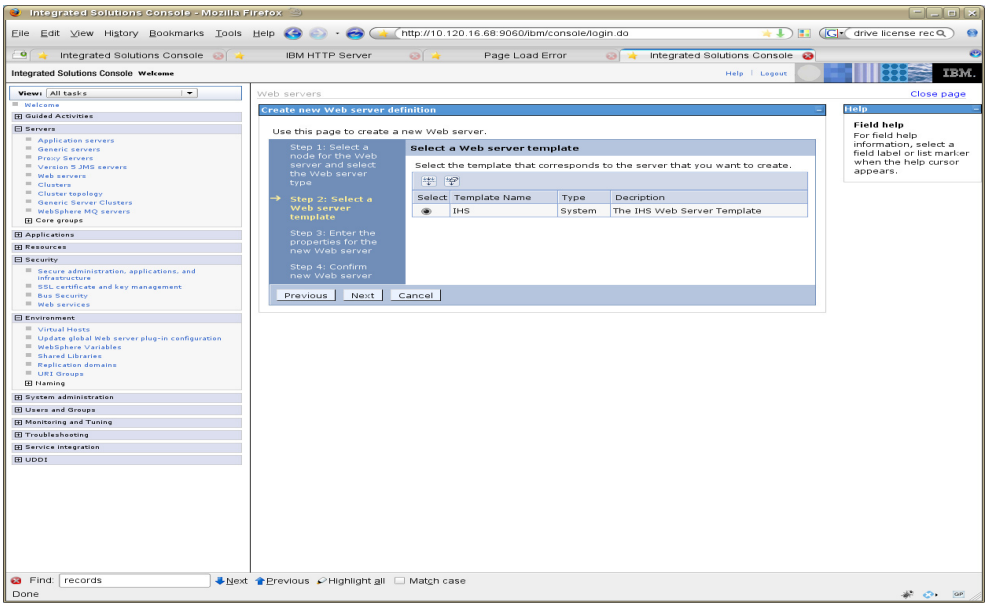
a. Fill in the fields:

- **Select node**: Select the node that you want to federate with (normally this is the node of the application server or cluster on which CS is installed).
- **Server name**: Enter the unique name for this web server, which was entered when you installed IHS.
- **Type**: Keep the type as **IBM HTTP Server**.

b. Click **Next**.



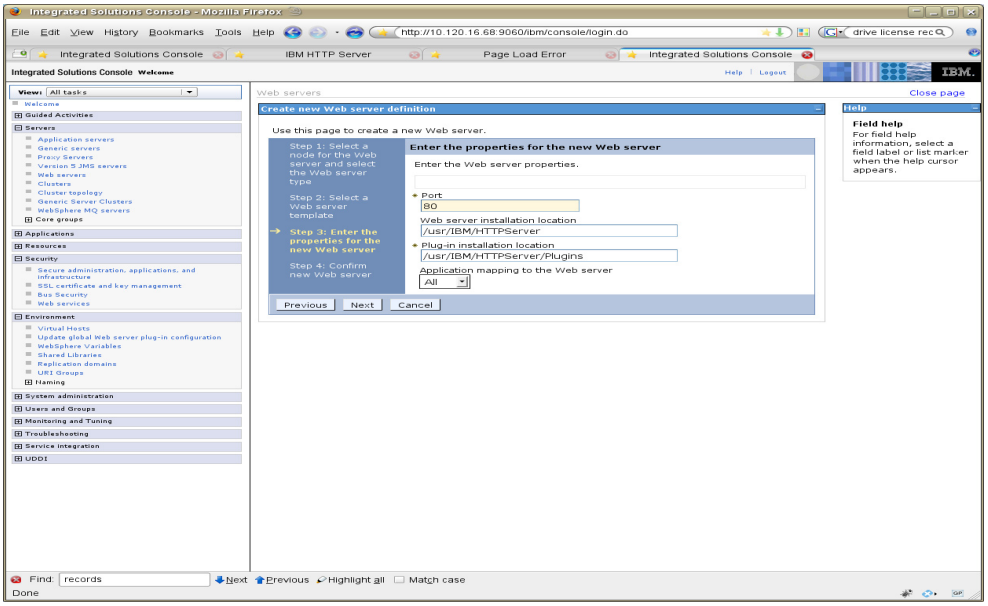
6. In the “Select a Web server template” screen click **Next**.



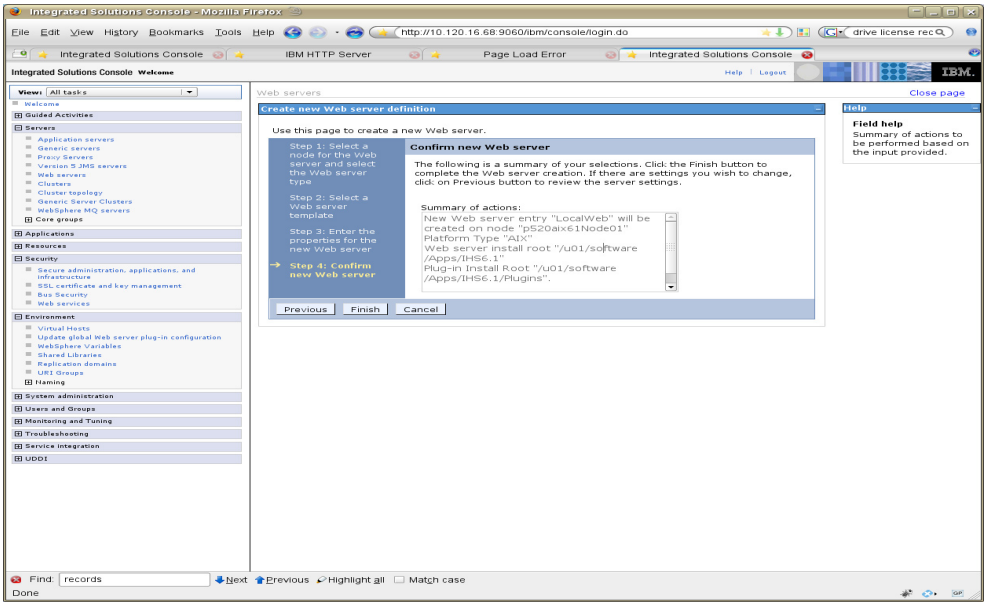
7. On the “Property Page”:

   a. Ensure that all entries are correct. The only entries that typically need to be changed are the locations for the IHS server and the Plugin Directory.

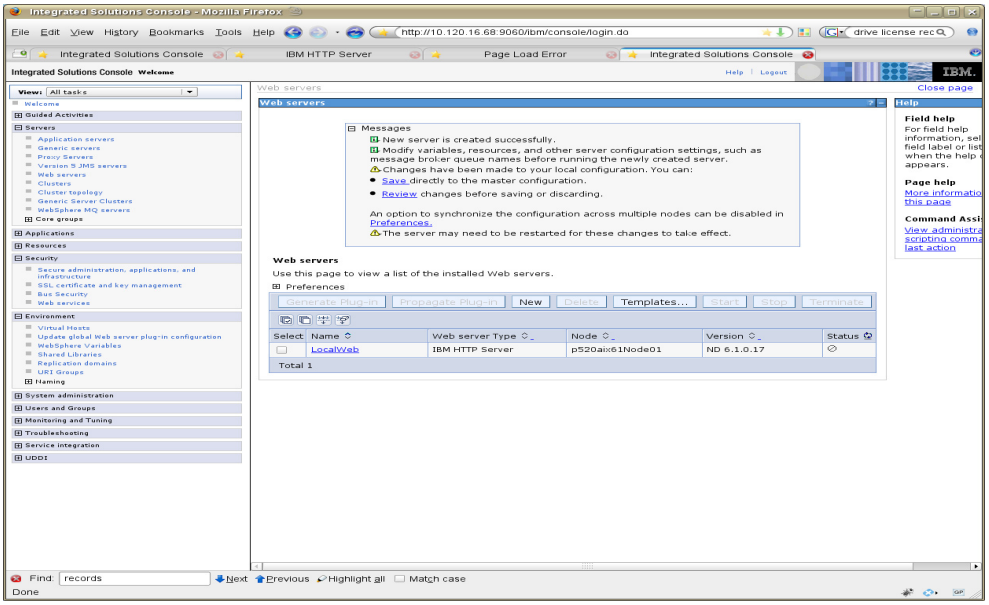
   b. Click **Next**.



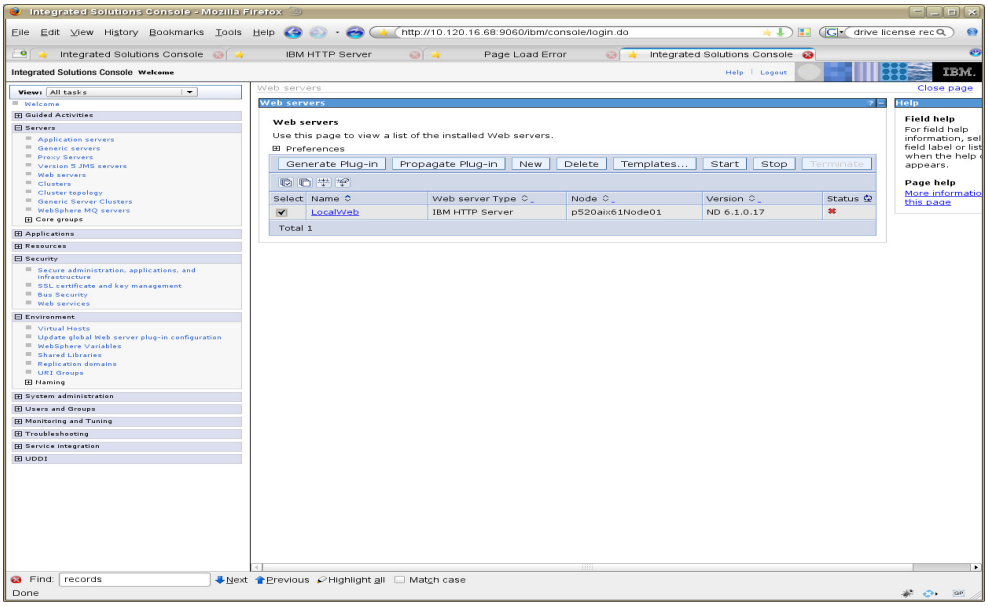
8. Confirm the new Web server, then click **Finish**.



9. Save the changes as requested.



10. You can now start and stop the web server from the WAS console, using the Web servers selection.



Chapter 8

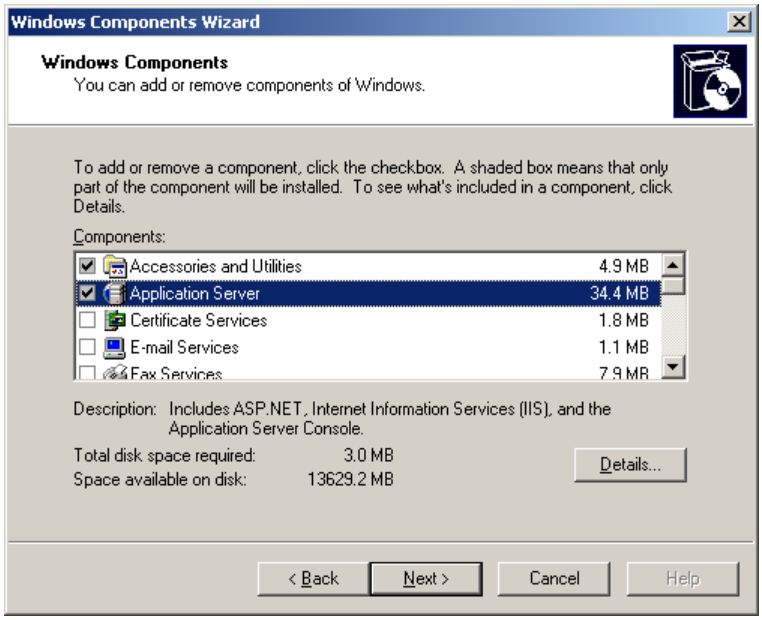
Installing Internet Information Services 6.0 on Windows

This chapter explains how to install and test Microsoft's Internet Information Services (IIS) 6.0.

This chapter contains the following sections:

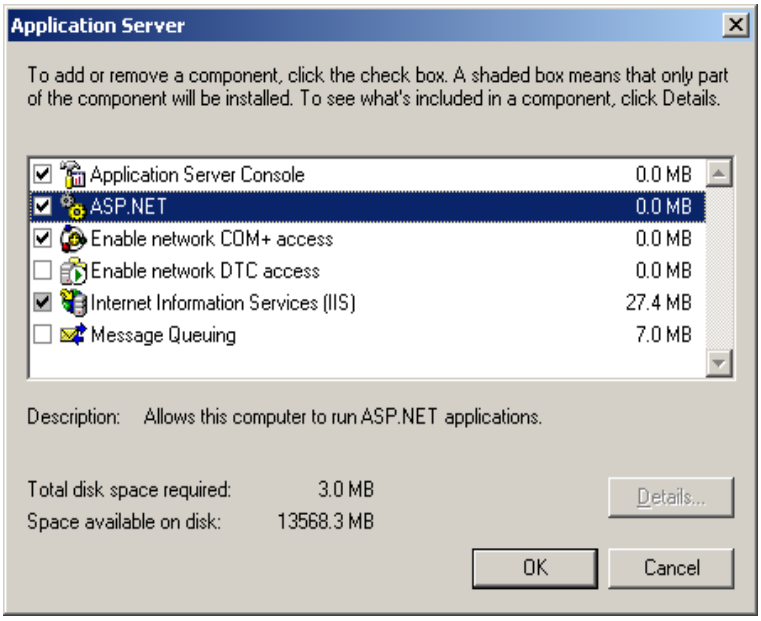
Step I. Install IIS

1. Select **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.
2. In "Add or Remove Programs," click **Add/Remove Windows Components**.
3. In the "Windows Components Wizard" select **Application Server**, then click **Details**.



4. In the "Application Server" screen select:
   - **Application Server Console**
   - **ASP.NET**
   - **Enable network COM+ access**
   - **Internet Information Services (IIS)**

   Click **OK**.



5. In the "Windows Components Wizard," click **Next**.
6. When the "Windows Components Wizard" completes the configuration process click **Finish**.

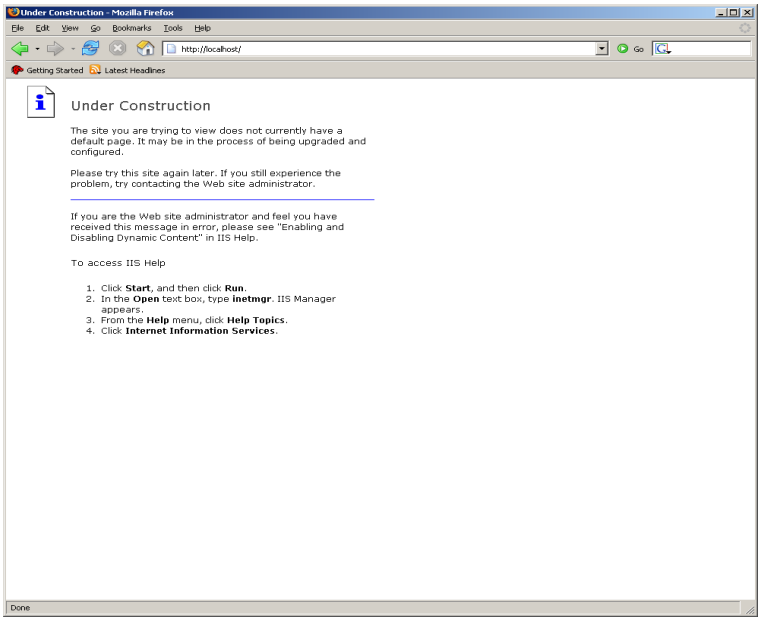
Step II. Verify the Installation

To verify that IIS can serve pages, test it from a web browser on the host machine and from the web browser of another machine on the network.

1. Start a web browser on the host machine that is running IIS.
2. Using the browser, go to the following URL:

   `http://localhost/`

3. If the browser displays an “Under Construction” page, then IIS is installed and running.

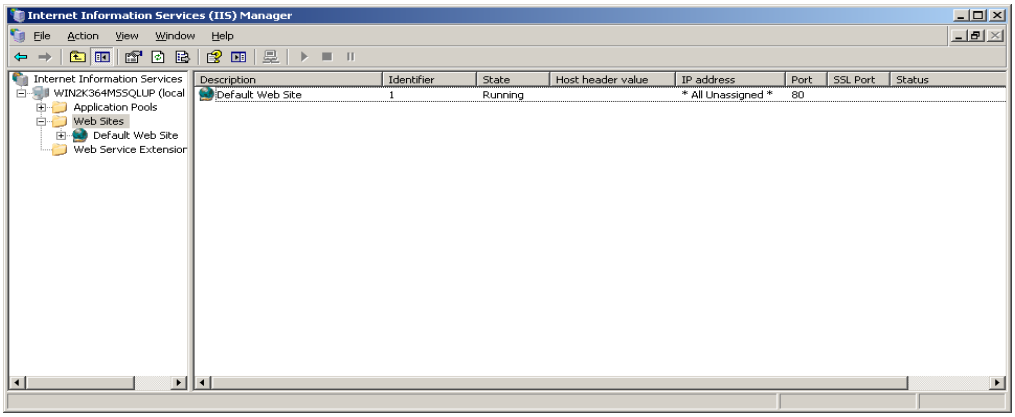


Step III. Starting and Configuring IIS

A. IIS Manager

1. Open the **Start** menu and click **Run** to access IIS Manager.
2. Type **`inetmgr`**, then click **OK**.
3. Click the **Web Sites** option when the IIS Manager loads.

   The right pane contains a list of the web sites that are managed including important information for each site, such as: the description, identifier, state, host header value, IP addresses, port, ssl port, and the status.

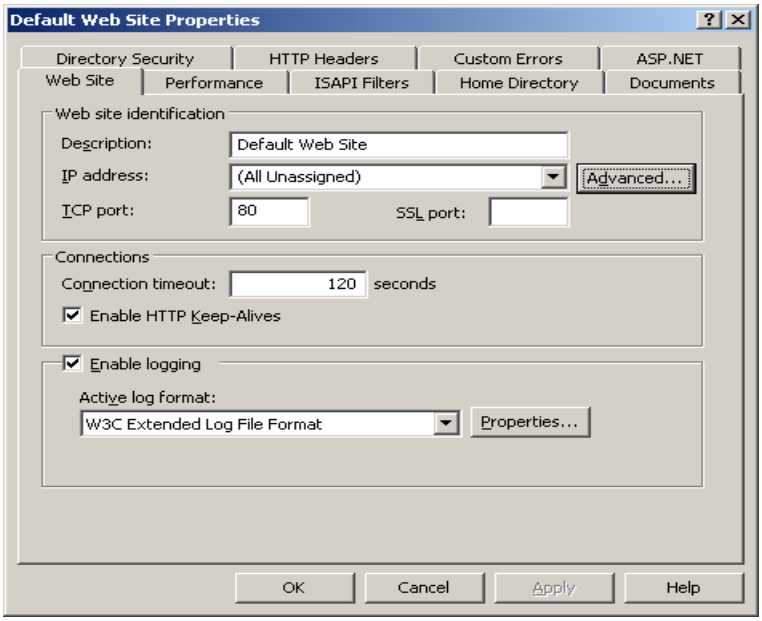


4. To restart IIS Manager, select the **Action** menu, then click **All Tasks** > **Restart IIS**.

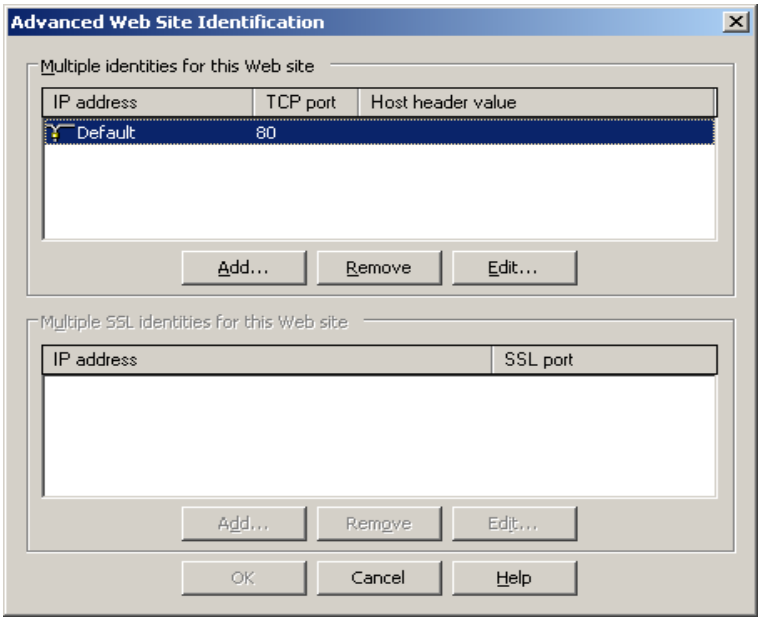
B. Changing the IIS Port

1. Open IIS Manager and expand **local computer** > **Web Sites**.
2. Right-click **Default Web Site**, and click **Properties**.

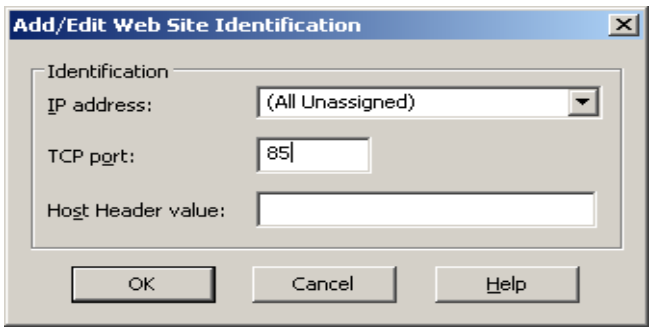
3. Next to **IP address**, click **Advanced**.



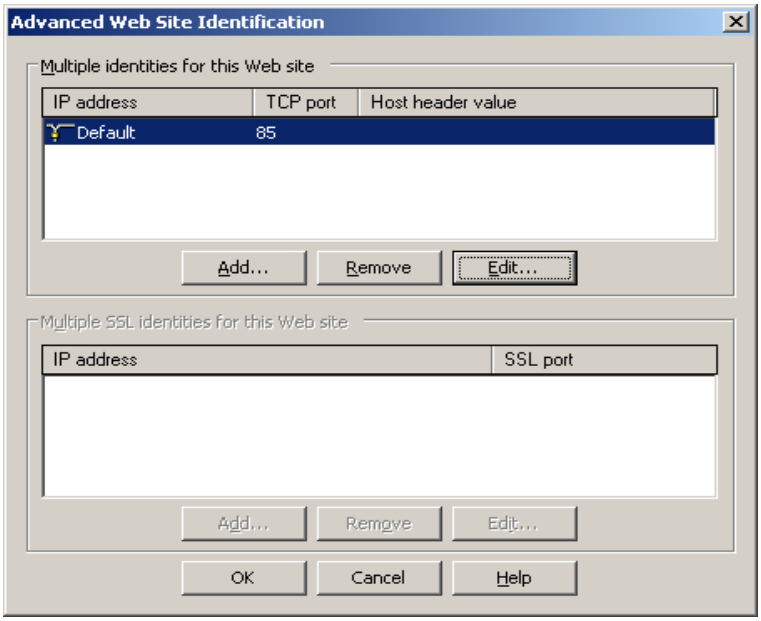
4. "Advanced Web Site Identification" enables you to specify a different port for each IP address. Select the entry for **Default** and click **Edit**.



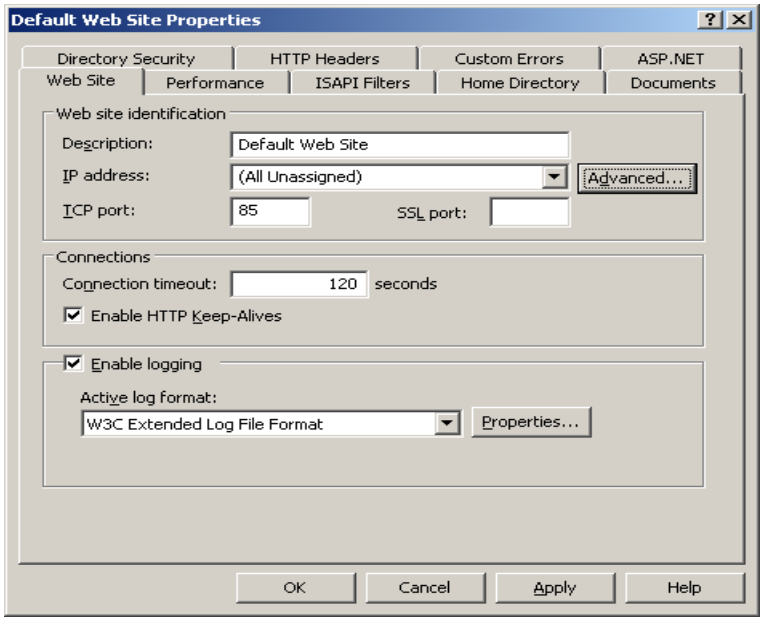
5. In the "Add/Edit Web Site Identification" screen select from the fields provided:
   - **IP address**: Either select a specific IP address, or select **(ALL Unassigned)**.
   - **TCP port**: Enter the desired port for the website to be accessed. If you selected a specific IP address, you can enter the **Host Header value** for that address. For example: `www.fatwire.com`.



6. In the "Advanced Web Site Identification" screen, click **OK**.



7. In the "Default Web Site Properties" screen, click **OK**.

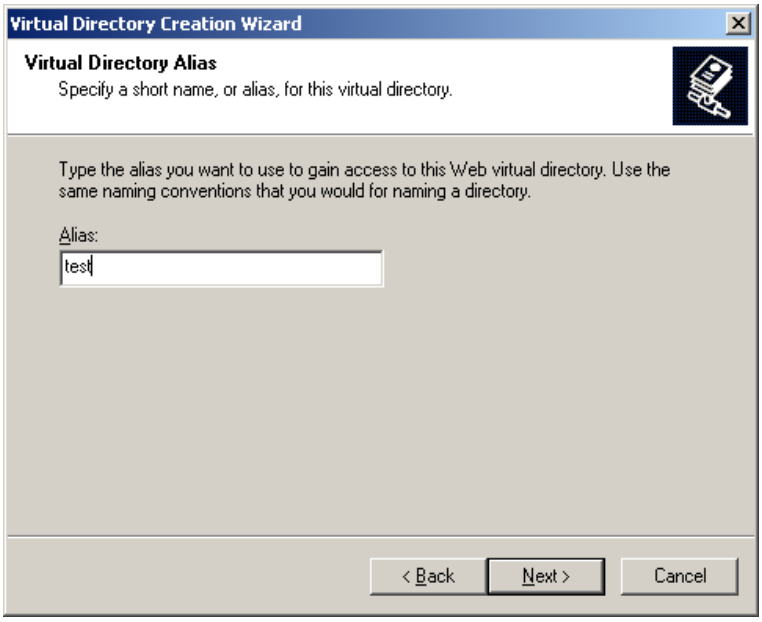


C. Create a Virtual Directory

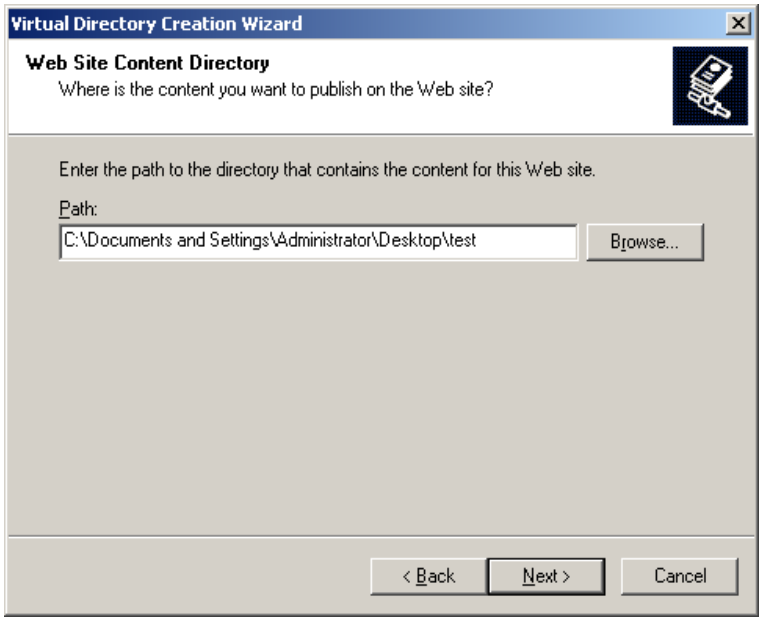
A virtual directory is used to make a local physical directory available through a web site by assigning it a simple URL.

1. Open IIS Manager and expand **local computer** > **Web Sites**.
2. Right-click **Default Web Site** and select **New** > **Virtual Directory**.
3. When the "Virtual Directory Creation Wizard" launches, click **Next**.

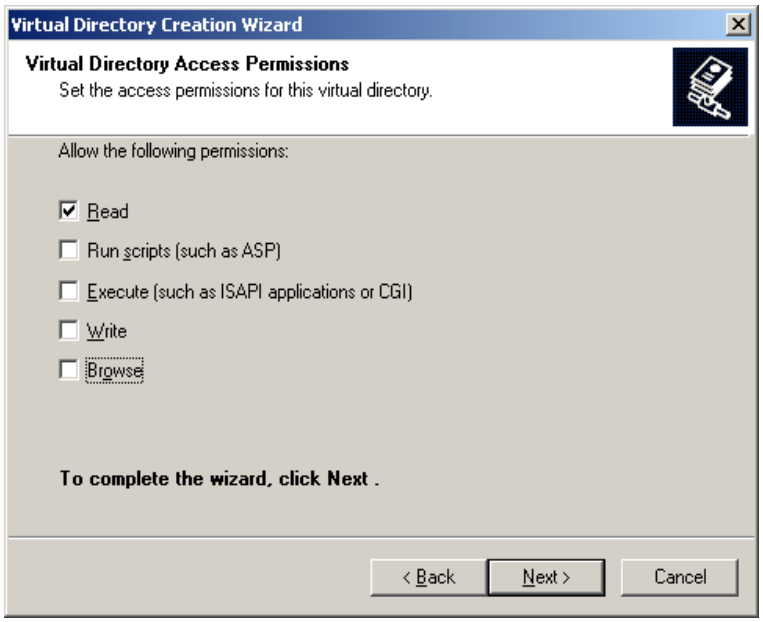
4. Enter an **Alias** for the virtual directory and click **Next**.



5. Browse to the physical directory to be shared and click **Next**.



6. Select the appropriate access permissions for the physical directory, depending on the file types, then click **Next**.

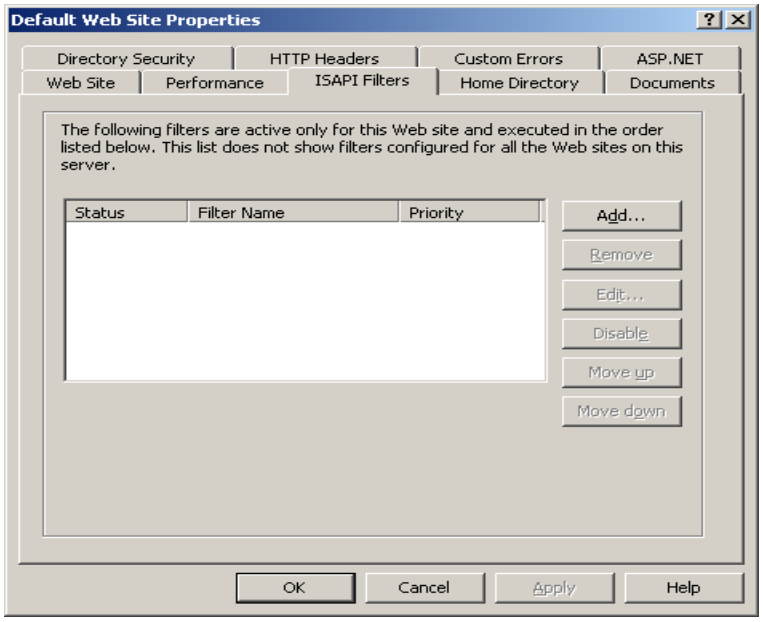


7. Click **Finish**.

D. Create a New ISAPI Filter

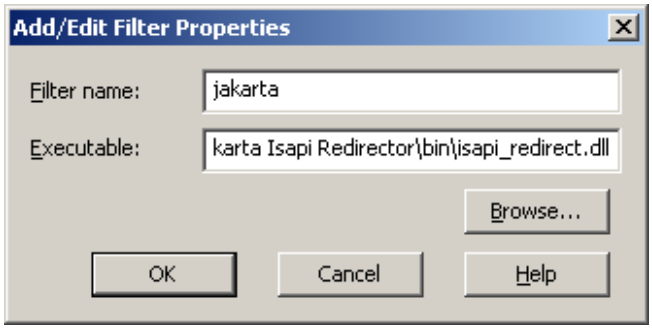
An ISAPI filter is used to change the default behavior of IIS and affects how `HTTP` requests are handled.

1. Open IIS Manager and expand **local computer** > **Web Sites.**
2. Right-click **Default Web Site** and click **Properties**.
3. Select the **ISAPI Filters** tab and click **Add**.



4. In the "Add/Edit Filter Properties" screen, fill in the fields provided:
   - **Filter name:** Enter a filter name.
   - **Executable:** Enter the locations for the Executable.

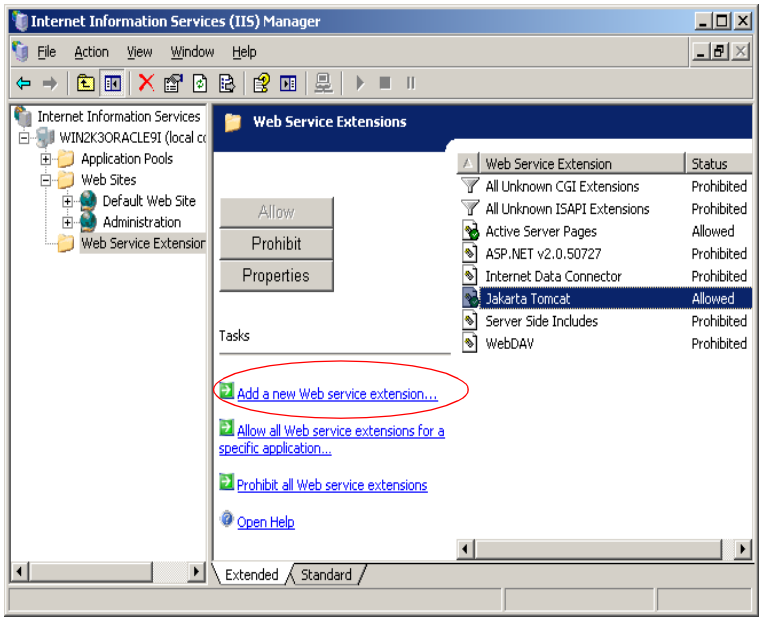
   a. Click **OK**.



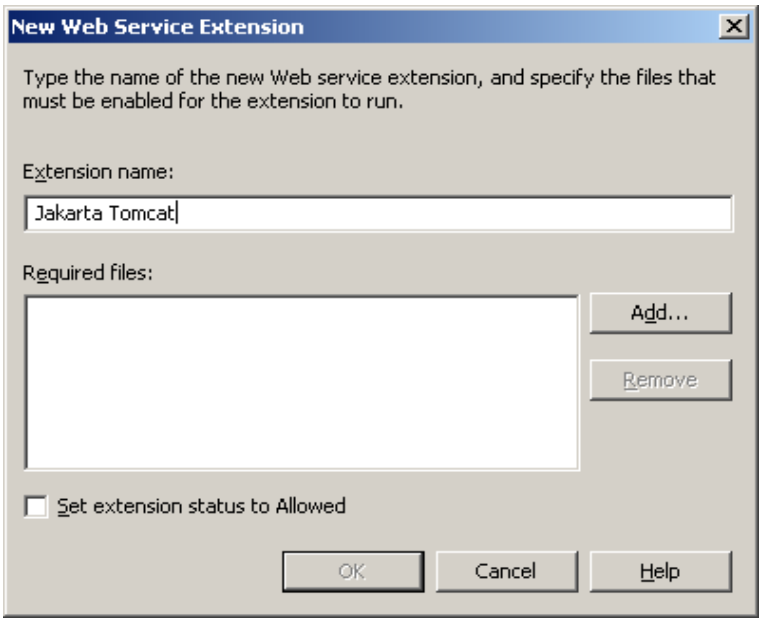
E. Create a New Web Service Extension

A web service extension is a program that extends the basic IIS functionality for serving static content.

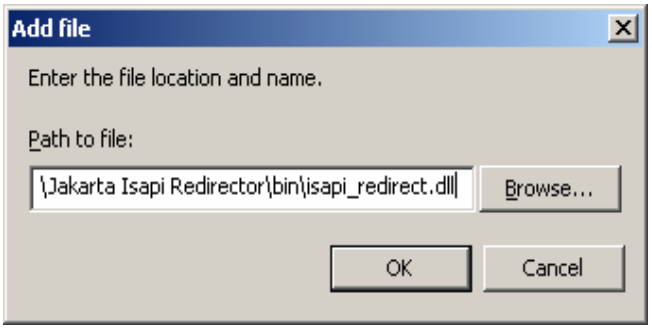
1. In the "IIS Manager" click **Web Service Extensions**, then click **Add a new Web service extension**.



2. Enter a name for the web service extension, then click **Add**.



3. Browse to the location of the web service extension file. Click **OK**.



4. Select **Set extension status to Allowed**, then click **OK**.

Chapter 9

Installing Internet Information Services 7.0 on Windows

This chapter explains how to install and test Microsoft's Internet Information Services (IIS) 7.0 on Windows 2008 Server.

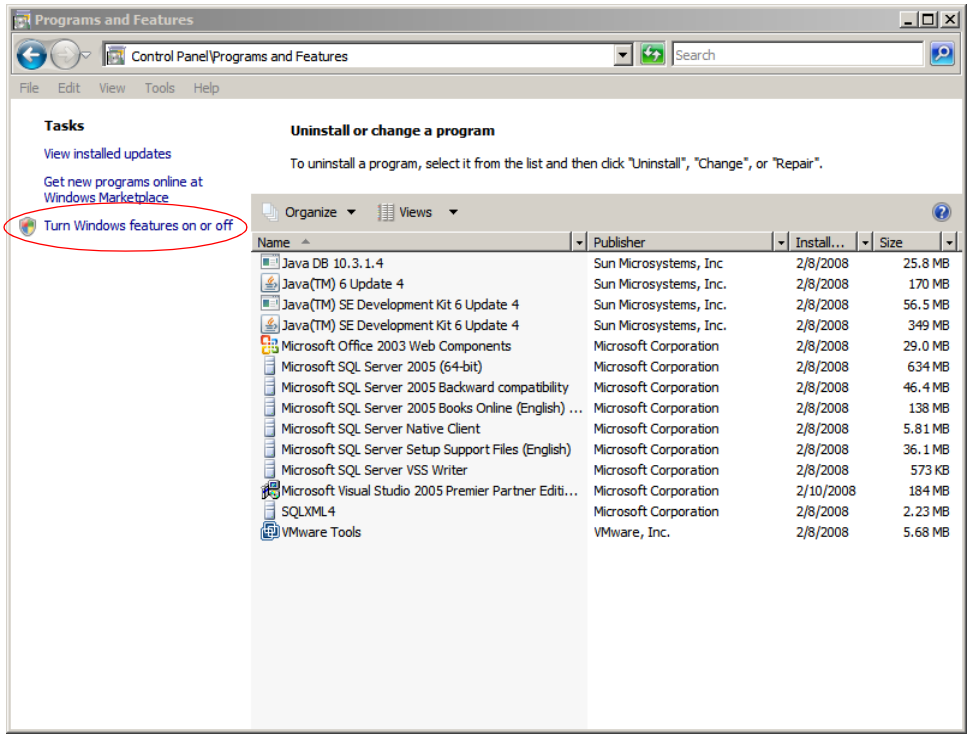
This chapter contains the following sections:

Step I. Install IIS

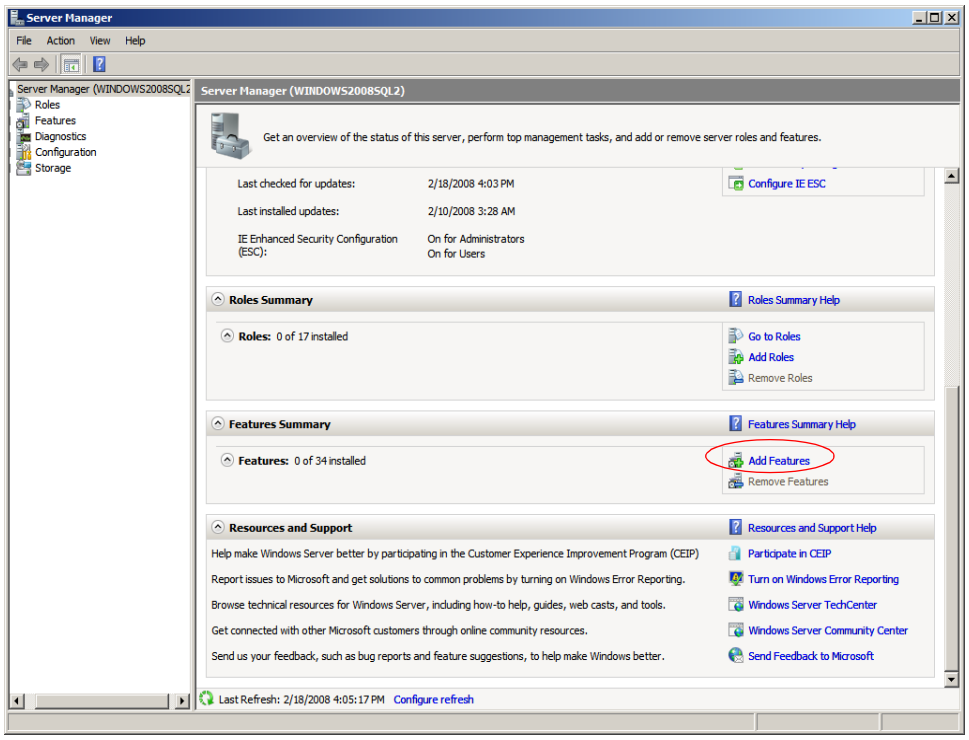
If IIS is not installed or is only partially installed, follow Microsoft's instruction for installing IIS 7.0 on Windows 2008 Server.

Here is a summary of the instructions:

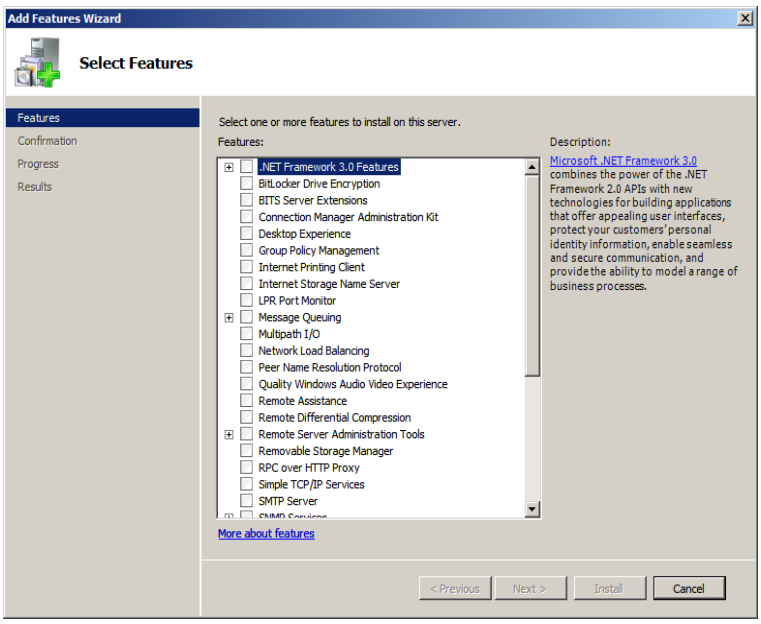
1. Select **Start > Settings > Control Panel**.
2. Select **Programs and Features**
3. Select **Turn Windows features on or off**.



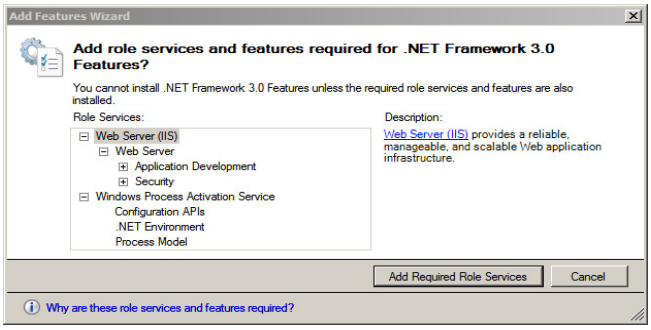
4. In the “Server Manager” window scroll down to the “Features Summary” section and click **Add Features**.



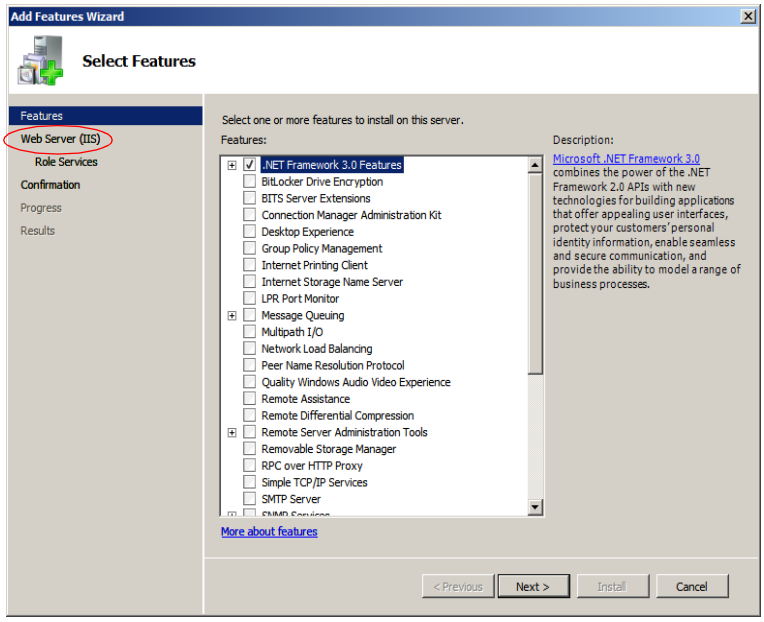
5. In the “Select Features” screen select **.NET Framework 3.0 Features**.



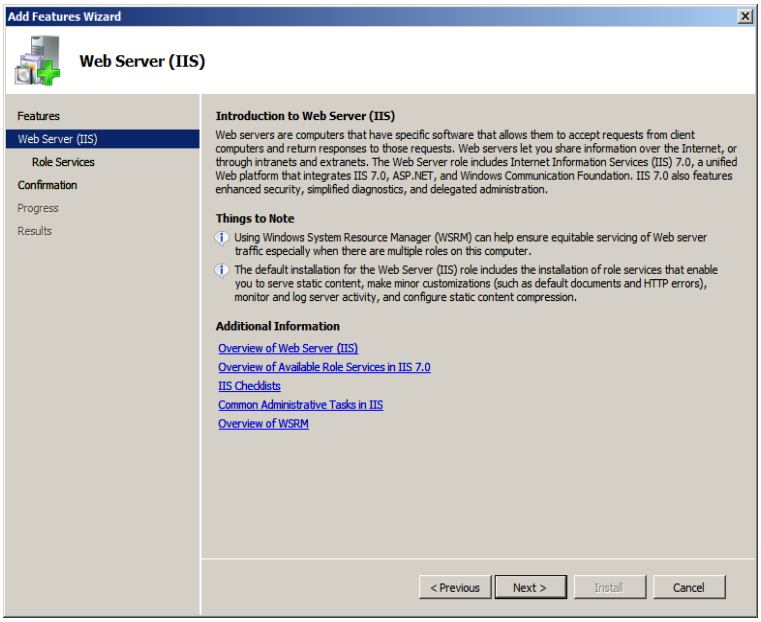
6. In the "Add Features Wizard" dialog box, select **Add Required Role Services**.



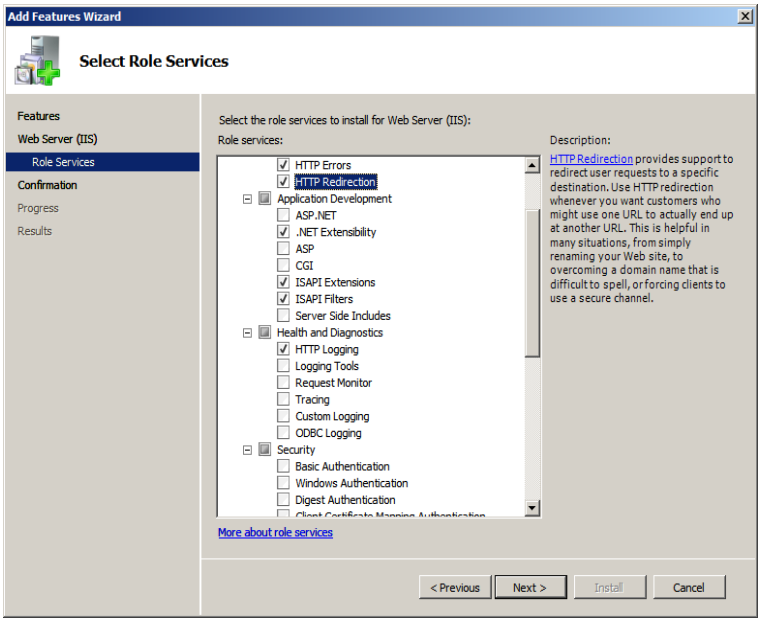
7. The **Web Server (IIS)** option appears in the "Add Features Wizard." Click **Next**.



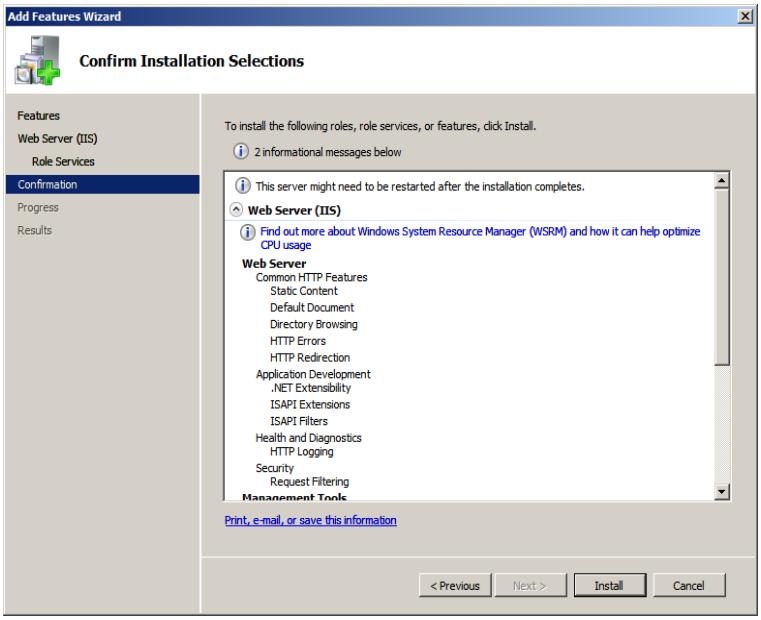
8. In the “Introduction to Web Server (IIS)” screen, click **Next**.



9. In the “Select Role Services” screen:
   a. Select the following:
      - **Common HTTP Features**
      - **ISAPI Extensions**
      - **ISAPI Filters**
      - **HTTP Logging**
      - **Management Tools**
      - Any other roles that are required for your installation, such as **HTTP Redirection**
   b. Click **Next**.

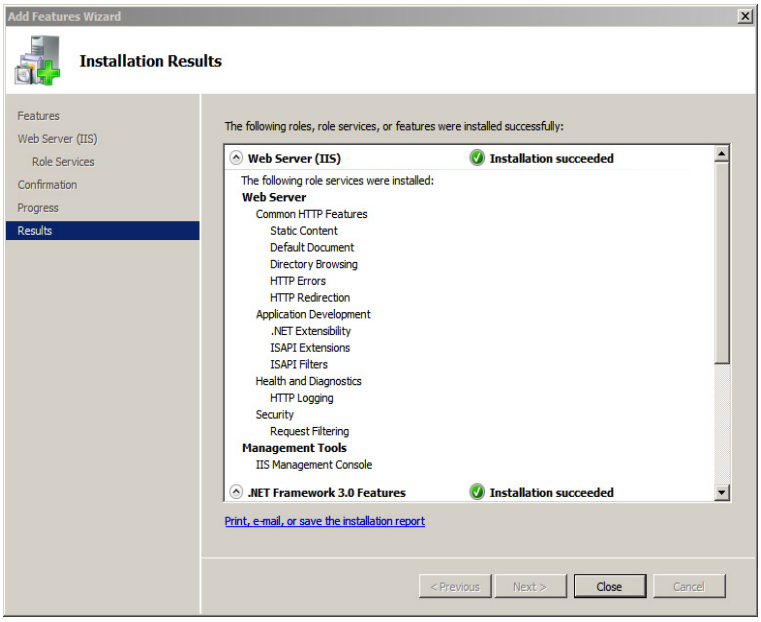


10. In the “Confirm Installation Selections” screen, confirm your choices and click **Install**.



11. Allow the installation to complete, then review the results.

12. Click **Close**.



13. It is suggested at this point to reboot, but it is not required.

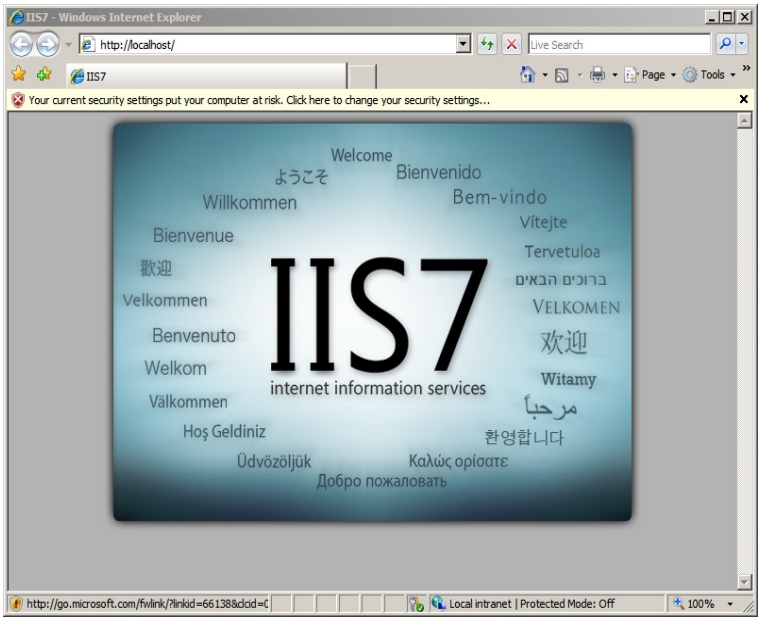
Step II. Verify the Installation

After installing IIS, you must verify the installation to determine whether it is serving pages properly. Test the installed IIS from the server that is hosting it as well as from another browser on the network.

To verify that IIS is serving pages

1. Start a browser on the host that IIS is running on.
2. From the browser, go to the following URL: **`http://localhost/`**

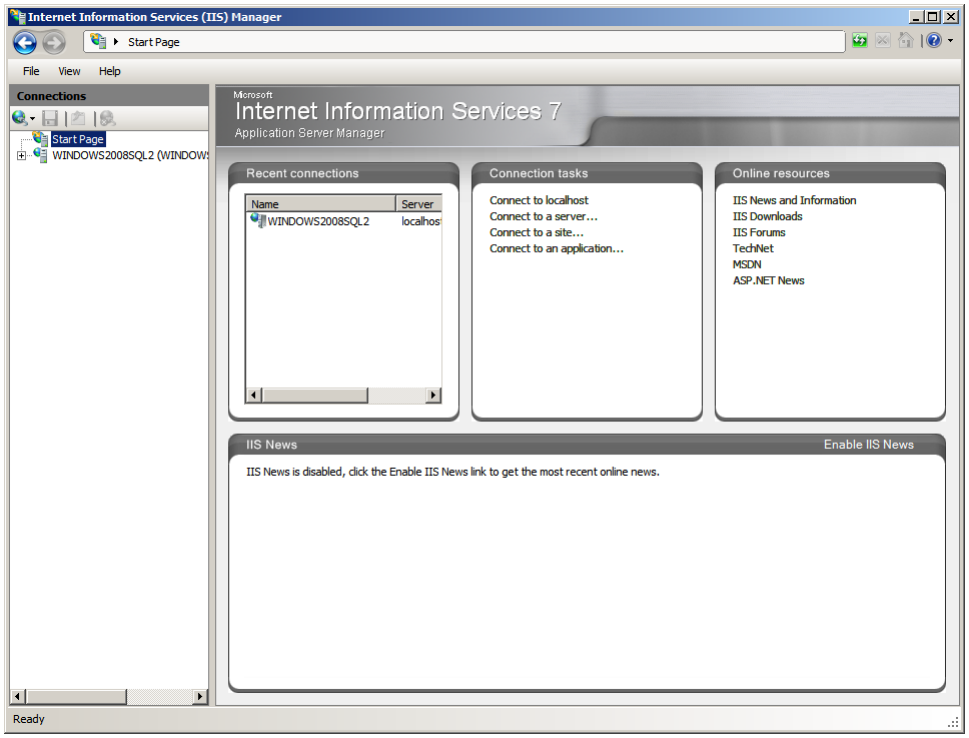
   IIS is installed and running if the browser displays the “IIS7” page.



Step III. Starting and Configuring IIS

A. IIS Manager

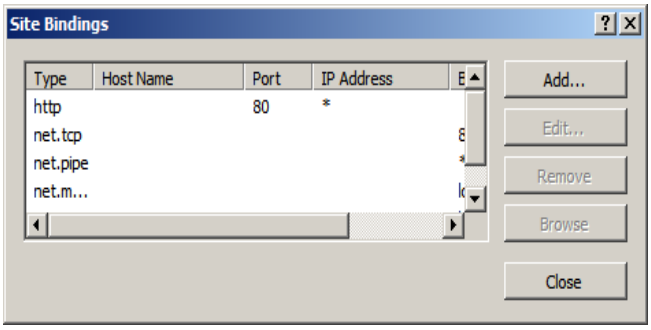
1. Start the management console, which is required before any other actions are taken.
2. Select: **Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager**
3. When the "Internet Information Services (IIS) Manager" loads:
   a. Expand the left-hand tree that starts with the current system's name.
   b. In the "Sites Entry" field select **Default Web Site**.



B. Changing the IIS Port

1. Open the management console and browser to the **Default Site**
2. Right-click the **Default Web Site** entry and select **Edit Bindings** from the menu.

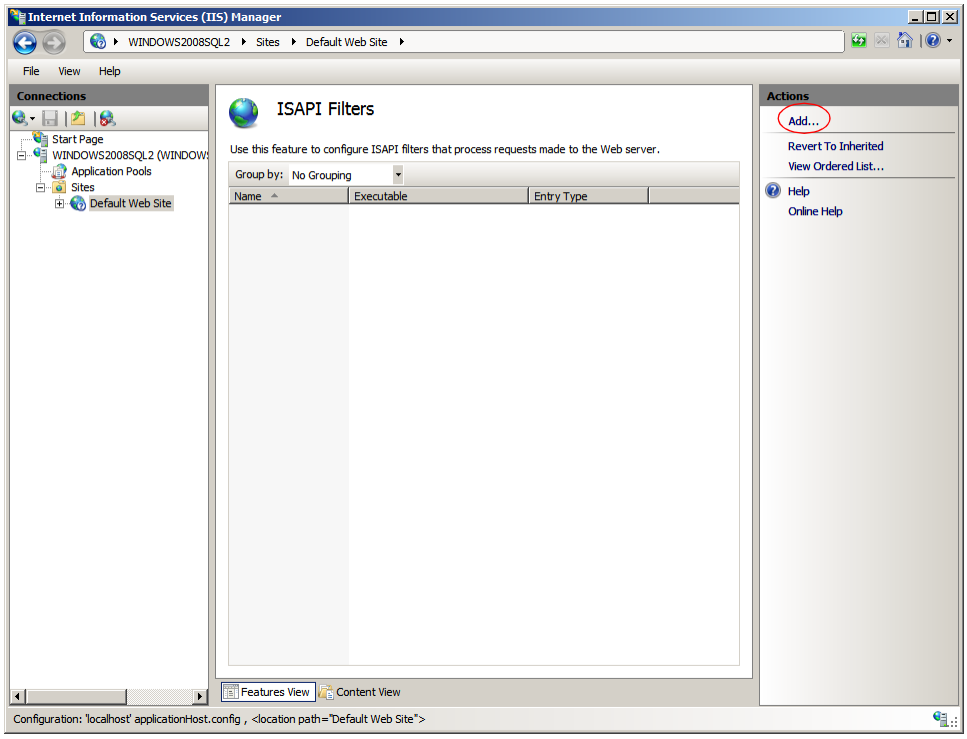
3. In the “Site Bindings” dialog box you can add or change the ports and IP address on which the Server IIS will bind.



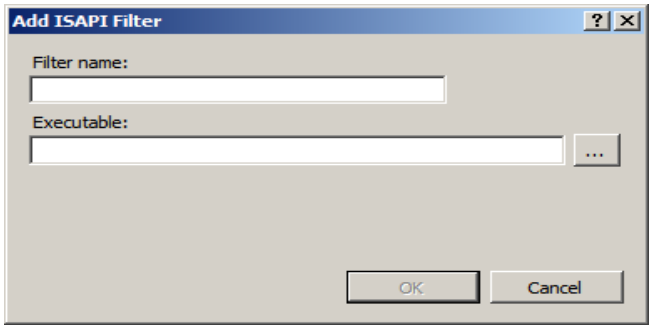
4. Click **Close** after all changes have been made.

C. Adding a New ISAPI Filter

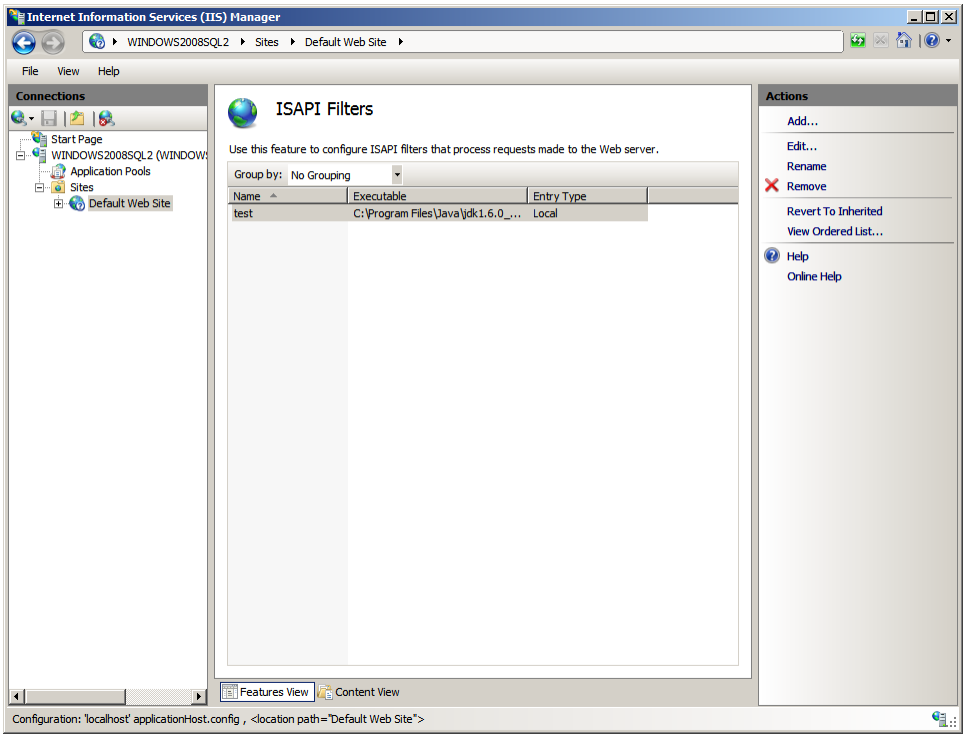
1. Open the management console and browser to the **Default Site**.
2. In the center list, click **ISAPI Filters** and click **Add**.



3. The “Add ISAPI Filter” dialog box appears.
   a. Fill in the fields provided:
      - **Filter name:** Enter a filter name.
      - **Executable:** Enter the location of the Executable.
   b. Click **OK**.

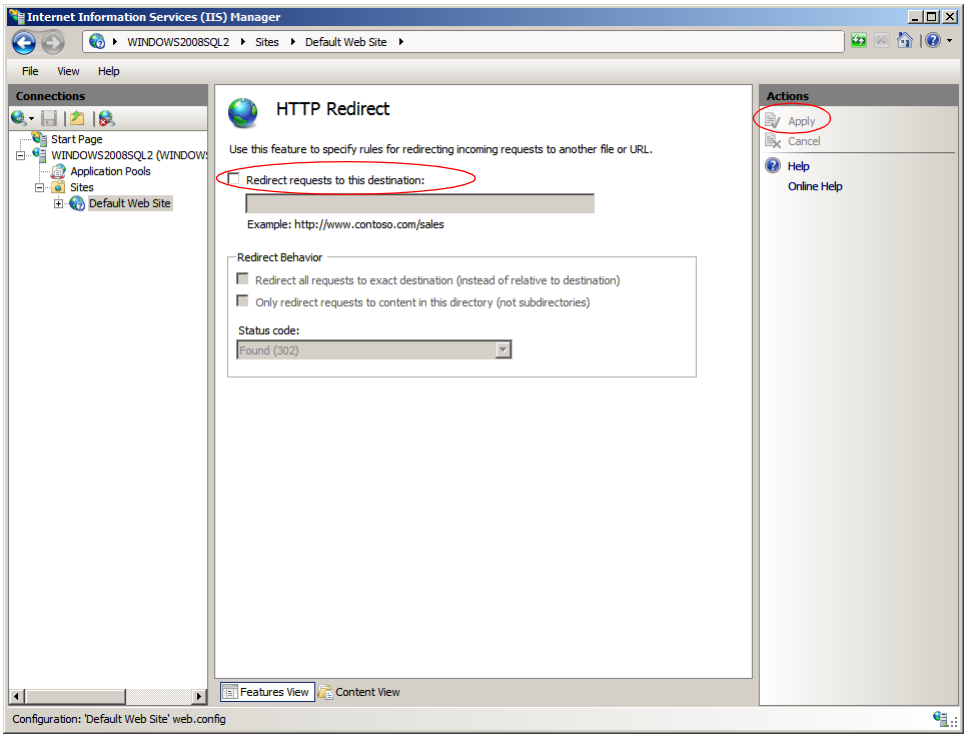


The new filter is added to the “ISAPI Filters” list.



Proxing Using IIS

1. Open the management console and browser to the Default Site.
2. In the center list click **HTTP Redirect**.
3. In the center panel of the "Internet Information Services (IIS) Manager":
   a. Select the **Redirect requests to this destination** option.
   b. Enter the location of the remote server in the text field (for Content Server or Remote Satellite Server include the context root).
   c. Click **Apply**.



Chapter 10

Installing Apache on Solaris and Linux

This chapter describes how to install and configure Apache HTTP Server on Solaris and Linux systems. As previously mentioned, you can install Apache on the same machine that will host WebLogic and Content Server, or you can install and use it on a separate host.

This chapter contains the following sections:

Step I. Install Apache

1. Apache HTTP Server can be pre-installed on Solaris 8, Solaris 9, Linux RedHat, and Linux SuSE systems. Determine whether Apache is installed on the environment(s) on which you plan to run it.
2. Do one of the following:
   - If Apache is already installed, continue with "Step II. Document Your Apache Parameters," on page 140.
   - If Apache is not already installed, you can do one of the following:
     - Install it from your source medium.
     - Download it from the Internet.
     - Build it from source; that is, select the modules and compile the Apache executable yourself. If you want to build it from source, refer to the information that the Apache Foundation makes available at `http://www.apache.org/` and follow their instructions.

Step II. Document Your Apache Parameters

We strongly recommend that you document the details of your Apache installation in Table 3, "Apache Parameters."

Table 3: Apache Parameters

Parameter	What it Holds	Your Value
Web Server Version (*`WebVersion`*)	The version of Apache that the host is running. Note that you must use a version that Content Server supports.	
Web Host Name (*`WebHost`*)	The name by which the Apache host machine is known on the network.	
Web Host IP Address (*`WebIP`*)	The numeric Internet Protocol address assigned to the Apache host machine.	
Web Server Port (*`WebPort`*)	The port number assigned for Apache communications. By default, it has the value 80.	
Apache Root Directory (*`ApacheRoot`*)	The top-level directory in which Apache is installed. Immediate subdirectories of *`ApacheRoot`* include `bin` and `conf`.	

Step III. Verify that Apache Contains the Correct Module

Note

This section applies only to Apache version 1.3x.

Apache is modular software, built from a set of modules. WebLogic Server requires that the `mod_so.c` module be present on the machine that is hosting the Apache web server. Please verify that your Apache server contains this module by using the command `httpd` with the `-l` option and search for `mod_so` in the output.

For example:

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

Examine the output and do one of the following:

- If the output from the preceding command contains `mod_so.c`, then your version of Apache contains the correct module. Proceed to "Step IV. Verify that Apache Runs Properly," on page 141.
- If the output from the preceding command does not contain `mod_so.c`, you must rebuild and reinstall Apache. For guidelines, see "Step I. Install Apache," on page 140.

Step IV. Verify that Apache Runs Properly

In this step, you will start Apache and verify that it is running properly. For verification instructions, see the Apache web site (given in "Step I. Install Apache," on page 140).

Next Step

Configure Apache to run with WebLogic and Content Server. For instructions, refer to the installation guide for your configuration.

Part 3

Installing and Configuring LDAP

If you choose to use LDAP, Content Server must have access to a supported LDAP server specifically configured for Content Server. This part describes how to install and configure a supported LDAP server for integration with Content Server.

Note

- You must set up a supported LDAP server **before** you run the CS-LDAP integrator.
- If you are integrating with LDAP, but no content management sites exist in Content Server, then upon completion of the LDAP integration, refer to instructions in the CS-LDAP integration guide (“Step 8. Post Integration. If Content Management Sites are Not Installed”).

This part contains the following chapters:

Chapter 11

Setting Up Sun Access Manager 7.0

This chapter provides instructions for setting up the currently supported Sun Access Manager for use with Content Server.

Note

Sun Access Manager is installed as part of Sun Portal Server 7, which means that either Sun Access Manager and Sun Directory Server were installed locally on your portal server, or you elected to configure Sun Access Manager to connect to a remote instance of Sun Java Systems Directory Server. In either case, you already have Sun Access Manager installed and configured for your application server and portal server.

Note that you must set up Sun Access Manager before you run the CS LDAP integrator.

This chapter contains the following sections:

Start/Stop Commands

This section lists commands for starting and stopping Sun Access Manager.

To start Sun Access Manager:

- On Solaris:

  `./usr/sbin/amserver start`
- On Unix (except Solaris):

  `<sun_portal_home>/identity/bin/amserver start`
- On Windows:

  Start --> **Programs** --> **Sun Microsystems** --> **Sun One Identity** --> **Start Sun One Identity Servers** --> **Start**

To stop Sun Access Manager:

- On Solaris:

  `./usr/sbin/amserver stop`
- On Unix (except Solaris):

  `<sun_portal_home>/identity/bin/amserver stop`
- On Windows:

  Start --> **Programs** --> **Sun Microsystems** --> **Sun One Identity** --> **Stop Sun One Identity Servers** --> **Stop**

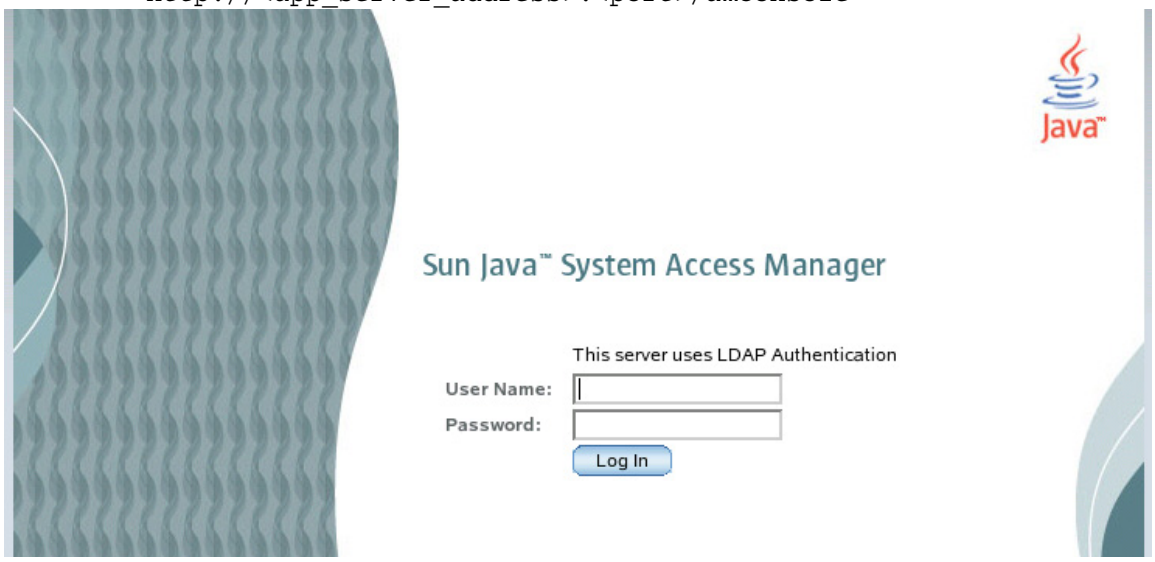
Creating CS Users in Sun Access Manager

In this section, you will use the Sun Access Manager console to create Content Server users in the backend LDAP server that is associated with Sun Access Manager.

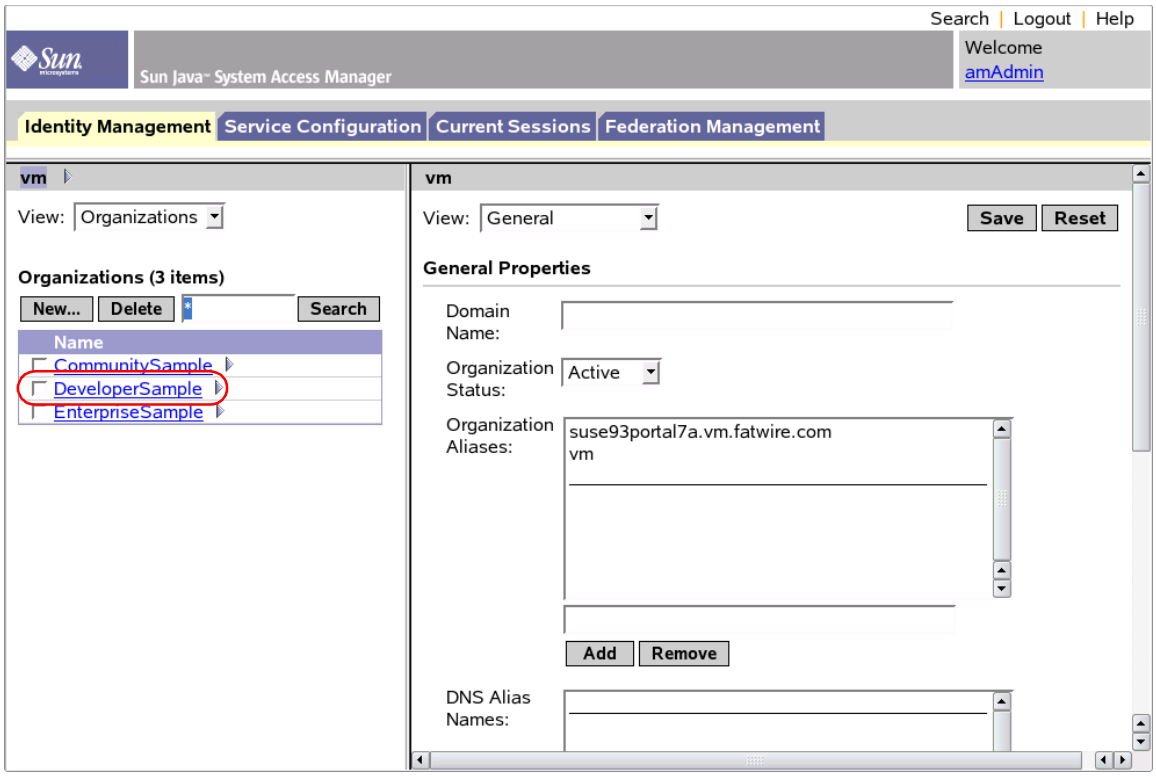
To create Content Server users in Sun Access Manager

1. Access the following URL:

   `http://<app_server_address>:<port>/amconsole`

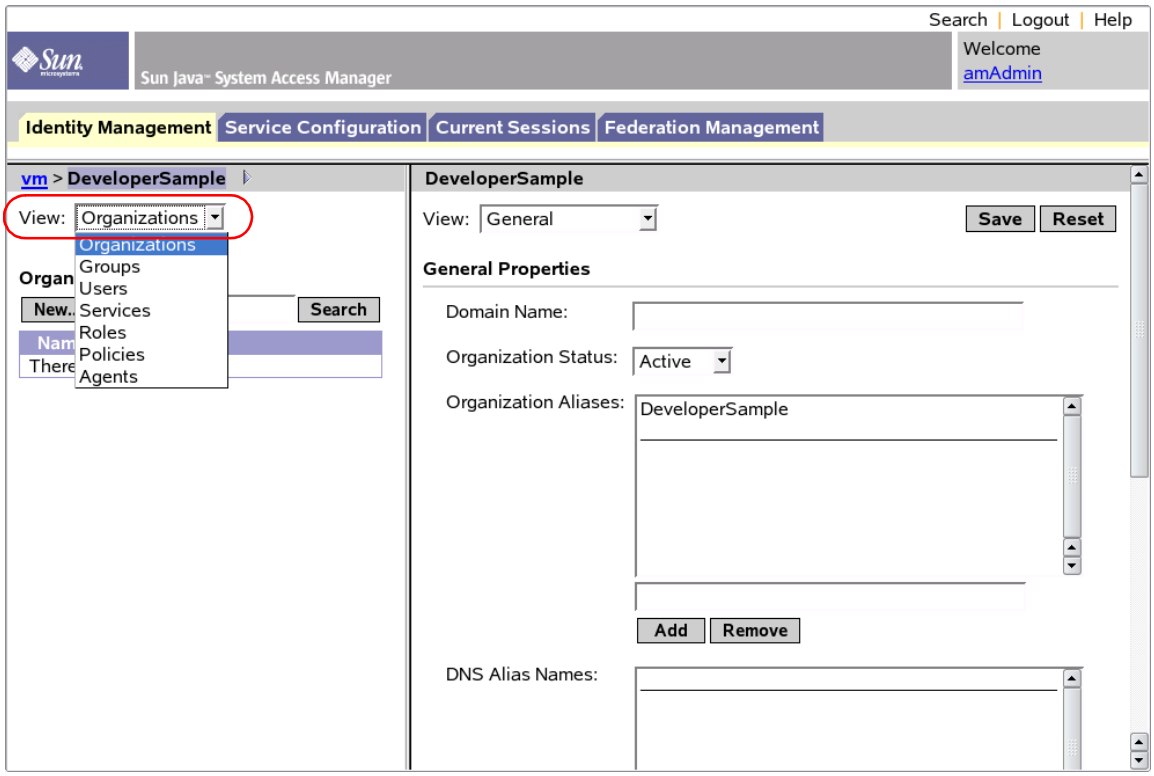


2. Log in using the user name (typically `amadmin`) and password that was selected during the installation of Sun Access Manager.
3. When logged in, you will see two large frames. The left-hand frame has a hierarchy that can be navigated. The right-hand frame has details for the item selected on the left.

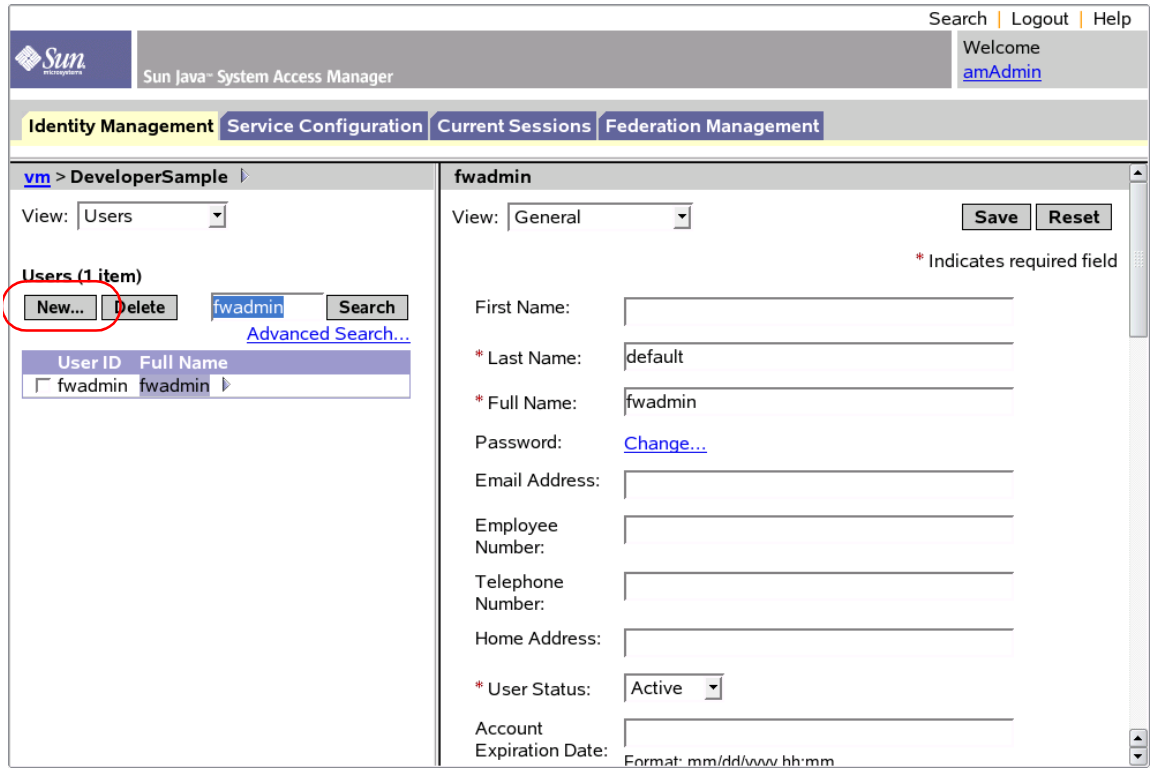


4. In the left-hand frame, click the link **DeveloperSample** (or the portal site which you used when installing Content Server).

5. Click the **View** drop-down menu. From here you may select **Roles**, **Groups**, or **Users**. As you will be adding a new user, select **Users**.

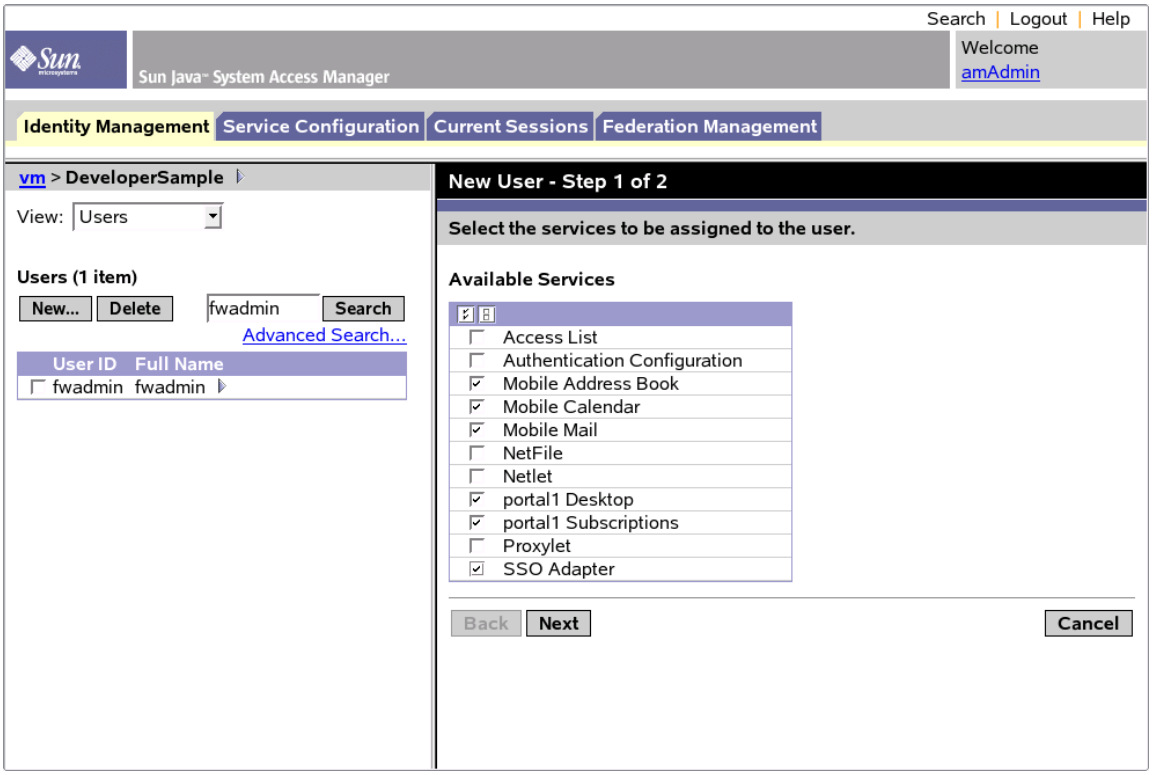


6. A list of all known users is displayed in the left frame. Click **New**.

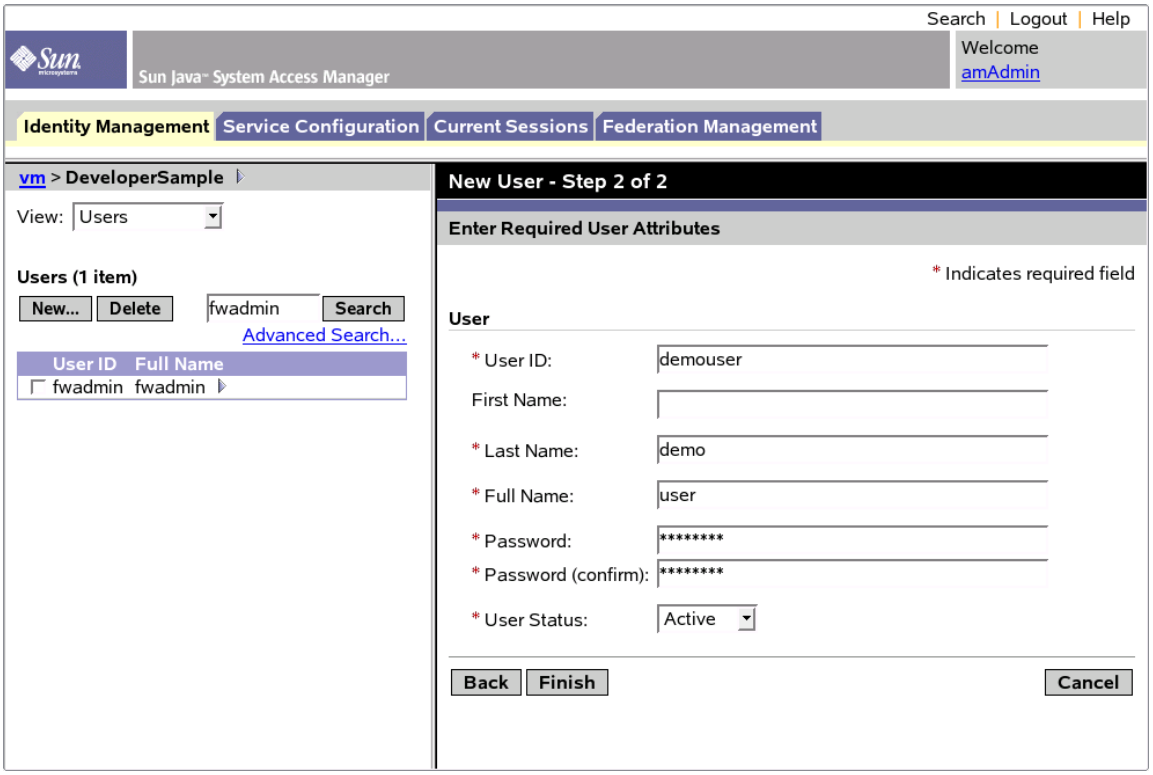


7. Select the following services from the list in the right-hand frame:
   - **Mobile Address Book**
   - **Mobile Calendar**
   - **Mobile Mail**
   - **Portal Desktop**
   - **Portal Subscriptions**
   - **SSO Adapter**

   Click **Next**.

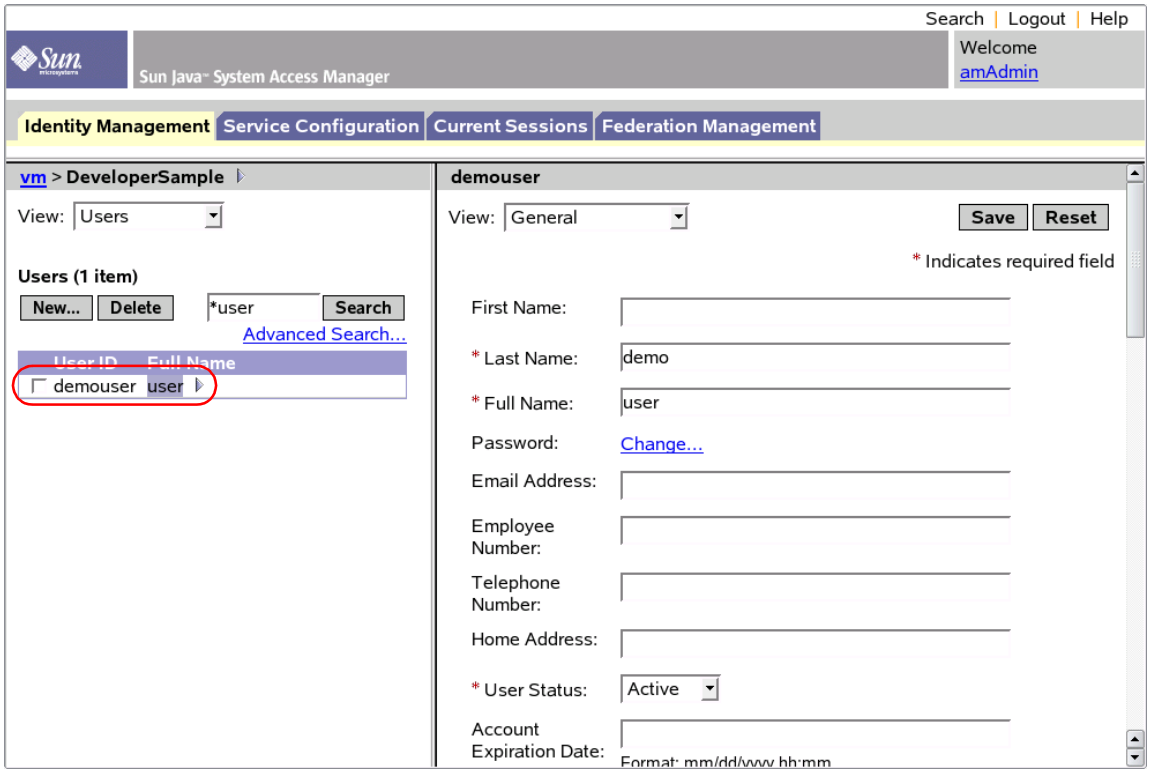


8. In the “New User” form, fill out the required fields (marked by a red *****). Ensure that “User Status” is set to **Active**. Click **Finish**.

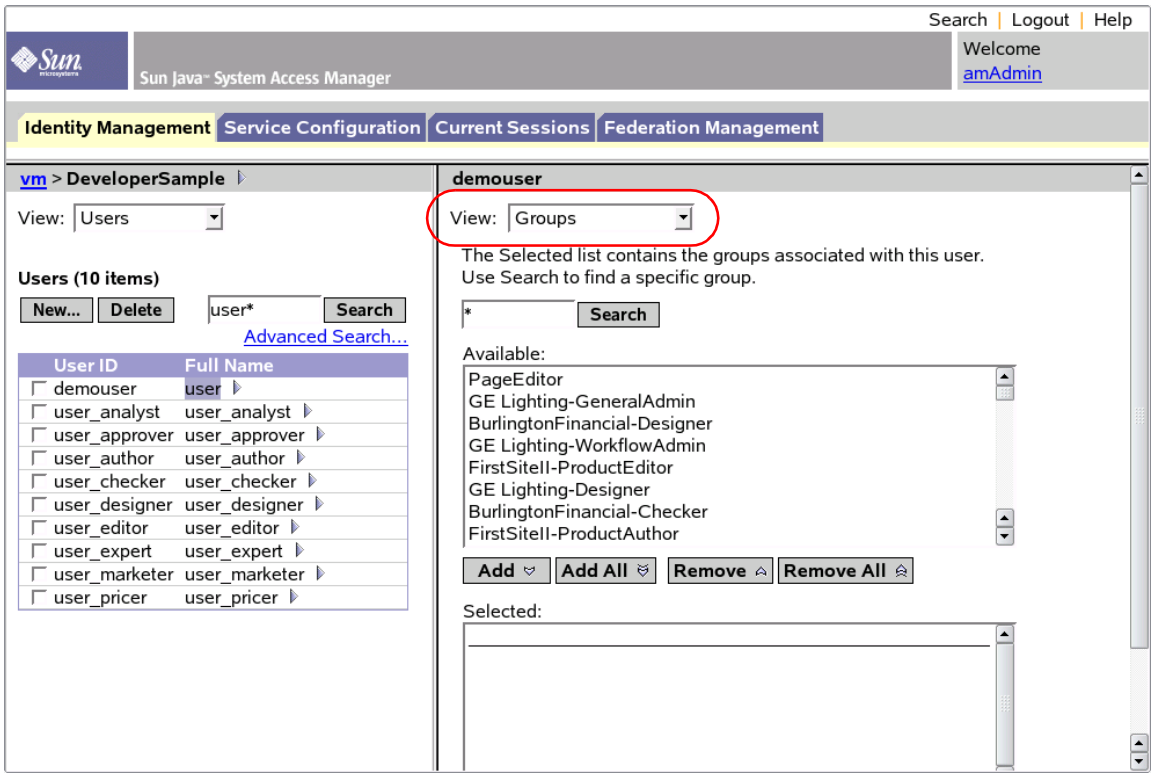


9. Assign Groups to the user:

a. Locate the newly created user (the fastest way is to use the **Search** function).



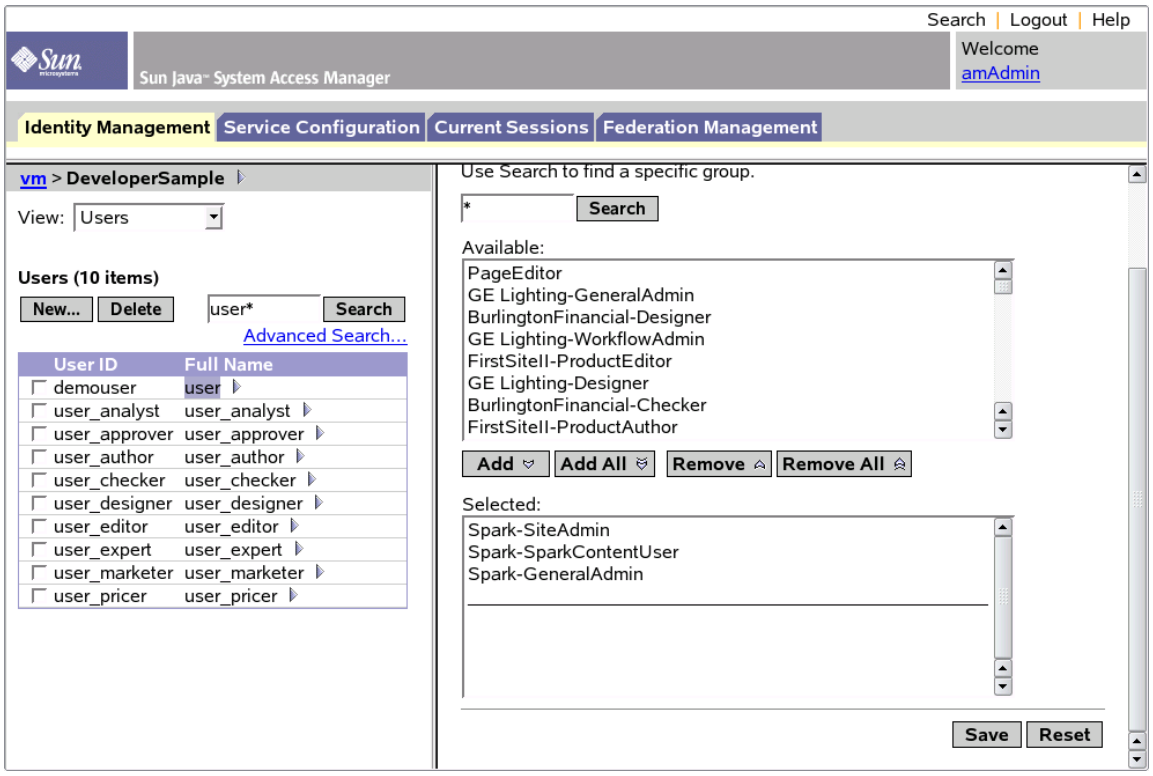
b. In the right-hand frame, select **Groups** from the "View" drop-down menu.



c. In the "Available" list box, select all Groups that you wish this user to have. In this example, three groups were assigned to the user: **Spark-SiteAdmin**, **Spark-SparkContentUser**, **Spark-GeneralAdmin** (listed in the "Selected" list box). For more detailed information about available groups, see the *Content Server Administrator's Guide*.

d. Click **Add**.

e. Click **Save**.



10. (Optional) Test your new user by logging in to the portal (must be the organization under which the user was created and Content Server was installed; for example, DeveloperSample Organization).

Chapter 12

Setting Up Sun Directory Server 6.0

This chapter shows you how to set up Sun Directory Server 6.0 for use with Content Server running on Sun Portal Server 7.

Note

You must set up Sun Directory Serve **before** you run the CS LDAP integrator.

This chapter contains the following sections:

Start/Stop Commands

This section contains commands for starting and stopping Sun Directory Server and the Sun Java Web Console.

Sun Directory Server

- To start:

  /opt/sun/ds6/bin/dsadm start <instance_dir>
- To stop:

  /opt/sun/ds6/bin/dsadm stop <instance_dir>

Sun Java Web Console

- To start:

  /opt/sun/webconsole/bin/smcwebserver start
- To stop:

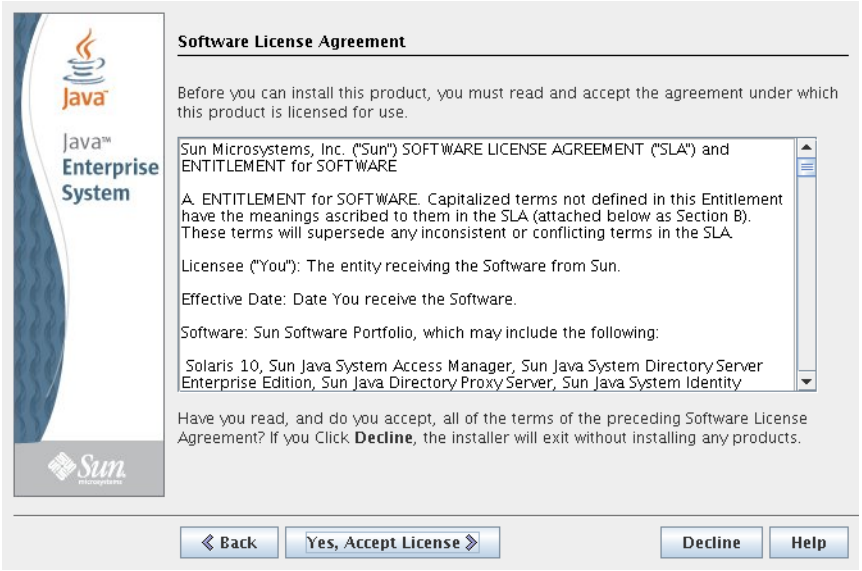
  /opt/sun/webconsole/bin/smcwebserver stop

Installing Sun Directory Server

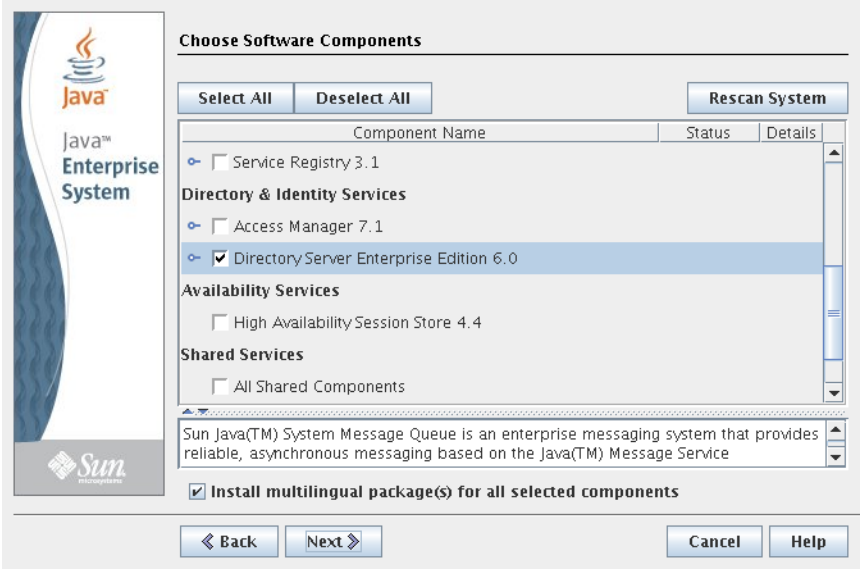
This section shows you how to install Sun Directory Server 6.

1. Download the Directory Server 6 package from the Sun website.
2. Decompress the file into a temporary directory and change to that directory.
3. Within the temporary directory, change to the directory corresponding to your operating system and launch the installer.
4. In the “Welcome” screen, click **Next**.

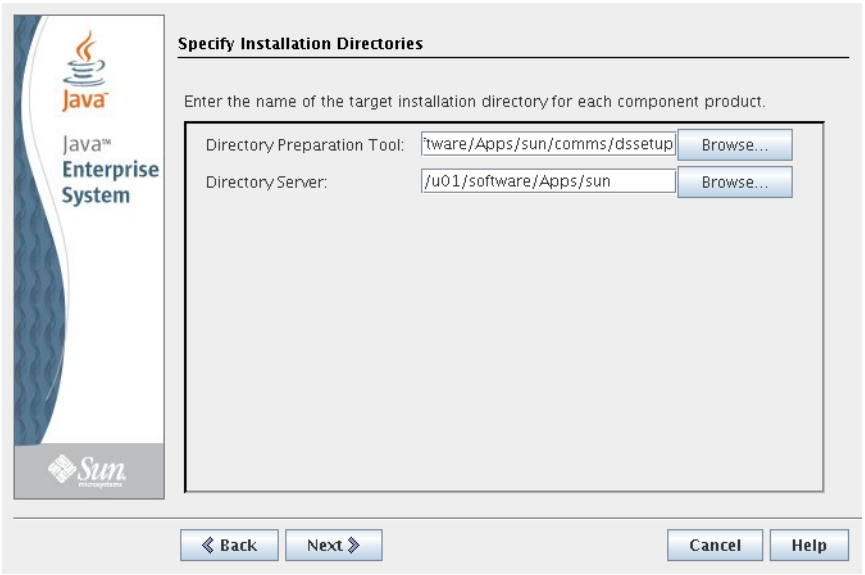
5. In the “Software License Agreement” screen, read the license agreement and click **Yes, Accept License**.



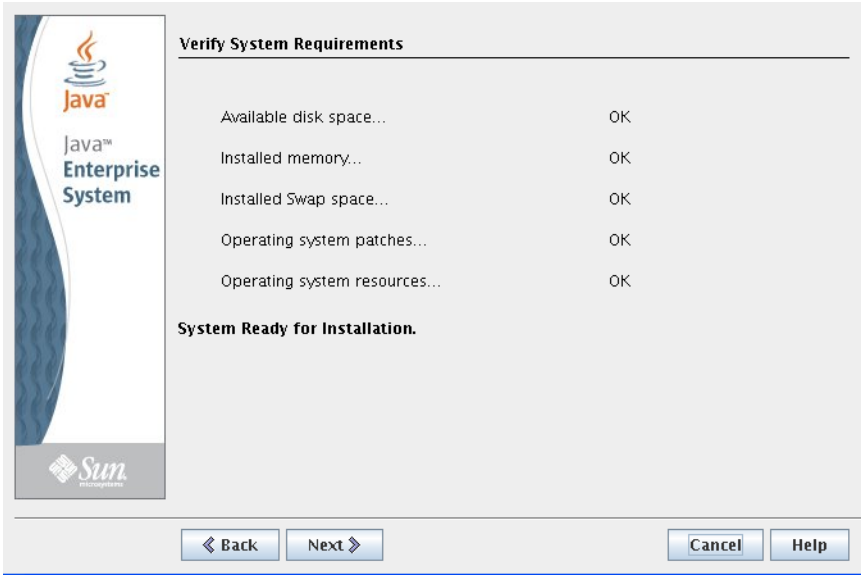
6. In the “Choose Software Components” screen, do the following:
   a. Select **Directory Server Enterprise Edition 6.0**.
   b. Expand the node and make sure that **Directory Service Control Center** is listed and selected.
   c. Click **Next**.



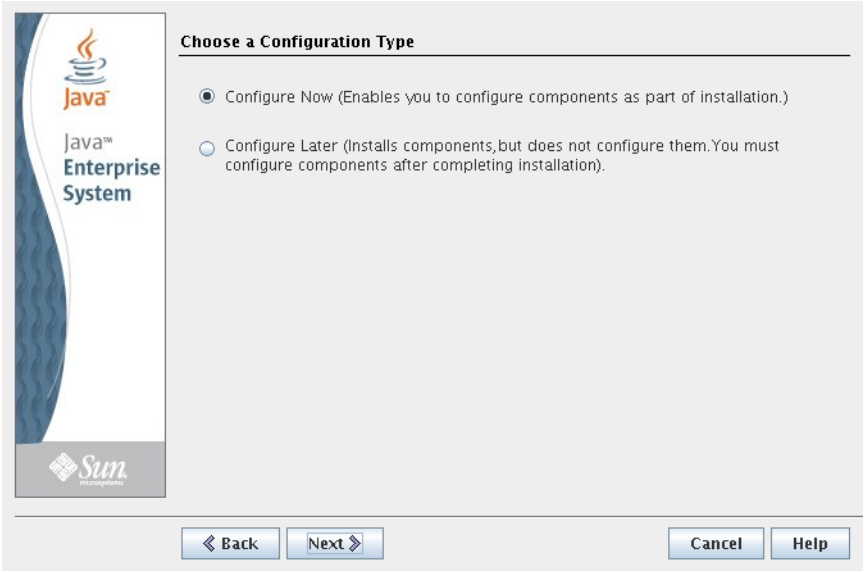
7. In the “Specify Installation Directories” screen, do the following:
   a. Enter the target installation directory for the Directory Preparation Tool.
   b. Enter the target installation directory for Sun Directory Server. (This directory will be referred to as `<dirserv_home>` in the remainder of this chapter.)



8. In the “Verify System Requirements” screen, wait until the status of all items reads “OK,” then click **Next**. If any of the items fail the verification, you must remedy the problem and restart the installation.

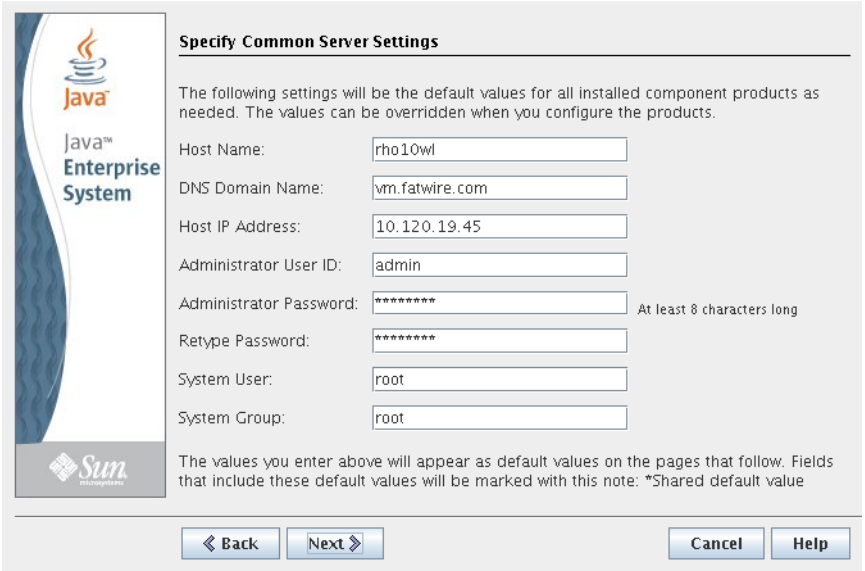


9. In the “Choose a Configuration Type” screen, select **Configure Now** and click **Next**.

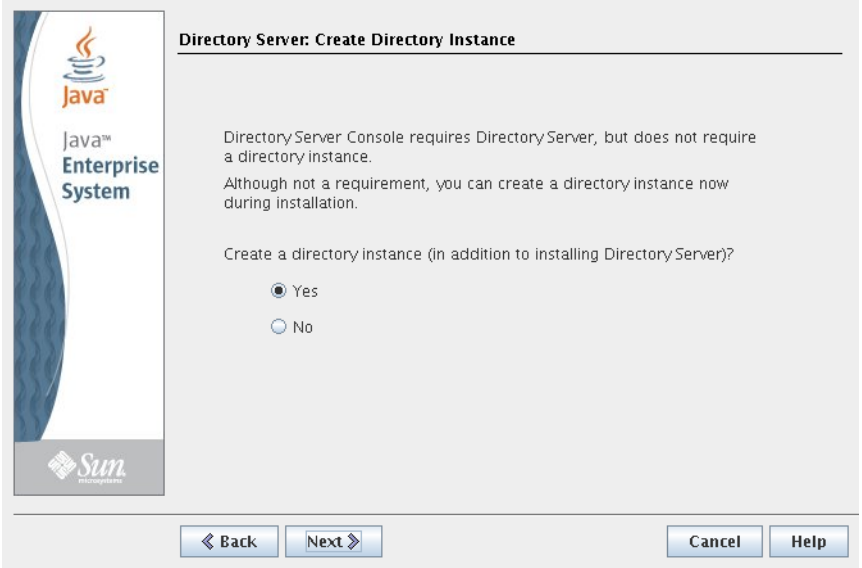


10. In the “Specify Common Server Settings” screen, enter the required information, then click **Next**.

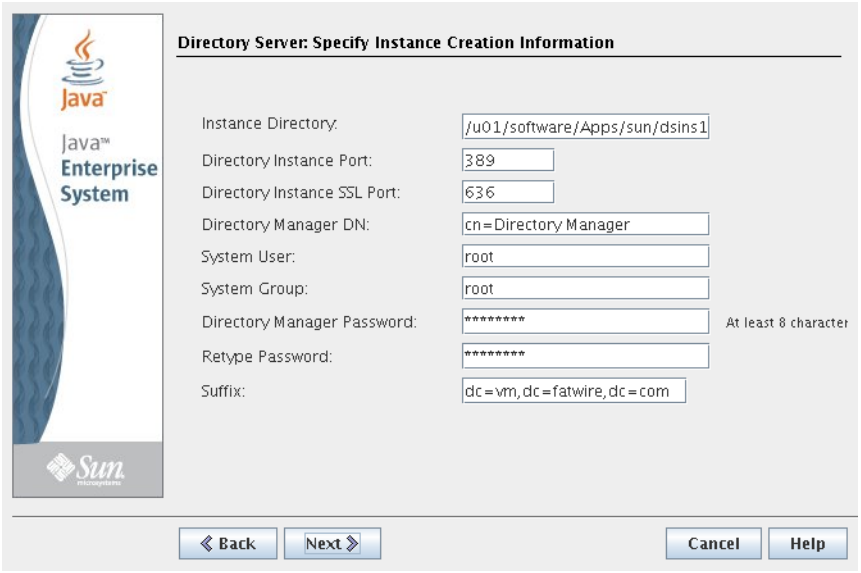
> **Note**
>
> The host name and IP address of the machine running Directory Server must have a valid DNS entry on your network.



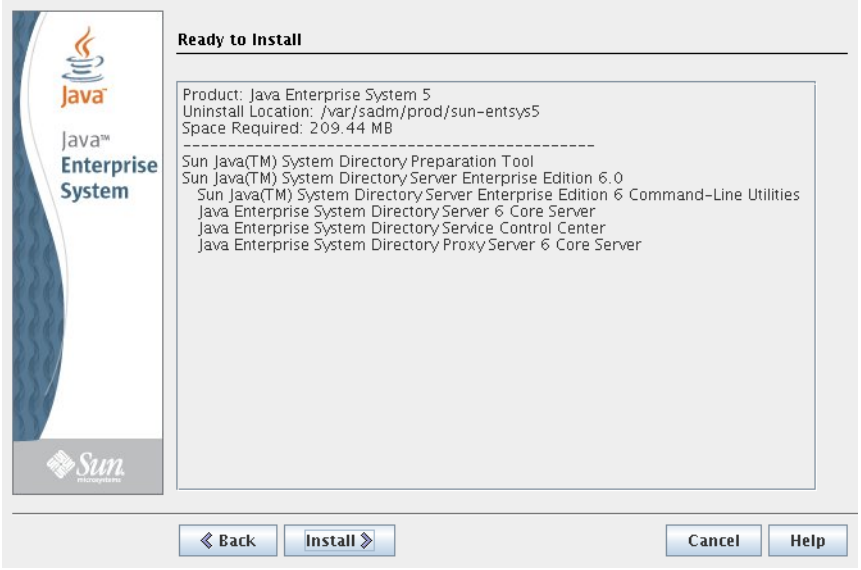
11. In the “Create Directory Instance” screen, select **Yes** and click **Next**.



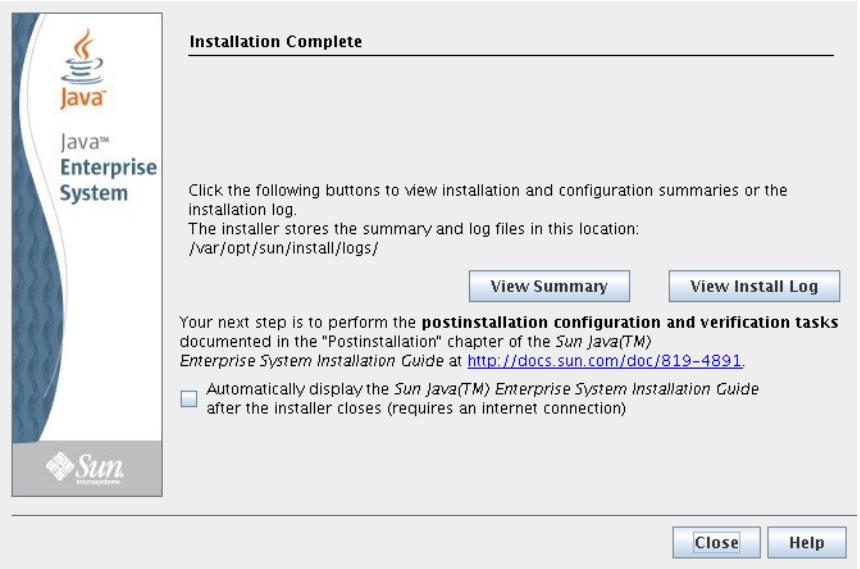
12. In the "Specify Instance Creation Information" screen, do the following:
    a. Specify the directory in which the new Directory Server instance will reside. (This directory will be referred to as `<instance_dir>` in the remainder of this chapter.)
    b. Specify the values for the **System User** and **System Group** fields.
    c. Specify a Directory Manager password.
    d. Specify the value for the **Suffix** field. (This value will be the **DN** value used to connect to this Directory Server instance; you will need it in step 4 on page 163.)
    e. Click **Next**.



13. In the "Ready to Install" screen, click **Install** and wait for the installation to complete.



14. In the “Installation Complete” screen, click **Close**.



15. Continue to the next section, “Post-Installation Steps,” to complete the installation.

Post-Installation Steps

Complete your Directory Server installation by performing the steps in this section. You must perform these steps **before** you run the Content Server LDAP integration program.

1. Start your new Directory Server instance:

   `/opt/sun/ds6/bin/dsadm start <instance_dir>`

2. Create an LDIF file named `csldap.ldif` with the following contents:

```
dn: dc=vm,dc=fatwire,dc=com
objectClass: dcObject
objectClass: organization
dc: vm
description: Directory Server ldif file
o: Fatwire Software

dn: ou=People,dc=vm,dc=fatwire,dc=com
objectClass: organizationalUnit
objectClass: top
ou: People

dn: ou=Groups,dc=vm,dc=fatwire,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Groups
```

3. Change to the `<dirserv_home>/ds6/bin` directory.

4. Import the LDIF file you created in step 2 on page 162 using the following command:

   `./dsconf import <ldif_file> <dn>`

   where:

   - `<ldif_file>` is the full path to the `csldap.ldif` file you created in step 2 on page 162, including the filename, and
   - `<dn>` is the value you entered in the **Suffix** field in step 12 on page 161.

   For example:

   `./dsconf import /u01/csldap.ldif dc=vm,dc=fatwire,dc=com`

   When you run the command, accept the certificate by answering **Yes** at the first prompt. At the second prompt, enter the Directory Manager password (you created this password in step 12 on page 161.)

Completing and Verifying the LDAP Configuration

This section shows you how to complete and verify your LDAP configuration using the Directory Service Control Center (used to manage Sun Directory Server.)

1. Start the Sun Java Web Console:

   `/opt/sun/webconsole/bin/smcwebserver start`

2. Initialize the Directory Service Control Center:

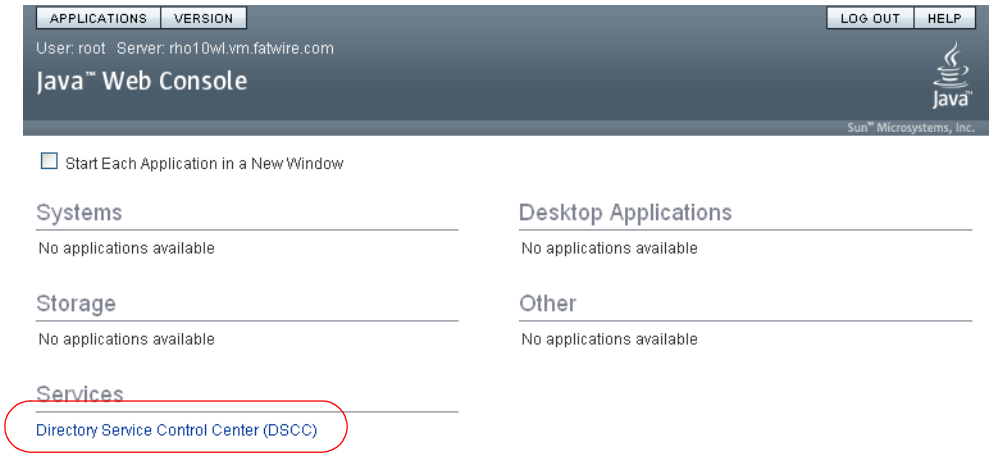
   a. Change to the `<dirserv_home>/dscc6/bin` directory.

   b. Execute the following command: **`./dsccsetup initialize`**

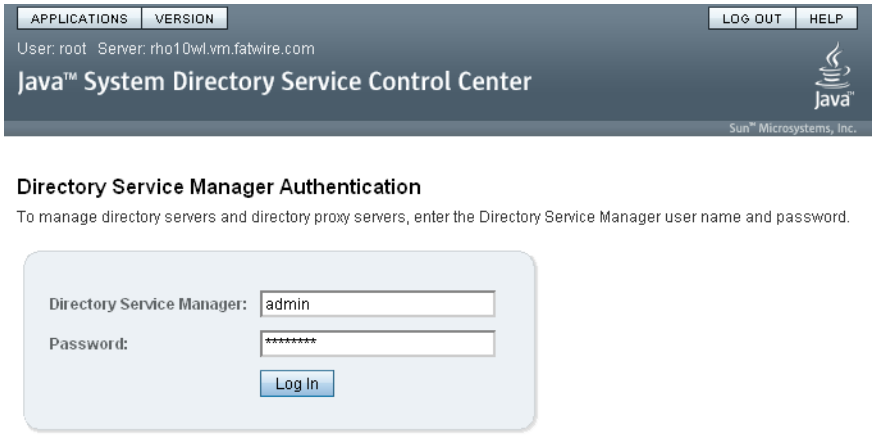
3. Log in to the Sun Java Web Console as the system user you used to install Sun Directory Server, via the following URL:

   `https://<server>:6789/`

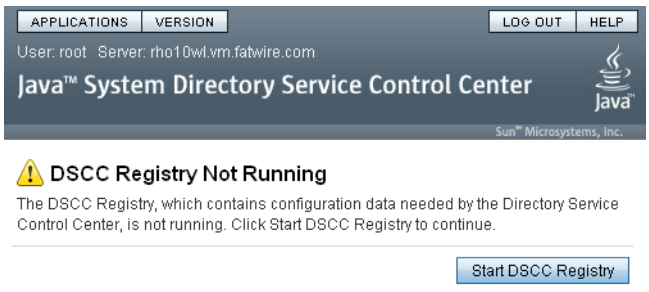
4. In the “Services” section, click **Directory Service Control Center (DSCC)**.



5. In the “Directory Service Manager Authentication” screen, log in as the `admin` user, using the Directory Manager password. (You created this password in step 12 on page 161.)



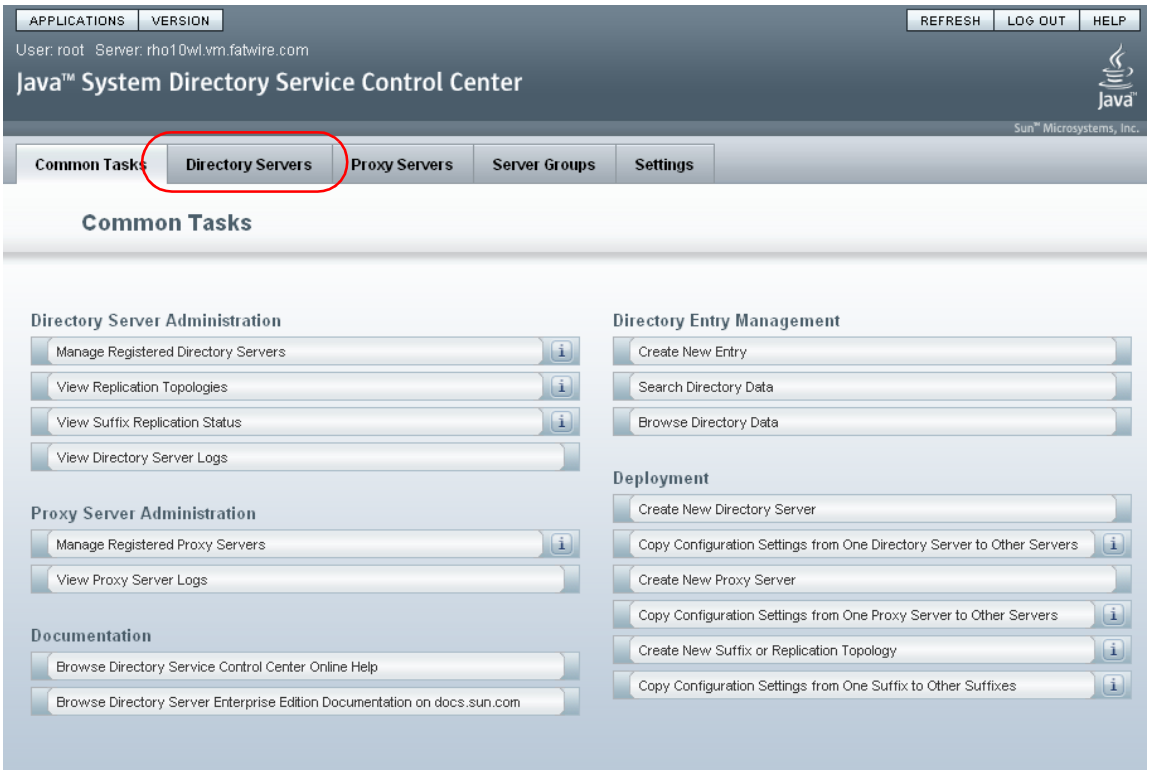
6. If you see a pop-up error message informing you that the DSCC registry is not running, click **Start DSCC Registry**.



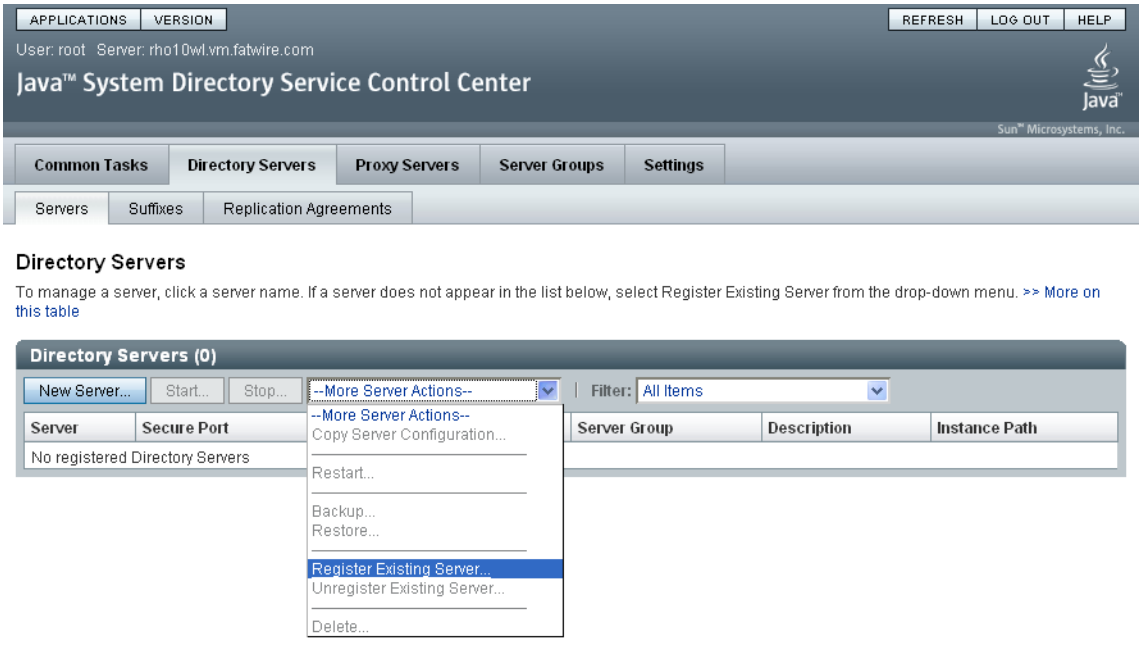
When the DSCC registry has started successfully, a confirmation message appears.

Click **Close** to close the pop-up window.

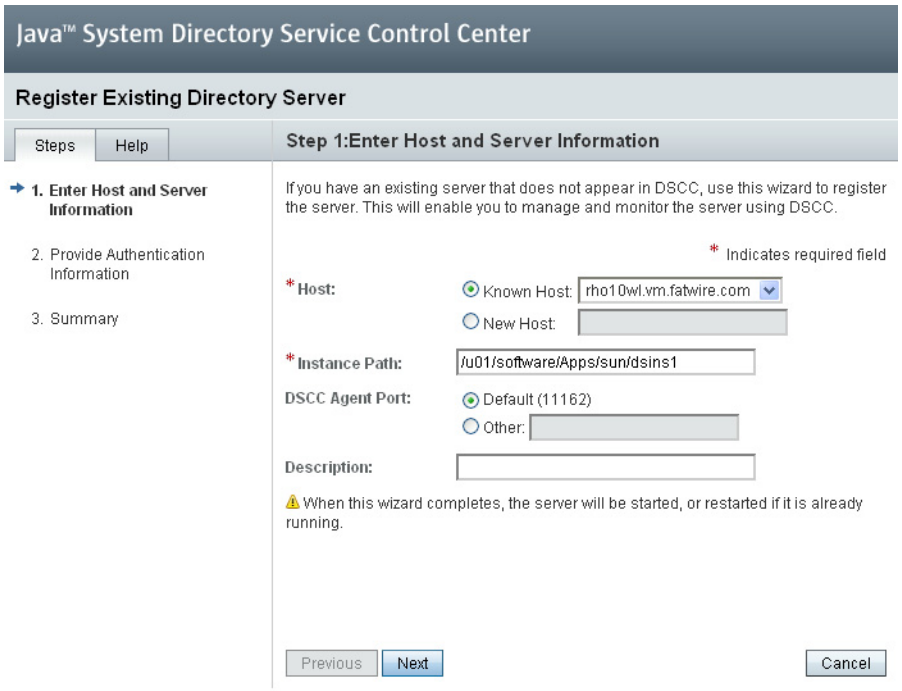
7. In the console, click the **Directory Servers** tab.



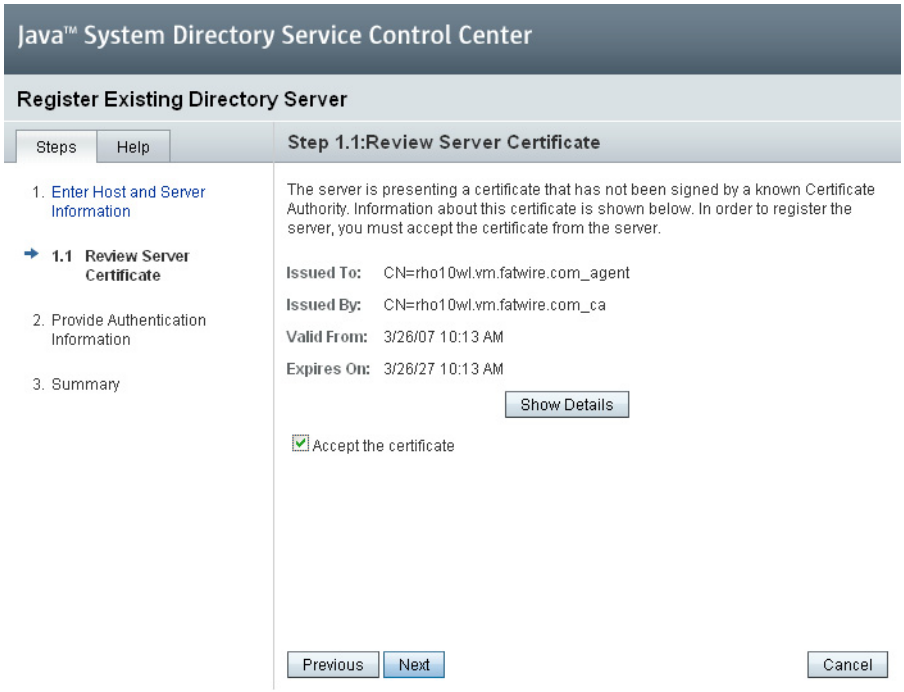
8. In the "More Server Actions" drop-down list, select **Register Existing Server**.



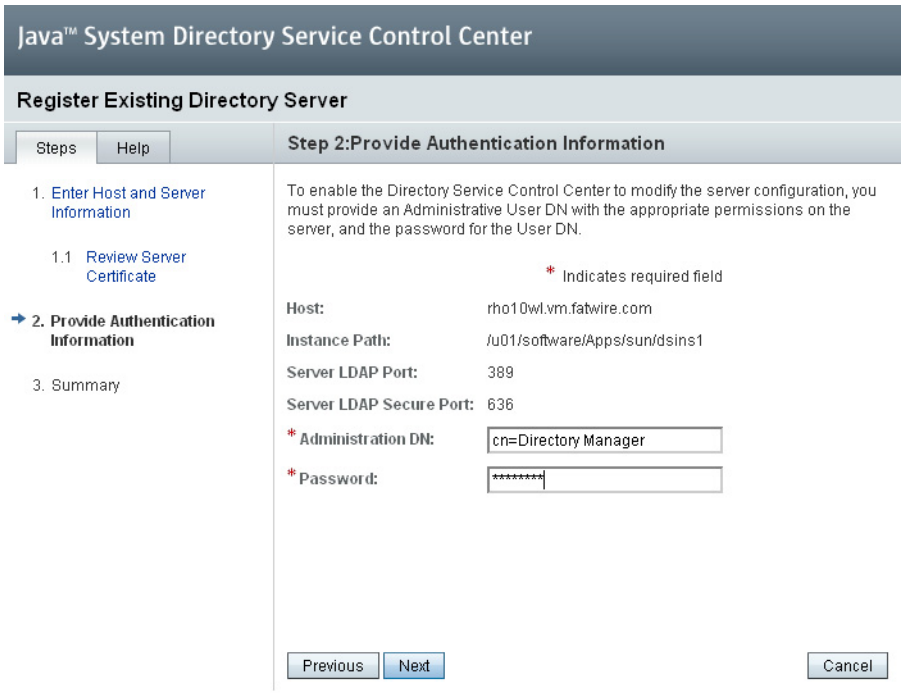
9. In the pop-up window that appears, enter the full path to the directory holding the target Directory Server instance (`<instance_dir>`) and click **Next**.



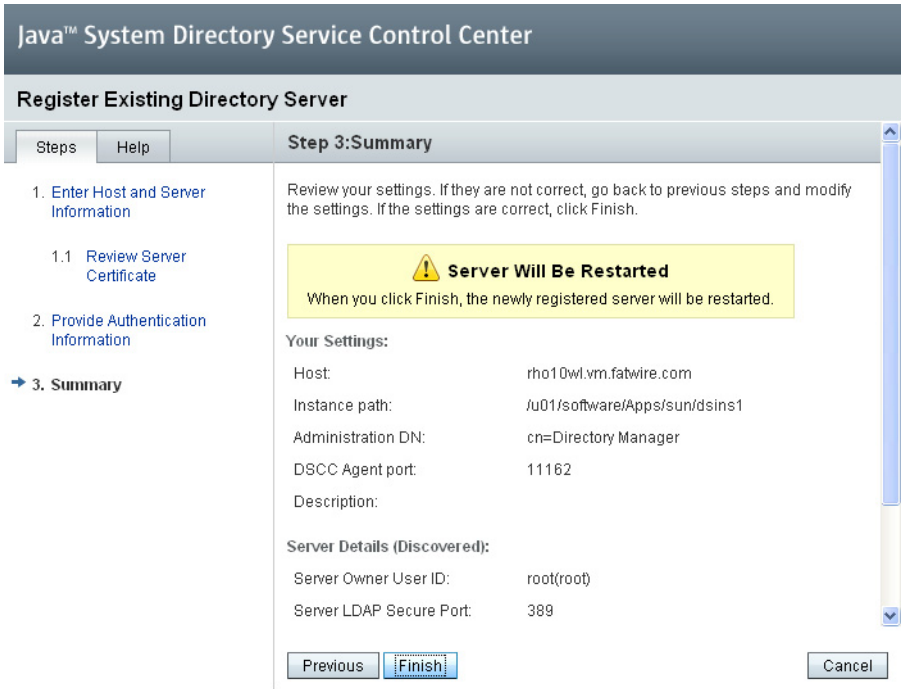
10. In the "Review Server Certificate" screen, select the **Accept the Certificate** check box and click **Next**.



11. In the “Provide Authentication Information” screen, enter the Directory Manager password into the **Password** field and click **Next**.

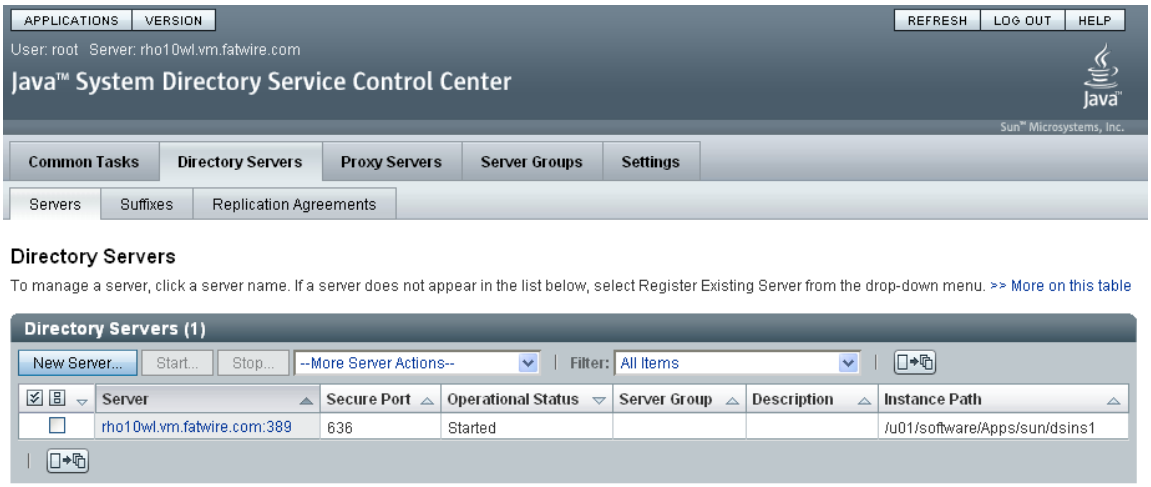


12. In the “Summary” screen, click **Finish** and wait for the instance to restart.

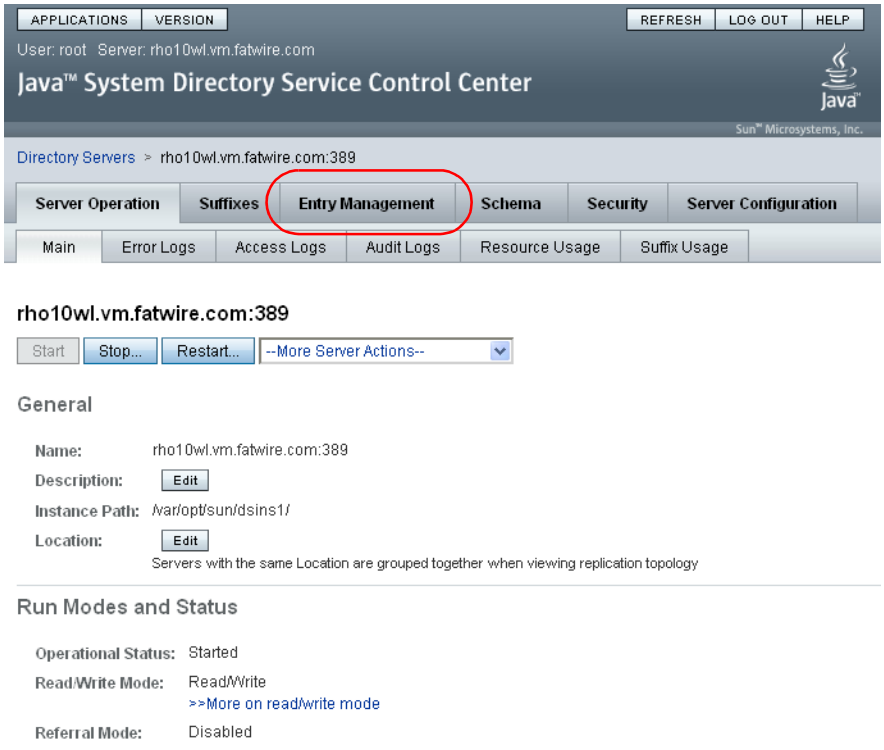


When the instance has restarted successfully, a confirmation message appears. Click **Close** to close the pop-up window.

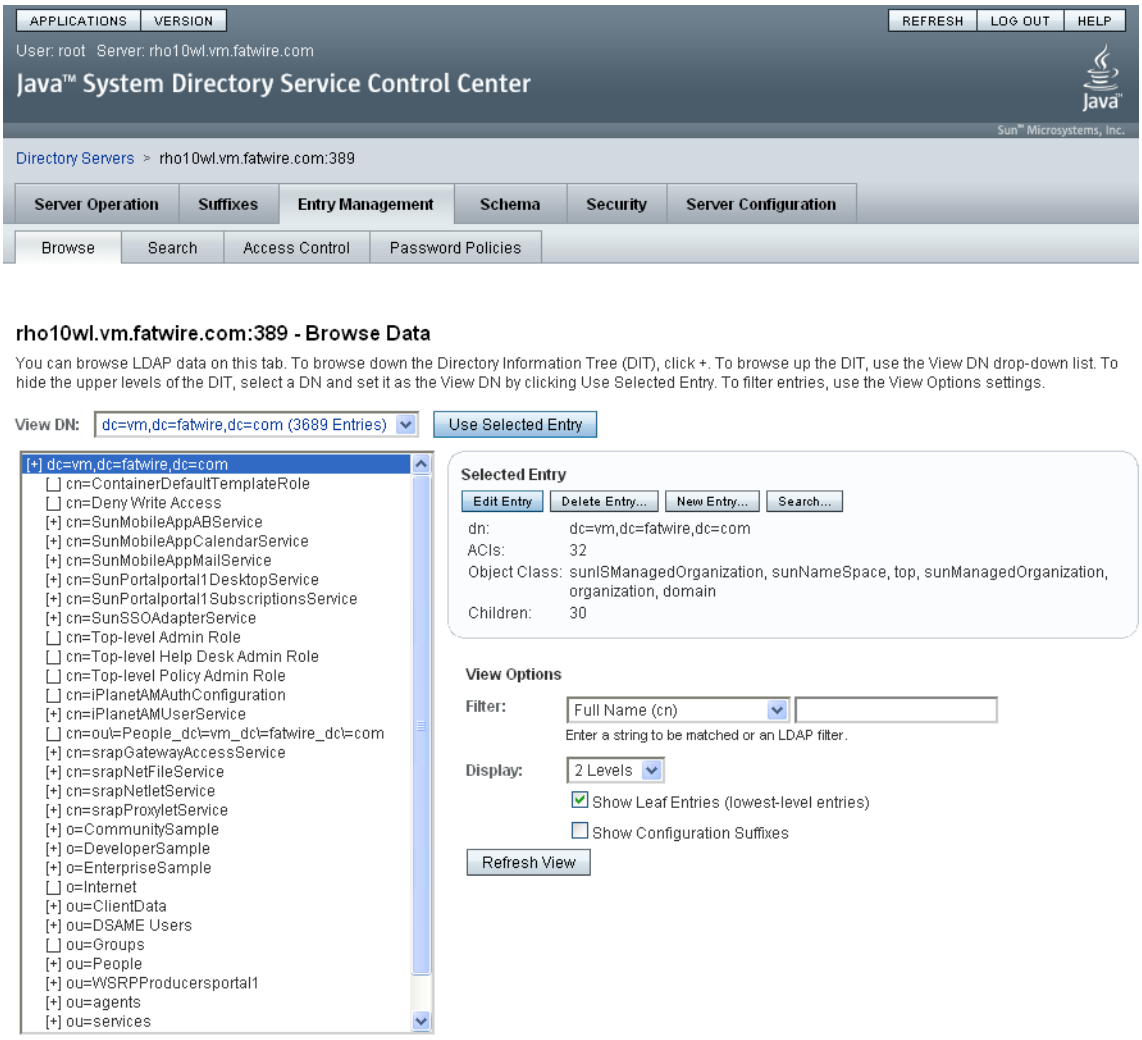
13. In the list of directory servers, click the Directory Server instance you just registered.



14. In the instance summary screen, click the **Entry Management** tab.



15. Examine the displayed LDAP directory data to make sure it is valid.



Modifying User Passwords

This section shows you how to modify user passwords in Sun Directory Server.

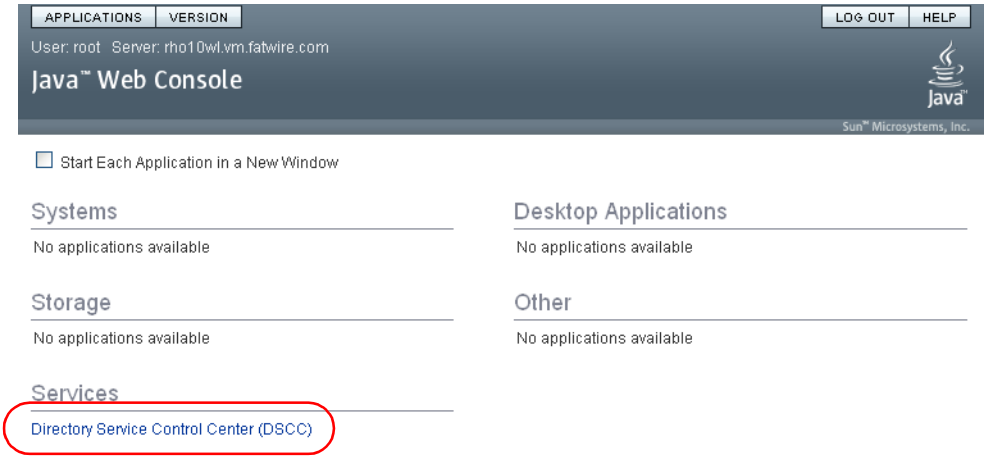
1. Start the Sun Java Web Console:

   `/opt/sun/webconsole/bin/smcwebserver start`

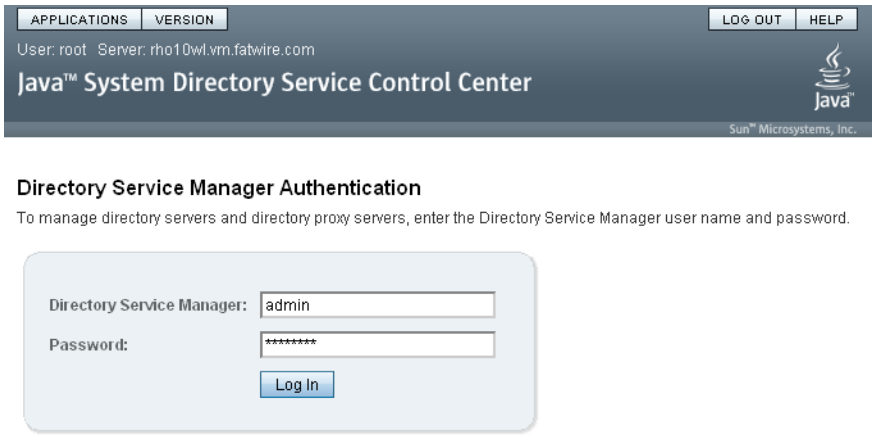
2. Log in to the Sun Java Web Console as the system user you used to install Sun Directory Server, via the following URL:

   `https://<server>:6789/`

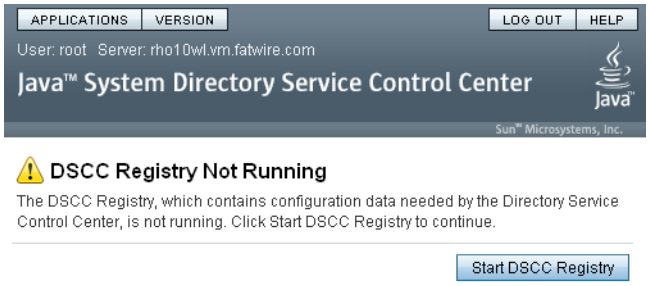
3. In the "Services" section, click **Directory Service Control Center (DSCC)**.



4. In the "Directory Service Manager Authentication" screen, log in as the `admin` user, using the Directory Manager password. (You created this password in step 12 on page 161.)



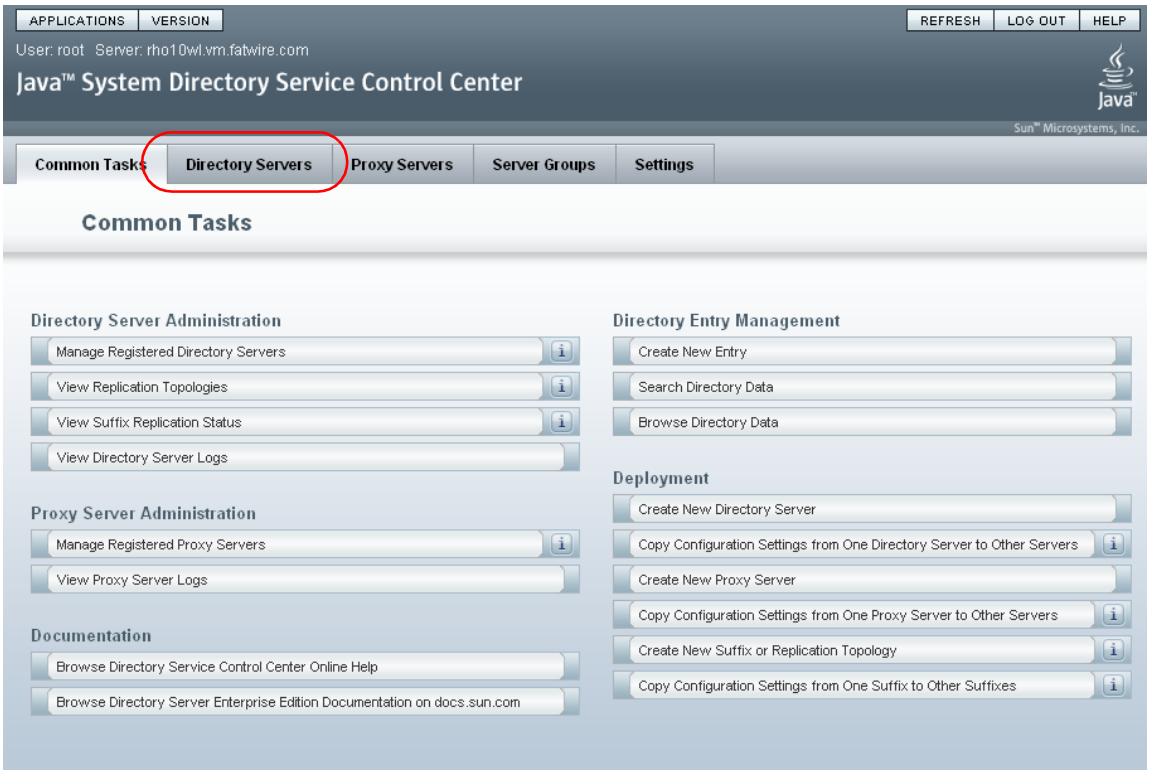
5. If you see a pop-up error message informing you that the DSCC Registry is not running, click **Start DSCC Registry**.



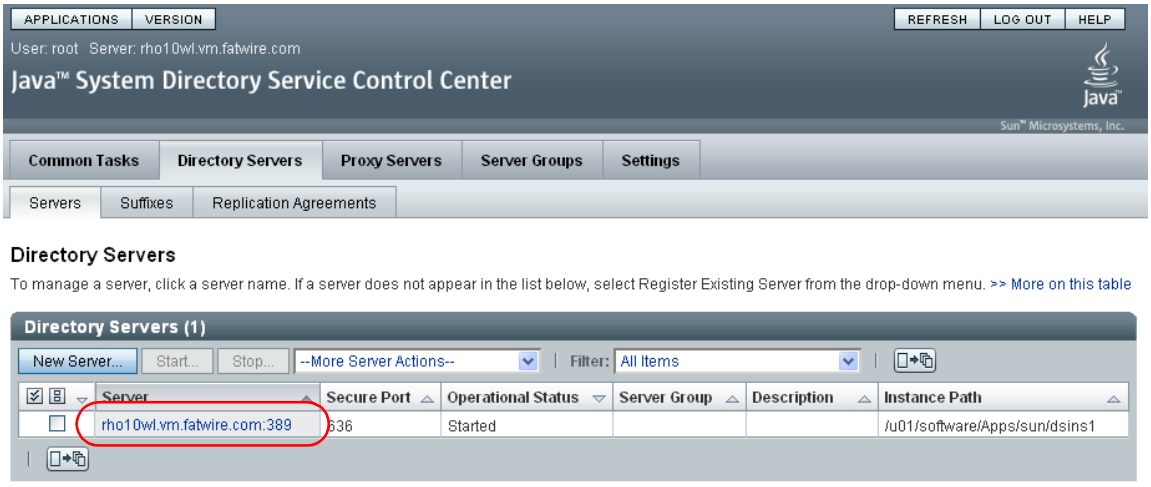
When the DSCC Registry has started successfully, a confirmation message appears.

Click **Close** to close the pop-up window.

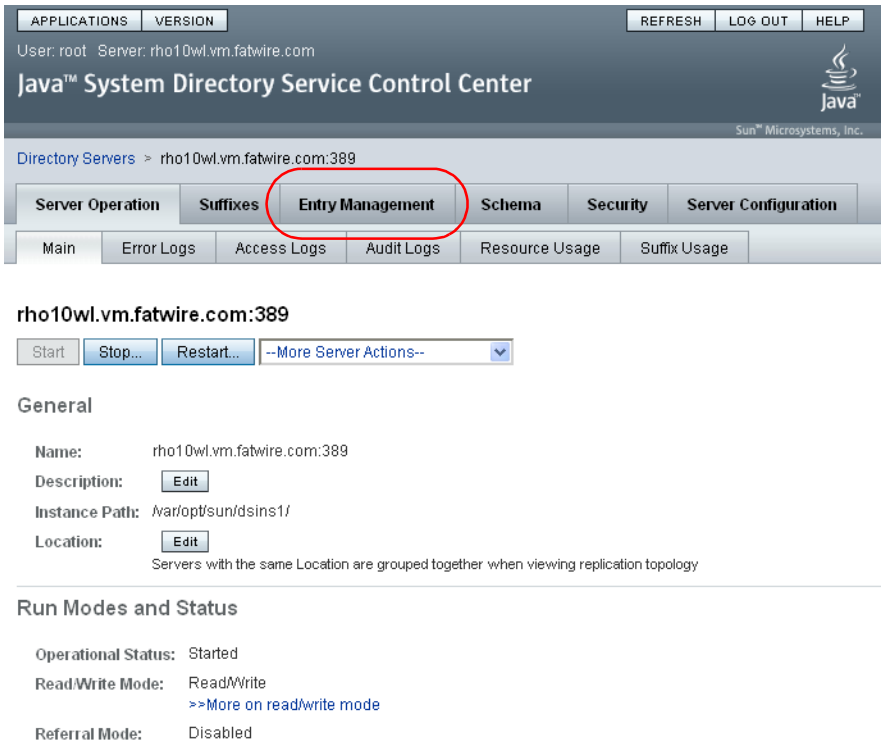
6. In the console, click the **Directory Servers** tab.



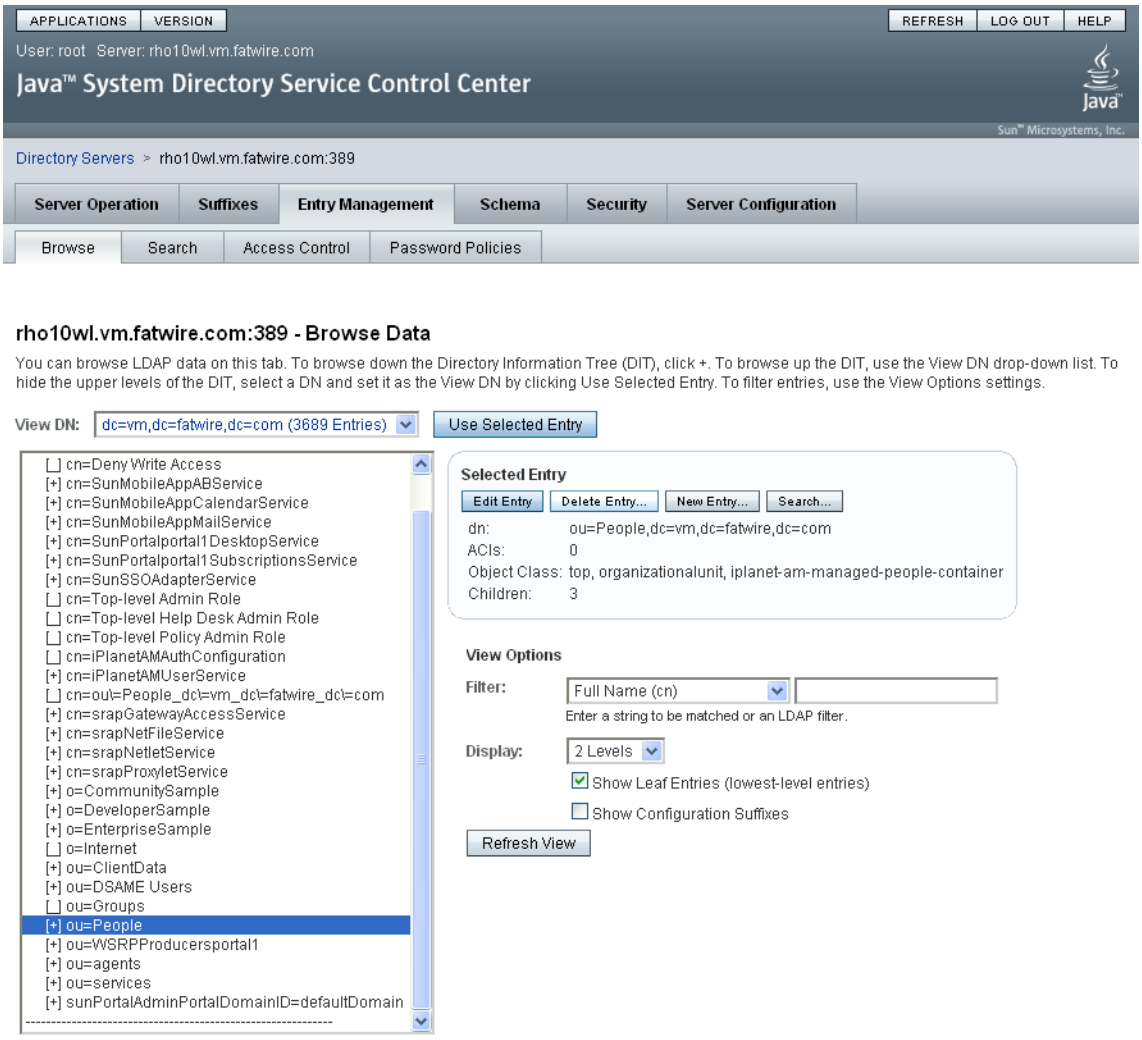
7. In the list of directory servers, click the desired Directory Server instance.



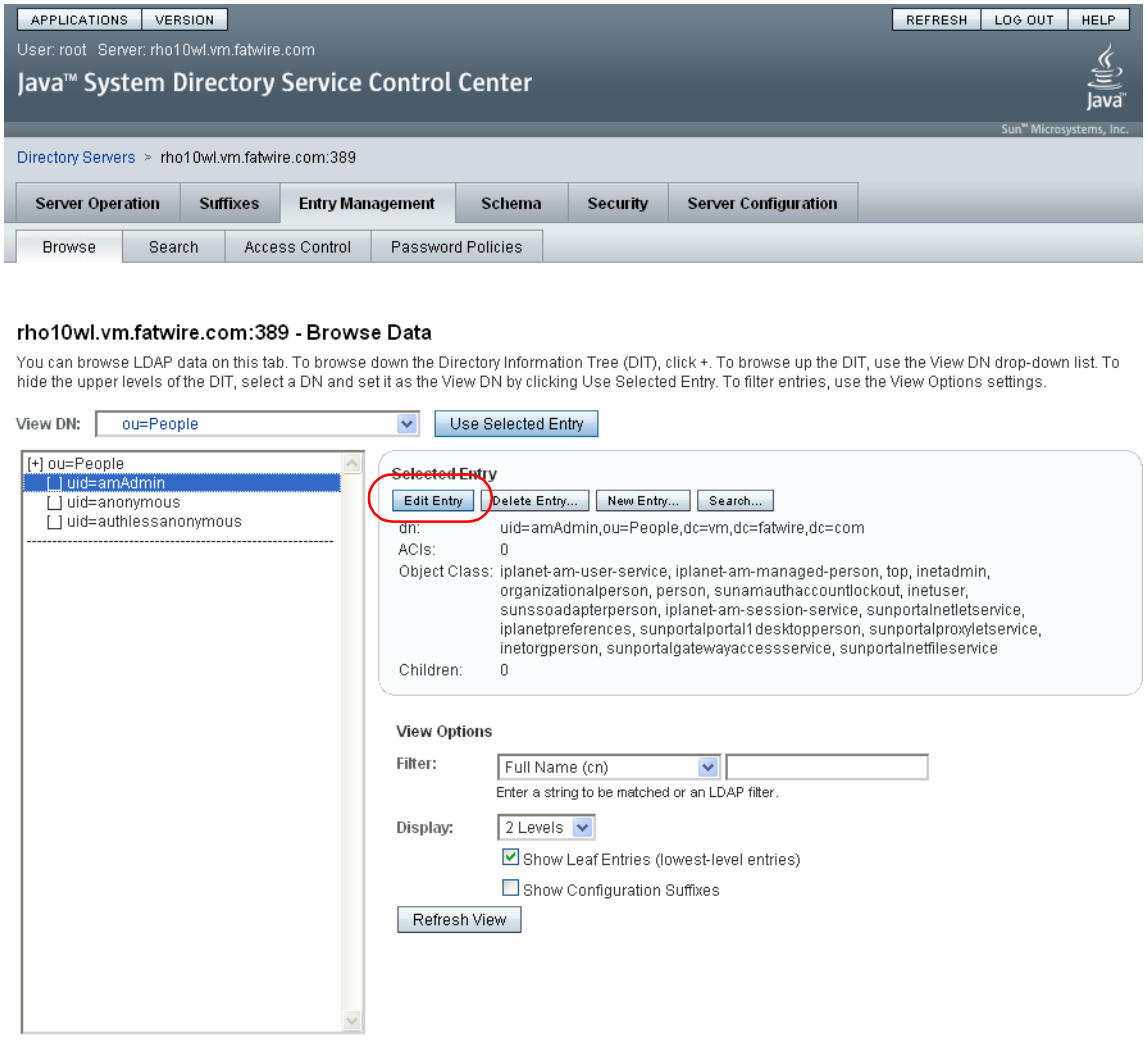
8. In the instance summary screen, click the **Entry Management** tab.



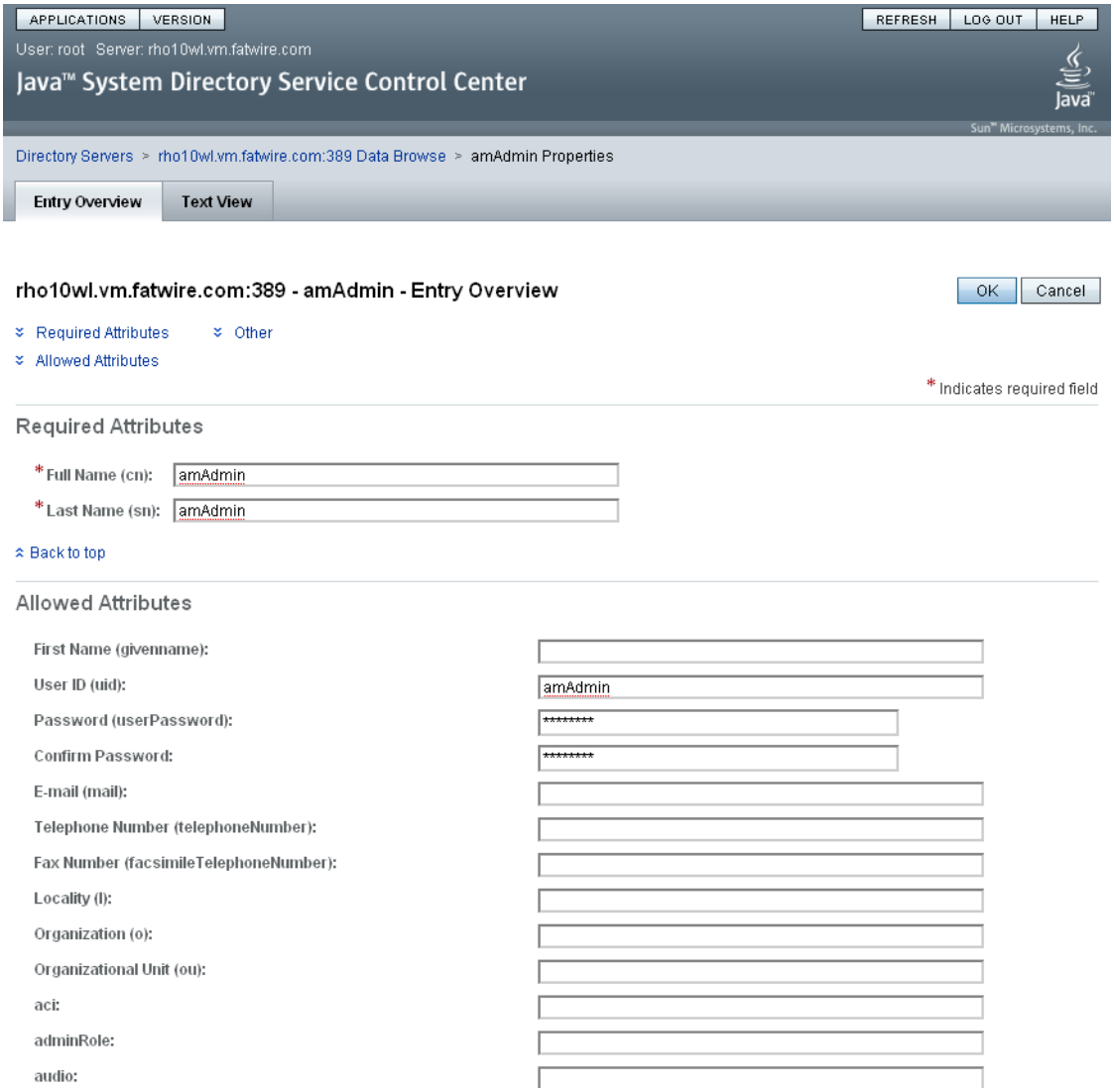
9. In the list of directory entries, navigate to and double-click the **ou=People** node.



10. Under the **ou=People** node, select the user whose password you want to modify. then click **Edit Entry** in the “Selected Entry” area.



11. Enter the new password into the **Password** and **Confirm Password** fields, then click **OK**.



12. Repeat steps 10 an 11 for each additional user whose password you want to modify.

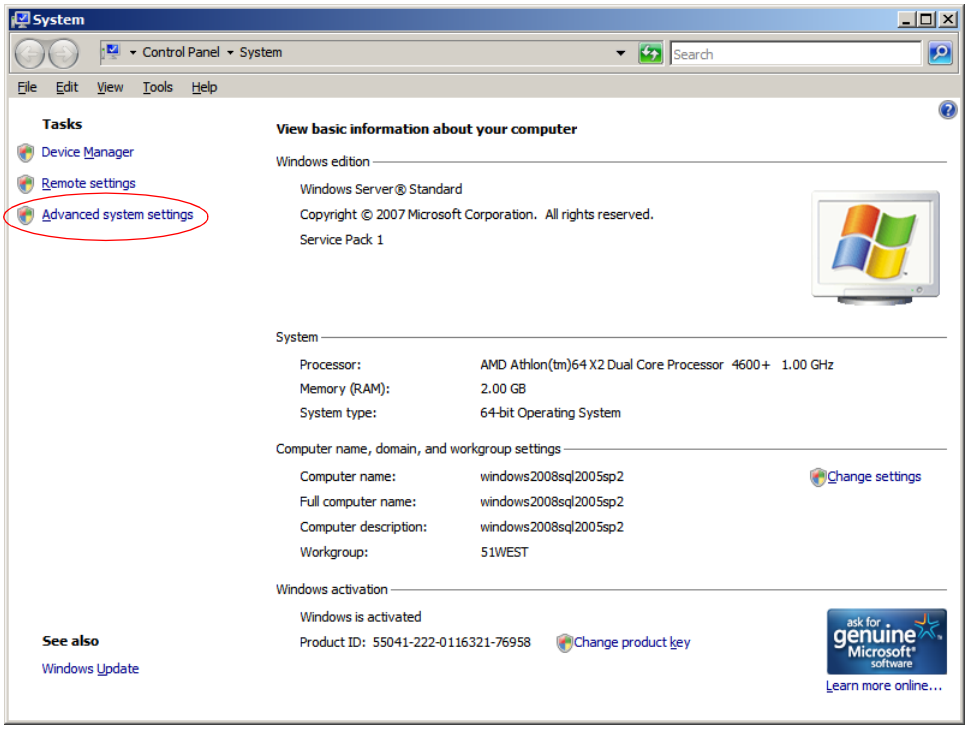
Chapter 13

Installing Active Directory Server 2008

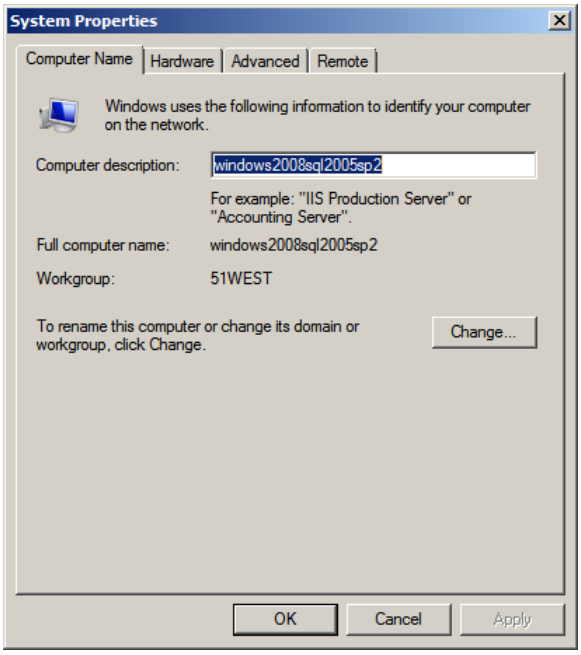
This chapter includes the following sections:

Installation Steps

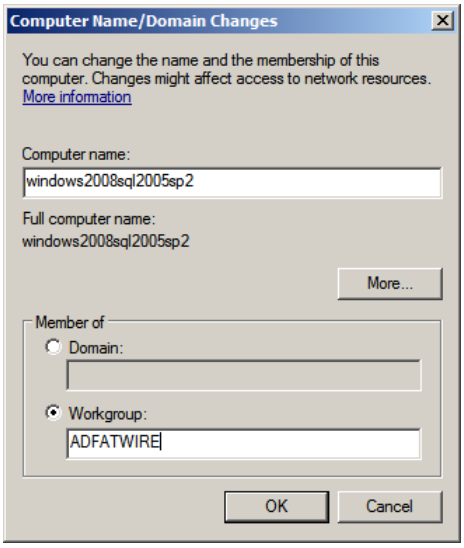
1. Install the Operating System:
   a. Install Windows Server 2008 (any Windows server except Web).
   b. When the installation is complete, leave the installation disc in the drive, you will need it to complete the installation of ADS.
   c. Set the Computer's **Name** and **Suffix**.
2. Open the "System Properties" dialog box.
   a. Click **Start**, then right-click the computer icon.
3. In the "System" window select **Advanced system settings**.



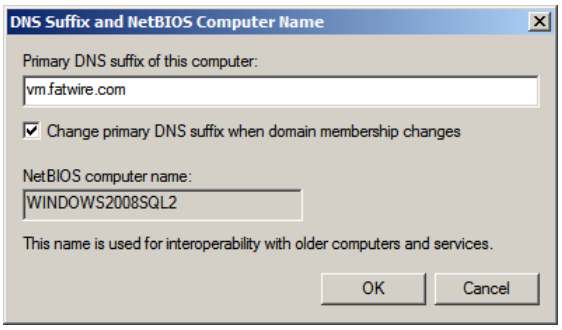
4. Select the **Computer Name** tab.
   a. Click **Change**.



5. In the pop-up window that appears, fill in the following fields:
   - **Computer name**: Enter the name you wish to designated for your computer. (Make a record of this name).
   - **Member of**: Select the **Workgroup** radio button, then enter a unique workgroup name. (Make a record of this name).



a. Click **More...**

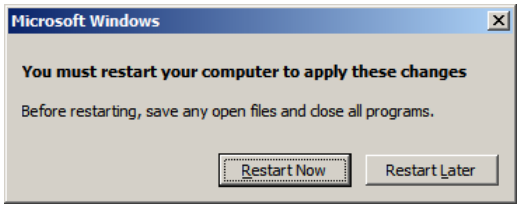


b. In the "DNS Suffix and NetBIOS Computer Name" dialog box fill in the fields:

- **Primary DNS suffix of this computer**: Enter the DNS suffix of your computer (Make a record of this suffix).
- **Change Primary DNS Suffix when domain membership changes**: If checkbox is selected, deselect it.

c. Click **OK** to close the dialog box.

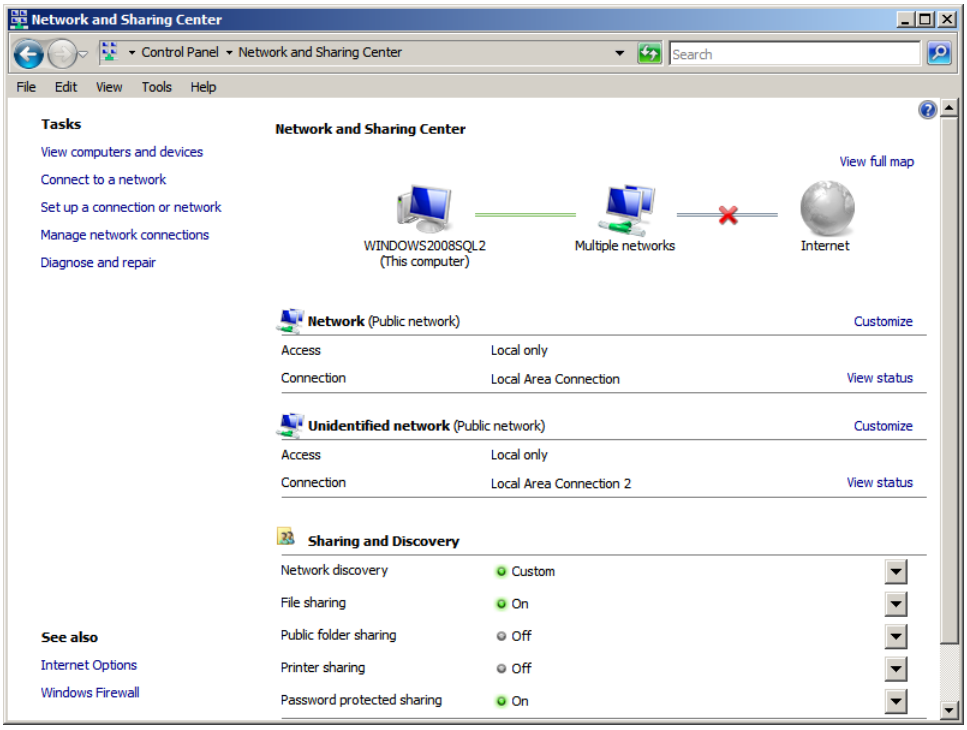
6. In the "Computer Name/Domain Changes" dialog box, click **OK**.
7. In the "System Properties" window click **Close**.
8. In the reboot dialog box click **Restart Later**.



Configuring the Network Settings

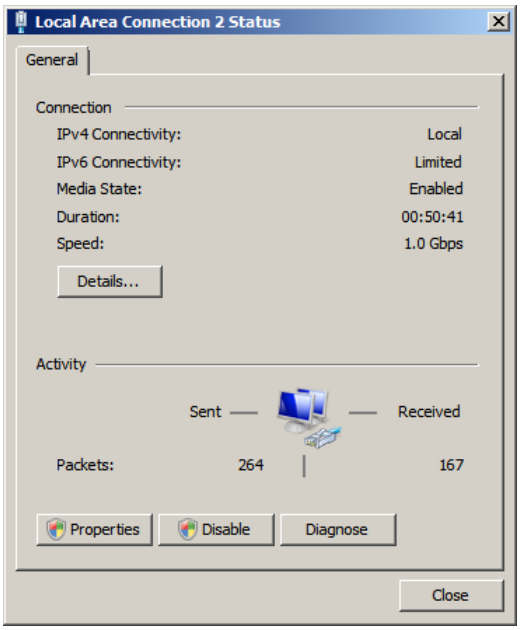
To configure the network settings:

1. Open "Network Properties."
   a. Select **Start > Control Panel**.
   b. Click the **Network and Sharing Center** icon.
   c. Select the Network Connection to edit (if you have more than one `see ipconfig` result, make sure to select the correct one).

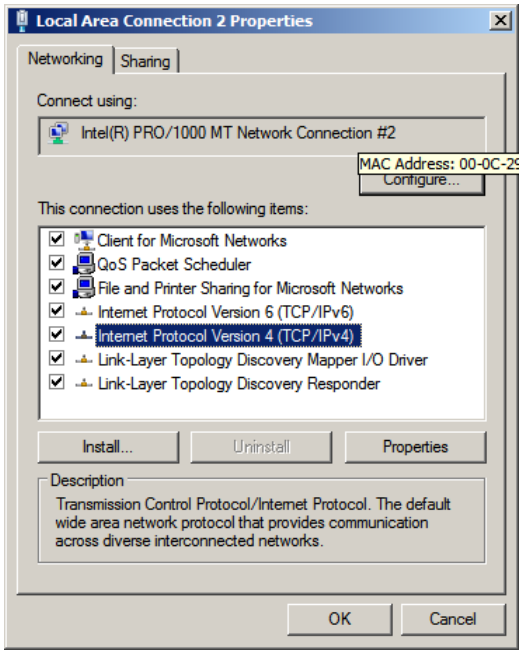


2. Select **View Status**, located next to the network connection you have selected.

3. Click **Properties**.

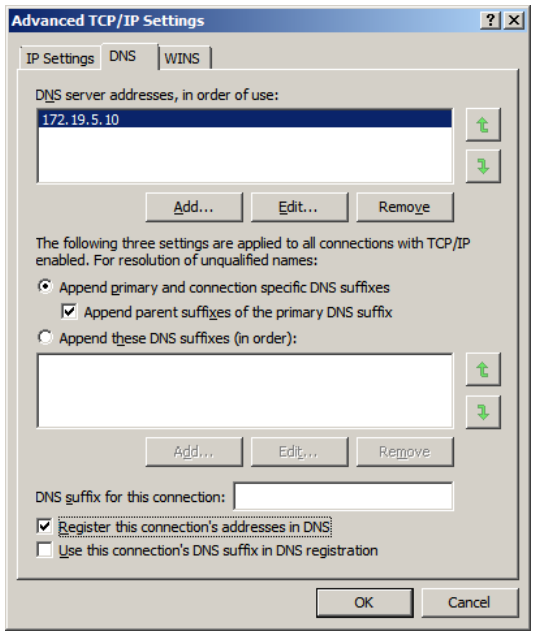


4. Select **Internet Protocol Version 4 (TCP/Iv4)**.



   a. Set the IP address to an unused, static IP address.
   b. Set the preferred DNS server to your computer's IP address.

c. Click **Advanced**:



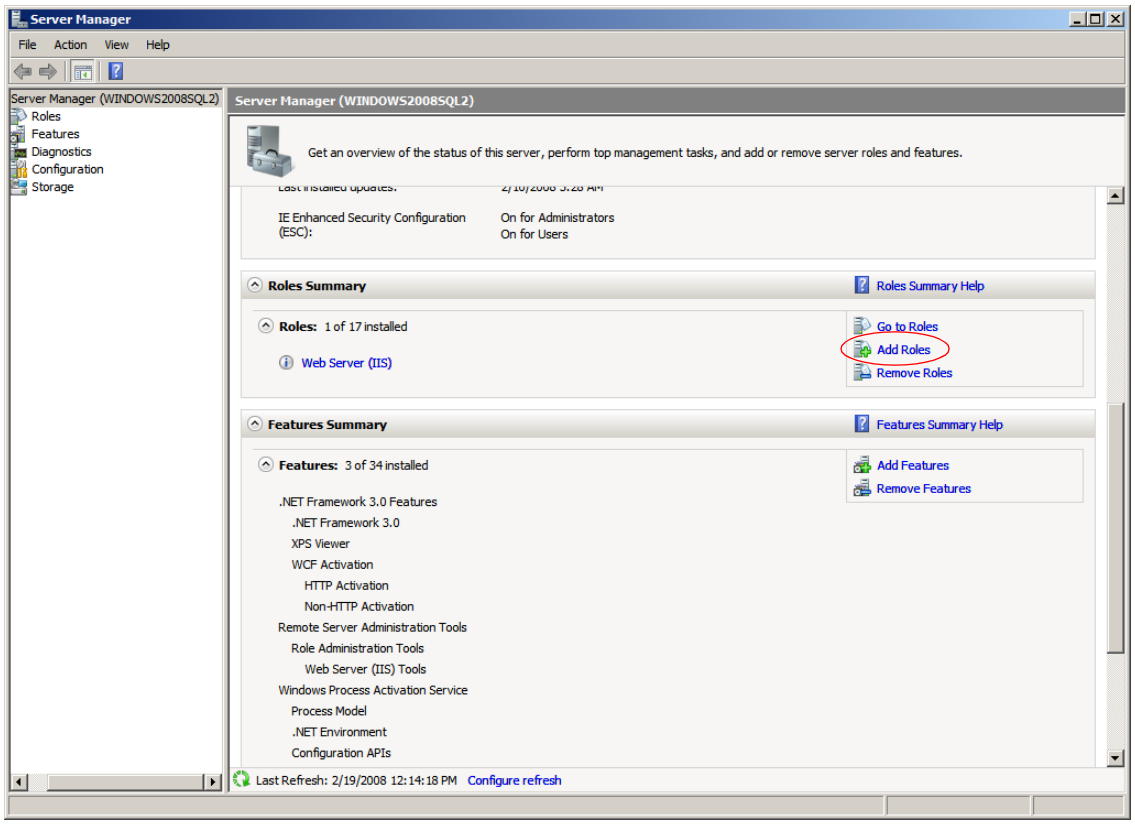
- Select the check box **Append primary and connection-specific DNS suffixes**.
- Select the check box **Append parent suffixes of the primary DNS suffix**.

5. Click on until you have exited the properties pane, then click **Close**.

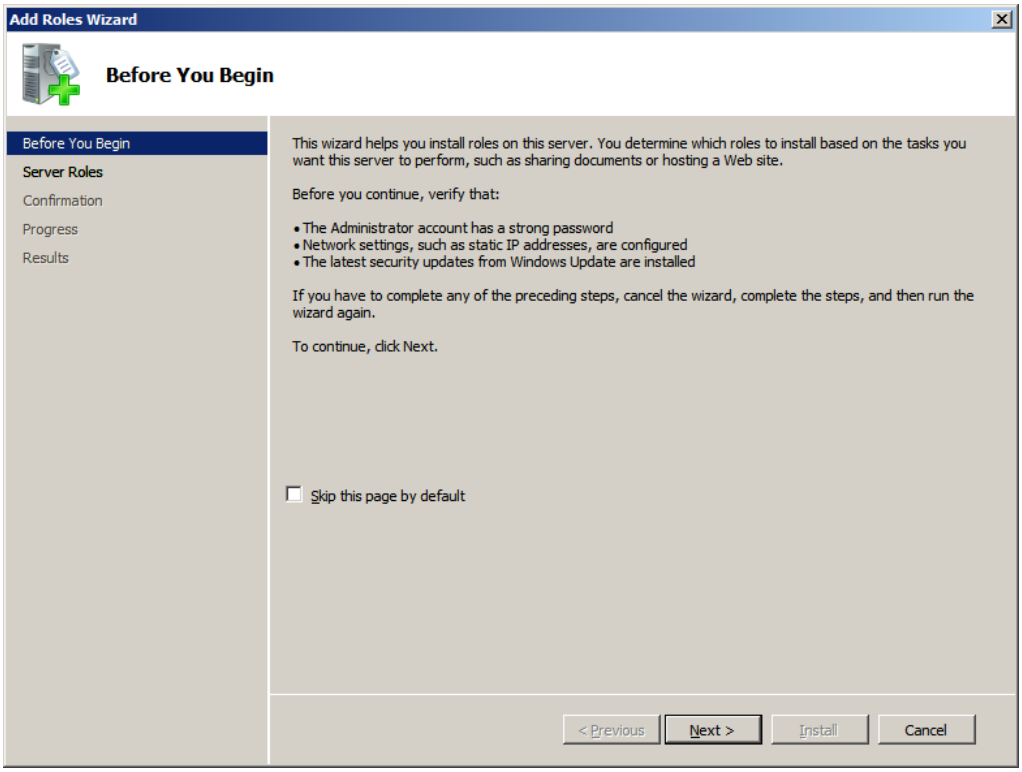
6. Restart the computer.

Installing Active Directory 2008 Services

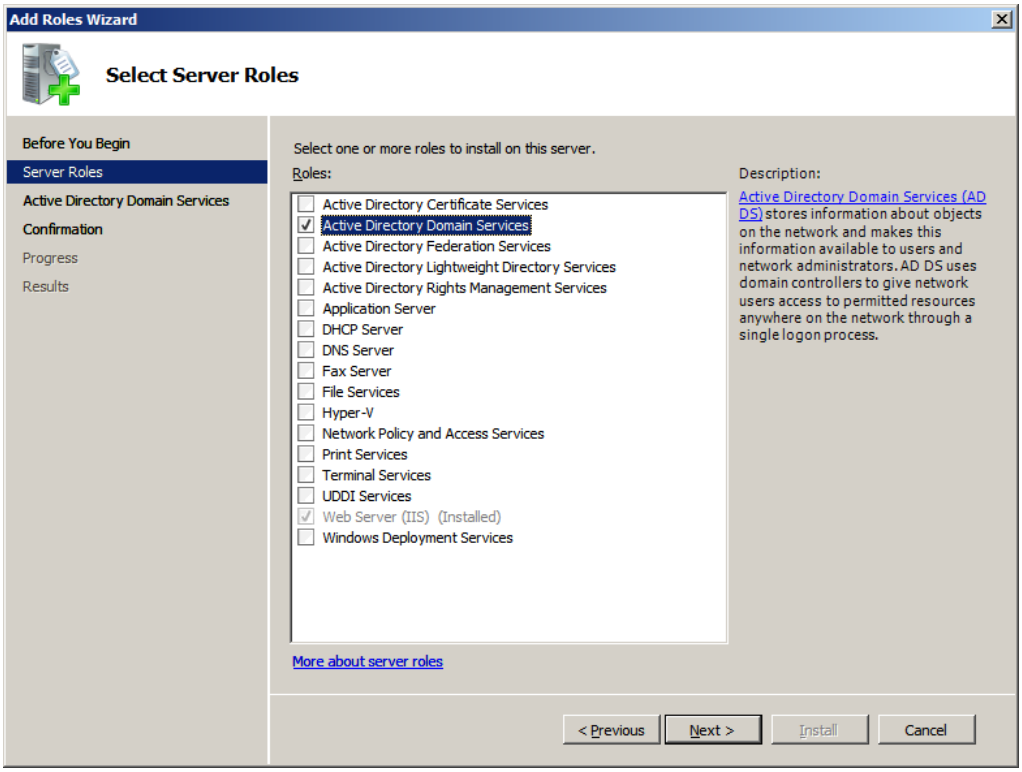
1. Select **Start** > **Server Manger**.
2. In the "Roles" section click **Add Roles**.



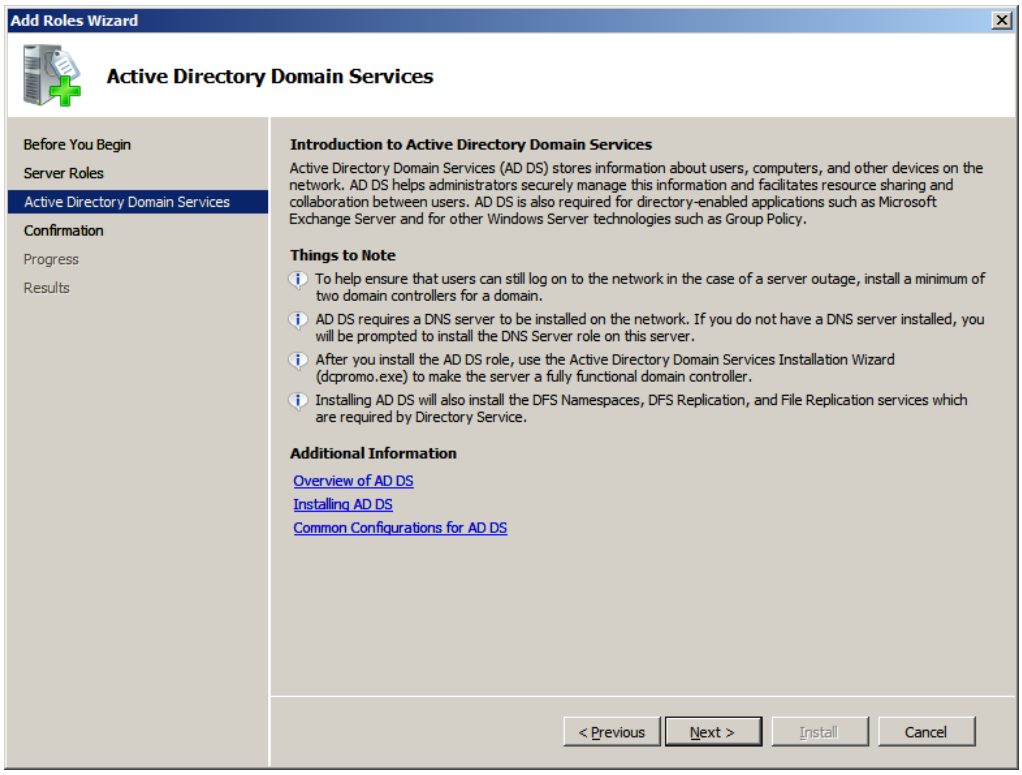
3. In the "Add Roles Wizard" click **Next**.



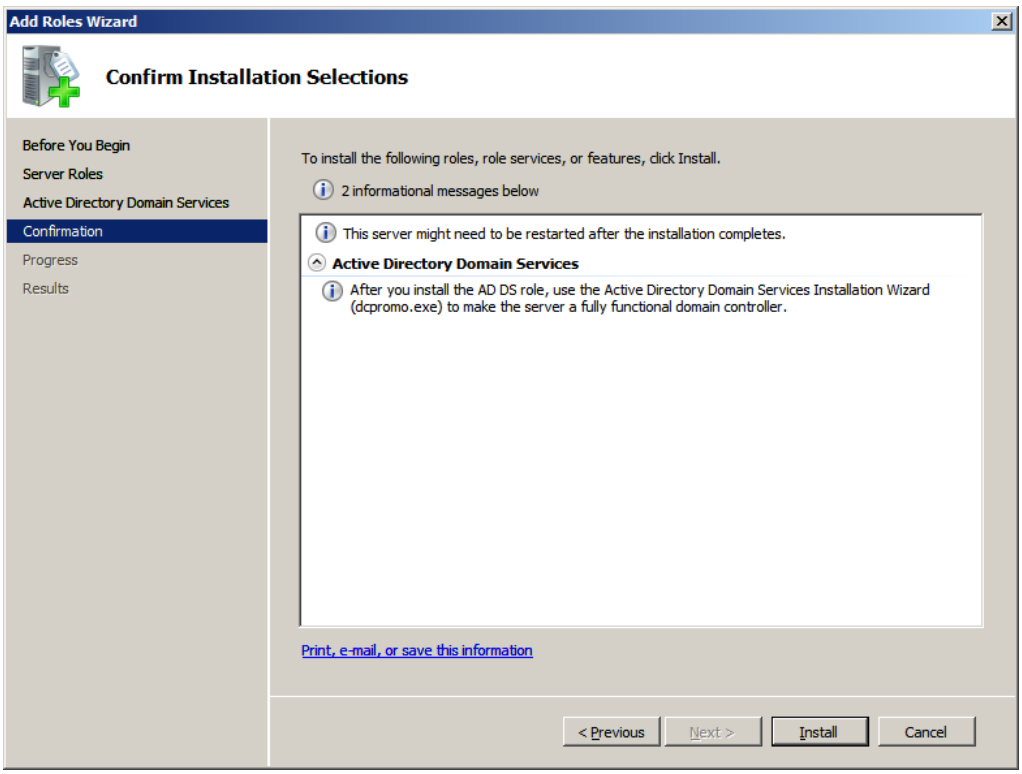
4. Select **Active Directory Domain Services** and click **Next**.



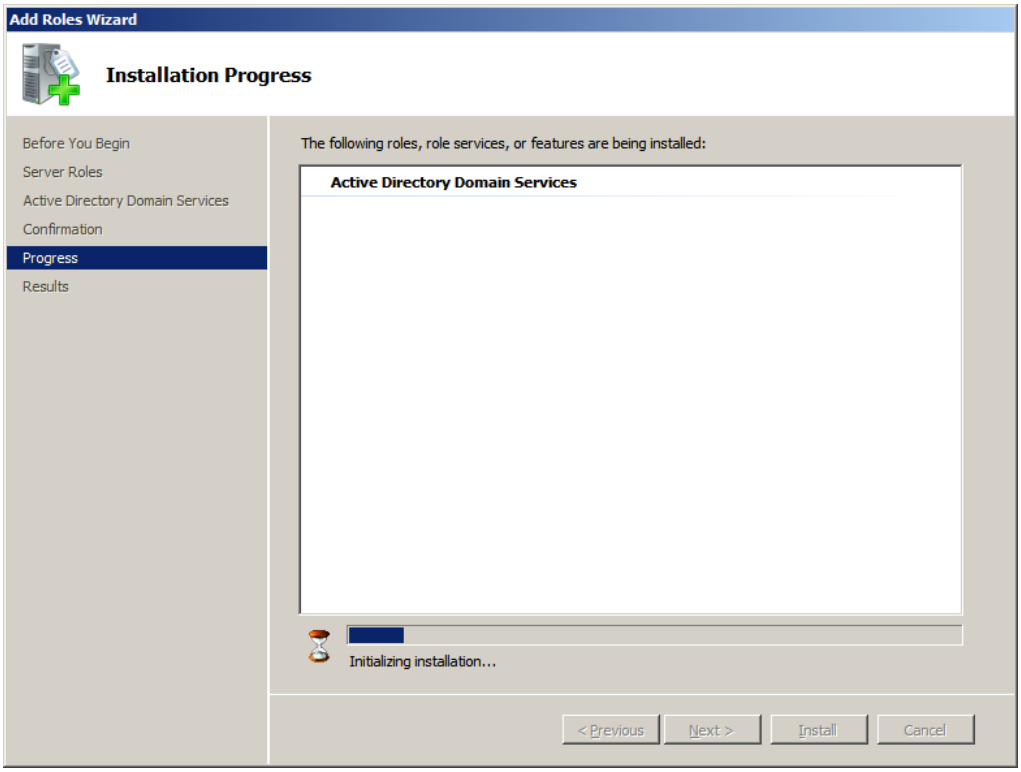
5. Review the list of additional services to be installed along with Active Directory and click **Next**.



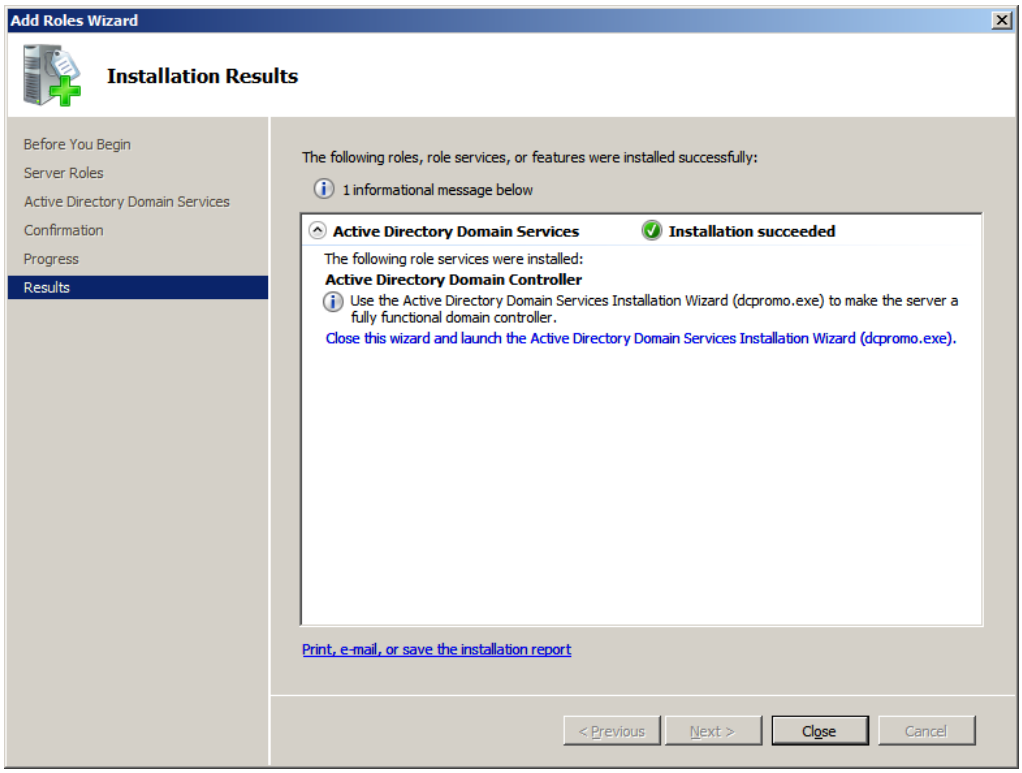
6. Click **Install** to begin installation of "Active Directory 2008."



7. Allow the installation to complete.



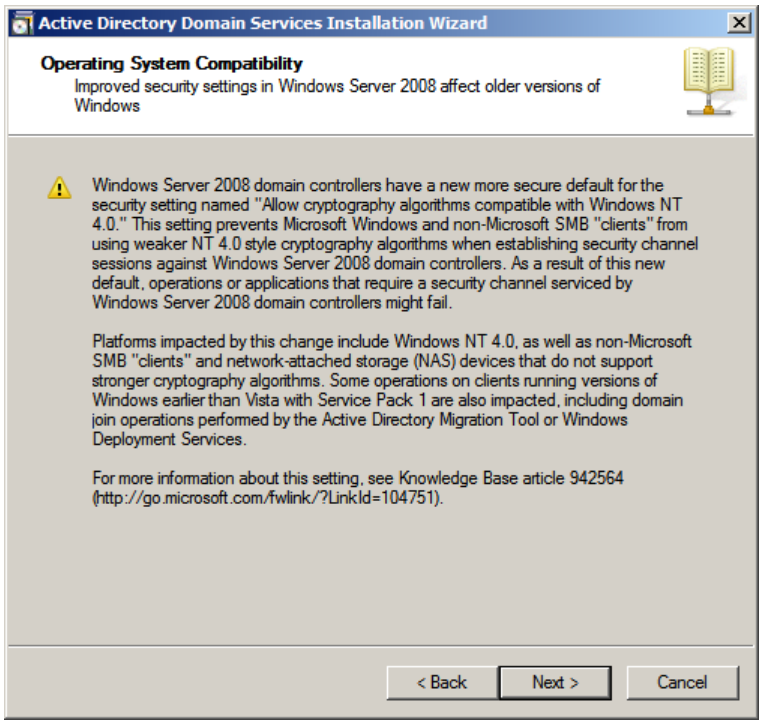
8. Review the results of the "Add Roles Wizard" page. Click: **Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)**.



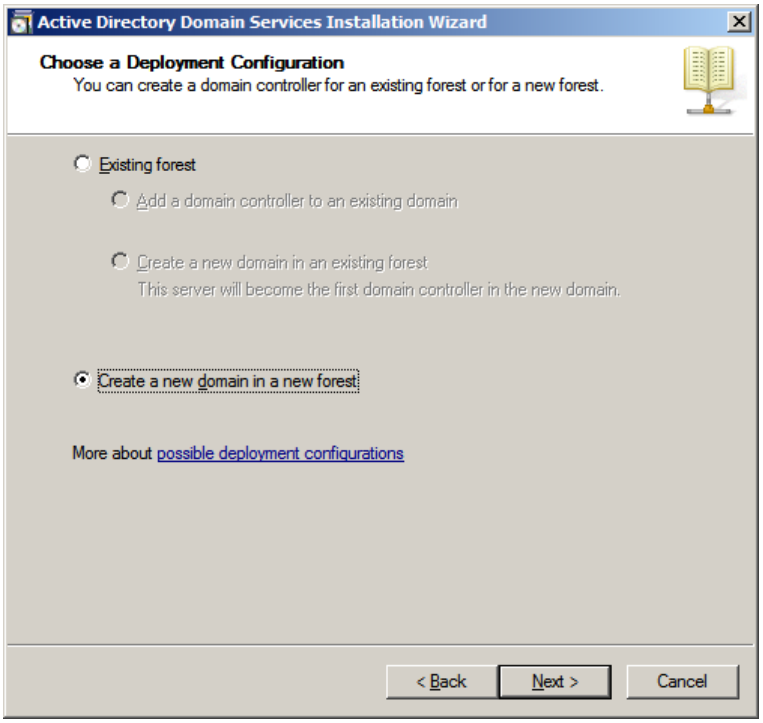
Installing Active Directory 2008 Installation Wizard

1. In the welcome screen click **Next**.

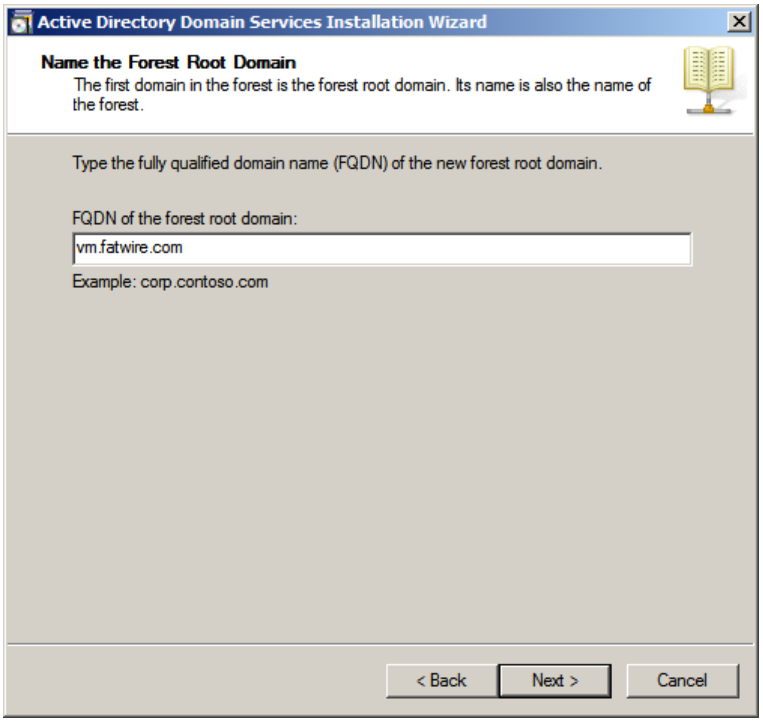
2. In the "Operating System Compatibility" screen click **Next**.



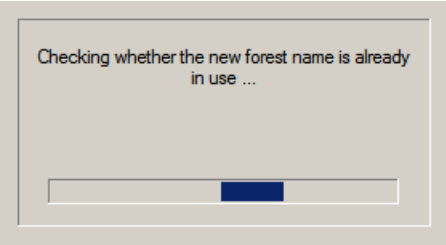
3. In the "Choose a Deployment Configuration" screen select **Create a new Domain in a forest**, then click **Next**.



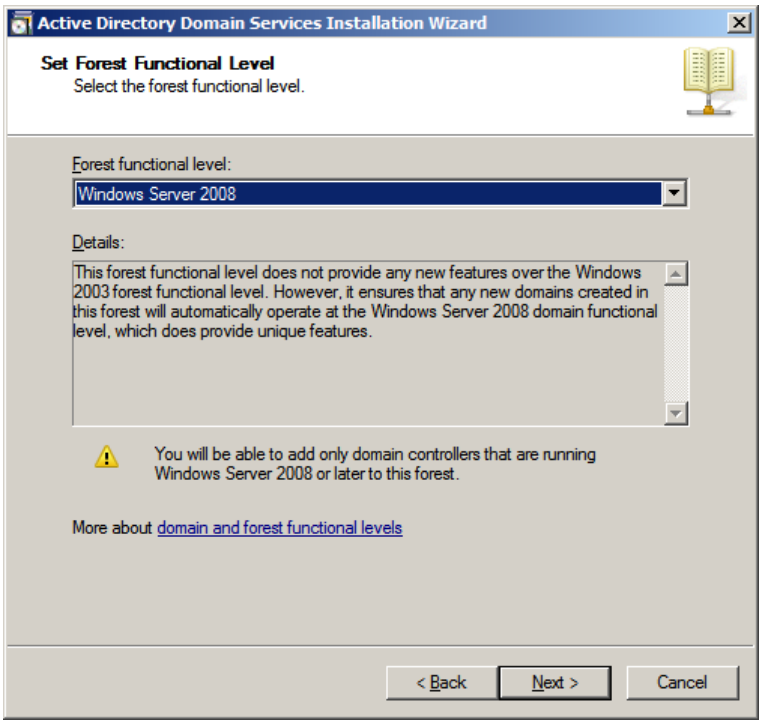
4. Name the "Forest Root Domain":
   a. Enter the name of the new forest, which is the DNS root domain that you created previously. Click **Next**.



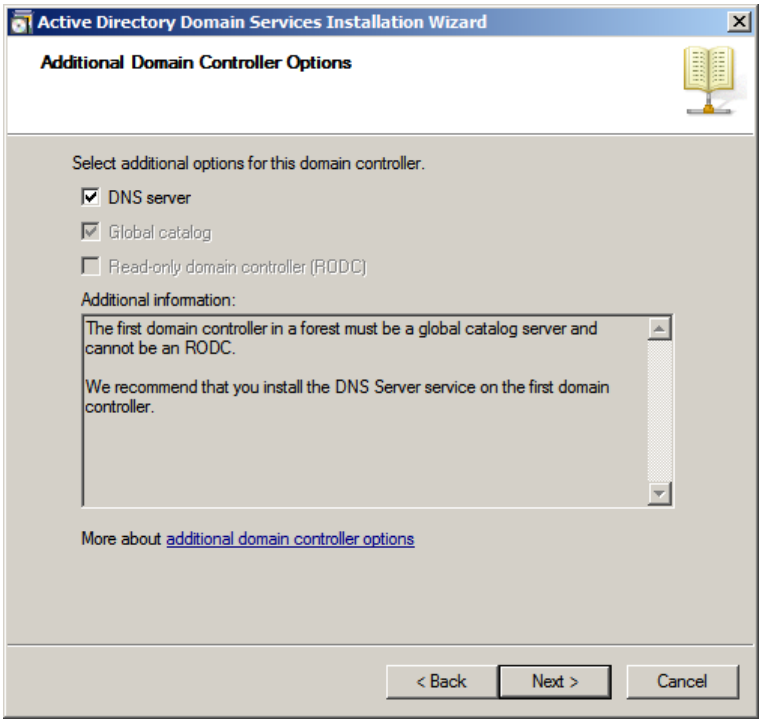
b. Allow the check dialog to complete.



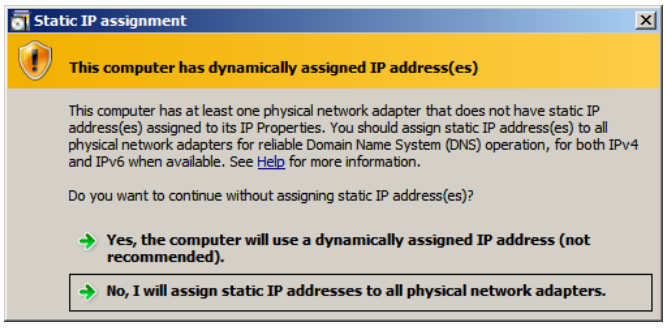
5. In the "Set Forest Functional Level" screen select **Windows Server 2008**, then click **Next**.



6. In the "Additional Domain Controller Options" screen, ensure that **DNS Server** is selected, then click **Next**.

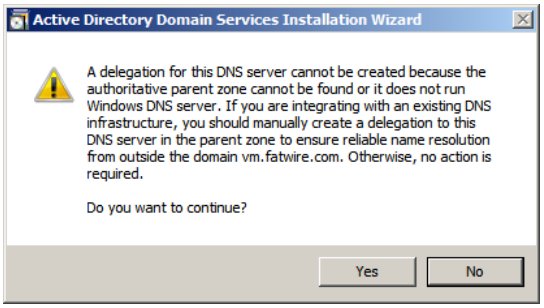


- If you have a DHCP based adapter you will see the following pop-up message:



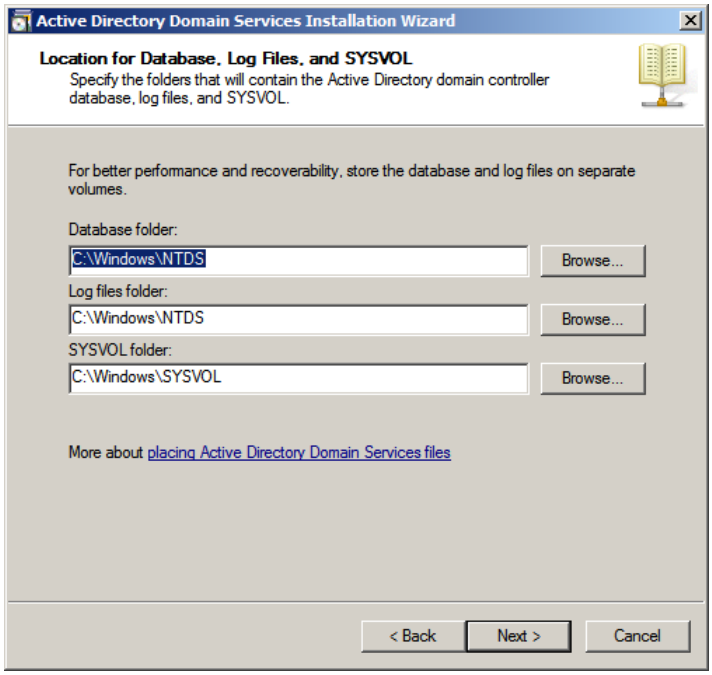
Select **No, I will assign static IP addresses to all physical adapters** to continue with the installation. After the installation completes you can change any DHCP adapter back.

7. If the DNS zone you are creating does not have an authoritative parent zone, the following pop-up message may be displayed:

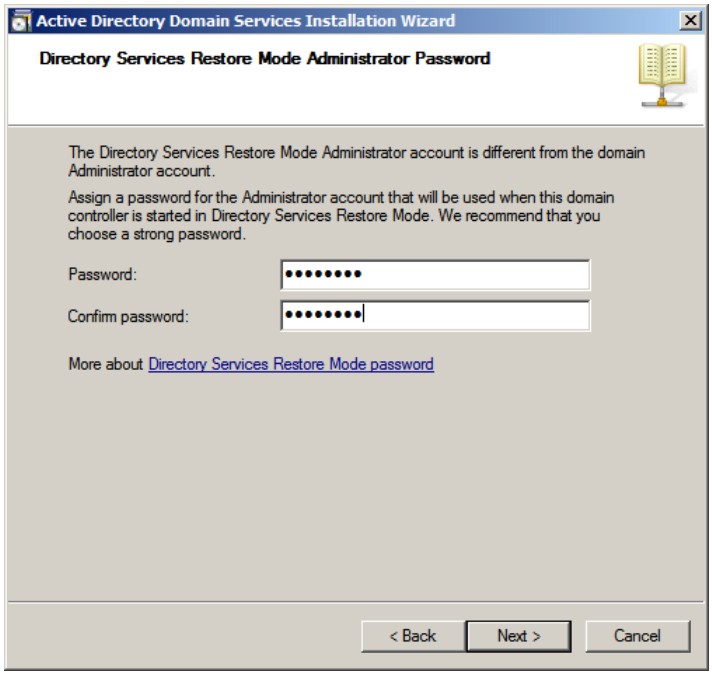


Select **Yes** to continue with the installation.

8. In the "Location for Database, Log Files, and SYSVOL" screen select the default in the **Database folder** field or change it as required by your system, then click **Next**.



9. In the "Directory Services Restore Mode Administrator Password" screen, enter a password and make a record of it.

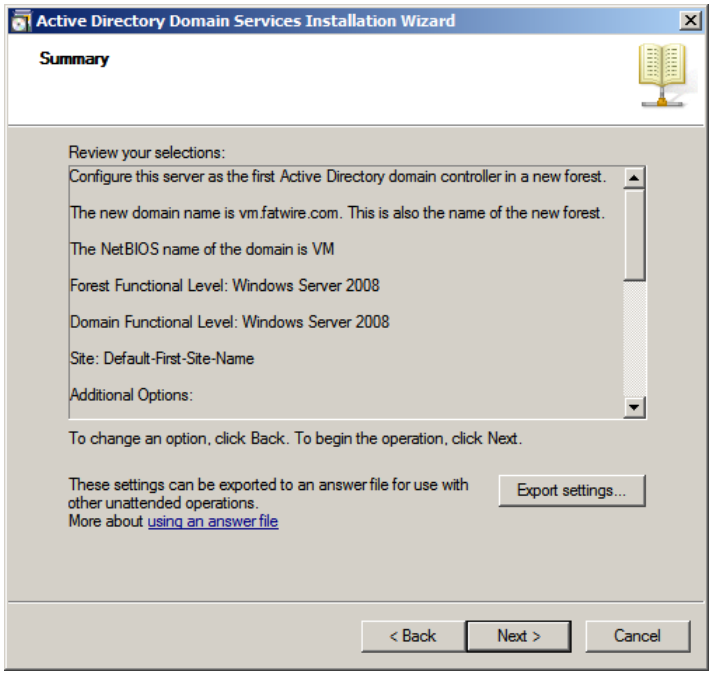


10. In the "Summary" screen:

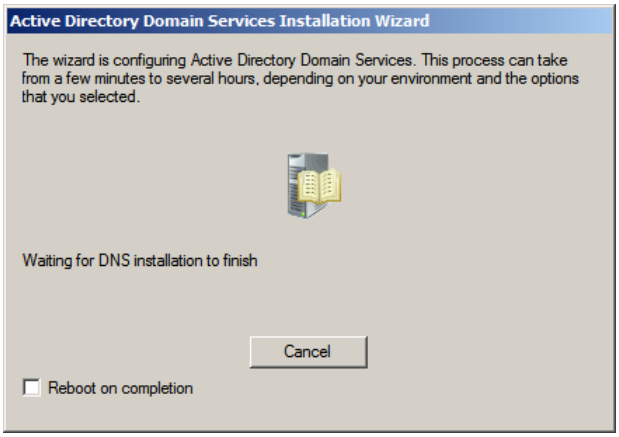
a. Review your settings.

b. Export your settings.

c. Click **Next**.



11. Wait for the installation to complete.

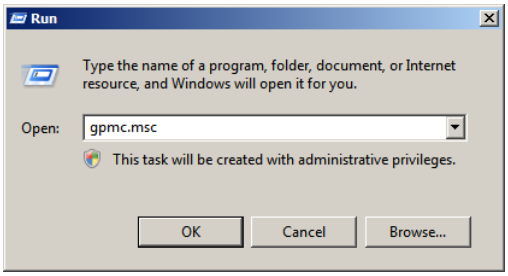


12. In the Active Directory Domain Services Installation Wizard, click **Finish** to complete the installation.

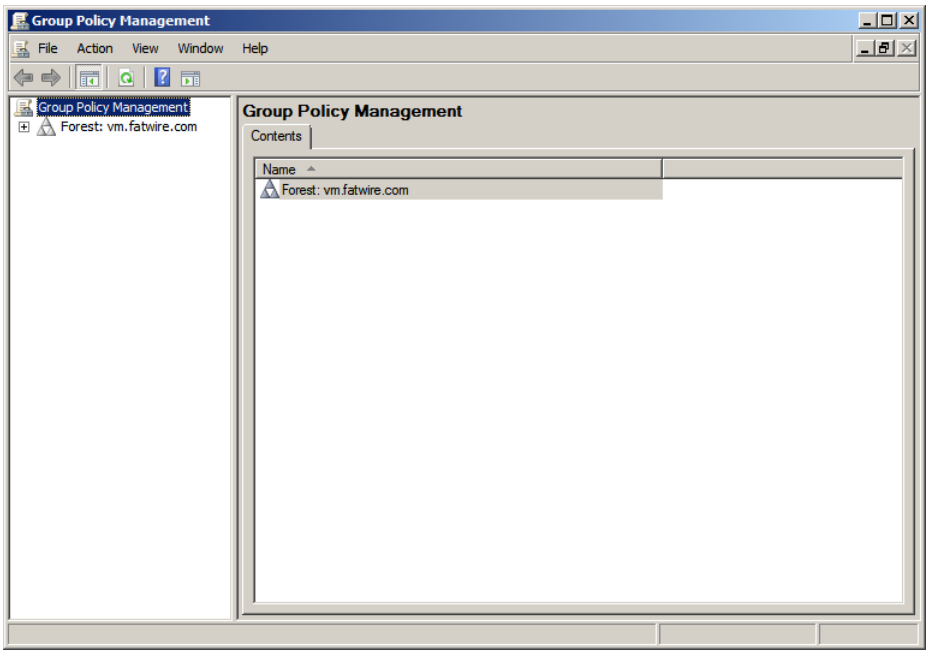
13. Reboot the System.

Checking Group Policies

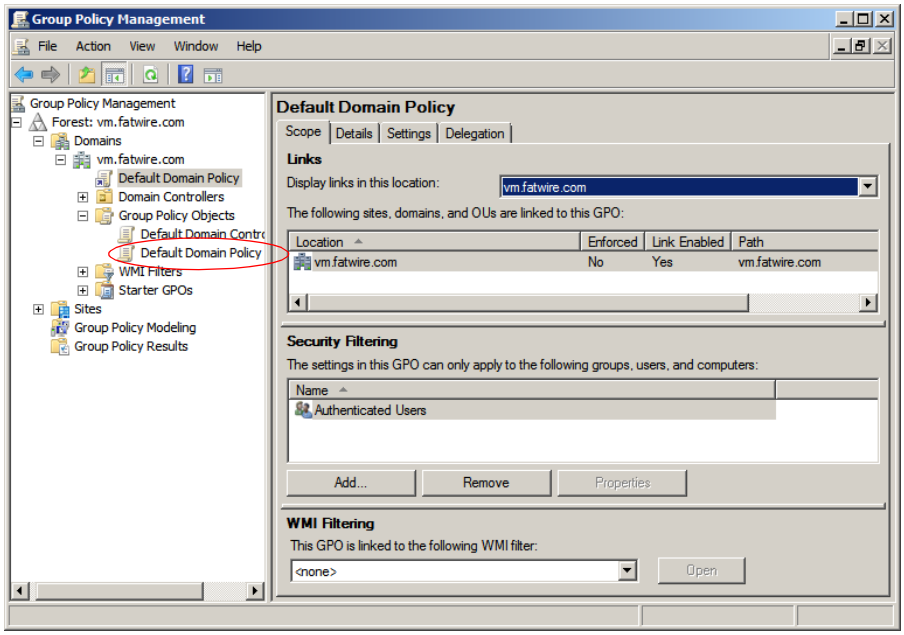
1. Select **Start** > **Run**.
   a. Enter `gpmc.msc` in the available field.
   b. Click **OK**.



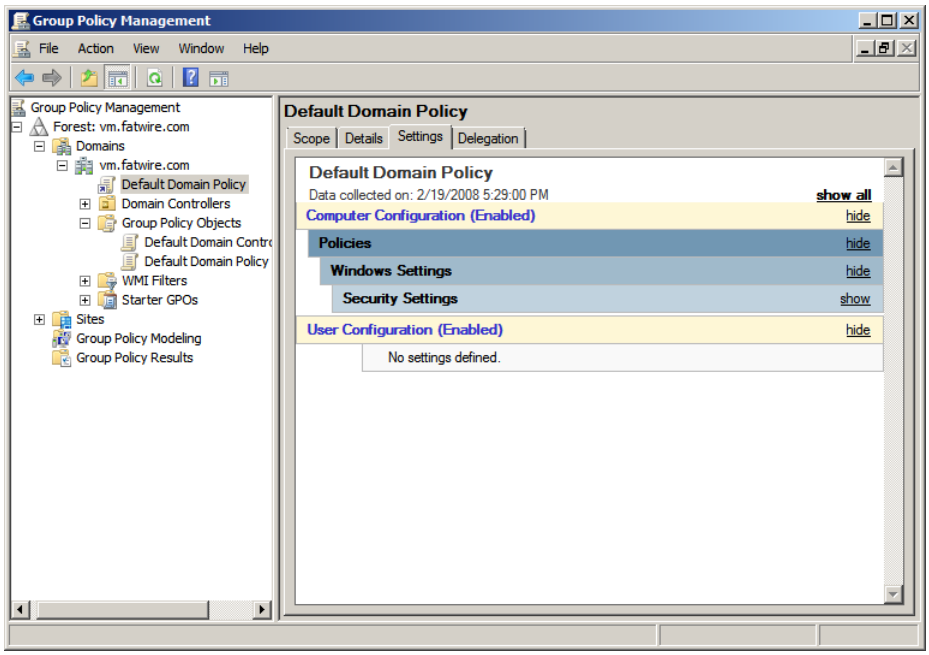
2. "Group Policy Management" opens.



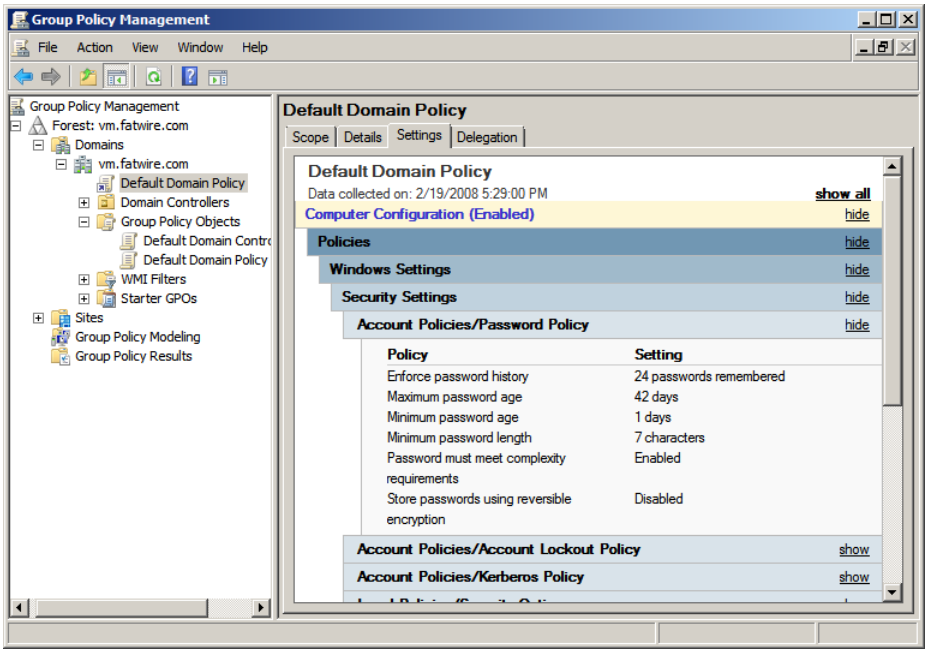
a. Expand the tree **Domains** > *your domain name*, then select **Default Domain Policy**, located in the left panel of the "Group Policy Management" screen.



b. Select the **Settings** tab.



c. Expand **Security** > **Account Policy/Password Policy** section, by clicking **show**.



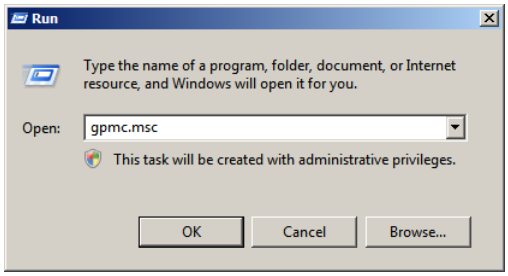
3. Review the "Policy" list. The option **Password must meet complexity requirements** is set to true by default. Change this option to **Disabled** (default Content Server passwords do not meet these requirements).

Changing Group Policies

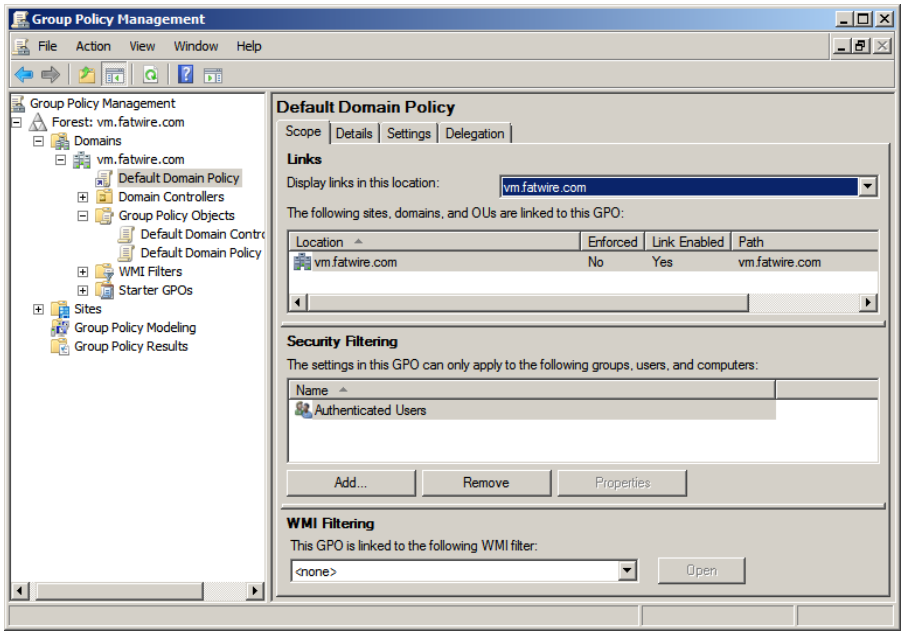
1. Select **Start** > **Run**.

a. Enter: `gpmc.msc` in the field provided.

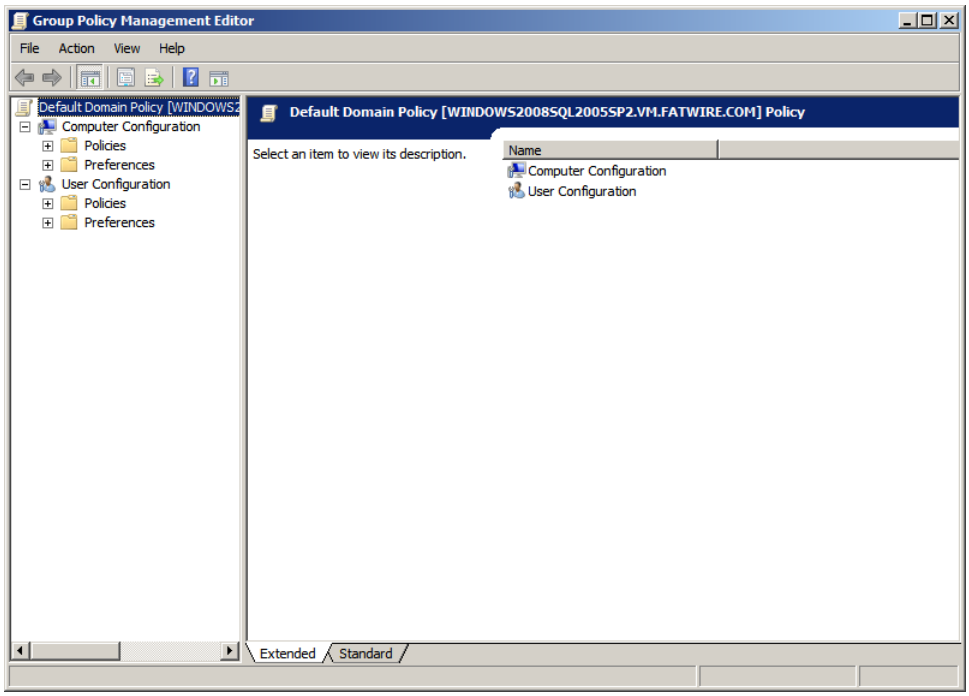
b. Click **OK**.



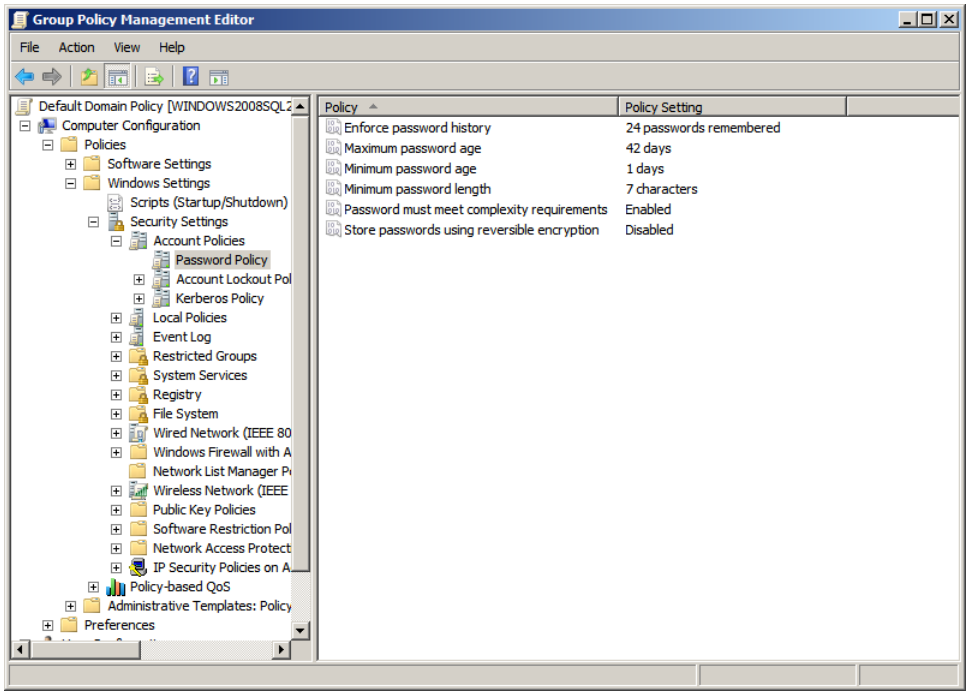
2. In the "Group Policy Management" screen expand the tree **Domains** > *name of your domain*. Select the **Default Domain Policy**, located on the right of the screen, then select **edit**.



3. The "Group Policy Management Editor" window opens.

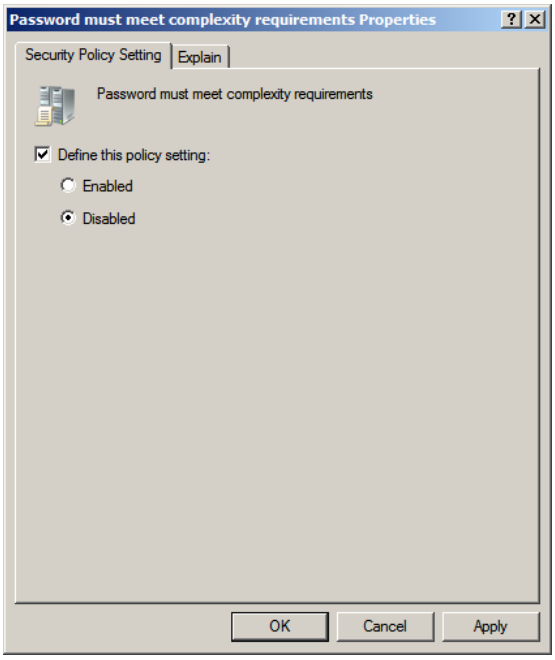


a. In the left hand tree expand: **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Account Settings** > **Password Policy**



b. Right-click **Password must meet complexity requirements**, located on the right side of the screen, then select **Properties**.

c. In the "Password must meet complexity requirements Properties" dialog box select the radio button **Disabled**, then click **OK**.



d. Close the “Group Policy Management Editor” and “Group Policy Management” windows.

4. The domain will no longer check for password complexity. Content Server default passwords can now be used.

   When Content Server is installed you can reverse step 2 by clicking **Enabled** to re-engage the security settings.

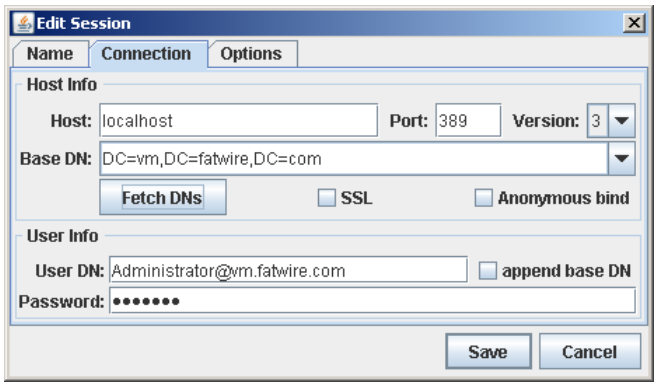
Connecting to ADS Using an LDAP Browser

This section shows you how to connect to Active Directory Server using an LDAP browser.

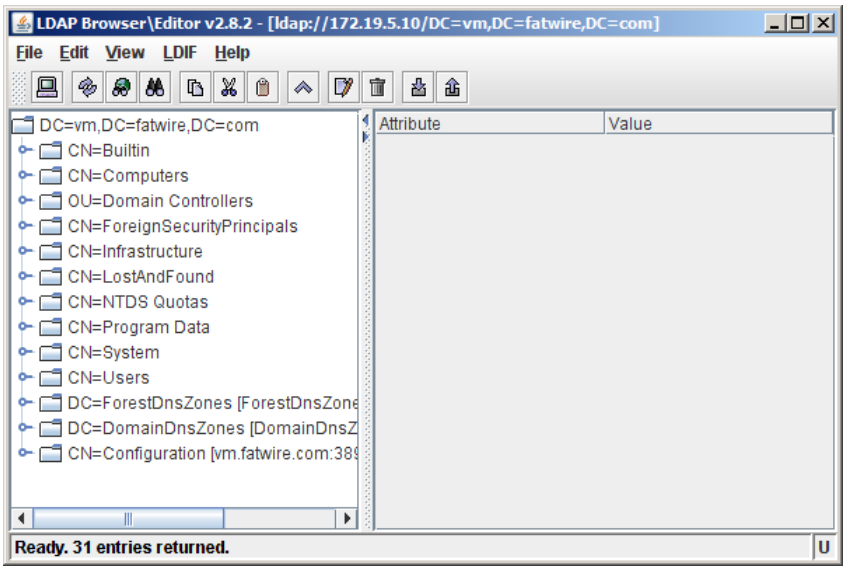
Note

You cannot add groups, set passwords, or activate accounts using an LDAP browser.

1. Open the LDAP browser.
2. Select the **Quick Connect** tab.
3. Fill out the following information:
   - **Host:** `localhost` (if connecting remotely, enter the actual host name)
   - **Base DN:** `<DNS_suffix>` (the part of the DNS name after the host name)
   - **Anonymous bind:** deselect
   - **User DN:** `administrator@<DNS_suffix>`
   - **Append base DN:** deselect
   - **Password:** `<ADS_password>` (you created this password in step 9 on page 196)
4. Click **Connect**.



5. Show the default view on the LDAP tree.



Chapter 14

Setting Up IBM Tivoli Directory Server 6.x

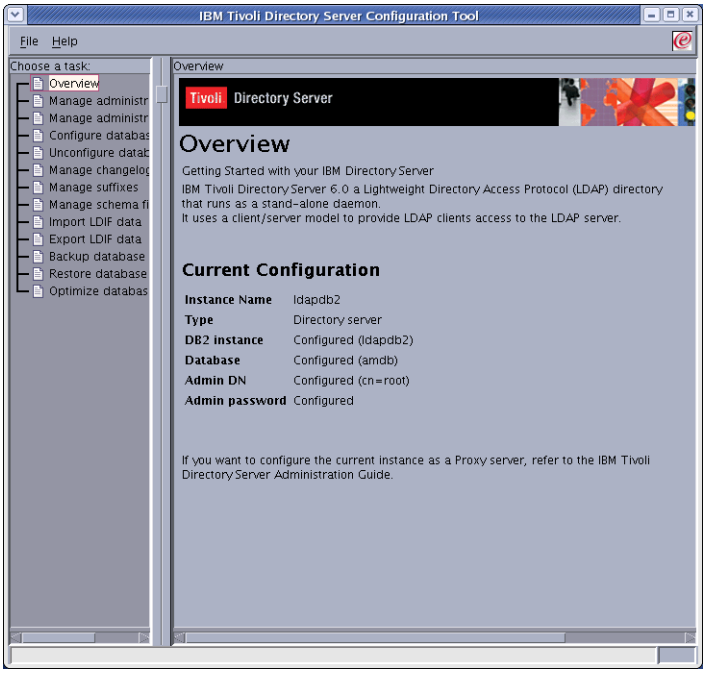
This chapter contains the following sections:

Note

In this guide, Tivoli Directory Server is also referred to as “TDS.”

IBM Tivoli Directory Server Commands

Table 4: IBM Tivoli Directory Server Commands

Action	Command
Starting an instance	`<LDAP Install directory>/sbin/idsslapd -I <instance name>`
Stopping an instance	`<LDAP Install directory>/bin/ibmdirctl stop -h localhost -D cn=root -w <password for cn=root>`
Checking an instance	`<LDAP Install directory>/bin/ibmdirctl status -h localhost -D cn=root -w <password entered for cn=root>`
Displaying list of instances	`<LDAP Install directory>/sbin/idsilist`
Loading the instance administration tool	`<LDAP Install directory>/sbin/idsxinst`
Loading the configuration tool for an instance	`<LDAP Install directory>/sbin/idsxcfg -I <name of instance>` 

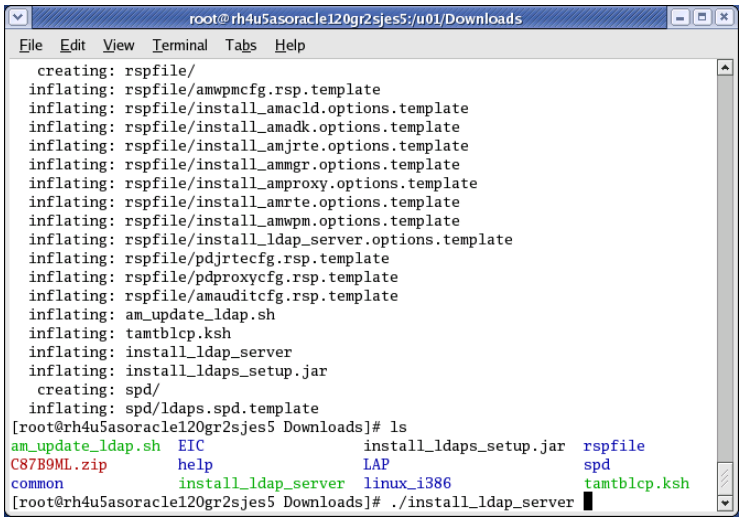
Before Installing IBM Tivoli Directory Server

1. Create the following group: `idsldap`
2. Create a user for the LDAP instance and write down the password, for example, `ldapdb2`. This password will be used in step 7 of "Installing IBM Tivoli Directory Server."
3. Check that **`pdksh`** is installed.

Installing IBM Tivoli Directory Server

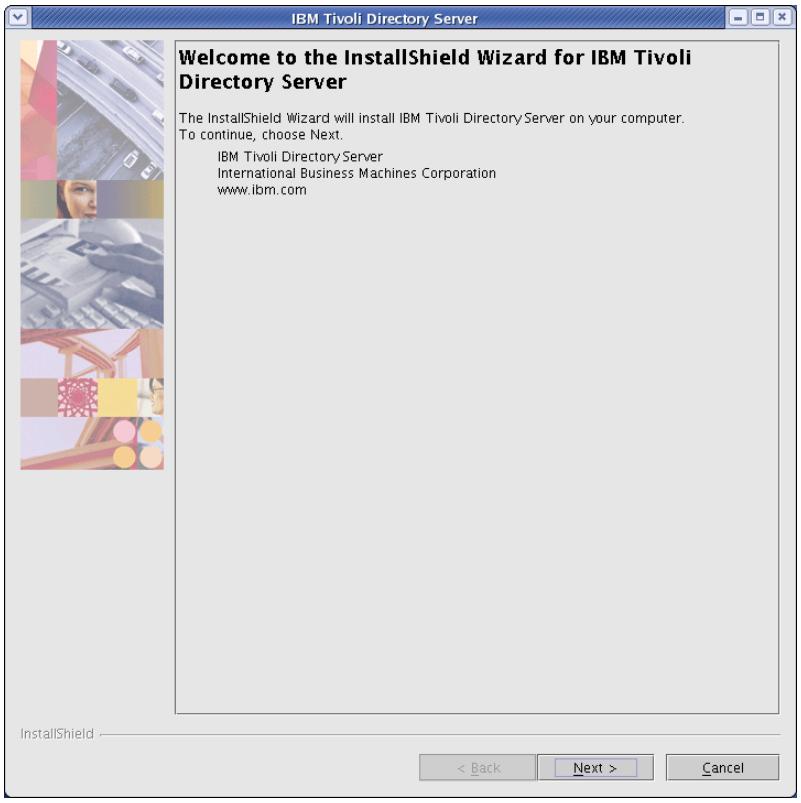
1. Download the Tivoli Directory Server from IBM.
2. Unzip the archive into a temporary directory.
3. Go to the temporary directory and run:

   `./install_ldap_server`.

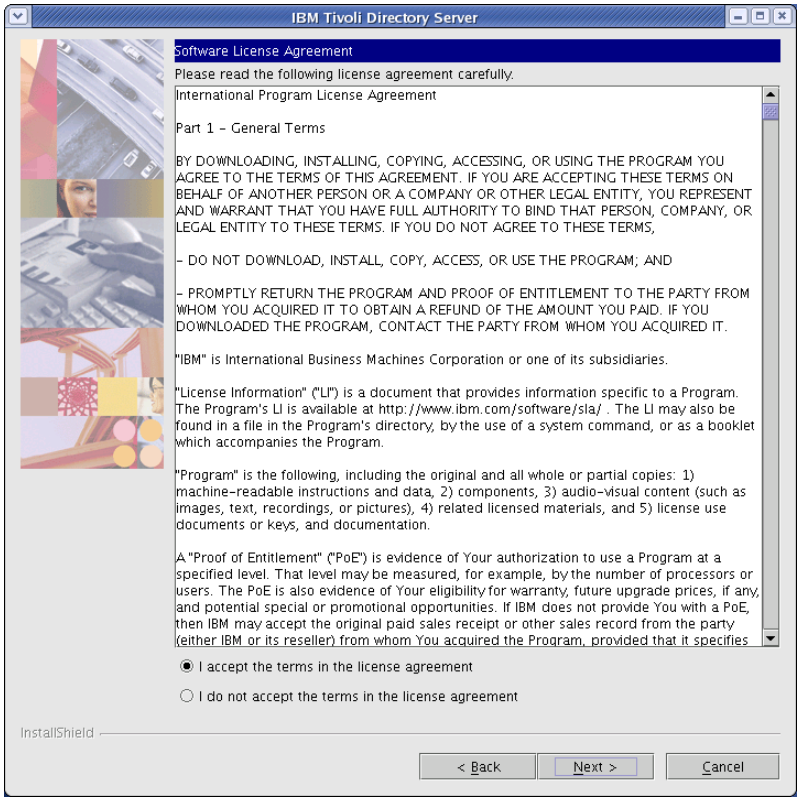


4. When the installation dialog box appears, select your language and click **OK**.

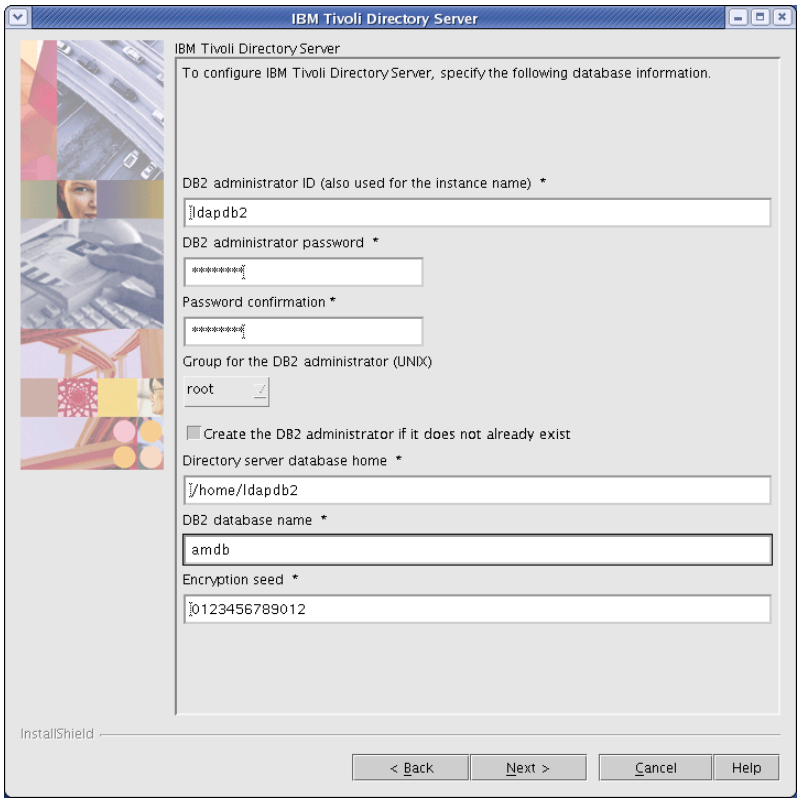
5. Click **Next**.


IBM Tivoli Directory Server
Welcome to the InstallShield Wizard for IBM Tivoli Directory Server
The InstallShield Wizard will install IBM Tivoli Directory Server on your computer. To continue, choose Next.
IBM Tivoli Directory Server
International Business Machines Corporation
www.ibm.com
InstallShield
< Back
Next >
Cancel

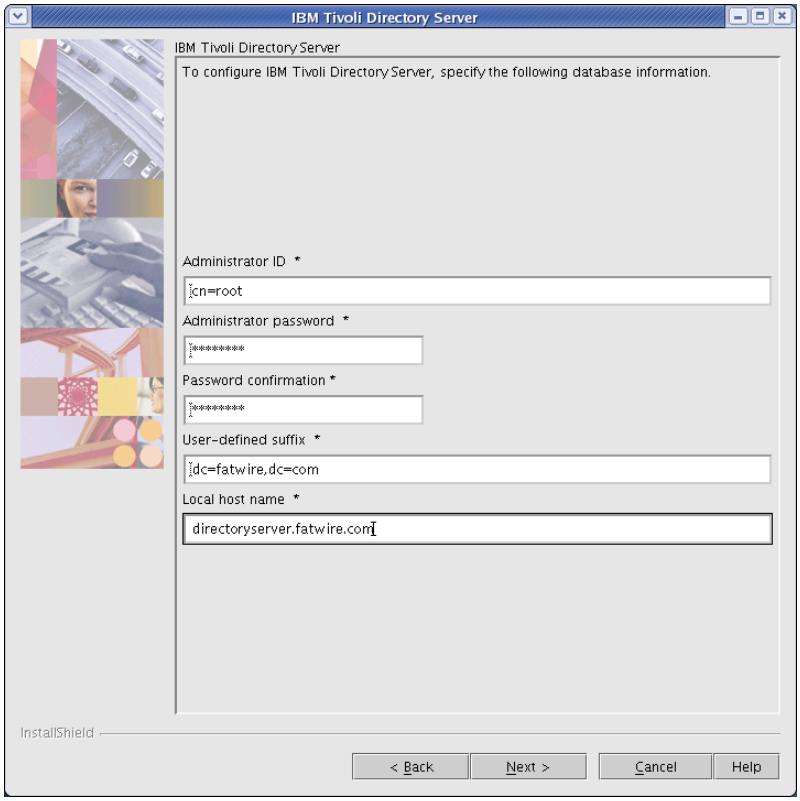
6. On the “License Agreement” screen select **I Accept the terms in this license agreement**, then click **Next**.



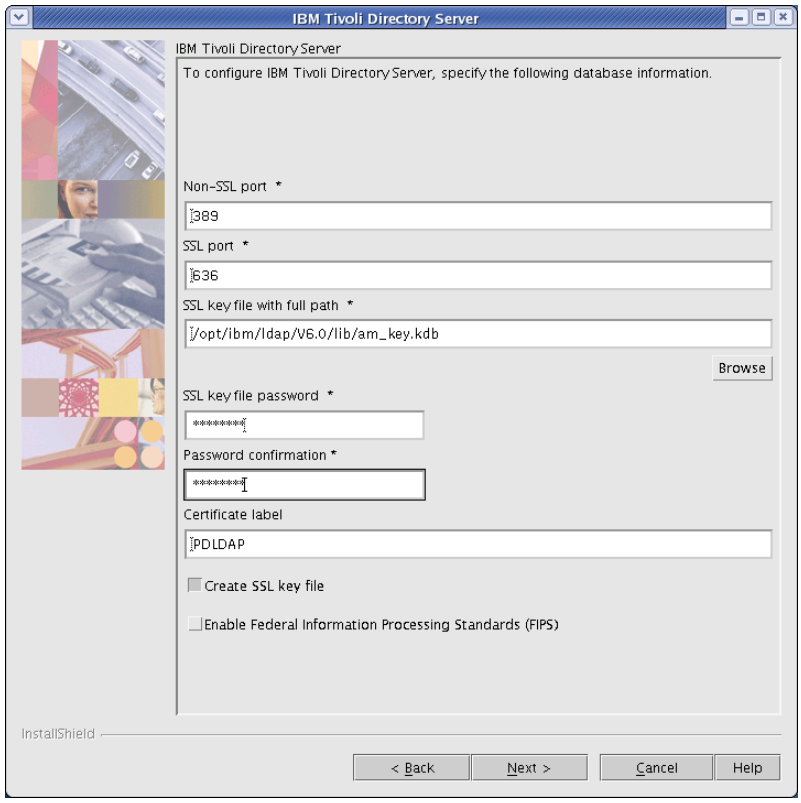
7. On the first configuration screen, fill in the fields:
   - **DB2 administrator ID**: Name of the user you created for the LDAP instance.
   - **DB2 administrator password**: Enter the password (`ldapdb2`) given to the LDAP instance user in step 2, “Before Installing IBM Tivoli Directory Server.”
   - Keep the default values for the other fields.
   - Click **Next**.



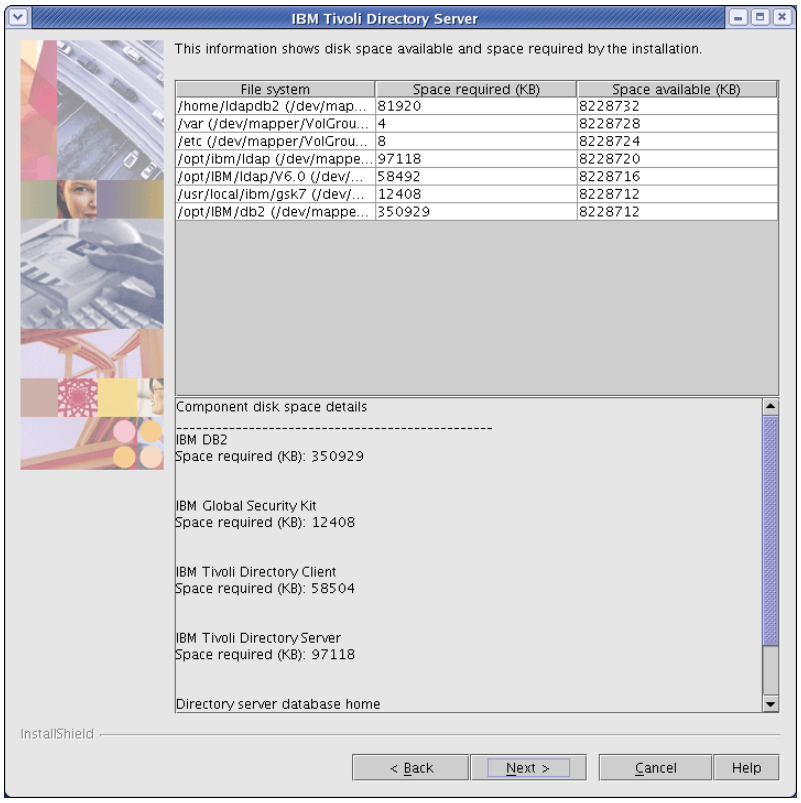
8. On the second configuration screen, fill in the fields:
   a. **Administrator password**: Enter a password and remember it. This password will re-occur throughout the configuration and will be referred to as `sn=root`.
   b. **User-defined suffix**:
      `dc=<domain>,dc=<ext>`
      For example, if your domain is `fatwire.com`, then the User-defined suffix should read: `dc=fatwire,dc=com`.
   c. Confirm that the **Local hostname** is correct.
   d. Click **Next**.



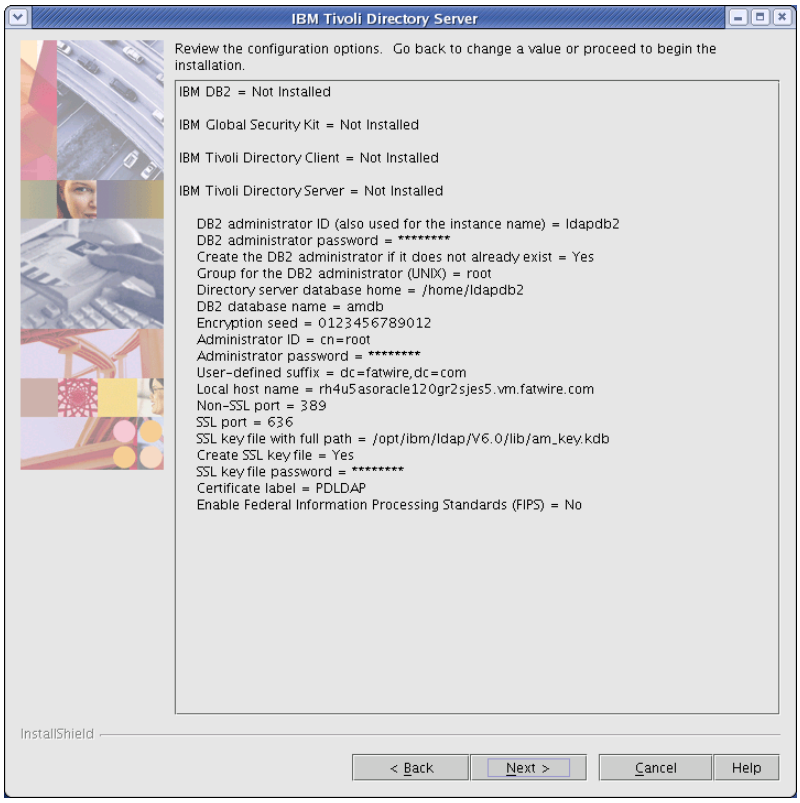
9. On the third configuration page:
   a. Fill in the fields:
      - **SSL key file password**: Enter a password for SSL.
      - **Non-SSL port**: Confirm the Non-SSL port value is set to `389`. If the Non-SSL has been changed, use the new value when installing CS.
   b. Click **Next**.



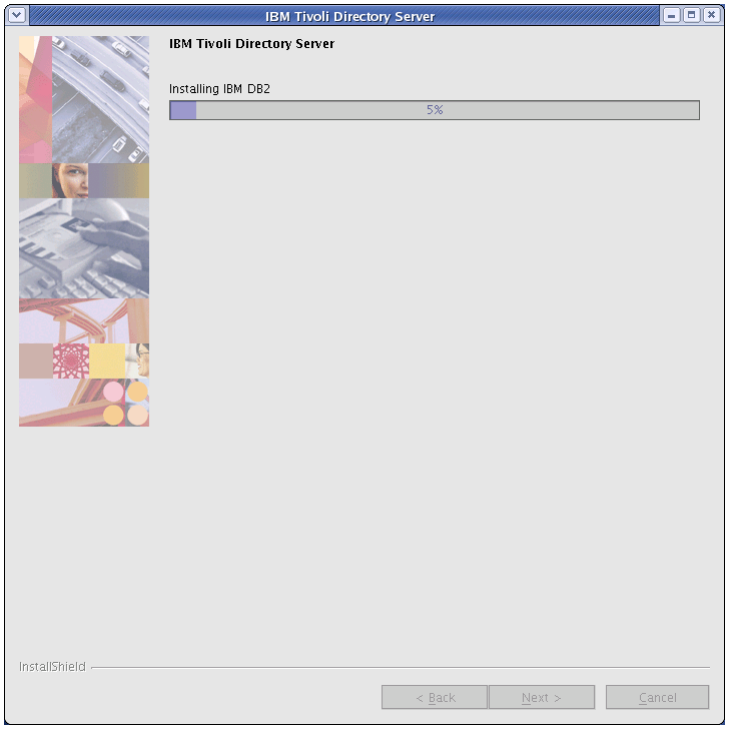
10. Confirm that enough disk space exists for the installation to succeed and click **Next**.



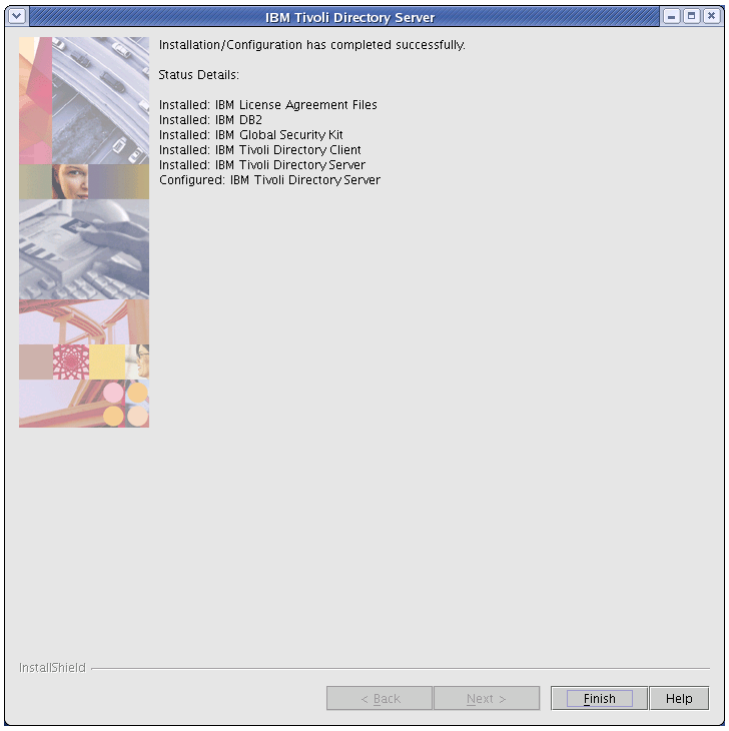
11. Review the summary and click **Next**.



12. Wait for the installer to finish.



13. Click **Finish**. The installation is now complete.



Configuring Tivoli Directory Server

Note

Only IBM TDS with `sha` encryption is supported by Content Server.

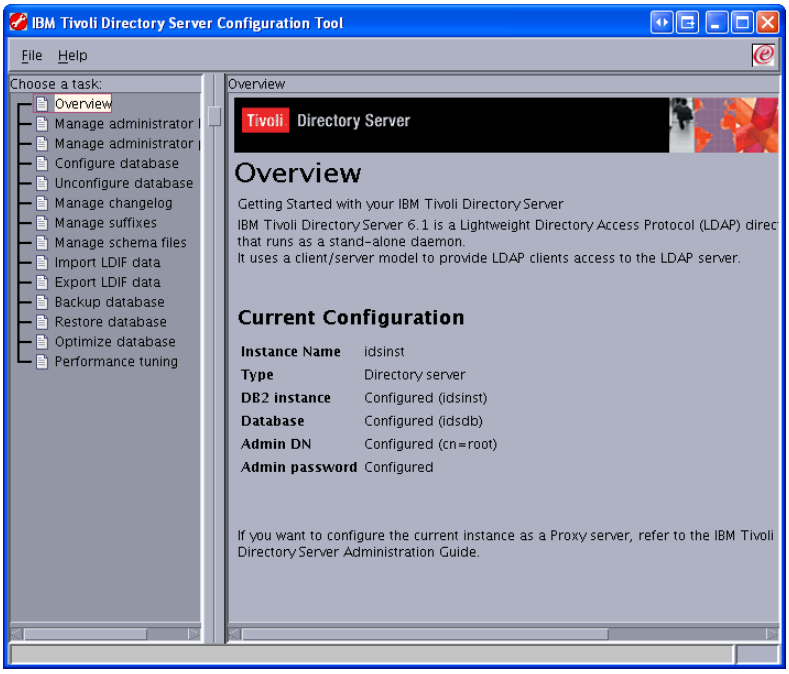
1. In a text editor open:
   `/home/<ldap user>/idsslapd-<ldap user>/etc/ibmslapd.conf.`
2. Search for the `ibm-slapdPwEncryption` parameter and change the value to `sha`.
3. Save the change in the text editor.

Completing and Verifying the LDAP Configuration

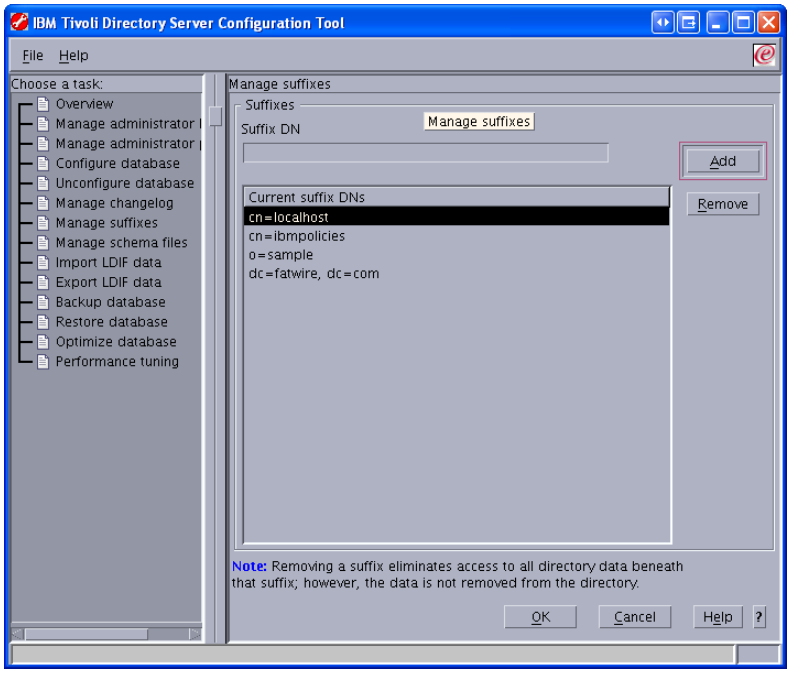
1. Start the IBM TDS instance:
   `<`**`LDAP Install directory`**`>/sbin/idsslapd -I <`**`instance name`**`>`

2. Start the IBM TDS instance configuration tool (your display must be set in order to continue the configuration process):

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



3. Select **Manage suffixes**.



4. Make sure the User-defined suffix that was specified during installation appears in the list, then click **OK**.

Importing an LDIF file (LDAP Browser)

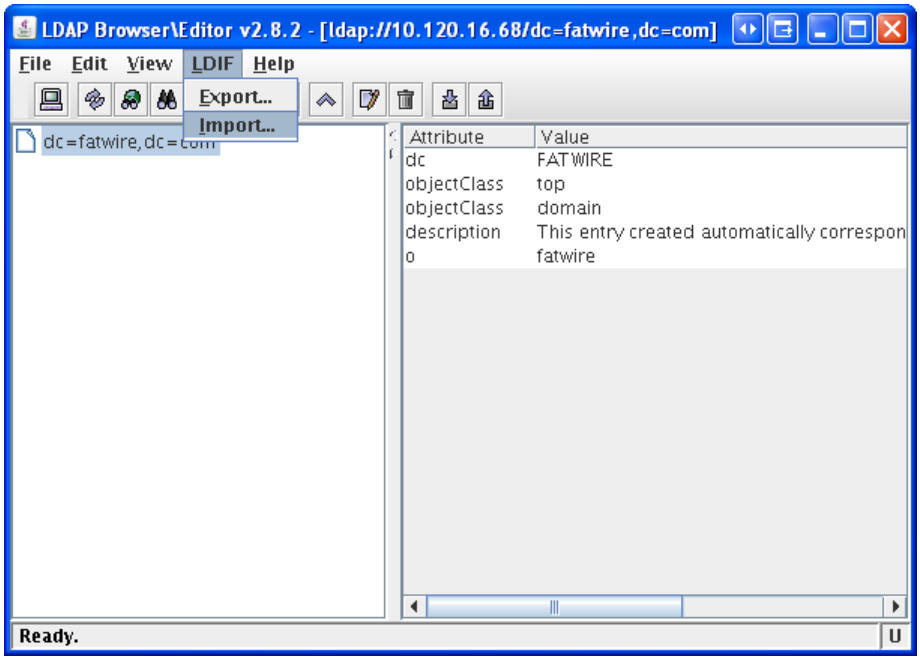
1. Start the IDM TDS instance:

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

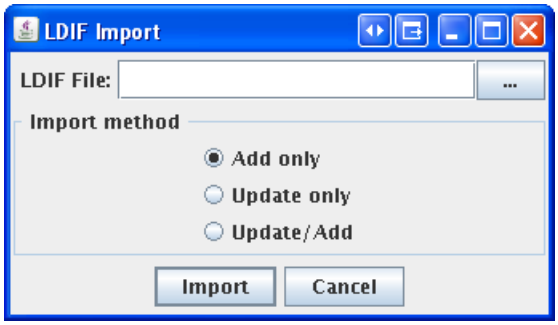
2. Connect to IBM TDS using the LDAP browser, for instructions see "Connecting to IBM TDS Using the LDAP Browser," on page 222.

3. Select: dc=<**domain**>,dc=<**ext**>

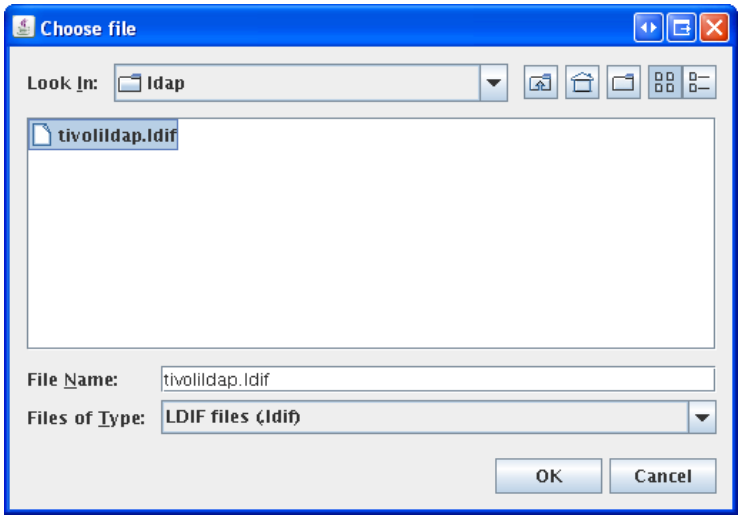
   a. Click the **LDIF** menu, and select **Import**.



4. Click the **Add only** button.



5. Browse to the LDIF file `<cs_install_dir/ldap>/tivolildap.ldif` and click **OK**.



6. Click **Import**.

> **Note**
>
> The root entry will fail to import because it already exists, but all others will import successfully.

7. Click **OK**.

Importing an LDIF file (Configuration Tool)

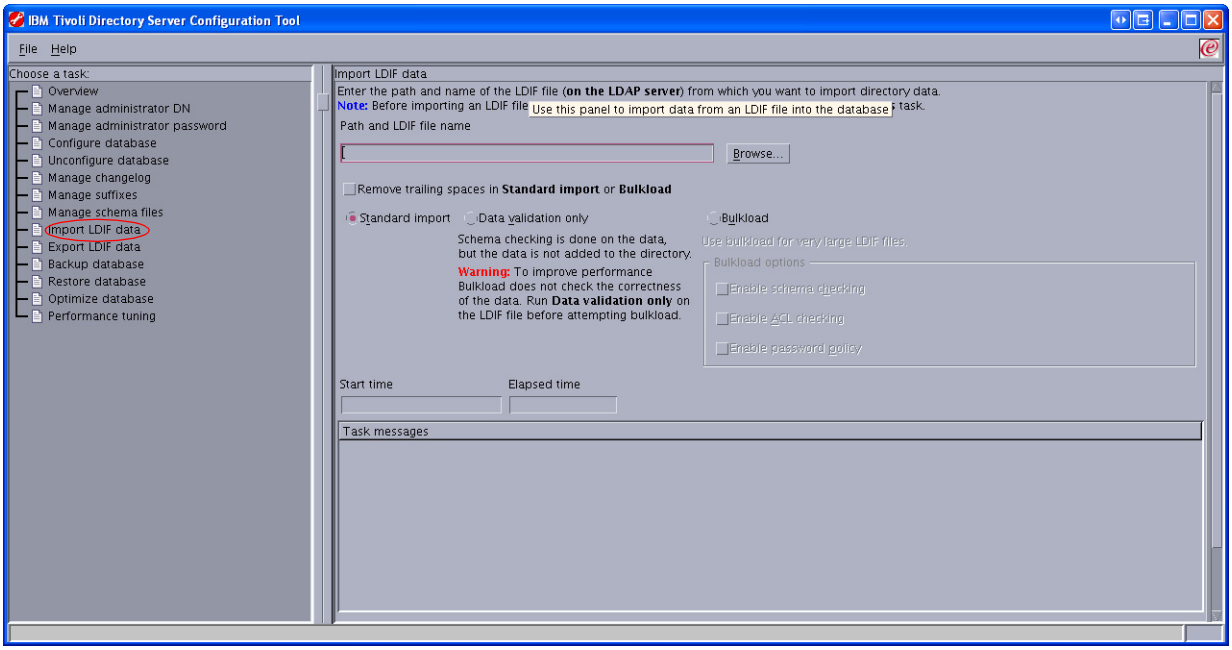
1. Convert the LDIF file to Unix format using the `dos2unix` utility.
   - **Linux**:
     ```
     dos2unix <tivolildap.ldif>
     ```
   - **Solaris**:
     ```
     mv tivolildap.ldif > tivolildap2.ldif
     dos2unix tivoli.ldap2.ldif > tivolildap.ldif
     ```
2. Stop the IBM TDS instance:

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

3. Start the IBM TDS instance configuration tool (your display must be set in order to continue with the import process):

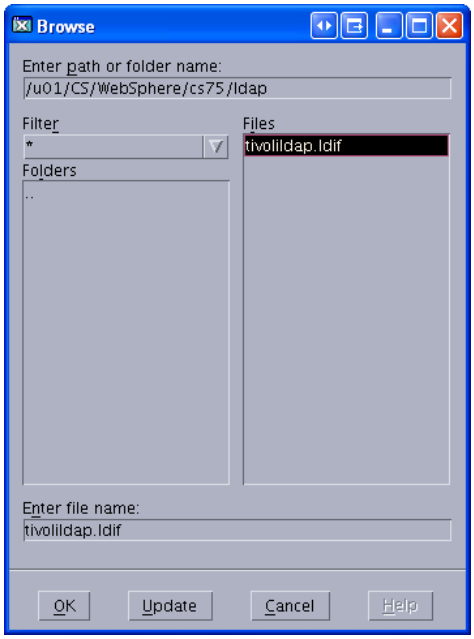
   `<LDAP Install directory>/sbin/idsxcfg -I <name of instance>`

4. Select **Import LDIF data**.

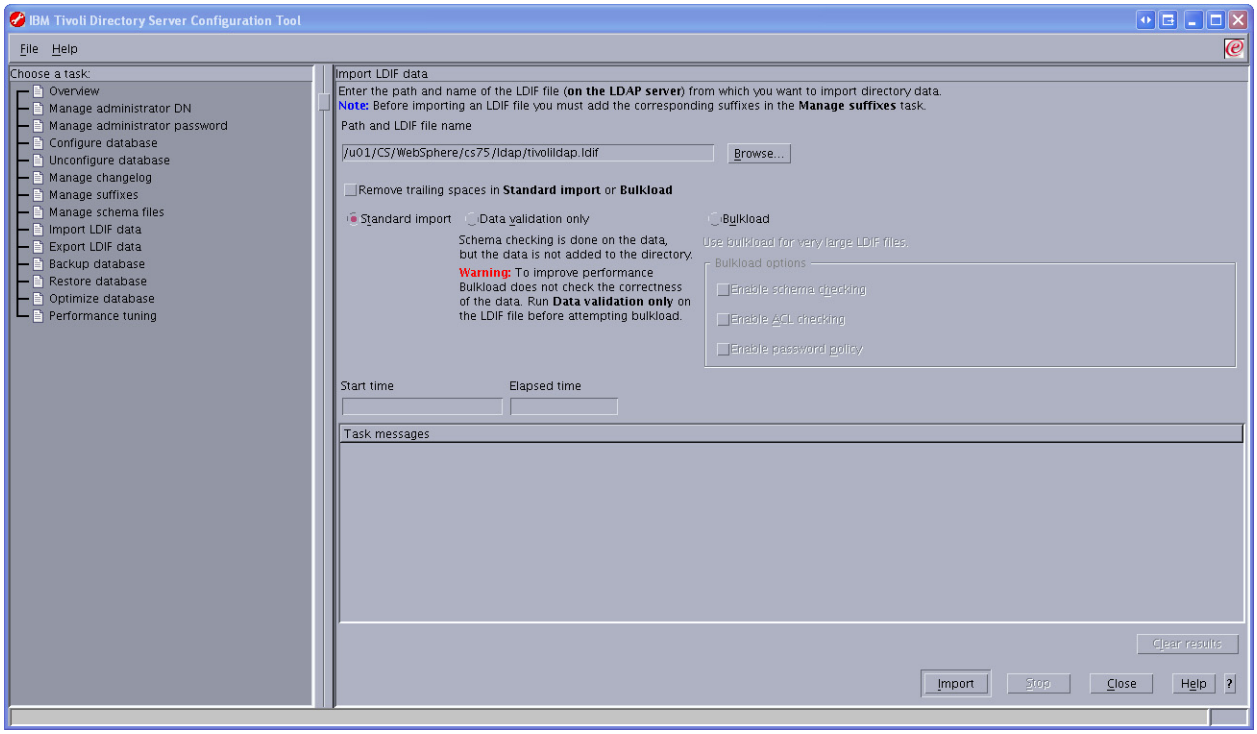


5. Click **Browse**.

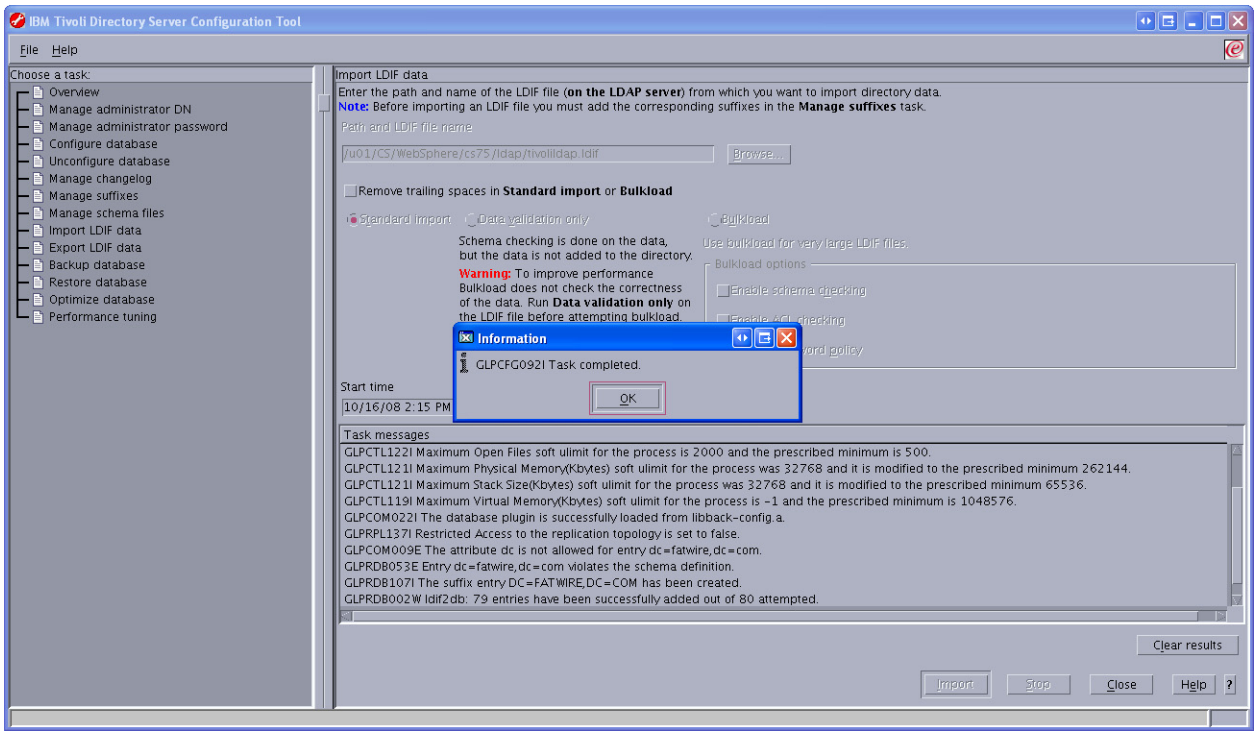
6. Browse to the LDIF file you wish to import and click **OK**.



7. Click **Import**.



8. Click **OK** when the import is complete.



Adding Users and ACLs using an LDIF file

1. Create a blank LDIF file (for example, `addstuff.ldif`).
2. For each user that you wish to add, add the following to the LDIF file:

```
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. For each ACL you wish to add, add the following to the LDIF file:

```
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. Import the LDIF file by following the steps in the section “Importing an LDIF file (LDAP Browser),” on page 217 or “Importing an LDIF file (Configuration Tool),” on page 218.

Connecting to IBM TDS Using the LDAP Browser

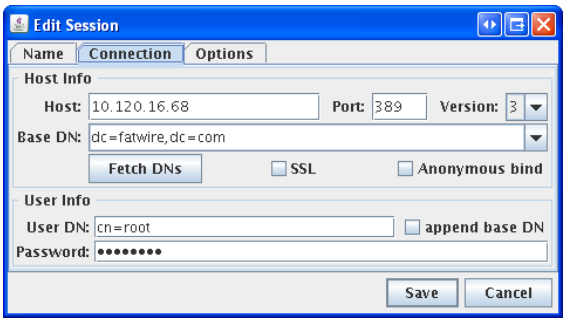
1. Download and install the LDAP browser.
2. Start the LDAP browser:

   ```
   ./lbe.sh
   ```
3. Fill in the required fields:
   - **Host**: Enter the IP or hostname of IBM TDS.

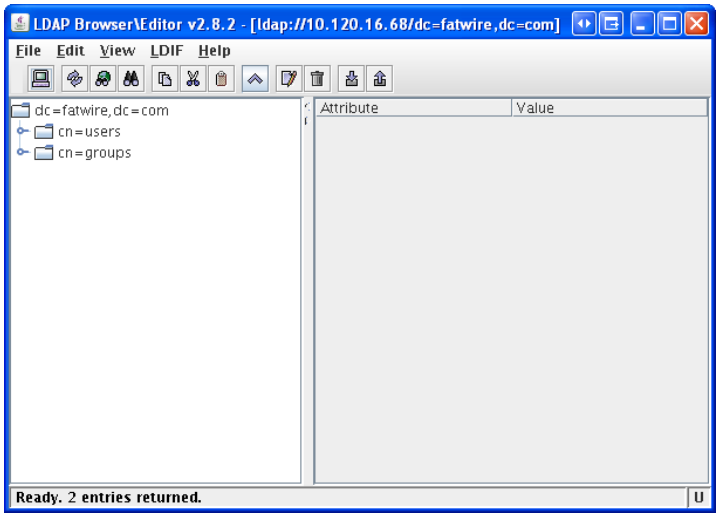
   Note

   The default port which IBM TDS runs on is `389`.

   - **Port**: Enter the port on which IBM TDS is running.
   - **Base DN**: Enter the user-defined suffix that was entered during the installation of IBM TDS (see step 8 on page 211 for more information about the User-defined suffix).
   - **Anonymous bind**: Deselect the check box
   - **User DN**: Enter `cn=root`
   - **Password**: Enter the password for `cn=root`



4. Click **Save**.



Chapter 15

Setting Up OpenLDAP 2.3.*x*

This chapter explains how to set up OpenLDAP for use with Content Server.

Note

You must set OpenLDAP **before** you run the CS LDAP integrator.

It contains the following sections:

OpenLDAP Commands

This section contains the most commonly used OpenLDAP commands. Use it as a reference when configuring OpenLDAP for use with Content Server.

Starting OpenLDAP

Note

This section assumes that the `slapd` daemon is located in `/usr/local/libexec`. Depending on your installation, the daemon might be located elsewhere. In such cases, substitute the correct path in the commands listed in this section.

- To start OpenLDAP normally, use the following command:

  `/usr/local/libexec/slapd`

- To start OpenLDAP with full debugging (useful when diagnosing configuration issues and installing Content Server), use the following command:

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

Searching an OpenLDAP Server

To search an OpenLDAP Server, do the following:

1. Execute the following command:

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

   where `<domain>` and `<extension>` are the values you specified in step a on page 230.

2. When prompted for a password, enter the Root DN user password you specified in step d on page 231.

   A typical response from the **`ldapsearch`** command looks as follows:

```
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
```

Adding an LDIF File to an OpenLDAP Server

To add a well-formed LDIF file to your OpenLDAP Server, use the **ldapadd** command:

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

where:

- <domain> and <extension> are the values you specified in step a on page 230.
- <root_dn_password> is the Root DN user password you specified in step d on page 231.
- <LDIF_file_name> is the name of the LDIF file you are adding.

Installing OpenLDAP

This section explains how to install OpenLDAP.

Note

OpenLDAP is bundled with most Linux distributions. If OpenLDAP is already installed on your system, skip this section.

To install Open LDAP

1. Download the OpenLDAP `tgz` archive from the OpenLDAP web site:

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

   For example: `openldap-stable-20070110.tgz`

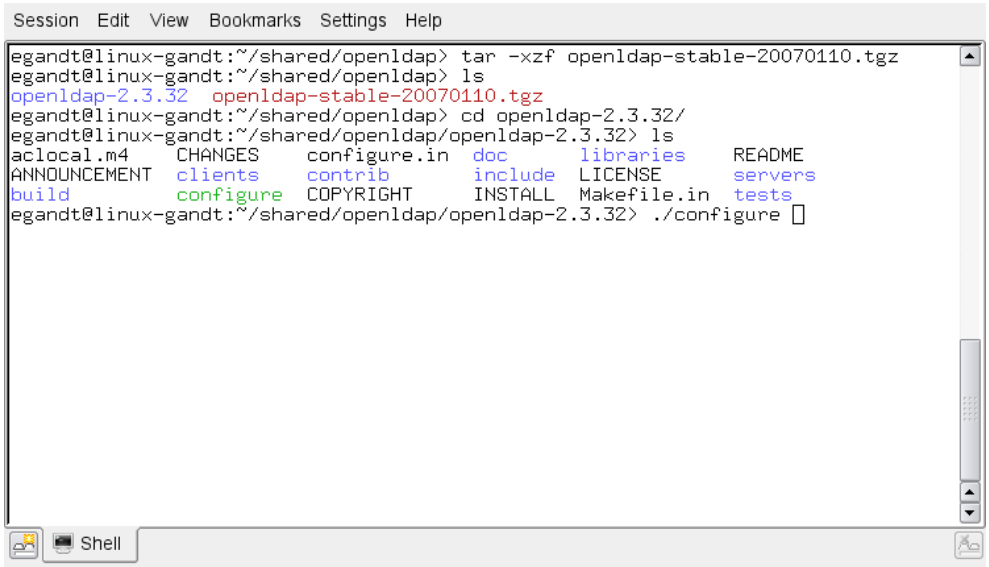
2. Decompress the archive:

   - If you are using GNU, use the following command:

     `tar-xvzf openldap-stable-20070110.tgz`

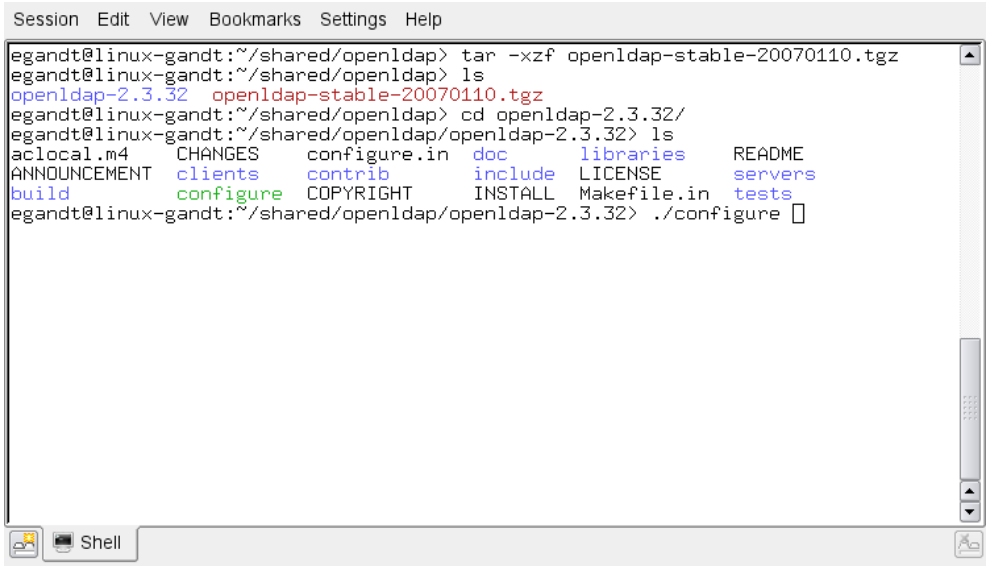
   - If you are not using GNU, use the following command:

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



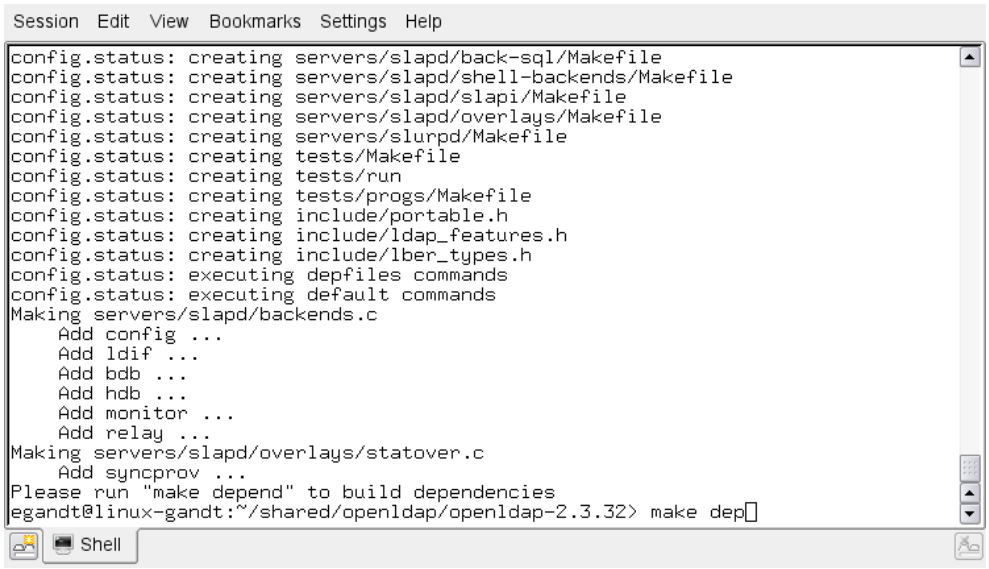
3. Change to the directory containing the OpenLDAP source. For example:

```
cd openldap-2.3.32
```



4. Configure the OpenLDAP source as follows:

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



The suggested options are:

- **`--enable-crypt`** — enables password encryption
- **`--with-tls`** — enables TLS/SSL support

Note

If you want to customize OpenLDAP for your system, run **`./configure --help`** for a complete list of configuration options.

5. Compile OpenLDAP dependencies: **`make depend`**
6. Compile OpenLDAP: **`make`**
7. Install OpenLDAP: **`make install`**

> **Note**
>
> By default, OpenLDAP is installed in `/usr/local`.

Configuring OpenLDAP

This section shows you how to configure your OpenLDAP installation.

1. Edit the `ldap.conf` file as follows:

> **Note**
>
> If you installed OpenLDAP manually by following the steps in the previous section, `ldap.conf` is located in `/usr/local/etc`.

   a. Specify your Base DN. Locate the following line (or create it if it does not exist):

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

   where `<domain>` and `<extension>` are, respectively, the domain and TLD of your LDAP server.

   The Base DN for OpenLDAP should always be two dc's in length. For example, if your full domain is `vm.fatwire.com`, your Base DN would be `fatwire.com`, and your `BASE` line would look as follows:

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

   b. Specify your URI(s). Locate the following line (or create it if it does not exist):

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

   Enter the host names and/or IP addresses on which on which OpenLDAP is to listen for connections. Separate the entries with spaces. For example:

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

2. Edit the `sldapd.conf` file as follows:

> **Note**
>
> If you installed OpenLDAP manually by following the steps in the previous section, `sldapd.conf` is located in `/usr/local/etc`.

   a. Locate the following section:

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

   and replace it with:

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

where `<domain>` and `<extension>` are the values you specified in step 1a.

b. Specify your suffix. Locate the following line (or create it if it does not exist):

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

where `<domain>` and `<extension>` are the values you specified in step 1a.

c. Specify your Root DN user. (The Root DN user is used to access the LDAP Server.) Locate the following line (or create it if it does not exist):

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

Enter `Manager` as the user name and replace `<domain>` and `<extension>` with the values you specified in step 1a.

d. Specify a password for the Root DN user. Locate the following line (or create it if it does not exist):

```
rootpw<password>
```

> **Note**
>
> The password can be either encrypted or unencrypted. (Encrypted passwords start with `{SSHA}`). If you wish to use an encrypted password, do the following:
>
> 1. Generate an encrypted password (hash) using the **`slappasswd`** command. The command generates a valid encrypted password (hash) and prints it to the terminal.
> 2. Perform step e below.

e. (Optional) If you chose to use an encrypted password in the previous step, set the password type to SHA. Locate the following line (or create it if it does not exist):

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

This sets the password type to SHA (the default). You can set other password types; see the OpenLDAP documentation for more information.

3. Edit the `core.schema` file as follows:

> **Note**
>
> If you installed OpenLDAP manually by following the steps in the previous section, `core.schema` is located in `/usr/local/etc/schema`.

a. Locate the following section:

```
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. Comment the section out by placing a # character at the beginning of each line. Then insert the following modified section after it:

```
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 ))
```

The difference between the original and modified sections is the last line:

`MUST ( uniqueMember $ cn )` becomes `MUST ( cn )`

OpenLDAP is now configured.

Adding Content Server Schema to OpenLDAP

This section shows you how to add Content Server schema to your OpenLDAP server.

Note

If you are copying the contents of the sample LDIF file below, make sure to insert an empty line between `dn` sections and at the end of the file.

To configure OpenLDAP for Content Server

1. Create an LDIF file named `pre_cs_openldap.ldif` with the following contents:

```
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
```

   where `<domain>` and `<extension>` are the values you specified in step a on page 230.

   The file will create a new organization (`fatwire`) containing two sub-organizations (`Groups` and `People`) and the `Manager` user. The `Manager` user will be used to access the LDAP server.

2. Add the `pre_cs_openldap.ldif` file to your OpenLDAP server. Execute the following command:

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

   where:

- `<domain>` and `<extension>` are the values you specified in step a on page 230.
- `<root_dn_password>` is the Root DN user password you specified in step d on page 231.

3. Test your OpenLDAP server. Execute the following command:

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

where `<domain>` and `<extension>` are the values you specified in step a on page 230.

An example response from the **`ldapsearch`** command looks as follows:

```
# 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
```

If the `pre_cs_openldap.ldif` file was successfully inserted into the LDAP server, the `result:` line indicates `success`, at which point you are ready to run the Content Server LDAP integrator. For instructions, see the CS-LDAP integration guide.

Modifying User Passwords

When you ran the Content Server LDAP integrator, all Content Server users (except `fwadmin`, `ContentServer`, and `DefaultReader`) were assigned the password which you entered in the "Content Server Configuration" screen. For security reasons, you might want to manually assign unique passwords to those users.

Note

If you chose to use encrypted passwords when you configured OpenLDAP, you **must** change the passwords for all users on your CS system, or your Content Server installation will not function properly. This is because the CS LDAP integrator writes user passwords into OpenLDAP as plaintext, but OpenLDAP expects password hashes.

The following table shows the passwords you must assign to your Content Server users:

User	Password
`DefaultReader`	`SomeReader`
`ContentServer`	The password you supplied during CS installation
`fwadmin`	The password you supplied during CS installation
All other users on your CS system	The password you supplied during CS LDAP integration

This section covers the following methods for changing passwords in OpenLDAP:

- Modifying User Passwords Using an LDAP Browser
- Modifying User Passwords Using the ldapmodify Command

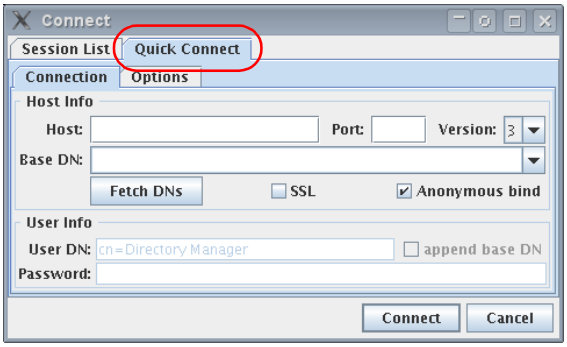
Modifying User Passwords Using an LDAP Browser

This section shows you how to modify user passwords using the free LDAP Browser/Editor program available at `http://www-unix.mcs.anl.gov/~gawor/ldap/`.

To modify user passwords in OpenLDAP using an LDAP browser

1. Download and install the LDAP browser.
2. Start the LDAP browser: **`./lbe.sh`**

3. Click the **Quick Connect** tab.

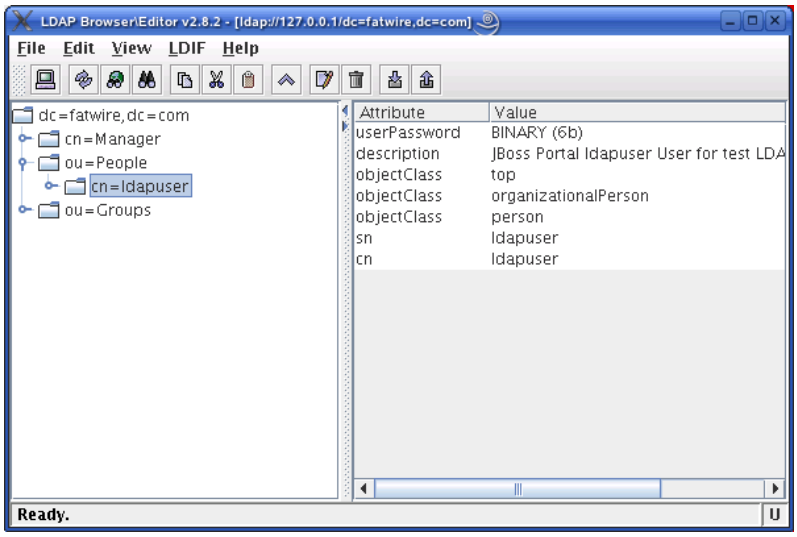


4. Fill out the fields as follows:

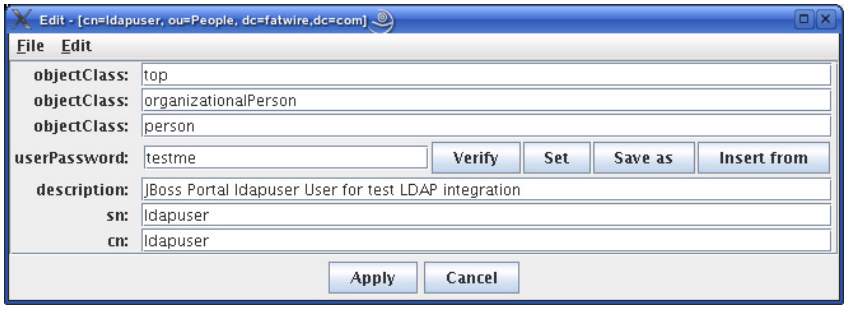
Field	Value
Hostname	The host name of your OpenLDAP server.
Port	**389**
Version	**3**
Base DN	The Base DN you specified in step a on page 230.
Anonymous bind	**Yes** (select check box)
User DN	**cn=Manager**
Append base DN	**Yes** (select check box)
Password	The Root DN user password you specified in step d on page 231.

5. Click **Connect**.

6. In the left-hand tree, expand the **ou=People** node.



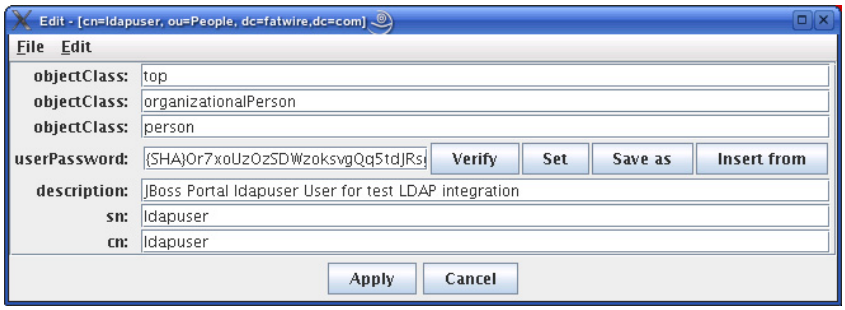
7. Double-click the user whose password you want to change and press **Ctrl-E**.
8. The plaintext password written by the CS LDAP integrator appears in the **userPassword** field. Click **Set**.



9. In the pop-up window, enter the user's password and click **Set**.

The password appears in its encrypted form.

10. Click **Apply** to save the new password.



11. Repeat steps 7–10 for each user whose password you want to change. When you are finished, test your integration by logging in to Content Server.

Modifying User Passwords Using the ldapmodify Command

The **ldapmodify** command provides you with an interface in which you can enter valid LDIF statements to make changes to the configuration of your OpenLDAP server. This section shows you how to use the **ldapmodify** and **sldappasswd** commands to change the passwords of LDAP users.

To modify user passwords in OpenLDAP using the ldapmodify command

1. Generate an encrypted password for each user. Run the **sldappasswd** command and enter the plaintext password which you want to encrypt. The command outputs the encrypted password (hash) to the terminal. For example:

   ```
   {SSHA}ydUT5RCpBAU80P0PW8gaHnsmYmLlmUL8
   ```

   Note

   If you are generating hashes for a large number of users, it is a good idea to store the hashes in a file, so that you can easily retrieve them in step 3. When you finish this procedure, make sure that you destroy the file in which the hashes are stored.

2. Execute the **ldapmodify** command as follows:

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

   where:

   - <domain> and <extension> are the values you specified in step a on page 230.
   - <root_dn_password> is the Root DN user password you specified in step d on page 231.

   When the command returns a blank line, you are ready to input LDIF statements.

3. Change the user's password. Issue the following commands:

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

      where user_name is the user name of the user whose password you want to change, and <domain> and <extension> are the values you specified in step a on page 230.

   b. **changetype:modify**

   c. **replace:userPassword**

   d. **userpassword:<password_hash>**

      where <password_hash> is the hash generated by the **sldappasswd** command in step 1 of this procedure.

   e. Press **Ctrl+D**.

   f. Repeat steps a–e for each user whose password you want to change. When you are finished, press **Ctrl+C** to terminate the **ldapmodify** command.

Chapter 16

Setting Up the WebLogic 9.*x* Embedded LDAP Server

This chapter provides instructions on setting up the currently supported WebLogic Embedded LDAP Server for use with Content Server.

Note

You must set up WebLogic LDAP **before** you run the CS LDAP integrator.

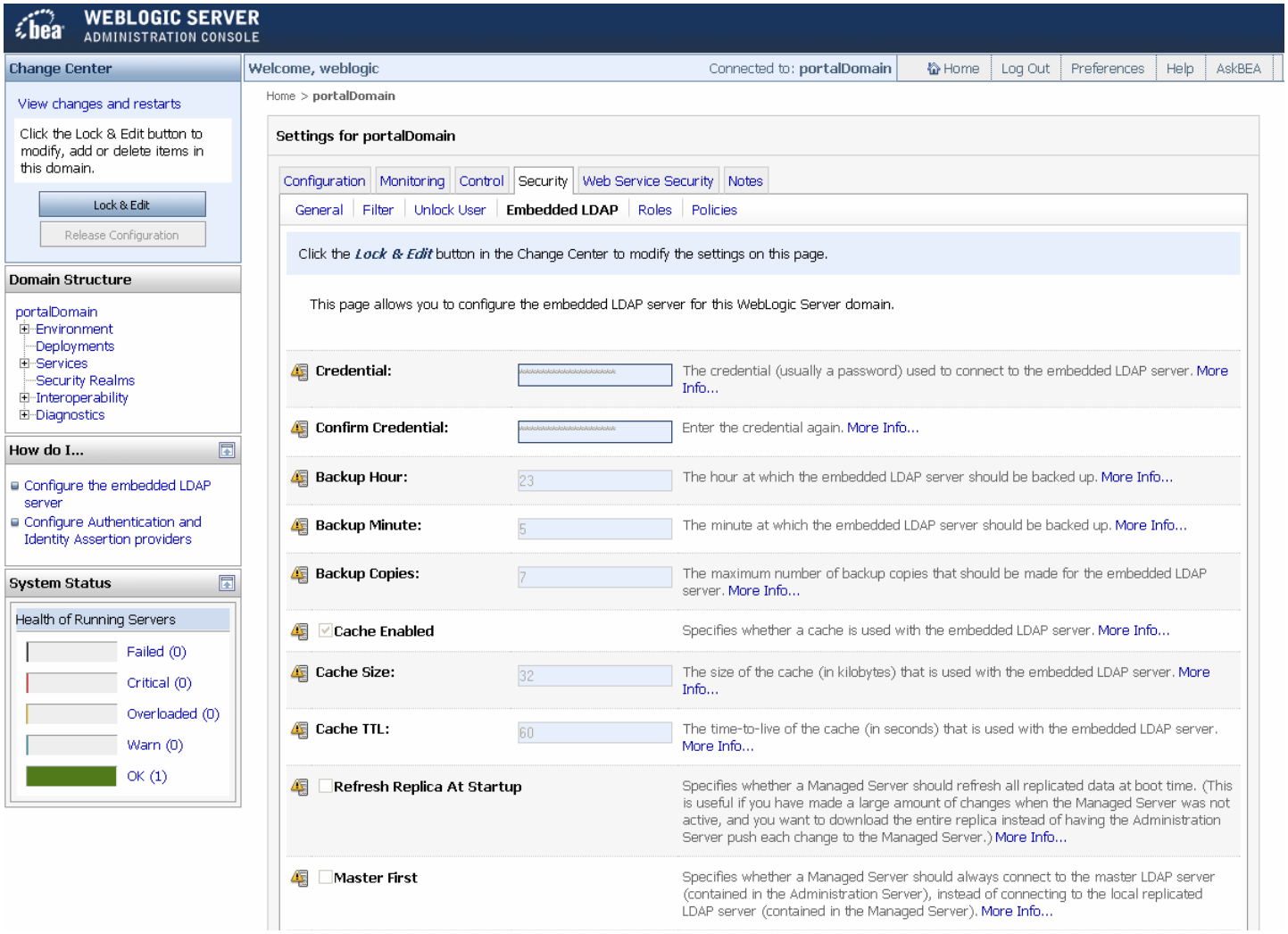
This chapter contains the following sections:

Enabling the WebLogic Embedded LDAP Server

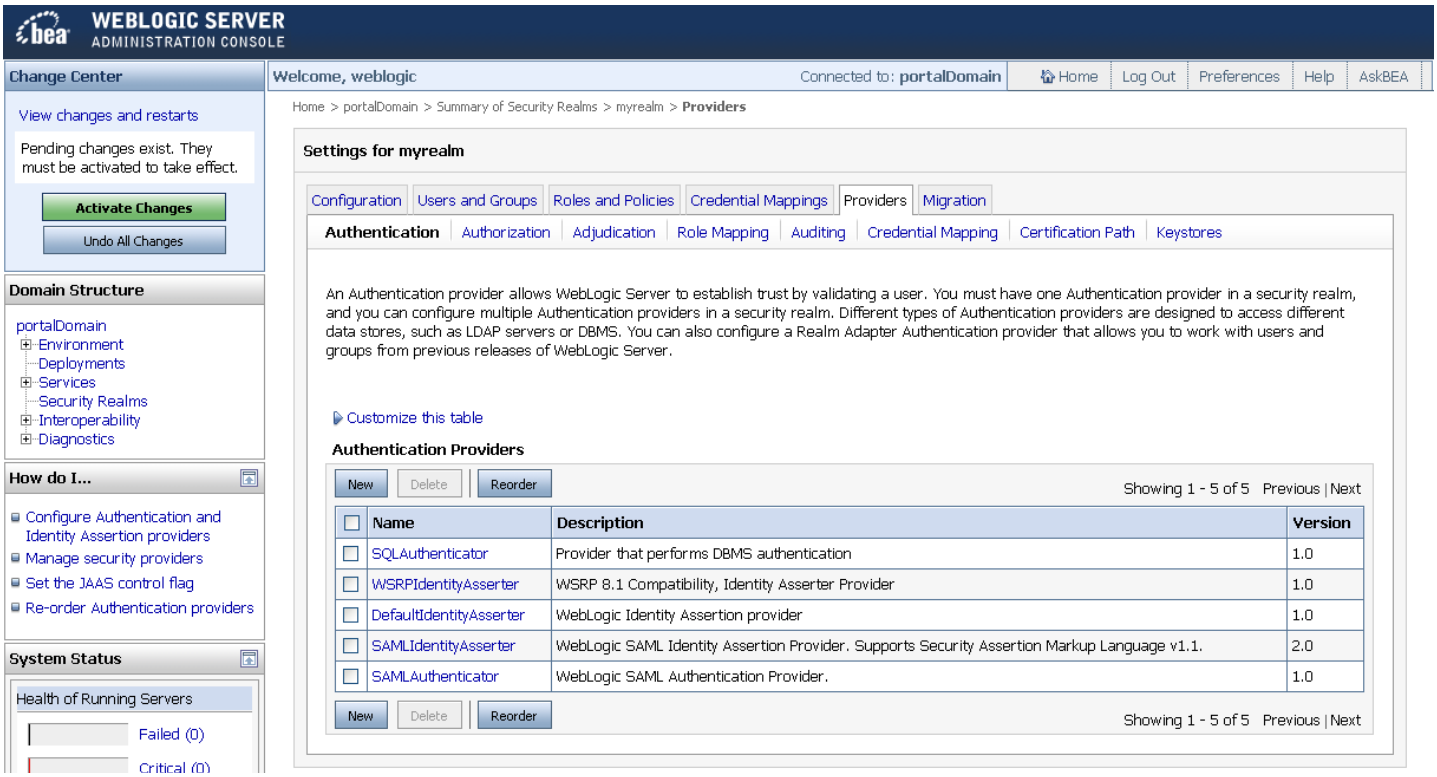
This section explains how to enable the WebLogic Embedded LDAP Server.

To enable the WebLogic Embedded LDAP Server

1. Log in to the WebLogic Server Administration Console.
2. In the "Domain Structure" tree at the left, click your WebLogic portal domain.
3. Set the Embedded LDAP password:
   a. In the workspace, select the **Security** tab, then select the **Embedded LDAP** sub-tab.
   b. In the "Change Center" pane in the upper left, click **Lock & Edit**.
   c. In the **Credential** field, enter the desired Embedded LDAP password. Reenter the password in the **Confirm Credential** field for verification.
   d. Click **Save**.



4. Create an Embedded LDAP authentication provider:
   a. In the “Domain Structure” tree, click **Security Realms**.
   b. In the workspace, click **myrealm** and select the **Providers** tab.



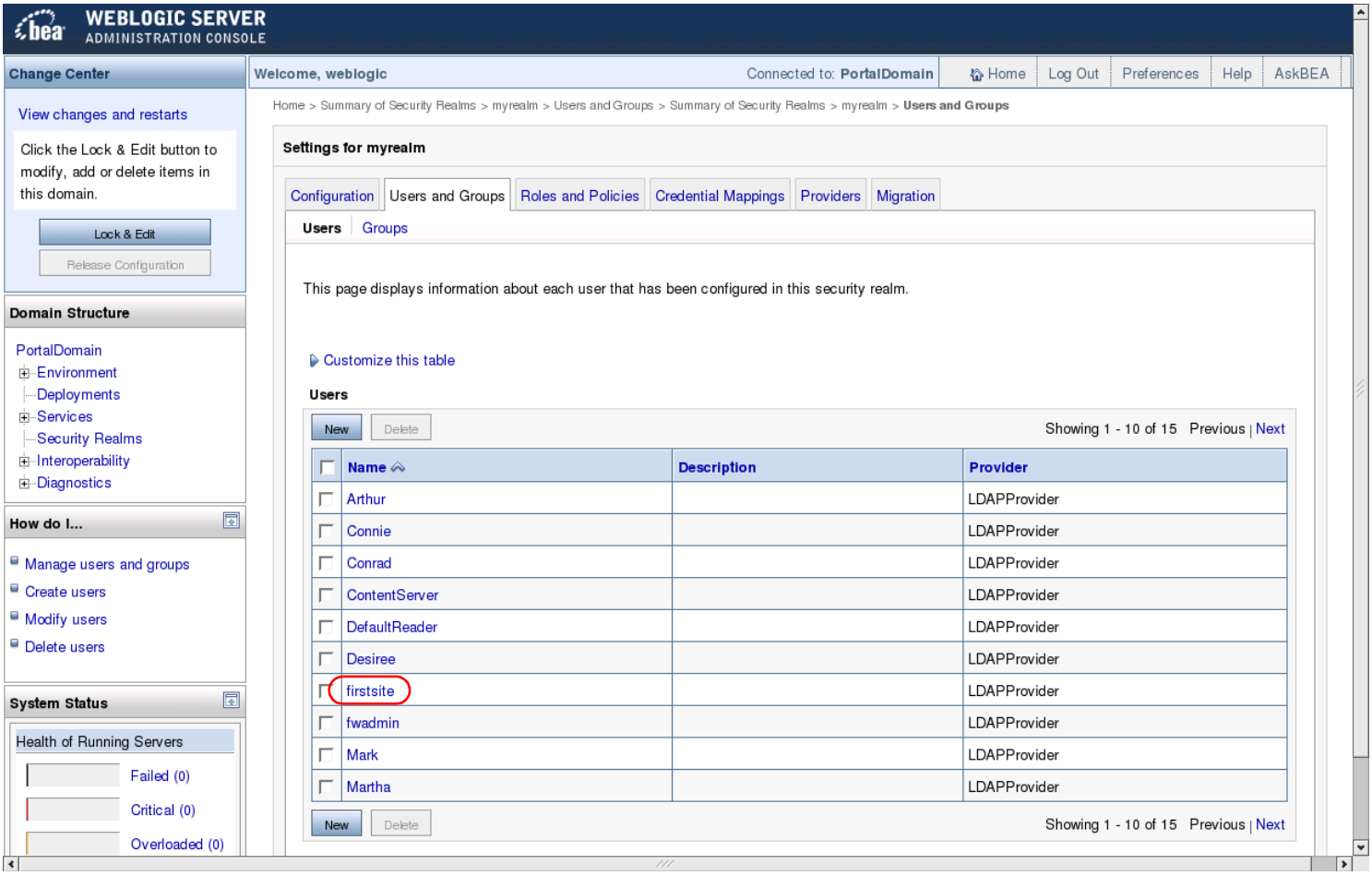
   c. Click **New**.
   d. In the **Name** field, enter a name for the authentication provider.
   e. In the “Type” drop-down list, select **DefaultAuthenticator**.
   f. Click **OK**. The new authentication provider appears in the provider list.
5. In the “Change Center,” Click **Activate Changes**.
6. Stop the admin server.

Modifying User Passwords

This section shows you how to modify user passwords in WebLogic LDAP Server.

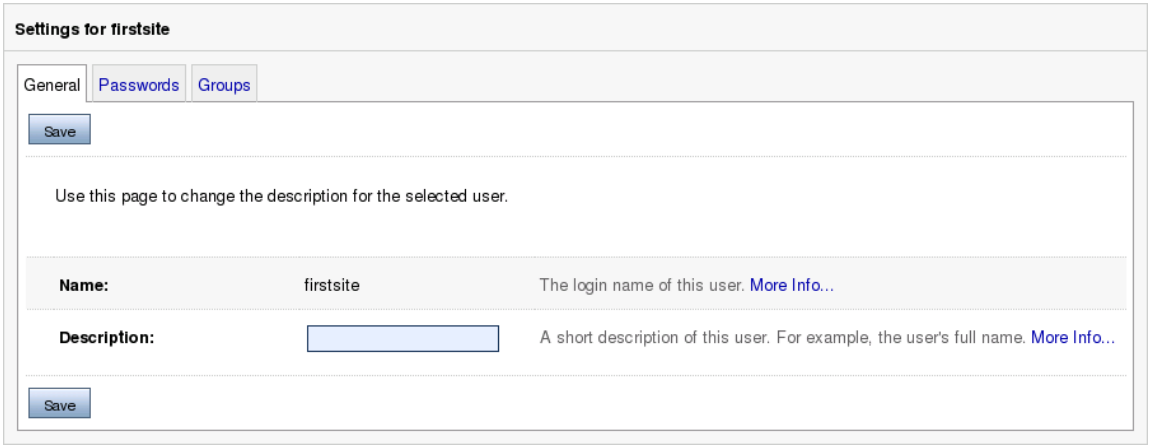
To modify user passwords in WebLogic LDAP Server

1. Log in to the WebLogic Server Administration Console.
2. In the "Domain Structure" tree, click **Security Realms**.
3. In the workspace, click **myrealm** and select the **Users and Groups** tab.

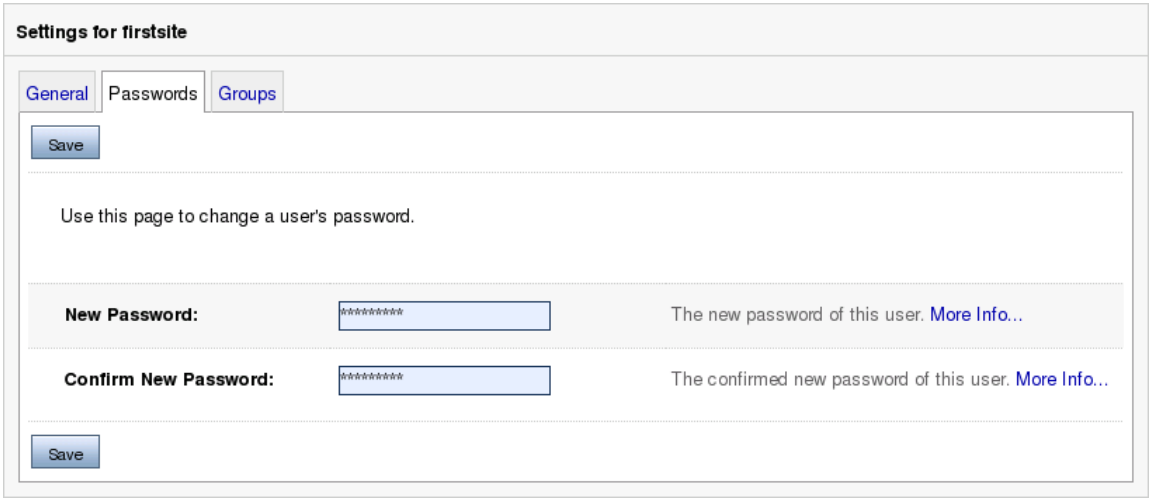


4. Click the user whose password you want to change.

The workspace displays the "Settings for *user name*" screen:

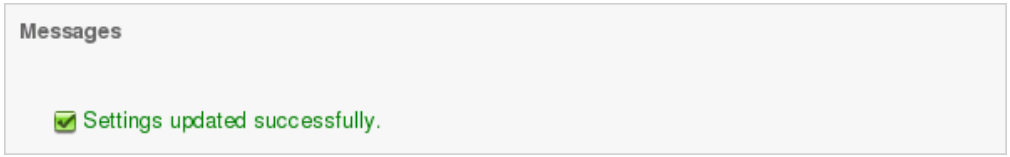


5. Select the **Passwords** tab and enter the new password into both fields.



6. Click **Save**.

   A confirmation message appears.



Chapter 17

Setting Up Oracle Directory Server 10.x

This chapter provides instructions for setting up the currently supported version of Oracle Directory Server (ODS) for use with Content Server.

Note

You must set up ODS **before** you run the CS LDAP integrator.

This chapter contains the following sections:

Start/Stop Commands

This section lists commands for starting and stopping Oracle Directory Server.

- To start:

  <oracle_home>/opmn/bin/opmnctl startproc ias-component=OID
- To stop:

  <oracle_home>/opmn/bin/opmnctl stopproc ias-component=OID

Installing Oracle Directory Server

This section shows you how to install Oracle Directory Server for use with Content Server.

A. Pre-Installation Steps

Complete these steps before installing Oracle Directory Server.

1. Download the following packages from Oracle's website:
   - Oracle Identity Management Infrastructure
   - Oracle Identity Federation
2. Create a temporary directory and decompress the installation packages to this directory using the following command:

   cpio idmv < <cpio_file>

   where `<cpio_file>` is the name of the package you want to decompress.
3. Create a new user account to run Oracle Directory Server (named `oracledir` in our example).

   Note

   If you have previously created a user to run Oracle applications on your system, skip this step. In such case, whenever the steps in the remainder of this chapter prompt you to provide the user name of your Oracle user, you must use your existing Oracle user.

   a. Create an Oracle group:

      groupadd oracledir

   b. Create an Oracle user:

      useradd -g oracledir -m -h <user_home_dir> oracledir

      where `<user_home_dir>` is the Oracle user's home directory.

   c. Set a password for the Oracle user:

      passwd oracldir

4. If you are installing on Linux, do the following (otherwise, skip this step):
   a. Add the following lines to the file `/etc/sysctl.conf`:

```
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
kernel.msgmnb=65535
kernel.msgmni=2878
kernel.sem = 256 32000 100 142
fs.file-max=131072
net.ipv4.ip_local_port_range = 1024 65000
net.core.rmem_default=262144
net.core.wmem_default=262144
net.core.rmem_max=262144
net.core.wmem_max=262144
```

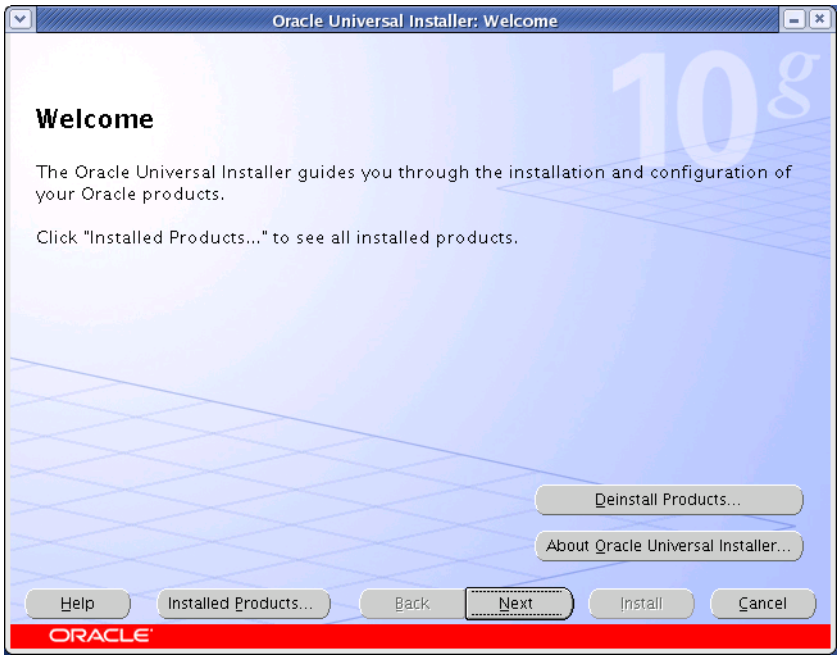
   b. Run the following command: **`sysctl -p`**
   c. Add the following lines to `/etc/security/limits.con`:

```
oracledir soft nproc 2047
oracledir hard nproc 16384
oracledir soft nofile 1024
oracledir hard nofile 65536
```

5. Log in as the Oracle user.

B. Install Oracle Directory Server

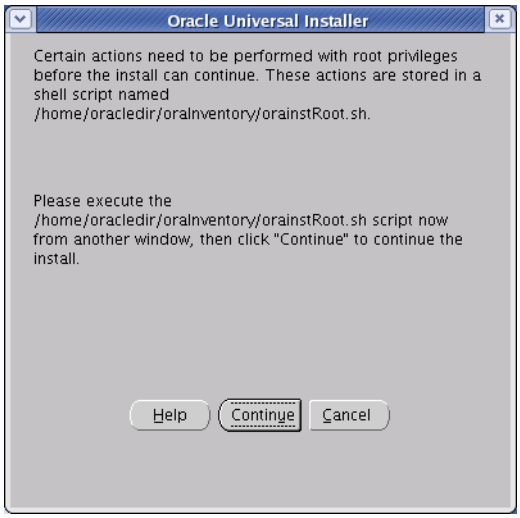
1. Complete the pre-installation steps listed in "A. Pre-Installation Steps," on page 246 if you have not already done so.
2. Change to the temporary directory into which you decompressed the Oracle Directory Server packages. Within the temporary directory, change to the `Disk1` subdirectory.
3. Start the installer: **`./runInstaller`**
4. In the "Welcome" screen, click **Next**.



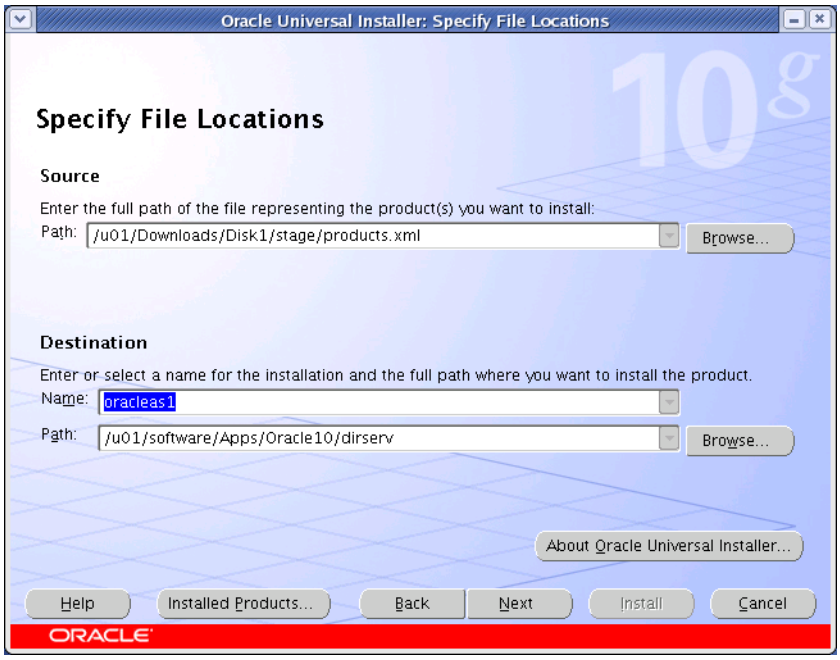
5. If no other Oracle products have been previously installed on this computer, do the following (otherwise, skip this step and continue to step 6 on page 250):

   a. In the “Specify Inventory Directory and Credentials” screen, specify the location of the Oracle inventory directory and specify the system group of your Oracle user, then Click **Next**.

   b. When the following pop-up dialog appears, run the requested script as the `root` user, then click **Continue**.

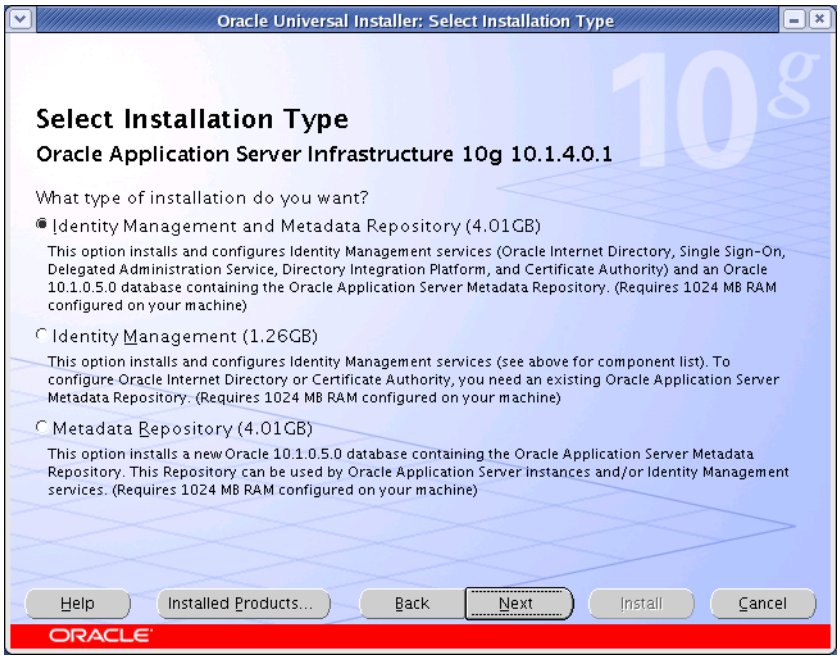


6. In the “Specify File Locations” screen, confirm the path and name of the destination directory, then click **Next**.



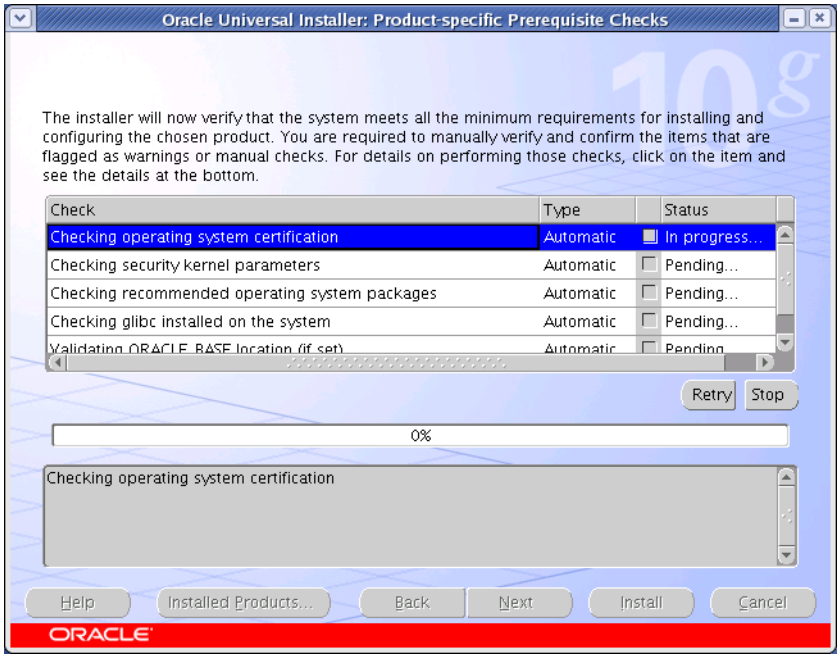
7. In the “Select a Product to Install” screen, select the **Oracle Application Server Infrastructure** radio button and click **Next**

8. In the "Select Installation Type" screen, select the **Identity Management and Metadata Repository** radio button and click **Next**.

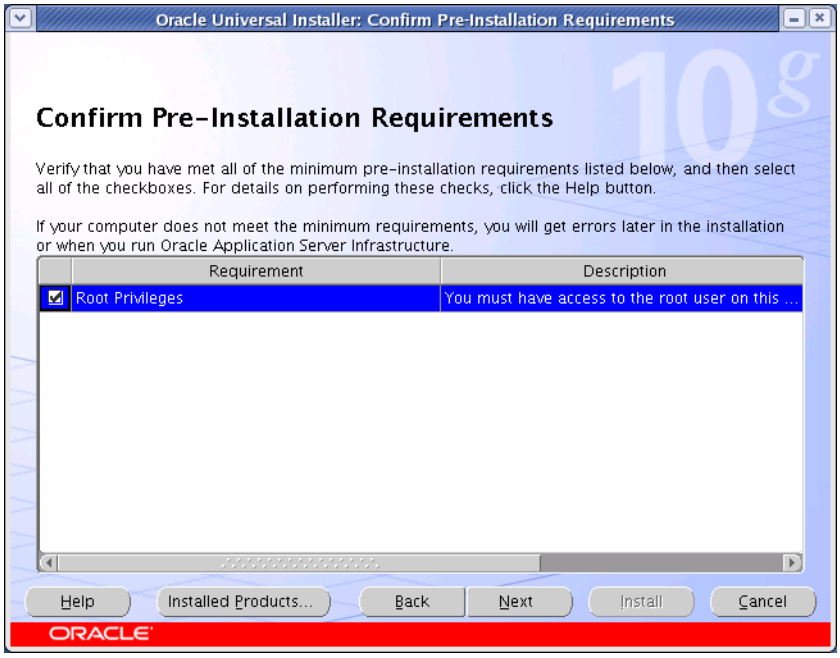


9. In the next screen, allow the prerequisite check to complete. If any checks fail, resolve the issue before continuing. When all checks report as successful, click **Next**.

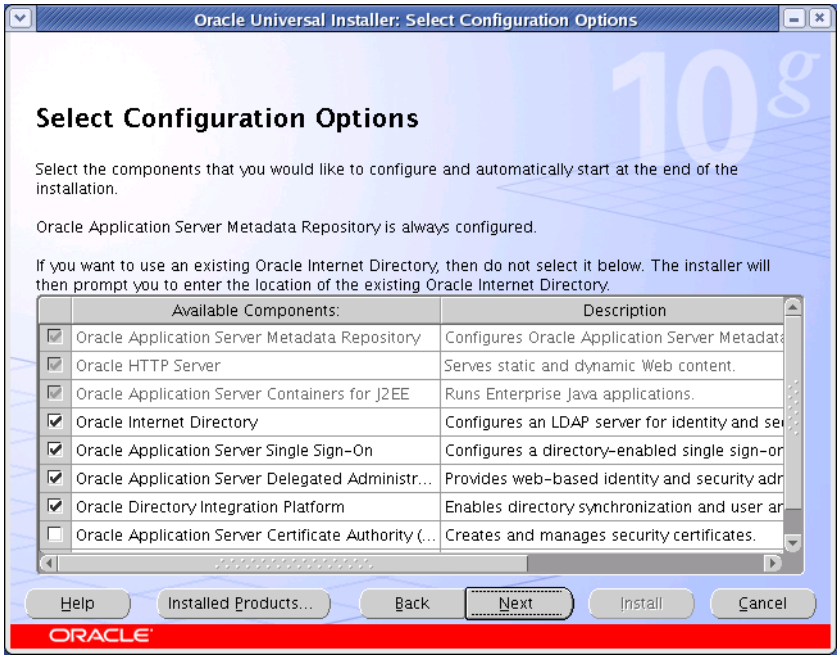
> **Note**
>
> If you see a dialog warning you that port `1521` is in use by an Oracle 10.x component, click **OK**. If the dialog reports that an application other than an Oracle 10.x component is using port `1521`, you must remedy the situation by following the instructions shown in the dialog before continuing.



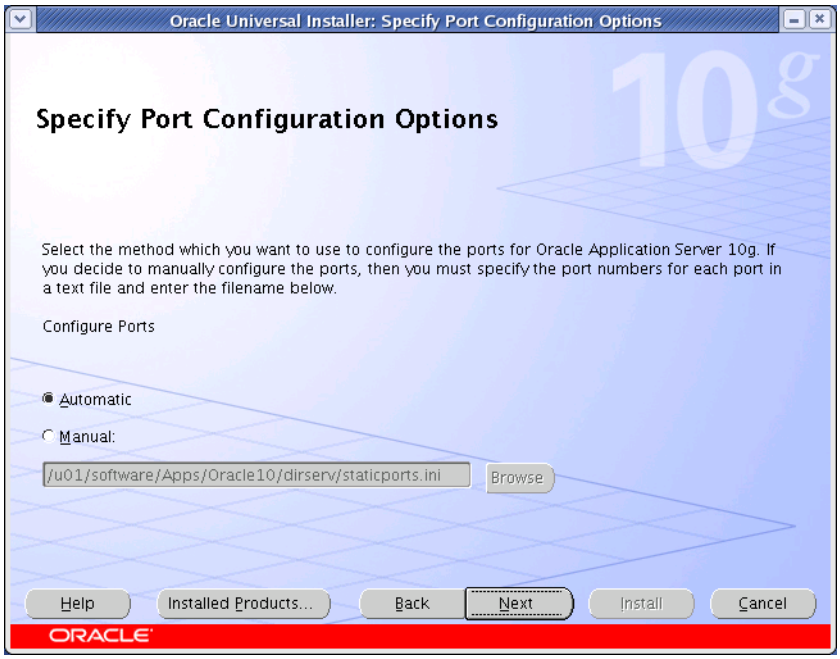
10. In the “Confirm Pre-Installation Requirements” screen, select the check boxes for all items in the list, then click **Next**.



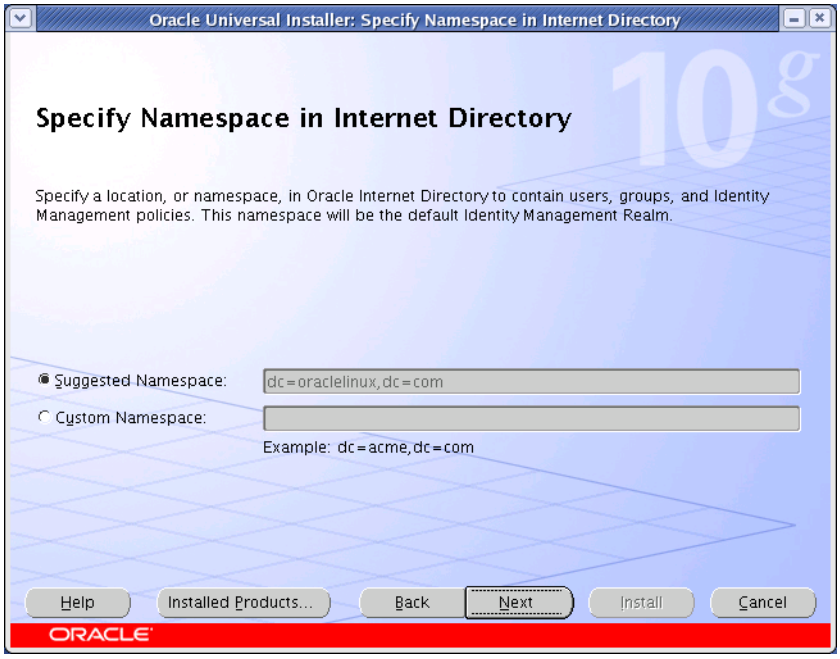
11. In the “Select Configuration Options” screen, click **Next** without making any changes.



12. In the "Specify Port Configuration Options" screen, select **Automatic** and click **Next**.

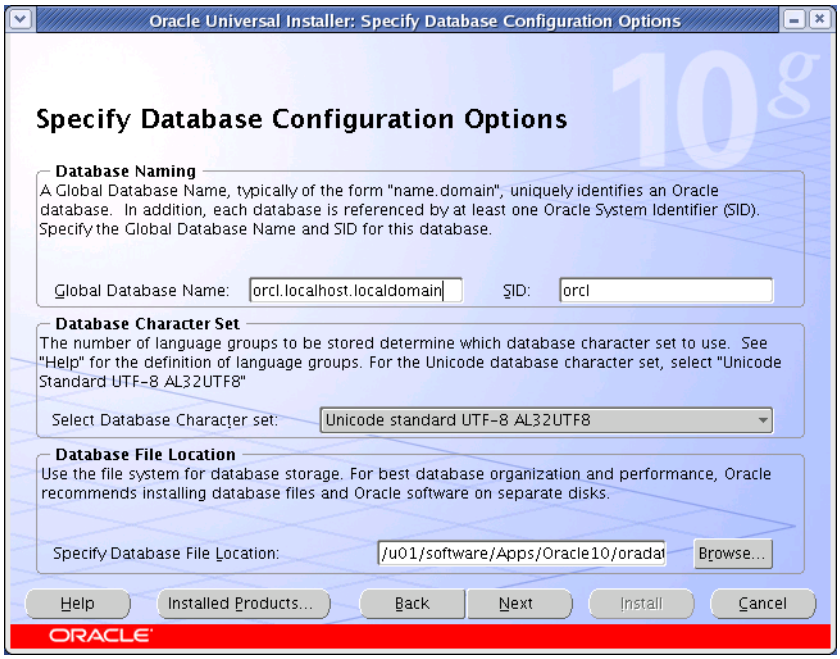


13. In the "Specify Namespace in Internet Directory" screen, select the **Suggested Namespace** radio button and make a record of the corresponding field value. Click **Next**.

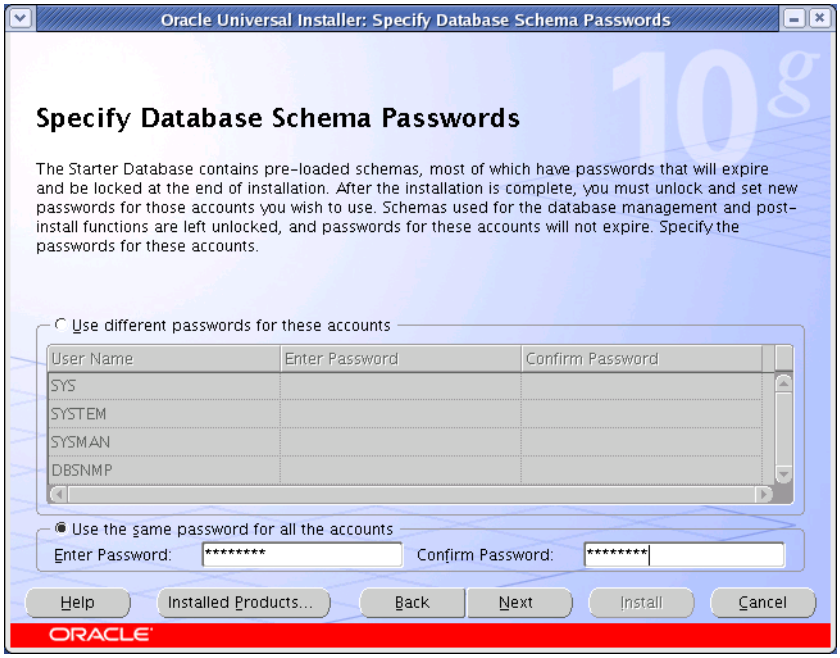


14. In the “Specify Database Configuration Options” screen, enter the required database information, then click **Next**. Make a record of the values you enter.

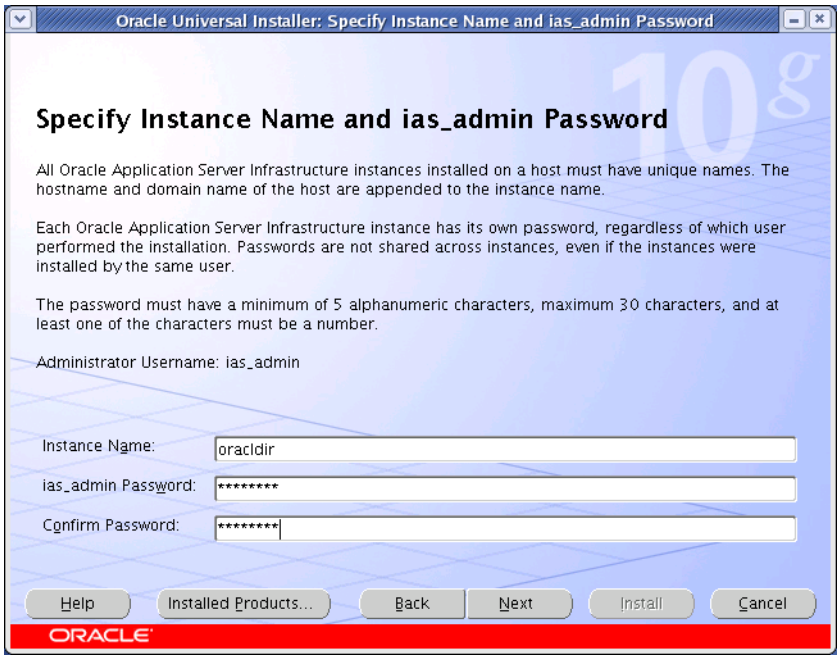
> **Note**
>
> If an Oracle database server resides on this machine, the installer will populate the fields in this screen automatically. However, FatWire strongly suggests that you you do not use these existing values and instead specify a new, unique SID and database storage (`oradata`) directory.



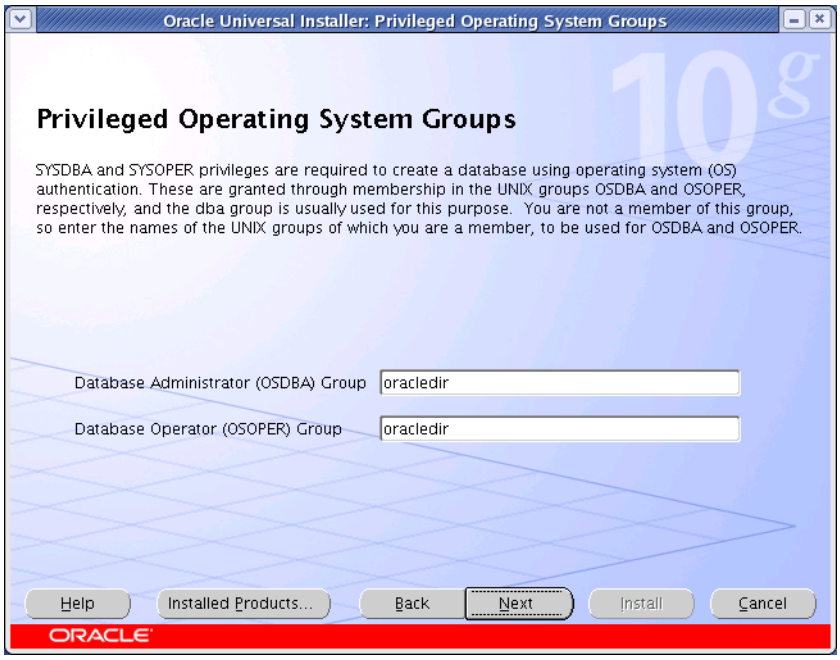
15. In the “Specify Database Schema Password” screen, select the **Use the same password for all accounts** radio button, then and enter and re-enter the desired password. Make a record of this password, then click **Next**.



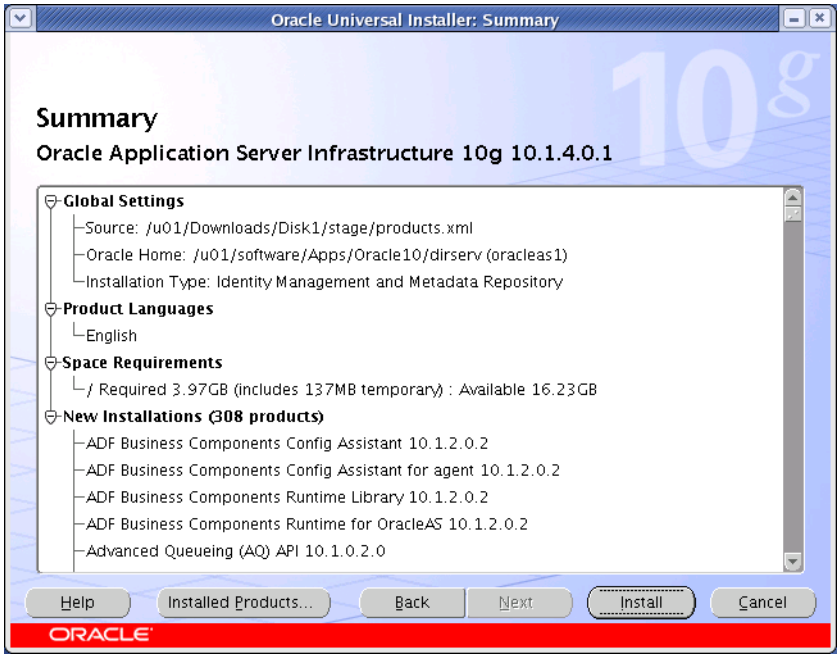
16. In the “Specify Instance Name and ias_admin password” screen, enter a unique instance name and a unique password. Re-enter the password and make a record of all values in this screen, including the administrator user name (`ias_admin`). When you are finished, click **Next**.



17. In the “Privileged Operating System Groups” screen, keep the default options and click **Next**.



18. In the “Summary” screen, review the configuration choices you have made, then click **Install**. Wait until the installation completes successfully.



19. When the following dialog appears, run the requested script as the `root` user, then click **OK**.

20. In the "Configuration Assistants" screen, allow all configuration steps to complete. If any of the steps fail, correct the indicated problem, then re-run the configuration process. When the configuration process completes successfully, click **Next**.

21. Allow the database configuration to complete.
22. In the "End of Installation" screen, click **Exit**.

Note

Make a record of the information displayed in the "Please Remember" dialog box (by copying and pasting it into a text file, for example) for future reference. Additional configuration information for your installation can be found in the file, `<ora_home>/config./ias.properties`. Specifically, look for the string, `OIDport`. This is the port on which Oracle Directory Server is listening for LDAP connections.

C. Post-Installation Steps

Complete these steps to test your Oracle Directory Server installation.

1. Test the management server:
   a. Log in to the Management Application using the following credentials:

> **Note**
>
> By default, the URL is `http://localhost.localdomain:1158/`. The URL for your system is also part of the text file you created in step 22 on page 258.

   User name: `ias_admin`

   Password: `<ias_admin_password>` (you created this password in step 16 on page 256)

   b. Log in to the Database Management Application using the following credentials:

> **Note**
>
> By default, the URL is `http://localhost.localdomain:5500/em`. The URL for your system is also part of the text file you created in step 22 on page 258.

   User name: `sys`

   Password: `<db_schema_password>` (you created this password in step 15 on page 256)

   Connect As: `SYSDBA`

2. Test the LDAP server:
   a. Change to the `<oracle_home>/bin` directory.
   b. Run the following command:

   `./ldapbind -h localhost -p <OIDport>`

   where `<OIDport>` is the port number you obtained in step 22 on page 258.

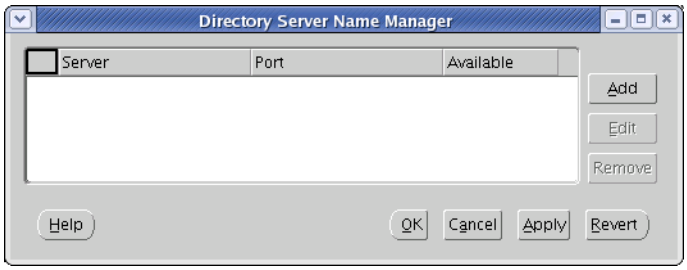
   Example output:

   ```
   bind successful
   ```

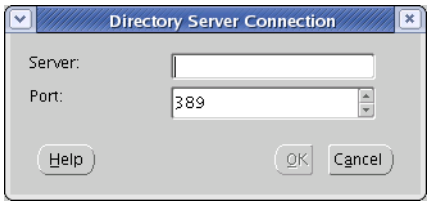
Accessing Oracle Directory Manager

1. Change to the `<oracle_home>/bin` directory:
2. Run the following command: **`./oidadmin`**
3. In the "Directory Server Connection" dialog box, click **OK**.

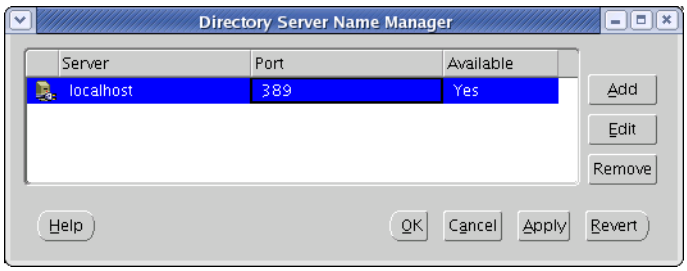
4. Add a connection entry for your Directory Server instance.
   a. In the "Directory Server Name Manager" screen, click **Add**.



   b. In the "Directory Server Connection" pop-up dialog, enter the following values, then click **OK**.
      - Server: `localhost`
      - Port: `<OIDport>` (the port number you obtained in step 22 on page 258)

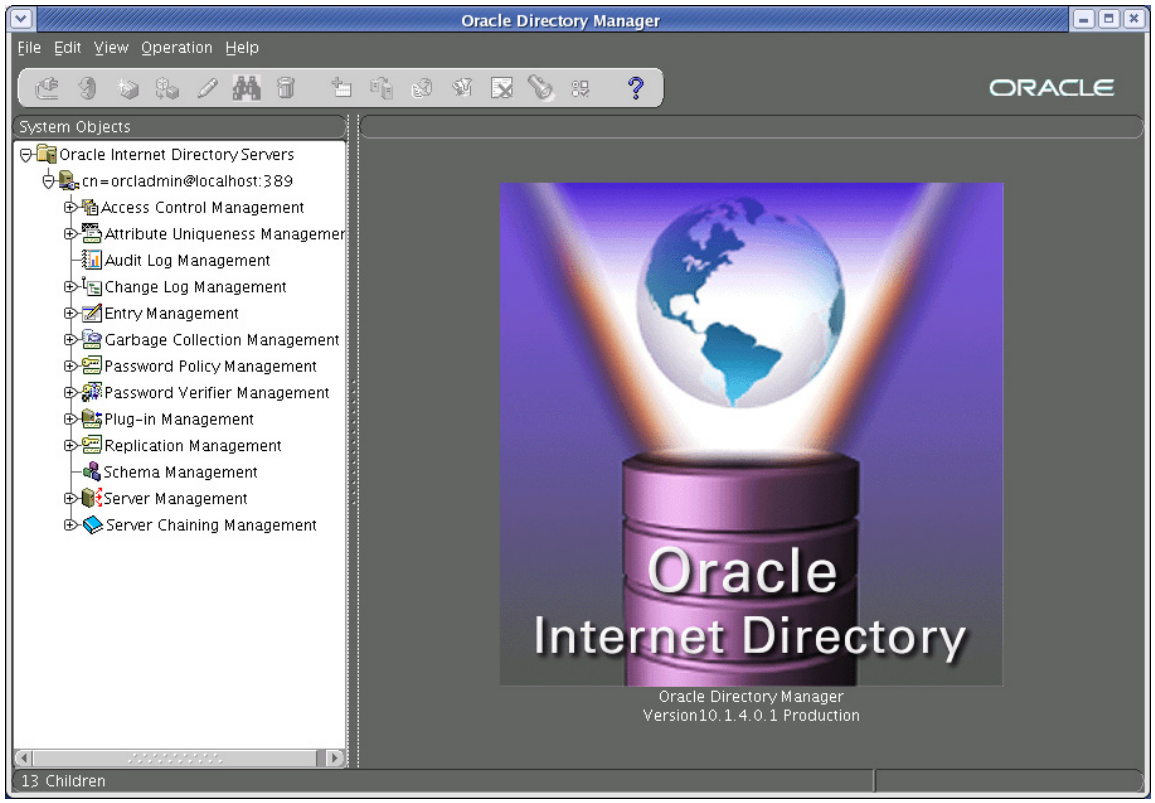


5. In the “Directory Server Name Manager” screen, select the new connection entry and click **OK**.



6. In the **Credentials** tab of the “Oracle Directory Manager Connect” screen, enter the following values:
   - **User:** `cn=orcladmin`
   - **Password:** `<db_schema_password>` (you created this password in step 15 on page 256)

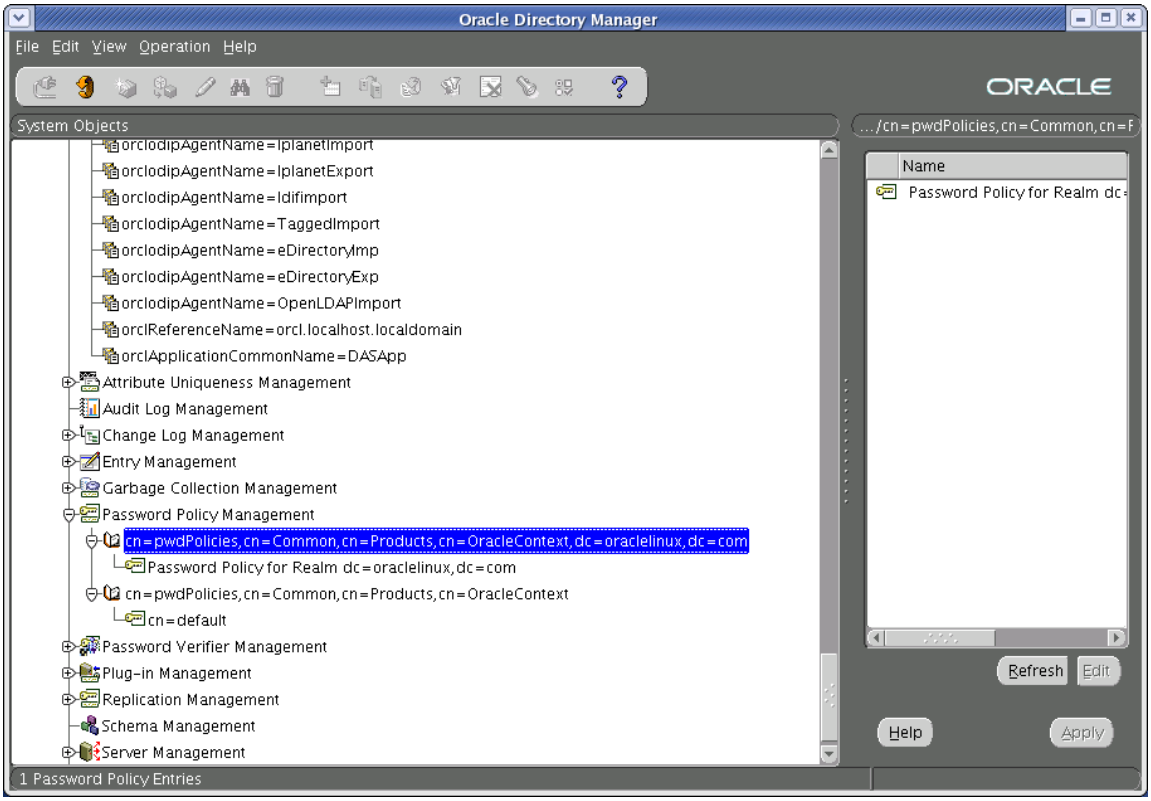
7. Click **Login**. Oracle Directory Manager loads.



Configuring ODS Password Security for Content Server

This section show you how to configure password security in Oracle Directory Server to meet Content Server's security requirements.

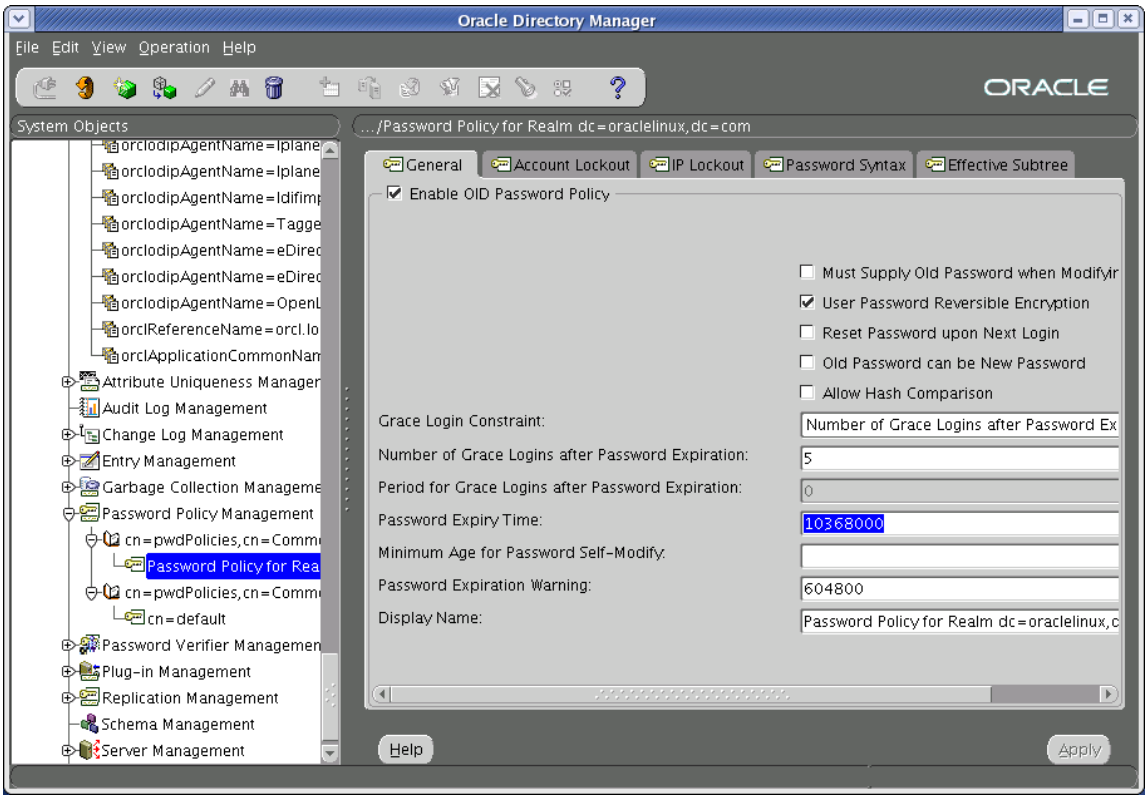
1. Log in to Oracle Directory Manager as `cn=orcladmin`. For instructions, see "Accessing Oracle Directory Manager," on page 260.
2. In the tree on the left, expand the **Password Policy Management** node, then the node containing your DN (that is, the namespace you selected in step 13 on page 254):



3. Under the node containing your DN, select the **Password Policy for Realm...** node.

4. Increase the password expiration time from 120 days to 5 years.

   In the **General** tab in the main pane, locate the "Password Expire Time" property. The default value of this property, expressed in seconds, is `10368000` (120 days). Change this value to `155520000` (5 years).



5. Select the **Password Syntax** tab.

6. Configure password syntax constraints as follows:

   a. Enable alpha-only passwords (that is, passwords that contain letters, but do not contain digits). You do this by setting the number of required numeric characters to none.

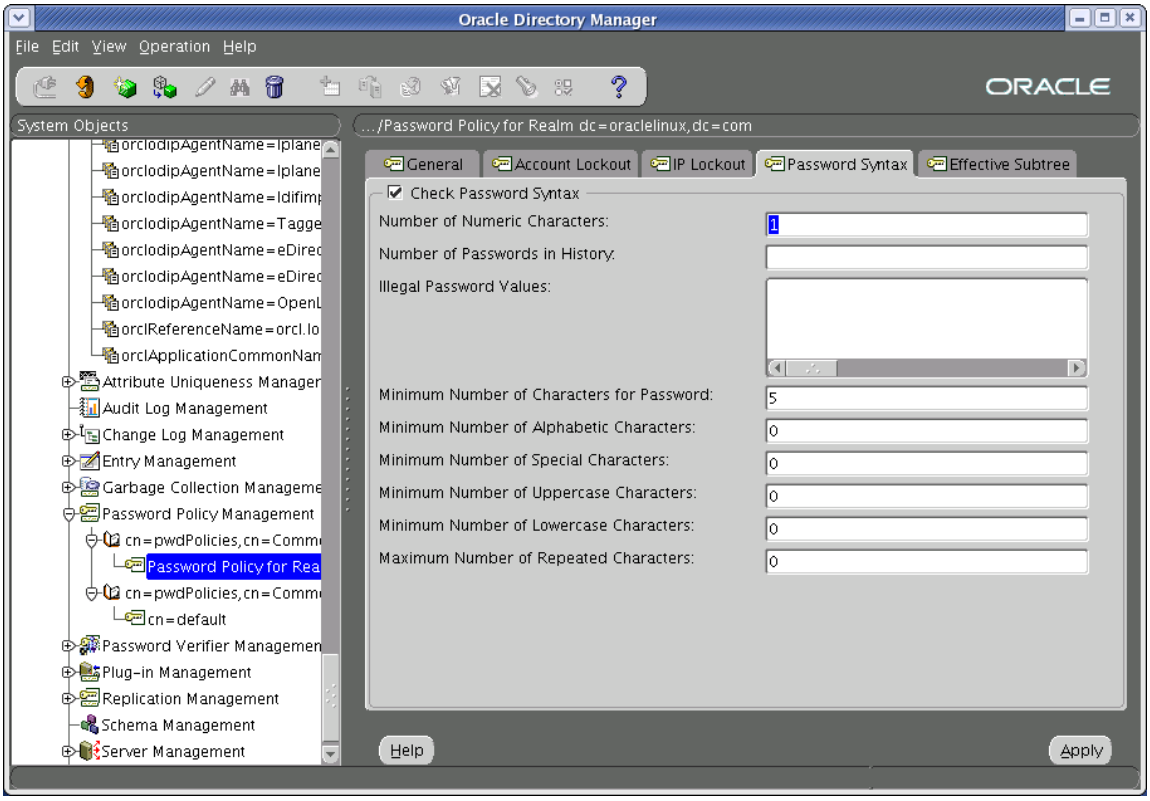
   Note

   Default Content Server passwords are alpha-only. If you are using these default passwords on your installation, you **must** enable alpha-only passwords in Oracle Directory Server.

   Locate the property named **Number of Numeric Characters** and change its value from `1` (default) to `0`.

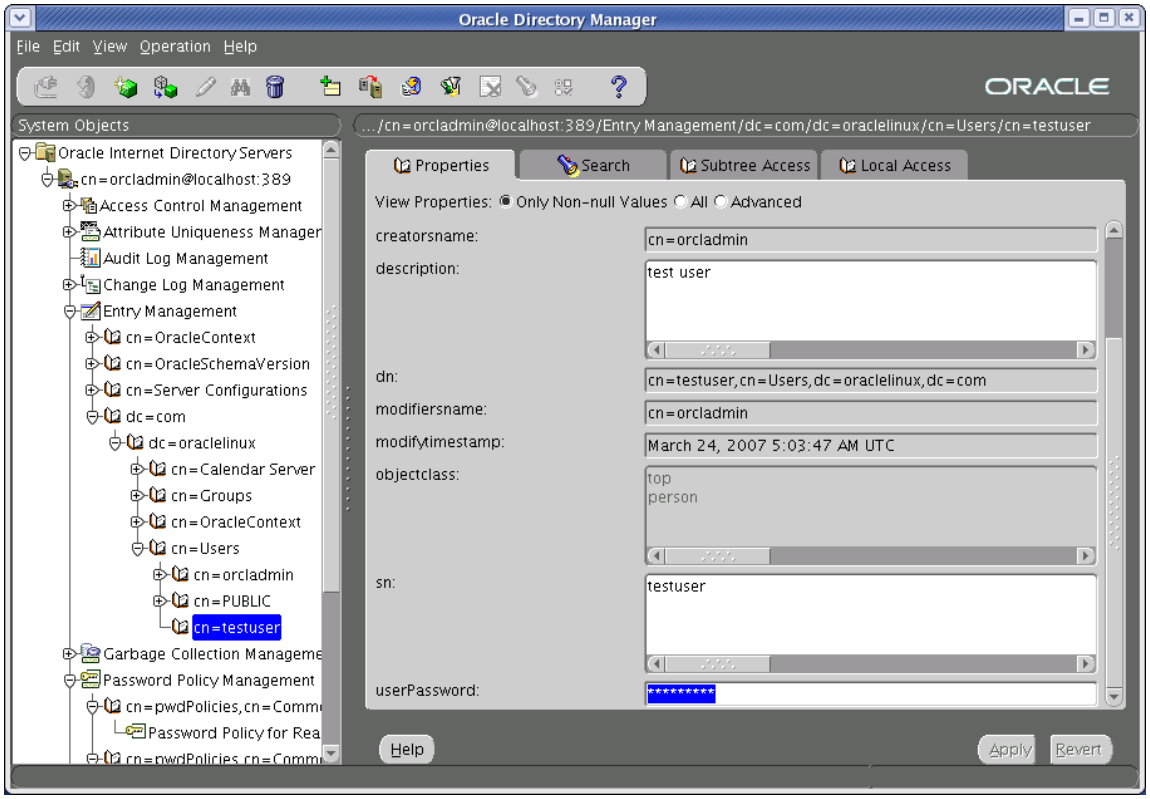
   b. Reduce the minimum password length to four characters. Locate the property named **Minimum Number of Characters for Password** and change its value from `5` (default) to `4`.

   c. Click **Apply** to save your changes.



Modifying User Passwords

1. Log in to Oracle Directory Manager as `cn=orcladmin`. For instructions, see "Accessing Oracle Directory Manager," on page 260.
2. In the tree on the left, expand the **Password Policy Management** node, then the node containing your DN (that is, the namespace you selected in step 13 on page 254).
3. Under the node representing your DN, expand the **cn=Users** node and select the user whose password you want to modify.
4. Select the **Properties** tab.
5. In the **userPassword** field, enter the new password.

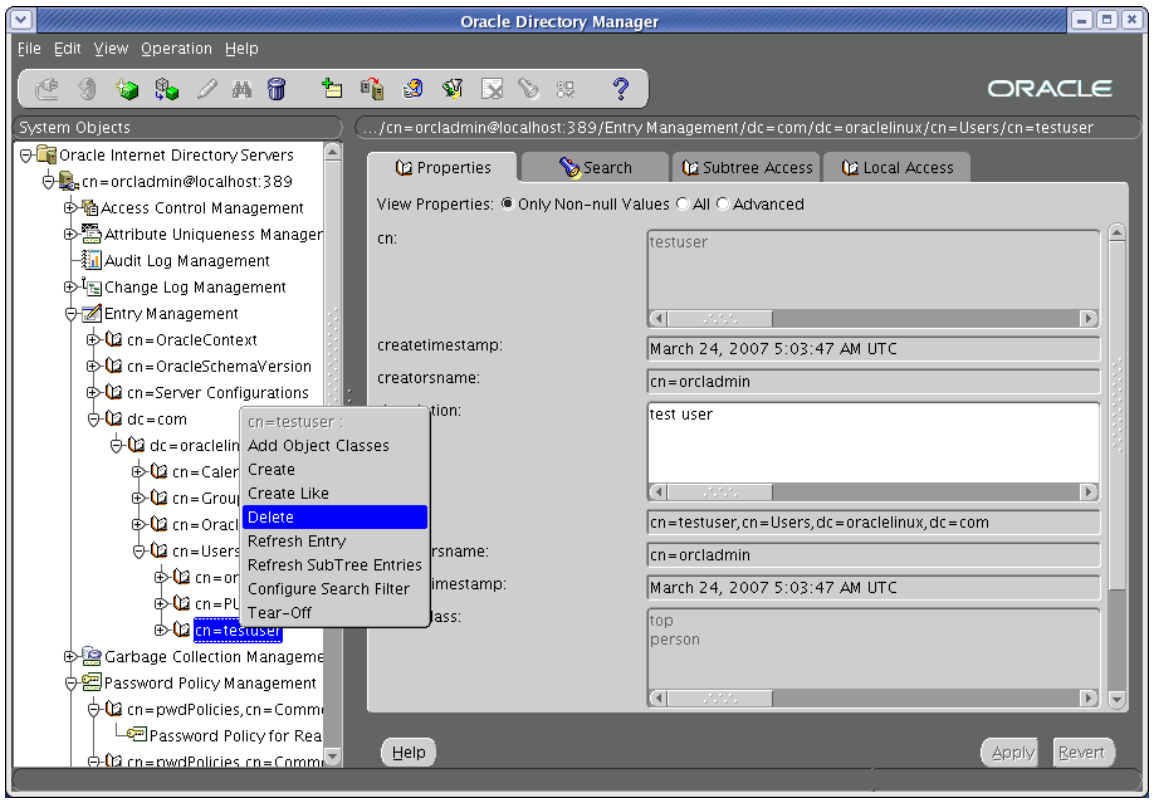


6. Click **Apply** to save your changes.

Deleting Users

This section shows you how to delete a user in Oracle Directory Server.

1. Log in to Oracle Directory Manager as `cn=orcladmin`. For instructions, see "Accessing Oracle Directory Manager," on page 260.
2. In the tree on the left, expand the **Password Policy Management** node, then the node containing your DN (that is, the namespace you selected in step 13 on page 254).
3. Under the node representing your DN, expand the **cn=Users** node and select the user you want to delete.
4. Right-click the selected user and select **Delete** from the context menu.



5. In the confirmation pop-up dialog that appears, click **OK**.

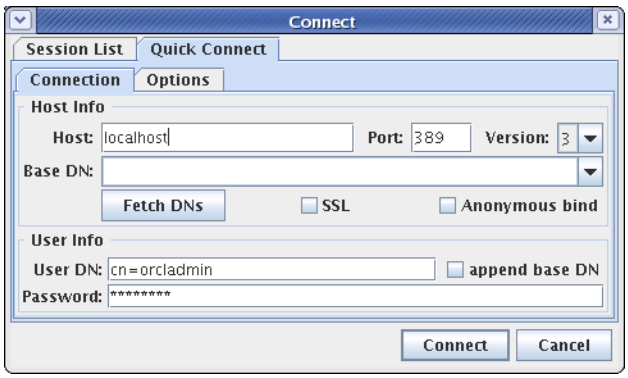
Connecting to ODS Using an LDAP Browser

This section shows you how to connect to Oracle Directory Server using an LDAP browser.

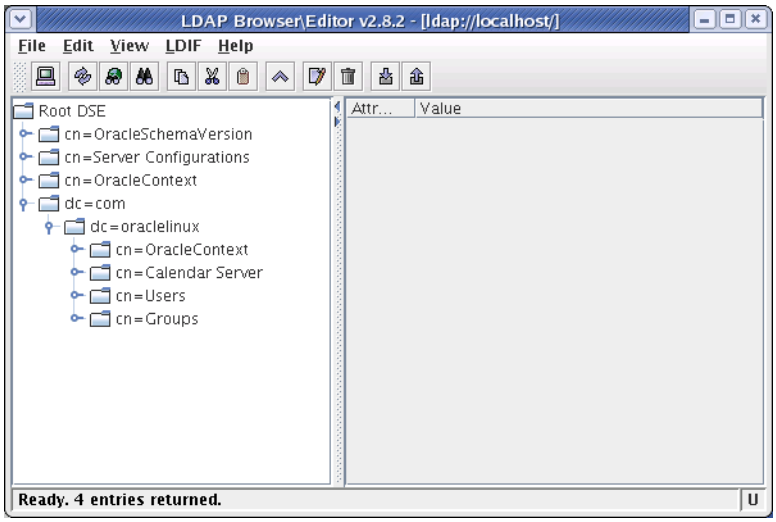
Note

You cannot add groups, set passwords, or activate accounts using an LDAP browser.

1. Open the LDAP browser.
2. Select the **Quick Connect** tab.
3. Enter the following information:
   - **Host:** `localhost` (if connecting remotely, enter the actual host name)
   - **Base DN:** leave blank
   - **Anonymous bind:** deselected
   - **User DN:** `cn=orcladmin`
   - **Append base DN:** deselected
   - **Password:** `<dbschema_password>` (you created this password in step 15 on page 256)



4. Click **Connect** to start your session.



5. Navigate to your DN (that is, the namespace you selected in step 13 on page 254).

Chapter 18

Setting Up MS Active Directory Server 2003

This chapter provides instructions for setting up the currently supported Microsoft Active Directory Server (ADS) for use with Content Server.

Note

You must set up ADS **before** you run the CS LDAP integrator.

This chapter contains the following sections:

Installing MS Active Directory Server

This section shows you how to install MS Active Directory Server 2003 for use with Content Server.

The procedure consists of the following steps:

A. Install the Operating System

On the target machine, install Windows Server 2003 (any flavor except Web will do).

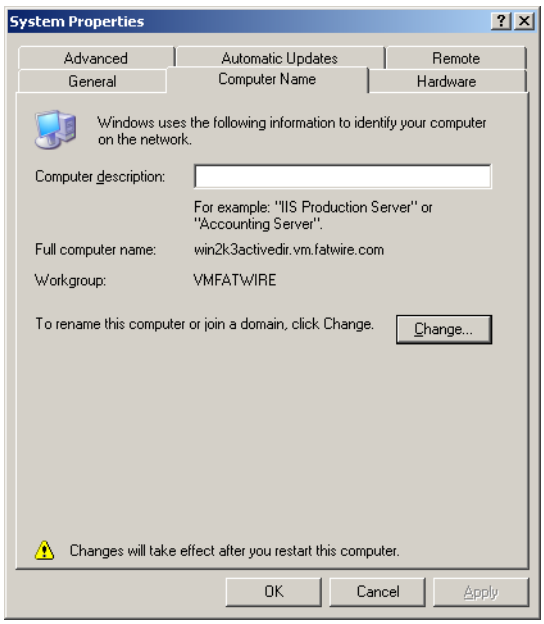
When the installation is complete, leave the installation disc in the drive – you will need it to complete the installation of ADS.

B. Set the Machine's Name and Suffix

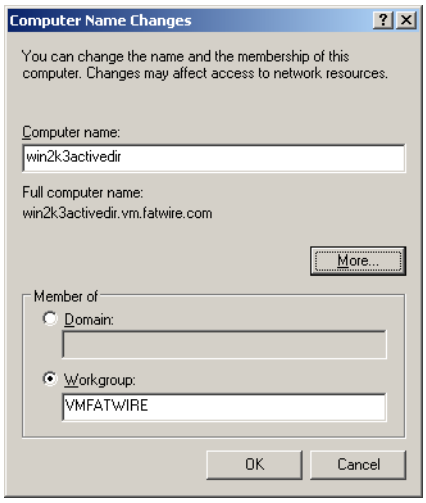
1. Open the "System Properties" dialog.

   This can be done in several ways. The fastest way is to right-click the **My Computer** icon on the desktop and select **Properties** from the context menu.

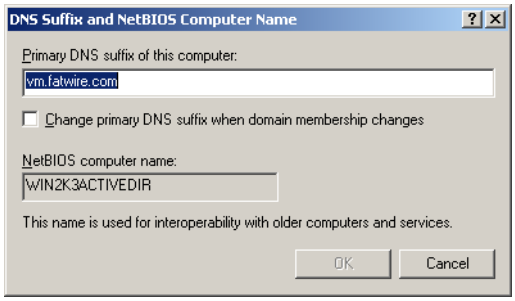
2. Select the **Computer Name** tab.
3. Click **Change**.



4. In the pop-up window that appears, do the following:
   a. Enter the desired name for this machine. Make a record of this name.
   b. Select the **Workgroup** radio button and enter a **unique** workgroup name. Make a record of this name.



   c. Click **More**.
   d. In the second pop-up window that appears, enter the DNS suffix for this machine. Make a record of this suffix.



   e. Make sure the **Change primary DNS suffix when domain membership changes** check box is **not** checked.
   f. Click **OK** to close the "DNS Suffix and NetBIOS Computer Name" pop-up window.
5. Click **OK** to close the "Computer Name Changes" pop-up window.
6. In the "System Properties" dialog box, click **OK**.
7. Restart the machine.

C. Configure the Machine's Network Settings

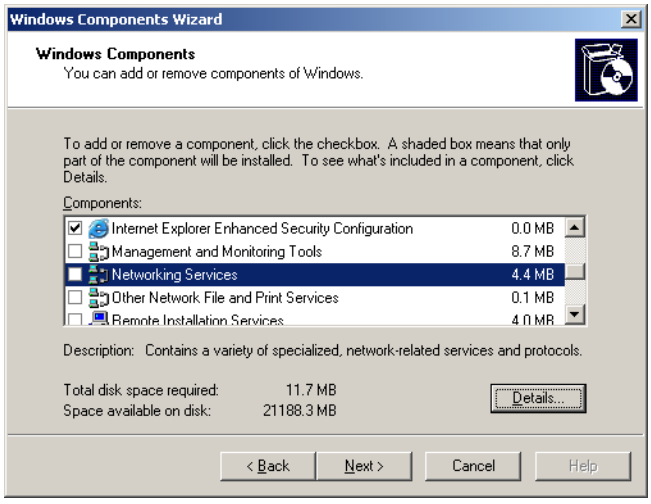
Configure the machine's network settings as follows:

1. Set the IP address to an unused static IP address.
2. Set the preferred DNS server to the machine's IP address.
3. Make sure that the **Append primary and connection-specific DNS suffixes** check box on the **Advanced** tab under **DNS** settings in the **TCP/IP Protocol** properties for the machine's network interface is selected.
4. Make sure that **Append parent suffixes of the primary DNS suffix** check box is selected.

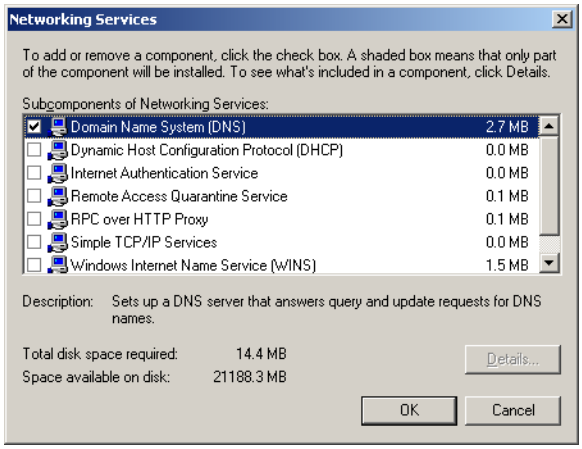
For instructions on configuring your machine's network settings, see the Windows Server 2003 documentation.

D. Install the Local DNS Server

1. Open the "Control Panel" and double-click **Add and Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. In the "Windows Components Wizard" pop-up window, select the **Networking Services** item (**not** its check box) and click **Details**.



4. In the pop-up window that appears, select the check box next to **Domain Name System (DNS)** and click **OK**. The pop-up window closes.

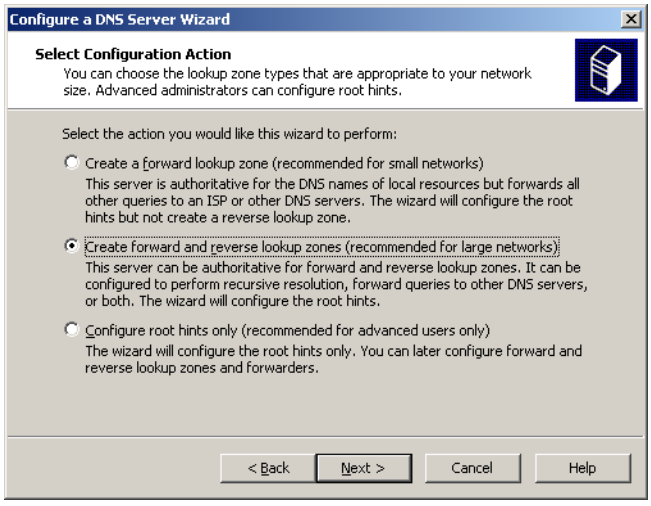


5. In the "Windows Component Wizard" screen, click **Next**.
6. When the installation completes successfully, click **Finished**.

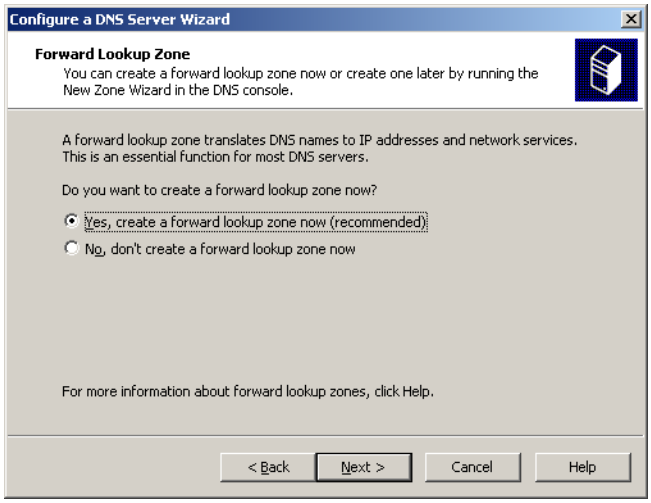
E. Configure the Local DNS Server

1. In the "Control Panel," double-click the **Administrative Tools** icon.
2. Double-click the **DNS** icon.
3. In the "dnsmgmt console," select the machine name you entered in step 4 on page 273.
4. Right-click the machine name and select **Configure this DNS Server** from the context menu.
5. In the "Configure a DNS Server Wizard" pop-up window that appears, click **Next**.

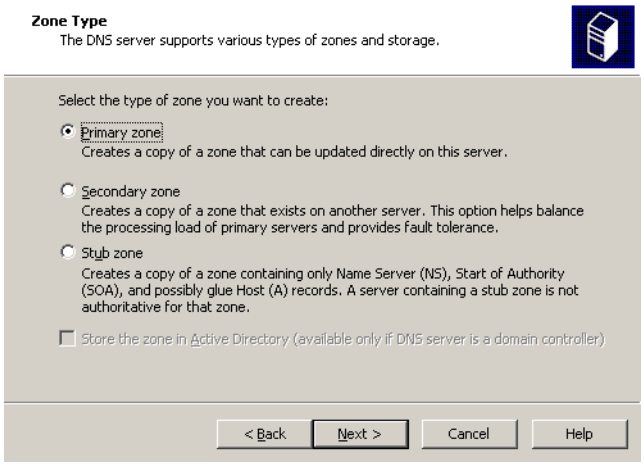
6. In the "Select Configuration Action" screen, select the **Create forward and reverse lookup zones** radio button and click **Next**.



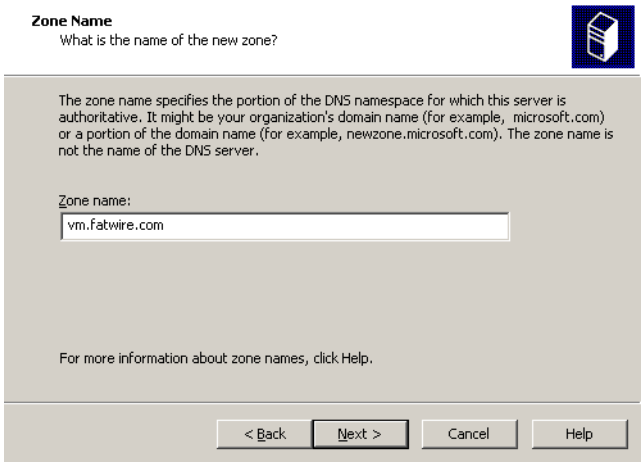
7. In the “Forward Lookup Zone” screen, select the **Yes, create a forward lookup zone (recommended)** radio button and click **Next**.



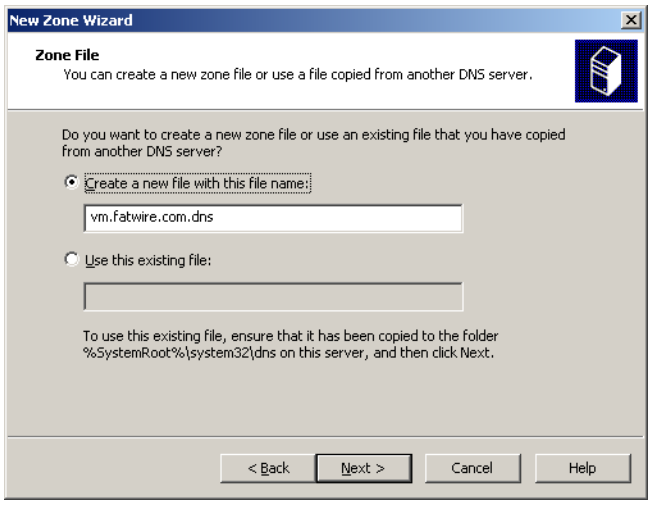
8. In the “Zone Type” screen, select the **Primary Zone** radio button and click **Next**.



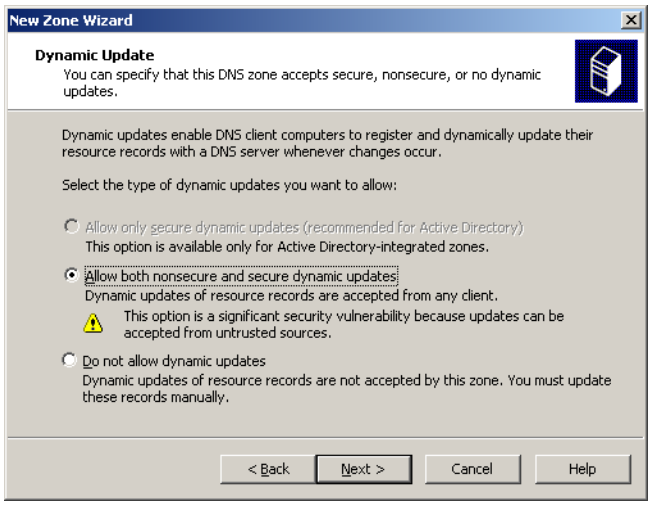
9. In the "Zone Name" screen, enter the name of the zone you are creating. The zone name is the domain suffix you entered in step d on page 273. Click **Next**.



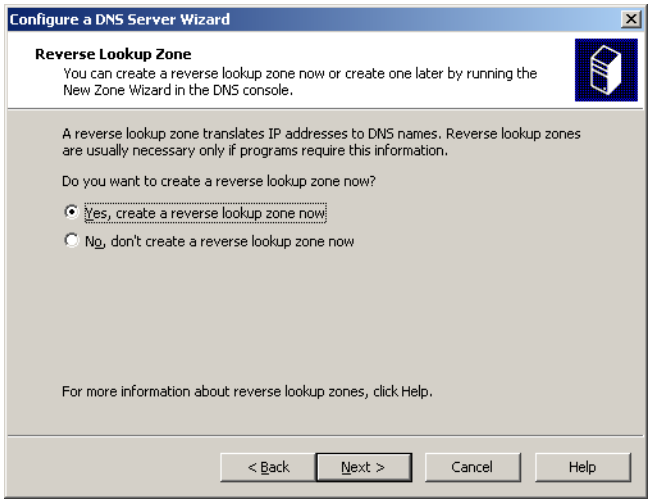
10. In the "Zone File" screen, keep the default zone file name and click **Next**.



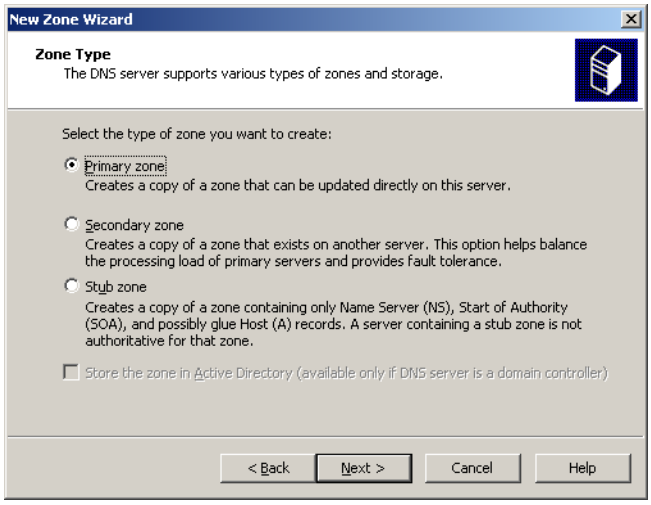
11. In the "Dynamic Update" screen, select the **Allow both nonsecure and secure dynamic updates** radio button and click **Next**.



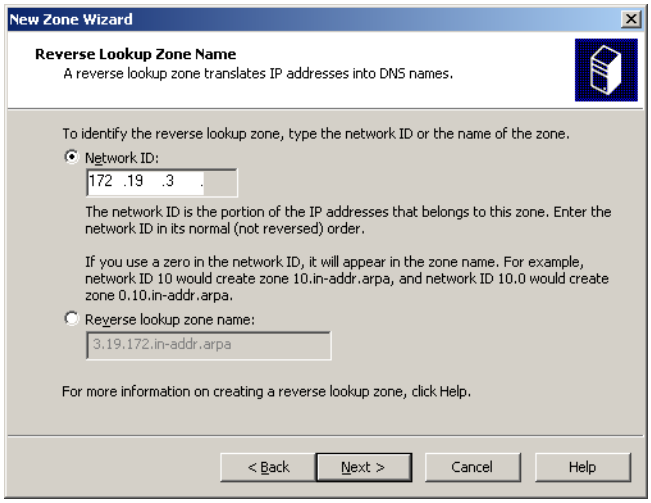
12. In the "Reverse Lookup Zone" screen, select the **Yes, create reverse lookup zone now** radio button and click **Next**.



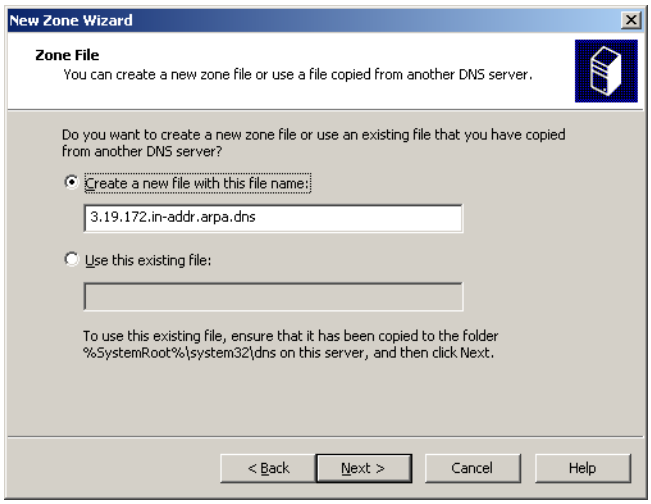
13. In the “Zone Type” screen, select the **Primary Zone** radio button and click **Next**.



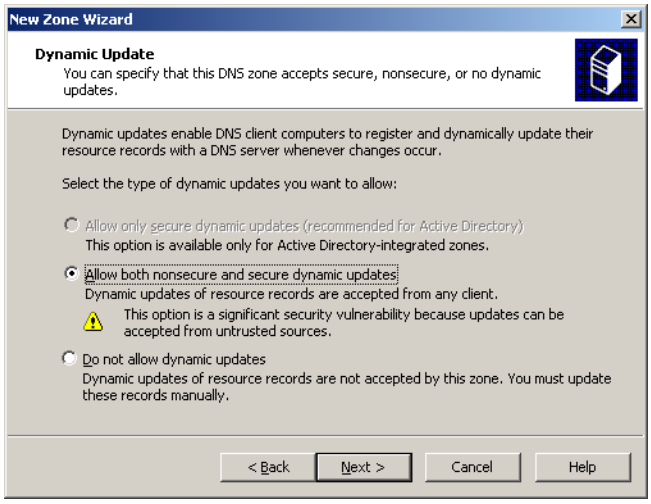
14. In the “Reverse Lookup Zone Name” screen, select the **Network ID** radio button and enter the first three octets of the machine’s IP address (you set this address in step 1 on page 274), then click **Next**.



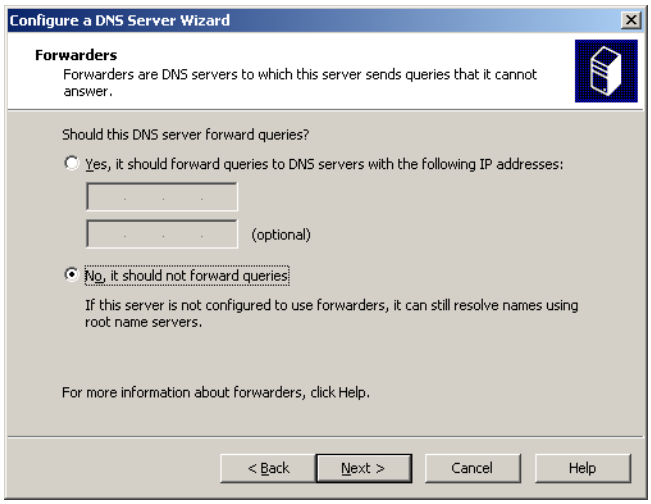
15. In the "Zone File" screen, keep the default zone file name and click **Next**.



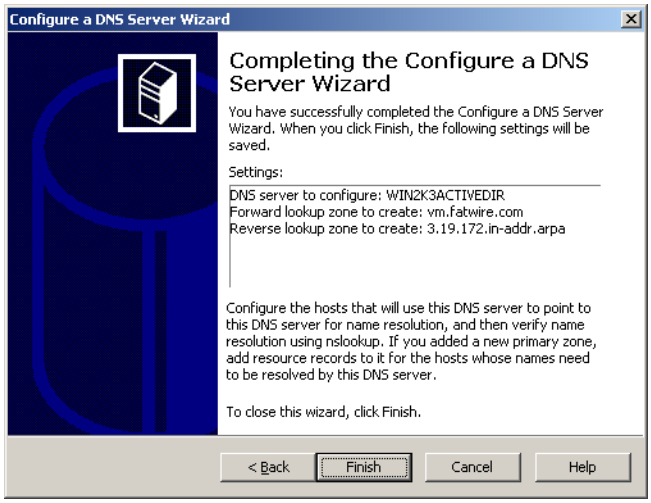
16. In the "Dynamic Update" screen, select the **Allow both nonsecure and secure dynamic updates** radio button and click **Next**.



17. In the "Forwarders" screen, select the **No, it should not forward queries** radio button and click **Next**.



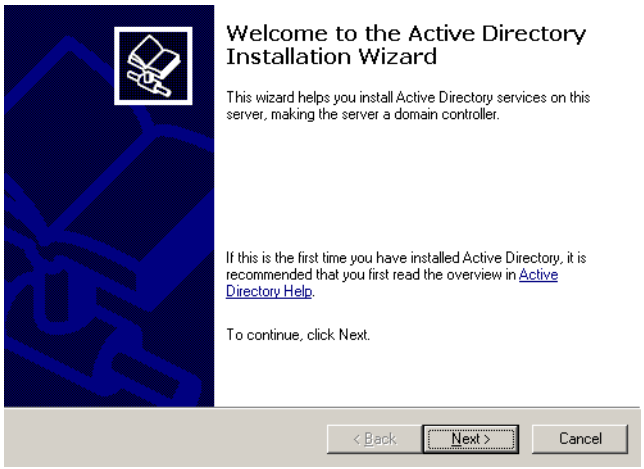
18. In the "Completing the Configure a DNS Server Wizard" screen, click **Finish**.



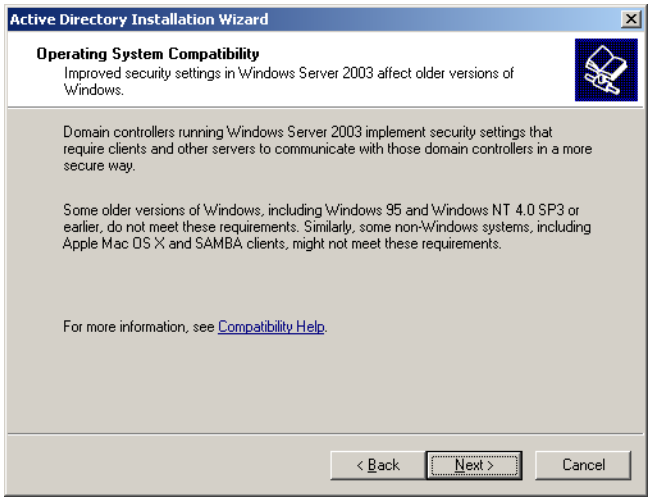
19. Close or minimize the DNS server window.

F. Install MS Active Directory Server 2003

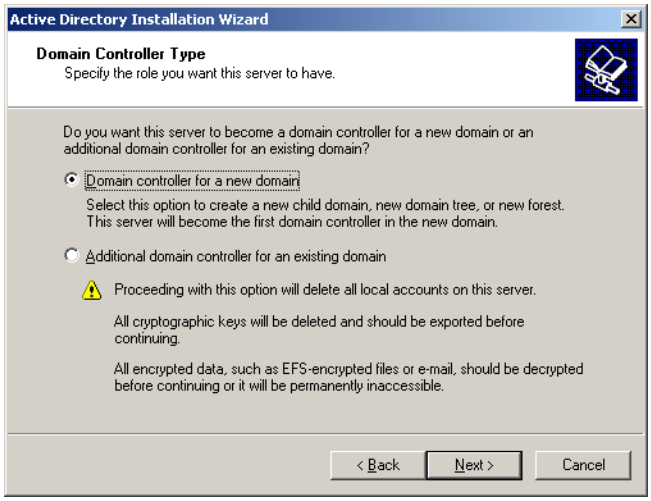
1. Click **Start**, then **Run**, and enter `dcpromo` in the "Run" dialog box.
2. In the "Welcome to the Active Directory Installation Wizard" screen, click **Next**.



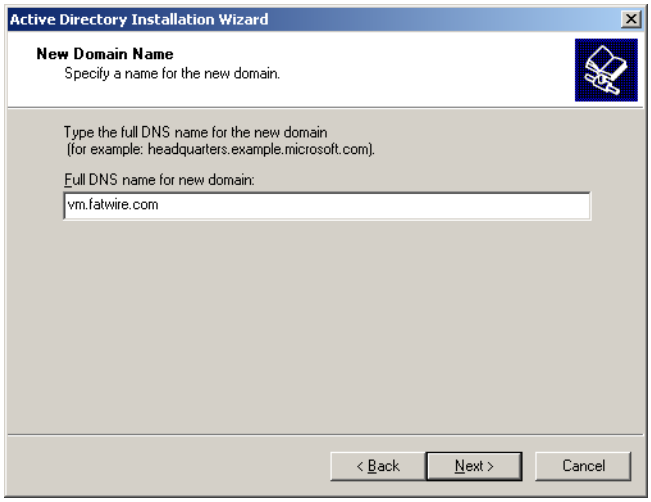
3. In the "Operating System Compatibility" screen, click **Next**.



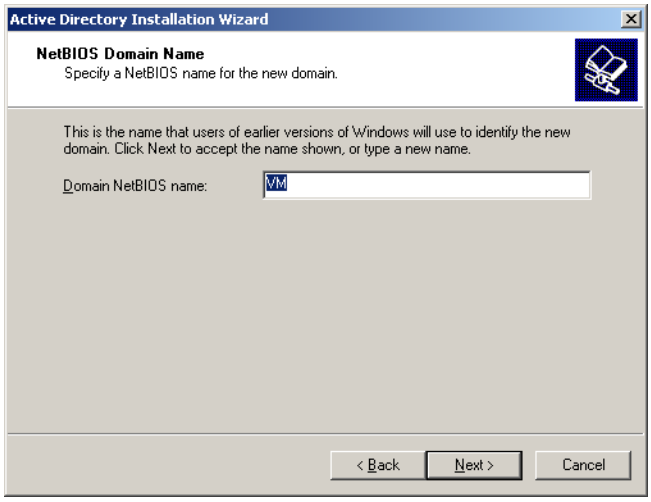
4. In the “Domain Controller Type” screen, select the **Domain controller for a new domain** radio button and click **Next**.



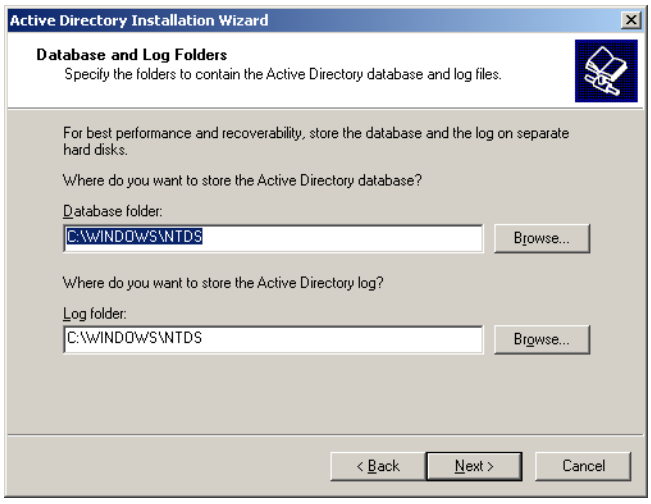
5. “In the “Create a New Domain” screen, select the **Domain in a new forest** radio button and click **Next**.
6. In the “New Domain Name” screen, enter the DNS name you entered in step 9 on page 278, then click **Next**.



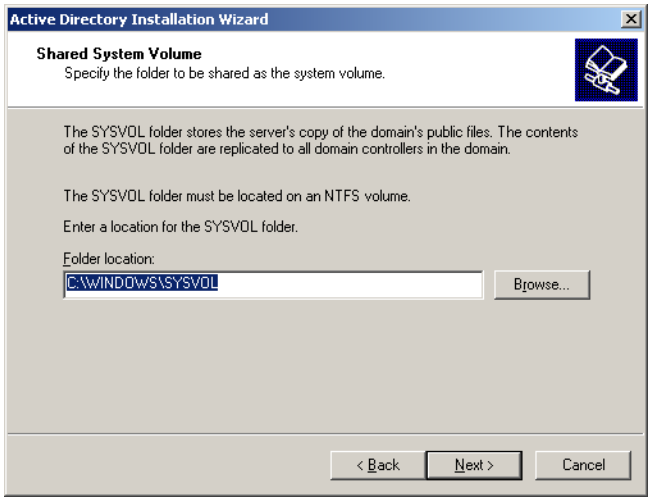
7. In the “NetBIOS Domain Name” screen, keep the default value and click **Next**. Make a record of this value.



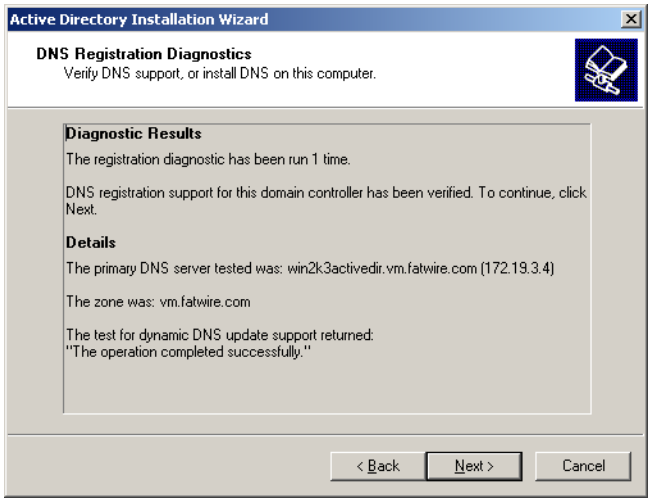
8. In the “Database and Log Folders” screen, click **Next**.



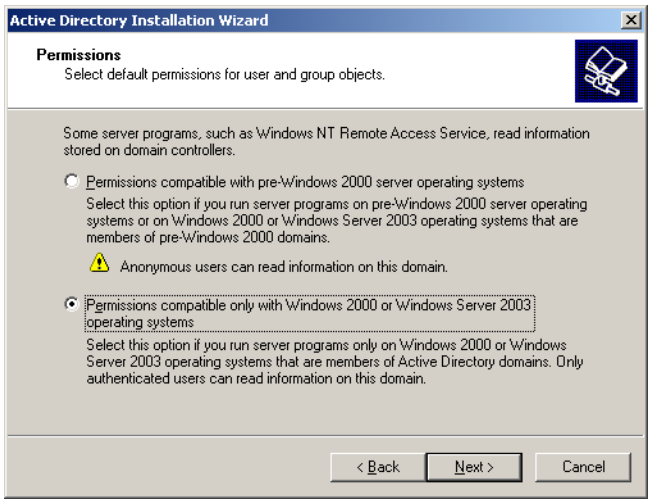
9. In the “Shared System Volume” screen, click **Next**.



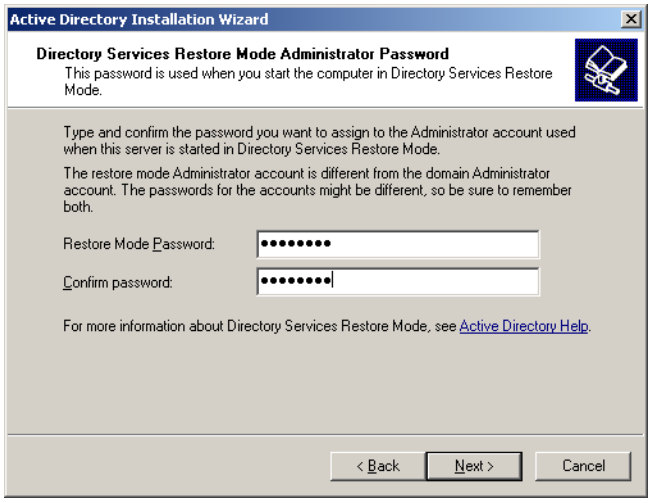
10. In the “Diagnostic Results” screen, make sure that the diagnostic has completed successfully, then click **Next**. If the diagnostic fails, correct the indicated problem, click **Back** and then **Next** to rerun the diagnostic.



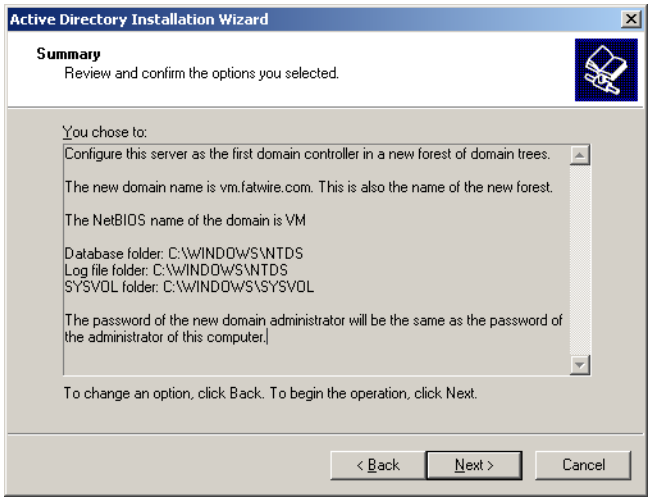
11. In the "Permissions" screen, select the **Permissions compatible only with Windows 2000 and Windows 2003 operating systems** and click **Next**.



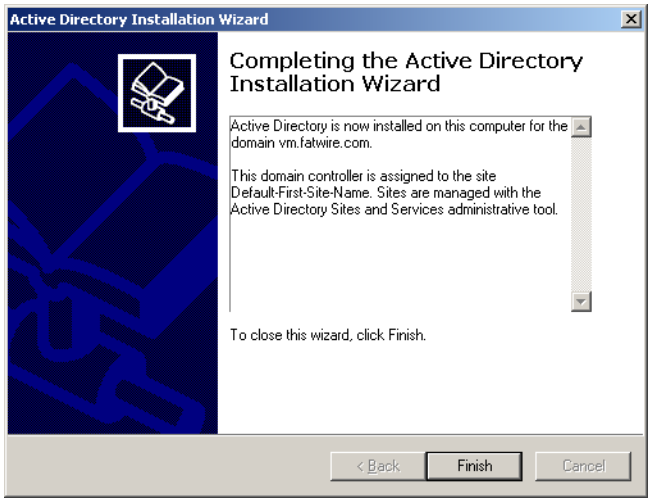
12. In the "Directory Services Restore Mode Administrator Password" screen, enter a password and click **Next**. Make a record of this password.



13. In the "Summary" screen, click **Next**.



14. In the "Completing the Active Directory Installation Wizard" screen, click **Next**.



15. In the pop-up dialog that appears, click **Reboot Now** and wait for the machine to restart.

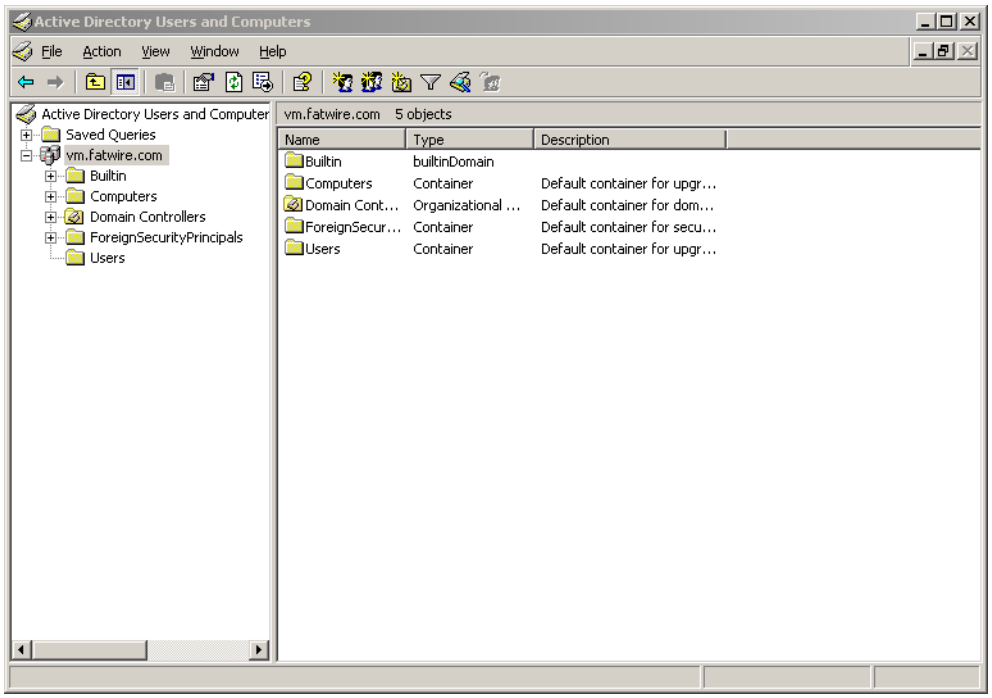
Active Directory Server is now installed and ready for use.

Accessing the “Active Directory Users and Computers” Console

You use the “Active Directory Users and Computers” console to manage your Active Directory Server configuration. To access the console, perform the following steps:

1. Click **Start**, then **Run** to bring up the “Run” dialog box.
2. In the “Run” dialog box, enter **`dsa.msc`**.
3. Click **OK**.

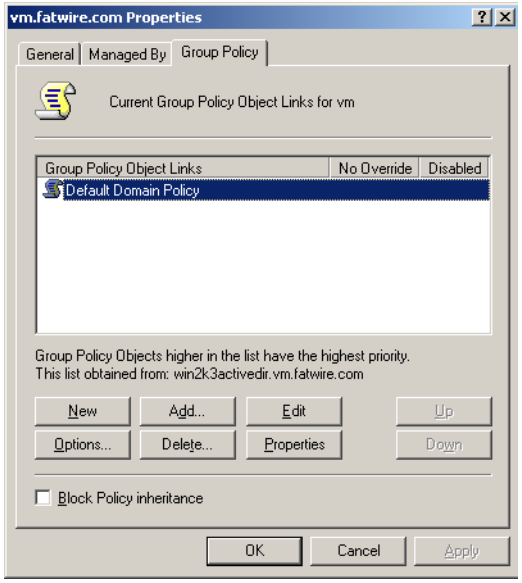
   The “Active Directory Users and Computers” console loads.



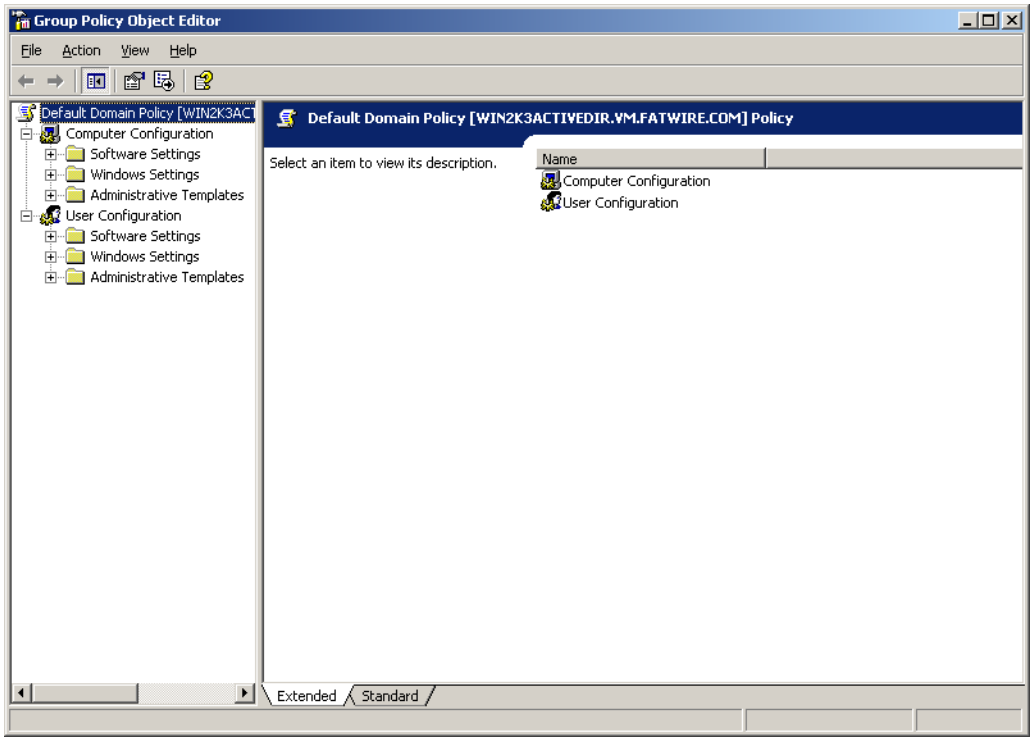
Configuring ADS Password Security for Content Server

This section shows you how to configure password security in Active Directory Server to meet Content Server's requirements.

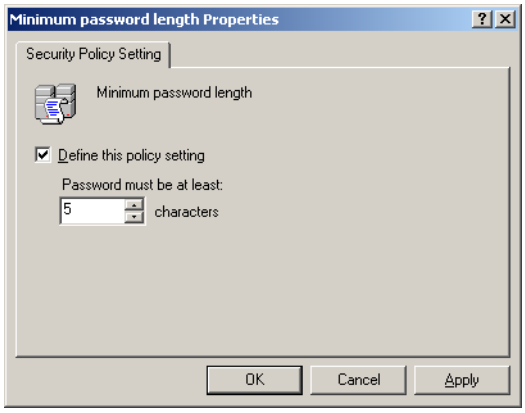
1. Open the "Active Directory Users and Computers" console.
2. In the tree on the left, right-click the desired domain and select **Properties** from the context menu.
3. In the dialog that appears, select the **Group Policy** tab.



4. The Group Policy Object Editor appears, showing the group policy you selected.



5. In the tree on the left, expand **Computer Configuration** > **Windows Settings** > **Security Settings** > **Account Policies** and select **Password Policy**.
6. In the main pane, double-click the **Minimum password length** item.
7. In the pop-up dialog that appears, enter `4` as the value and click **OK**.



8. Double-click the **Password must meet complexity requirements** item.
9. In the pop-up window that appears, select the **Disabled** radio button and click **OK**.
10. From the **File** menu, select **Exit**, then click **OK**.
11. Bring up the "Run" dialog, enter **`gpudate`**, and click **OK**.

Modifying User Passwords

This section shows you how to modify a user's password in Active Directory Server.

1. Open the "Active Directory Users and Computers" console.
2. In the tree on the left, select **Users**.
3. In the main pane, select the user whose password you want to modify.
4. Right-click the desired user name and select **Reset Password** from the context menu.
5. In the dialog that appears, enter and re-enter the new password, then click **OK**.

Deleting Users

This section shows you how to delete a user in Active Directory Server.

1. Open the "Active Directory Users and Computers" console.
2. In the tree on the left, select **Users**.
3. In the main pane, select the user whose password you want to modify.
4. Right-click the desired user name and select **Delete** from the context menu.
5. In the pop-up dialog that appears, click **Yes**.

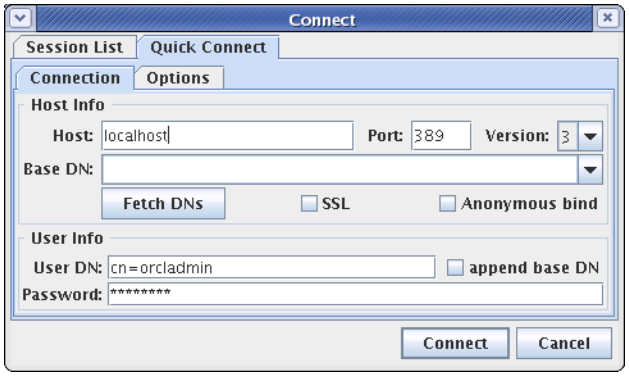
Connecting to ADS Using an LDAP Browser

This section shows you how to connect to Active Directory Server using an LDAP browser.

Note

You cannot add groups, set passwords, or activate accounts using an LDAP browser.

1. Open the LDAP browser.
2. Select the **Quick Connect** tab.
3. Fill out the following information:
   - **Host:** `localhost` (if connecting remotely, enter the actual host name)
   - **Base DN:** `<DNS_suffix>` (the part of the DNS name after the host name)
   - **Anonymous bind:** deselect
   - **User DN:** `administrator@<DNS_suffix>`
   - **Append base DN:** deselect
   - **Password:** `<ADS_password>` (you created this password in step 12 on page 287)



4. Click **Connect**.

Part 4

Virtualization

This part contains the following chapters:

Chapter 19

Creating and Configuring a Xen Virtual Machine

This chapter shows you how to create and configure a Xen Virtual Machine on Red Hat Enterprise Linux 5.0.

This chapter contains the following sections:

Important Commands

Command	Path
Start the `xend` control daemon	`service xend start`
Start the Virtual Machine Manager	`virt-manager`
Start a Virtual Machine	`xm create /etc/xen/<Virtual Machine name>`
Shut down a Virtual Machine	`xm shutdown /etc/xen/<Virtual Machine name>`
Suspend a Virtual Machine	`xm suspend /etc/xen/<Virtual Machine name>`
Resume a Virtual Machine	`xm resume /etc/xen/<Virtual Machine name>`
Configure the amount of startup memory for a Virtual Machine	`xm mem-set /etc/xen/<Virtual Machine name> <amount in megabytes>`
Configure the maximum allowable memory for a Virtual Machine	`xm mem-max /etc/xen/<Virtual Machine name> <amount in megabytes>`
Configure the number of vcpu's allocated to a Virtual Machine	`xm vcpu-set /etc/xen/<Virtual Machine name> <number of vcpu's>`
View the xend log	`xm log`
Save a Virtual Machine	`xm save /etc/xen/<Virtual Machine name> <path to save file>`
Restore a Virtual Machine	`xm restore <path to save file>`

Configure GRUB

The GRUB boot loader's configuration file contains the `kernel-xen` entries and a space separated list of arguments to be passed to the kernel at system boot time.

1. Enter the following path to open the boot loader's configuration file in a text editor:

   `/boot/grub/grub.conf`

   Example of `kernel-xen` entry:

```
itle Red Hat Enterprise Linux Server (2.6.18-3.el5xen)
root   (hd0; 0)
kernel  /xen.gz.-2.6.18-3.el5 dom0_mem=800M dom0_max_vcpus=1
module  /vmlinuz-2.6..18-3.el5xen ro root=/dev/VolGroup00/
LogVol00  rhgb quiet
module  /initrd-2.6.18-3. el5xenxen.img
```

2. To limit the amount of resources the `domain0` system management domain can use, add space separated kernel arguments to the end of the kernel line of the `kernel-xen` entry.

   Important kernel arguments:

   - `dom0_mem` - This argument limits the amount of memory that is available for `domain0`.
   - `dom0_max_vcpus` - This argument limits the amount of CPUs visible to `domain0`.

Paravirtualization

Requirements

Note

The latest version of most Linux distributions include the `xen-kernel` for paravirtualization support. Windows is not yet supported for paravirtualization.

- Guest operating system with Xen Paravirtualization support.
- Installation tree accessible via `http`, `nfs`, or `ftp`.

Creating an Installation Tree

An installation tree is the location for all the files that are needed to run and install the operating system. If a location is not already available via `http`, `nfs`, or `ftp`, one must be created using the installation disks or ISO images.

If you are using the installation CD-ROMs, complete the following steps:

1. Create a directory for your installation tree.
2. For each binary CD-ROM, execute the following:
   - `mkdir /mnt/cdrom`
   - `mount -r /dev/cdrom /mnt/cdrom`
   - `cp -var /mnt/cdrom <path to installation tree>`

Note

You may have to manually concatenate `TRANS.TBL` files.

   - `umount -v /mnt/cdrom`

If you are using ISO images, complete the following steps:

1. Create a directory for your installation tree.
2. For each ISO image, execute the following:
   - `mkdir /mnt/iso`
   - `mount -o loop <path to ISO> /mnt/iso`
   - `cp -var /mnt/iso/* <path to installation tree>`
   - `umount /mnt/iso`

Making the Installation Tree Available

Once the installation tree has been created, the Virtual Machine creation tool requires this tree be made available via `http`, `nfs`, or `ftp`.

HTTP (Recommended)

1. Install Apache Web Server.
2. Move the installation tree into the `htdocs` directory of Apache.

3. Start the Apache Web Server. Go to the bin directory of Apache and run the following command:

   apachectl start

4. Use the following URL:
   `http://<apache host>/<installation tree>`

NFS

1. Open: `/etc/exports` in a text editor.
2. Add an entry for your installation tree, for example:

   ```
   <path to installation tree> *
   (rw,async,no_root_squash,no_subtree_check)
   ```

3. Run the following commands:
   - **exportfs -a**
   - **/etc/init.d/nfs start**
   - **/sbin/service nfs reload**
4. Use the following URL:
   `nfs://<hostname>/<path to installation tree>`

FTP

1. Copy your installation tree to a shared directory of an `ftp` server.
2. Use the following URL:

   `ftp://<hostname>:<ftp port>/<path to installation tree>`

Full Virtualization

Requirements:

- CPU with full virtualization support

Check CPU for full virtualization support.

- To check for full virtualization support on an Intel CPU, enter the following command:

  grep vmx /proc/cpuinfo

  - If a list of CPU flags is outputted, then your Intel CPU supports full virtualization. For example:

```
flags   :  fpu tsc msr pae mce cx8 apic mtrr mca cmov pat pse36
clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall  nx lm
constant_tsc pni monitor ds_cpl vmx est tm2 cx16 xtpr lahf_lm
```

  - If nothing is outputted, your CPU does not support full virtualization.

- To check for full virtualization support on an AMD CPU, enter the following command:

  grep svm /proc/cpuinfo

  - If a list of CPU flags is outputted, then your AMD CPU supports full virtualization. For example:

```
flags   :  fpu tsc msr pae mce cx8 apic mtrr mca cmov pat pse36
clflush dt acpi mmx fxsr sse sse2 ss ht tm syscall nx mmtext
fxsr_opt  rdtscp lm 3dnowext  pni  cx16  lahf_lm  cmp_legacy  svm
cr8_legacy
```

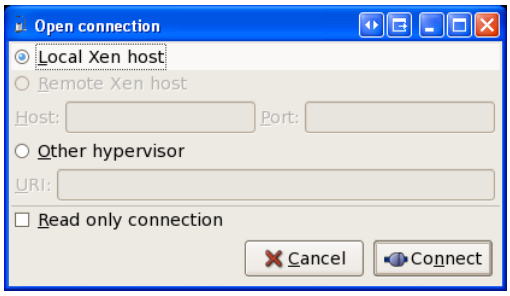
  - If nothing is outputted, your CPU does not support full virtualization.

Creating a New Virtual Machine

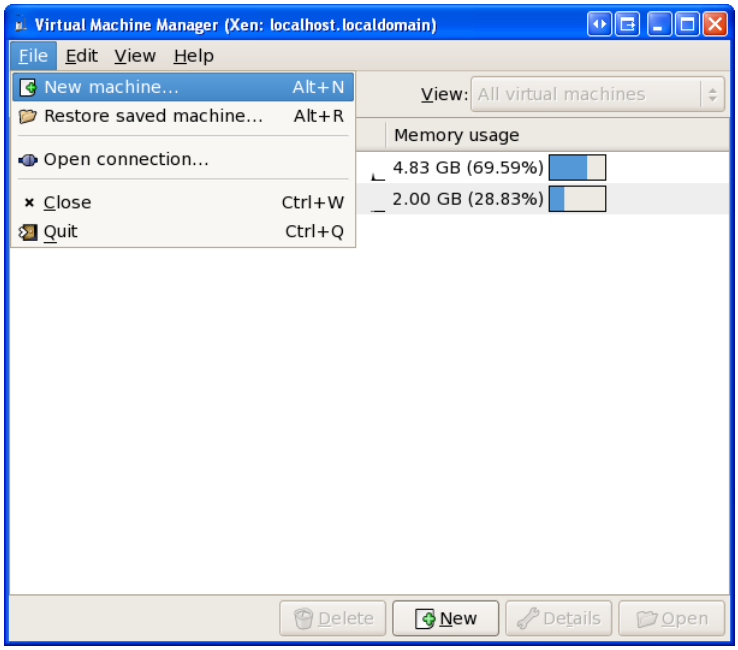
Note

A new virtual machine can be installed to a clean partition (recommended) or an image file on the host file system. If you will be installing on a clean partition, have this partition created before you go on to the next step.

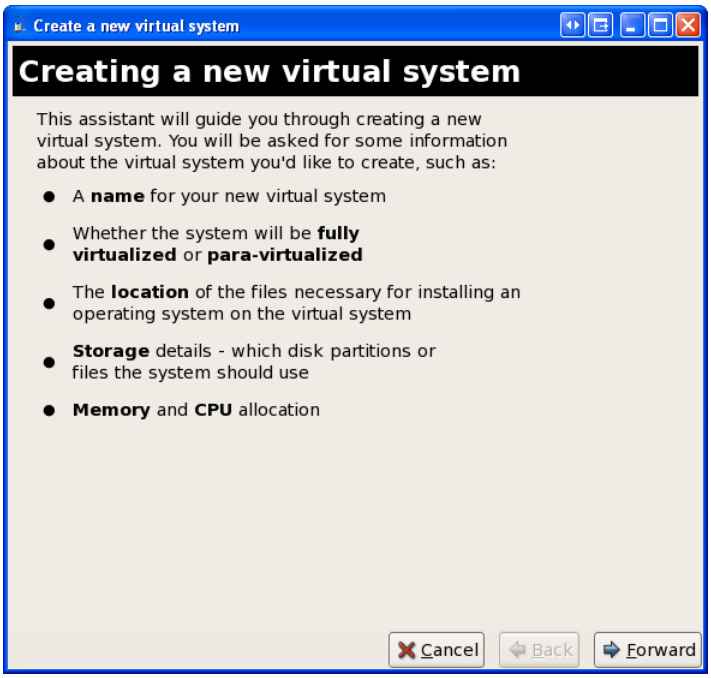
1. Open the Virtual Machine Manager by running the **`virt-manager`** command.
2. When the "Open Connection" window appears, select **Local Xen host**, then click **Connect**.



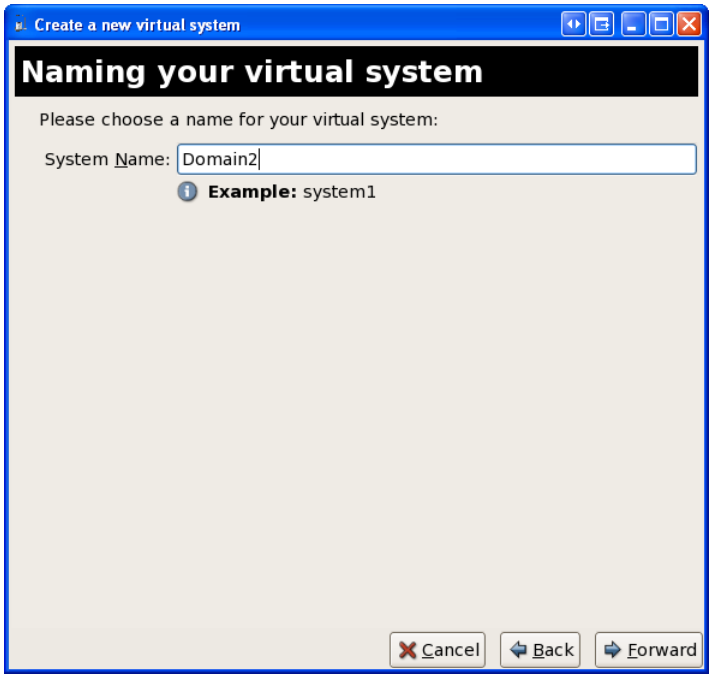
3. Click: **File > New machine**.



4. Click **Forward**.

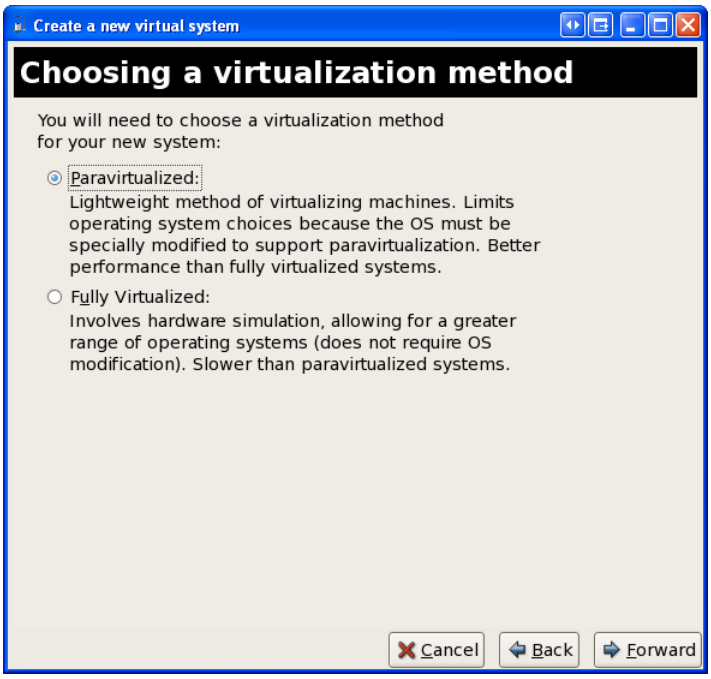


5. Enter a name for the Virtual Machine, then click **Forward**.

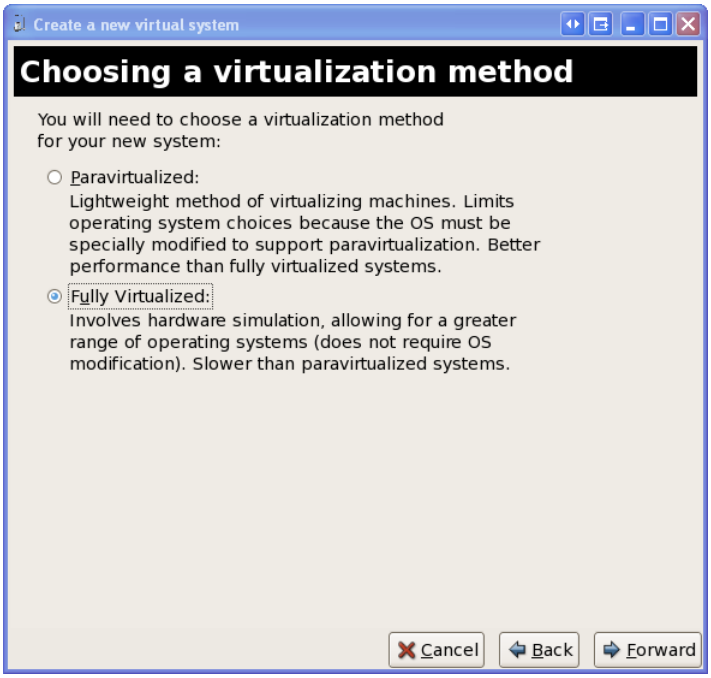


6. Select a virtualization method.

   a. If you will be installing a guest operating system that has been specifically configured for Xen Virtualization, select **Paravirtualized**, then click **Forward**.



   b. If you will be installing a guest operating system not specifically configured for Xen Virtualization, select **Fully Virtualized**, then click **Forward**.

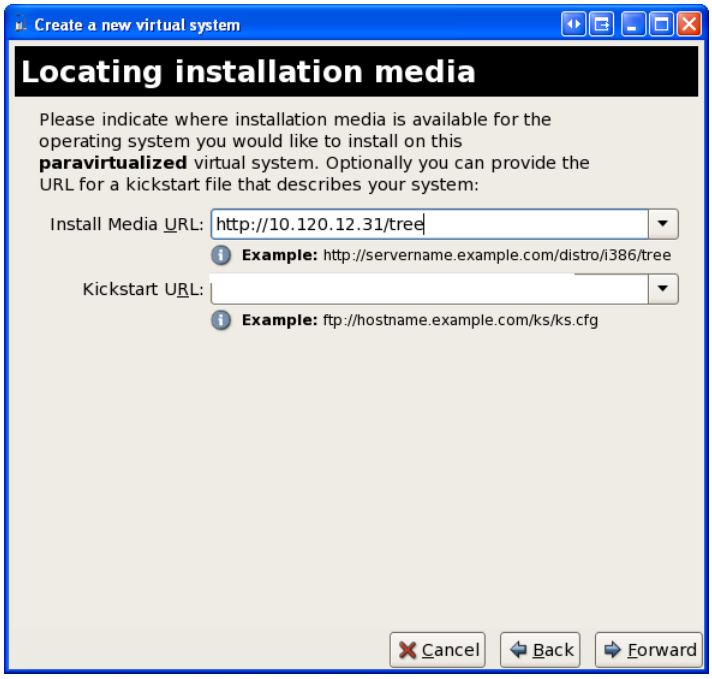


7. (Paravirtualization Only).
   a. Enter the URL to the installation tree created in the previous section.

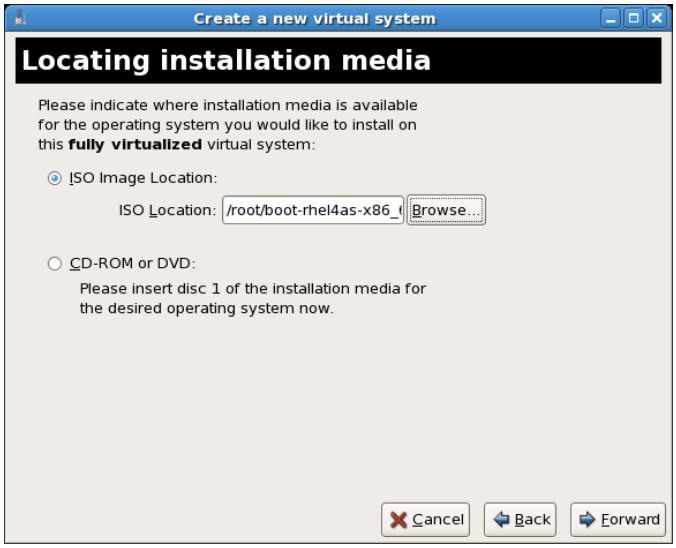
      For example:

      ```
      http://<hostname>:<port>/tree
      nfs://<hostname>:<port>/tree
      ftp://<hostname>:<port>/tree
      ```

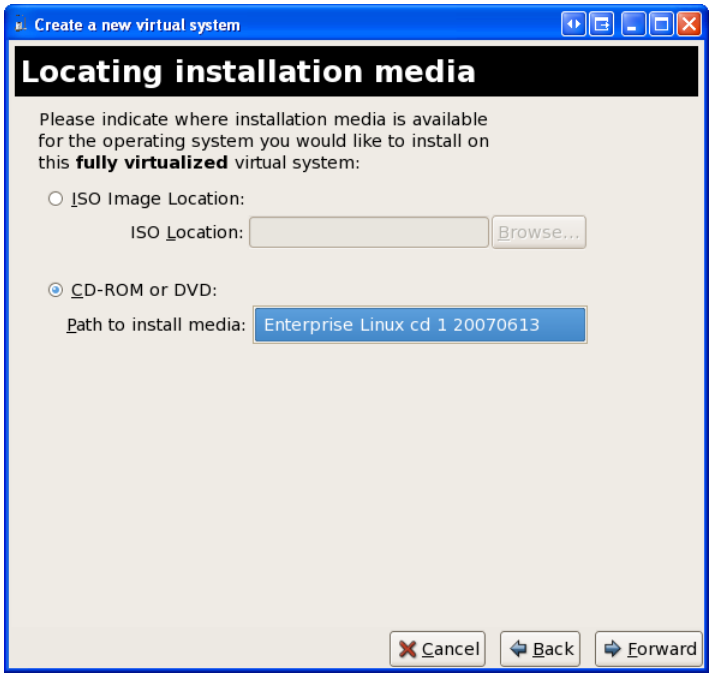
   b. Click **Forward**.



8. (Full Virtualization Only). Select the installation media location.
   - If **ISO Image Location** was selected, browse for the location of the ISO Image containing the operating system installer. Click **Forward**.

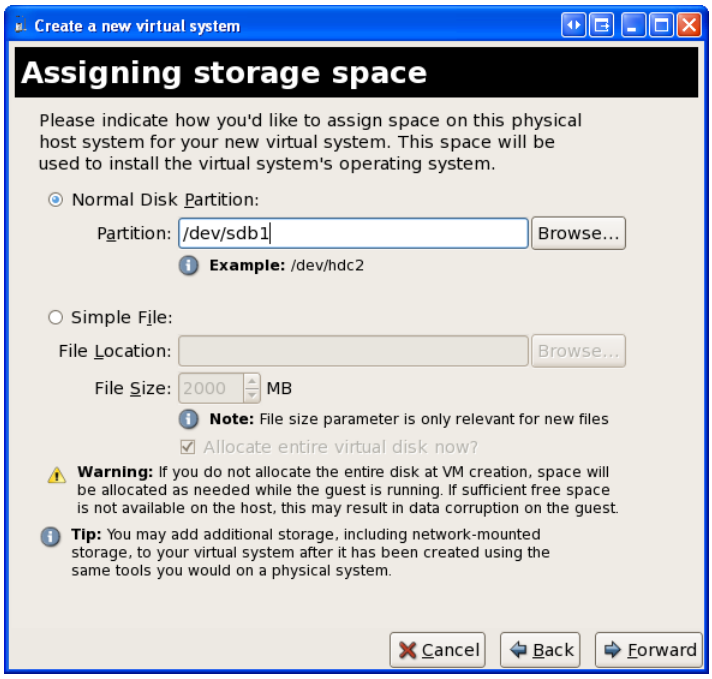


- If CD-ROM or DVD was selected, select the drive containing the installation media. Click **Forward**.

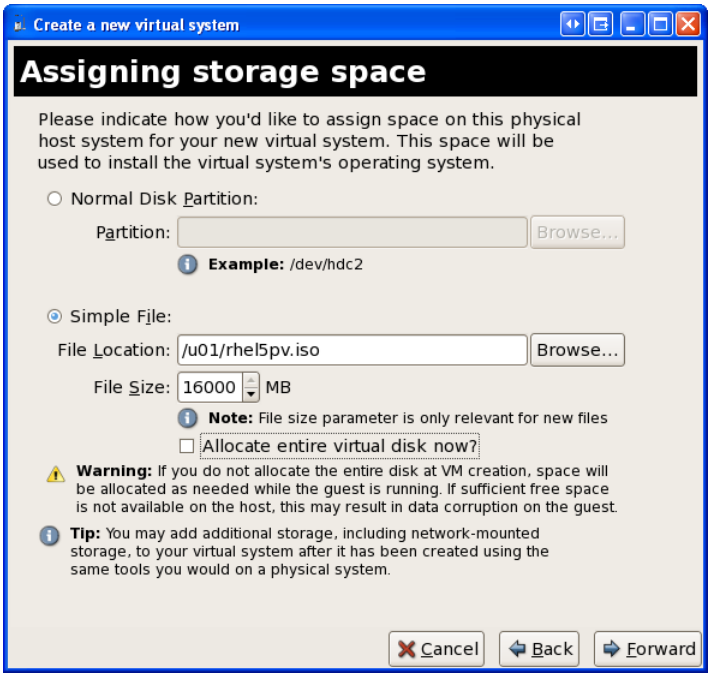


9. Select a storage method.

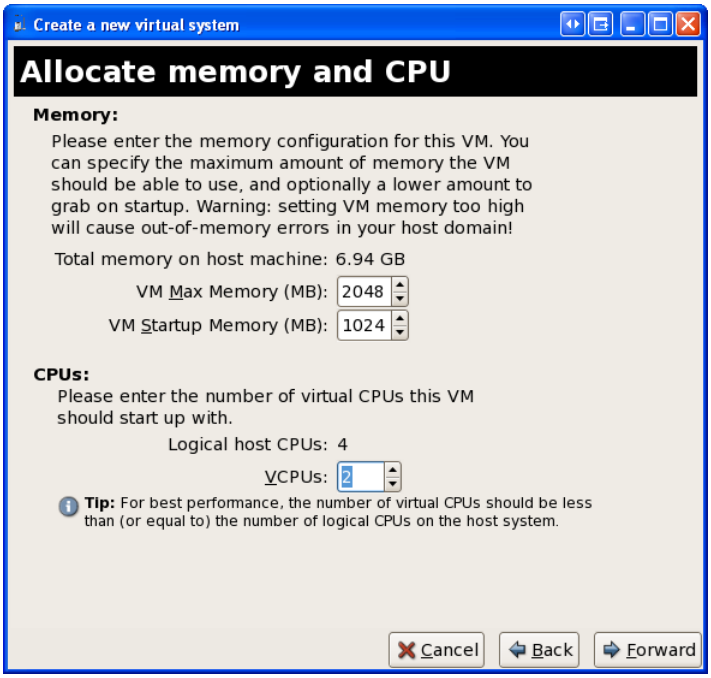
- If **Normal Disk Partition** was selected, enter the path to the disk partition the Virtual Machine will be stored on. Click **Forward**.



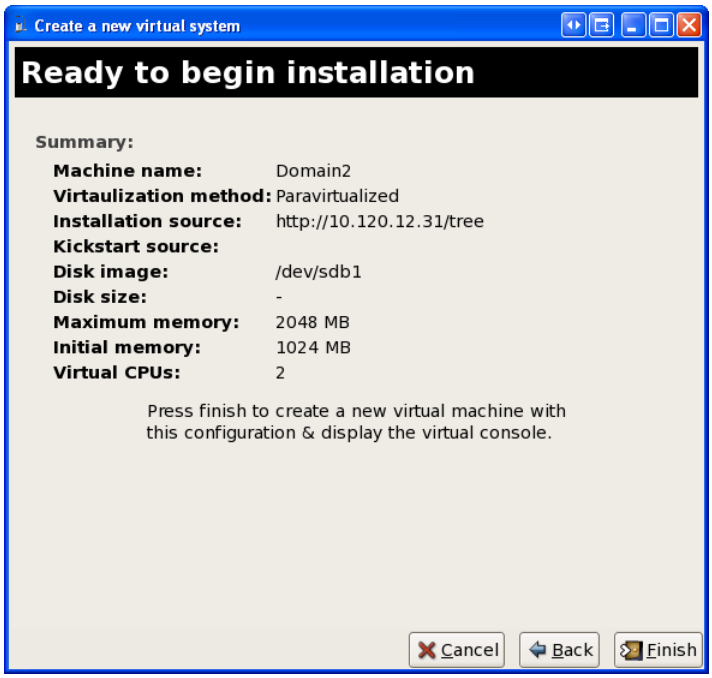
- If **Simple File** was selected, enter the path to the file that the Virtual Machine will be stored as, and select a file size. Click **Forward**.



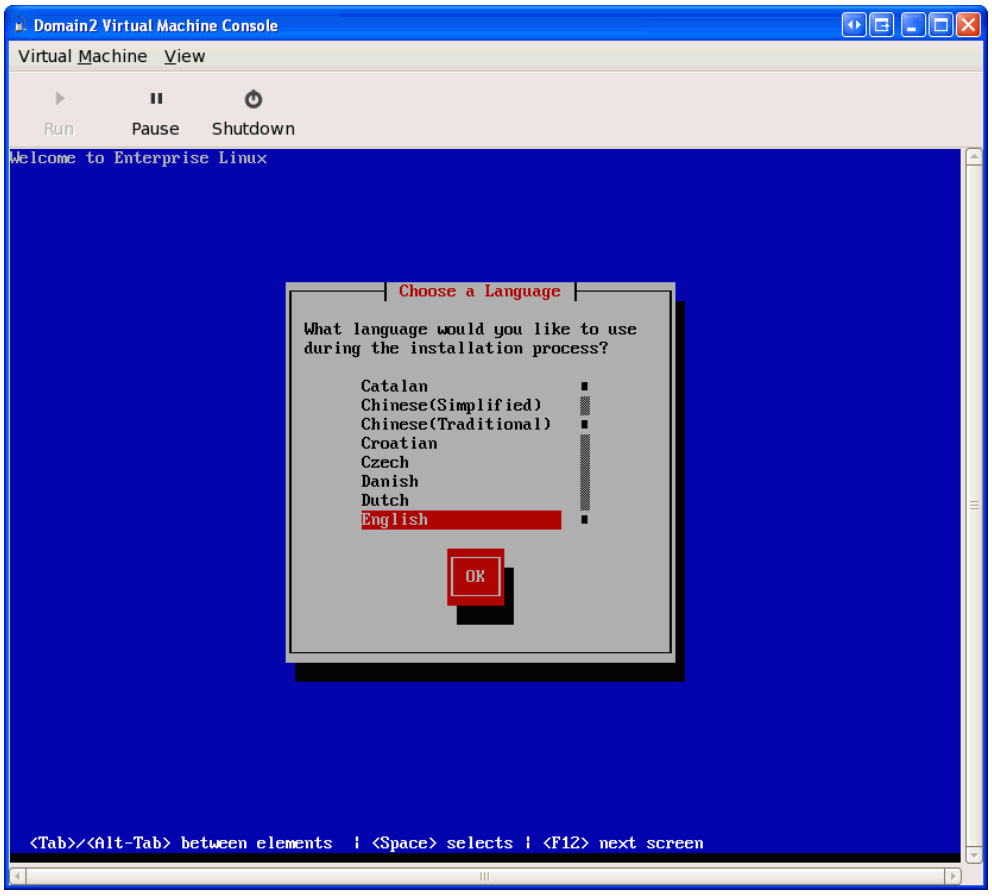
10. When the “Allocate memory and CPU” screen appears, fill in the fields provided, then click **Forward**.
    - **Memory:**
      - **VM Max Memory (MB):** Enter the maximum amount of memory to be allocated to this Virtual Machine.
      - **VM Startup Memory (MB):** Enter the amount of memory to be allocated at startup of this Virtual Machine.
    - **CPUs:** Enter the number of virtual CPUs to be allocated to this Virtual Machine.



11. Review the Virtual Machine settings, and click **Finish**.



12. A new Virtual Machine is now created and booted, running the installer of the operating system in your installer tree.



13. After the installation of your operating system is complete, click to reboot the server. The following events occur:

a. The Virtual Machine shuts down. Its name is removed from the Virtual Machine list in the Virtual Machine Manager.

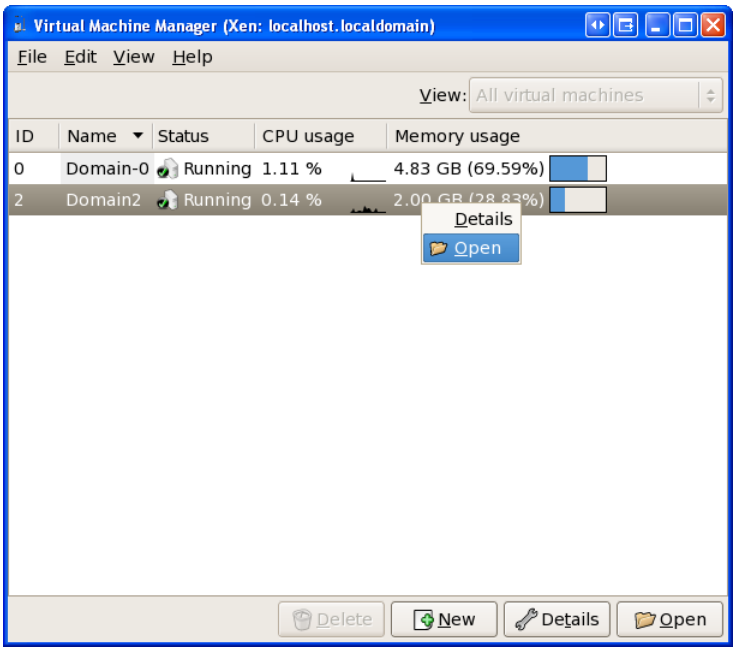
b. The Virtual Machine with the operating system you installed is relocated to the specified storage location. A configuration file is created in the `/etc/xen` directory. The file name is identical to the Virtual Machine name specified in the installation.

14. Run the following command to start the Virtual Machine:

```
xm create /etx/xen/<Virtual Machine name>
```

a. When started, the Virtual Machine will be added to the Virtual Machine list in the "Virtual Machine Manager."

b. Open the Virtual Machine from the "Virtual Machine Manager" by right-clicking the name and clicking **Open**.



Chapter 20

Creating a Zone in Solaris 10

This chapter provides instructions on how to create and configure a zone in Solaris 10.

This chapter contains the following sections:

Prerequisites

- Must be on Solaris 10 Update 4 (as this guide assumes that you are using such a version).
- It is preferred that one unused NIC is available and dedicated to each zone.
- Enough Disk space to create a zone and store the files associated with the zone. The actual space will depend on the application server used and the configuration. It is suggested that for a Sparse Zone you include enough space for Content Server, Application Server + 20%, and no less than 4GB of memory.
- Installation media for Solaris 10 Update 4, and a way to mount the media locally.

Setting Up a Zone in Solaris 10

Note

All commands are done as root

1. Create a directory as the root of your new zone (`/u01/zone1`) which will be used in this section: **`mkdir /u01/cs_zone1`**
2. Change permissions for `/u01/cs_zone1`: **`chmod 700 /u01/cs_zone1`**
3. Plumb the new interface in Solaris so that the zone will be able to find it. Ex. If the interface is named bgel: **`# ifconfig bge1 plumb`**
4. Create a new zone by running `zonecfg`, which will start `zonecfg` in interactive mode: **`# zonecfg -z cs_zone1`**
   a. Start creating a new zone: **`zonecfg:cs_zone1> create`**
   b. Set the path to the new zone (we will use the path created in step 1): **`zonecfg:cs_zone1> set zonepath=/u01/cs_zone1`**
   c. Add an NIC to this zone: **`zonecfg:apache> add net`**
      1) Configure the interface for the zone (assumes that the unused physical NIC is named bge1): **`zonecfg:cs_zone1:net> set physical=bge1`**
      2) Set the IP address to be used by this zone, in this case a Class C subnet with the address of `10.120.16.84`: **`zonecfg:cs_zone1:net> set address=10.120.16.84/24`**
      3) Exit the zone NIC config: **`zonecfg:cs_zone1:net> end`**
      4) Set the zone to automatically Start upon Boot (optional, but suggested): **`zonecfg:cs_zone1> set autoboot=true`**
      5) Check what the zone will look like with the `info` command:

```
zonecfg:cs_zone1> info
zonename: cs_zone1
zonepath: /u01/cs_zone1
autoboot: false
pool:
limitpriv:
```

```
inherit-pkg-dir:
        dir: /lib
inherit-pkg-dir:
        dir: /platform
inherit-pkg-dir:
        dir: /sbin
inherit-pkg-dir:
        dir: /usr
net:
        address: 10.120.16.84/24
        physical: bge1
```

6) Commit the changes: **zonecfg:cs_zone1> commit**

7) Exit the zone: **zonecfg:cs_zone1> exit**

5. Install the new zone. Use step 4a for a sparse zone and step 4b for a full zone.

   - If using a sparse zone run: **# zoneadm -z cs_zone1 install**
   - If using a full zone run: **# zoneadm -b cs_zone1 install**

   The output will closely resemble the following:

```
Preparing to install zone <cs_zone1>.
Creating list of files to copy from the global zone.
Copying <2560> files to the zone.
Initializing zone product registry.
Determining zone package initialization order.
Preparing to initialize <1736> packages on the zone.
Initialized <1736> packages on zone.
Zone <cs_zone1> is initialized.
Installation of these packages generated warnings: <SMCmake>
The file </u01/cs_zone1/root/var/sadm/system/logs/install_log>
   contains a log of the zone installation.
```

6. The zone is now configured and can be started, and logged into.

Important Commands for Solaris

Function	zoneadm Command
Starting up (booting a zone)	**# zoneadm -z cs_zone1 boot**
Rebooting a zone	**# zoneadm -z cs_zone1 reboot**
Shut down	**# zoneadm -z cs_zone1 halt**
Removal (deleting a zone)	**# zoneadm -z cs_zone1 uninstall**
Log in to a zone	**# zlogin -C cs_zone1**

First-Time Configuration for a Zone

The first time, you will be prompted for a number of parameters. The following are the values that will need to be changed based on your environment). These are the same as are asked for in any new installation of Solaris:

1. Select a Language:

   0. English

2. Select a Locale:

   0. English (C - 7-bit ASCII)

3. What type of terminal are you using?

   1) ANSI Standard CRT

4. Host name for bge1:1

   `sunloaner01cszone1`

5. Configure Kerberos Security

   [X] No

6. Name service

   [X] DNS

7. Domain name:

   `fatwire.com`

8. Server’s IP address:

   `xxx.xxx.xxx.xxx`

9. Search domain:

   `fatwire.com`

10. Select the correct time zone.

11. Enter a new root password.

    Setup of the new Zone is now complete.

Chapter 21

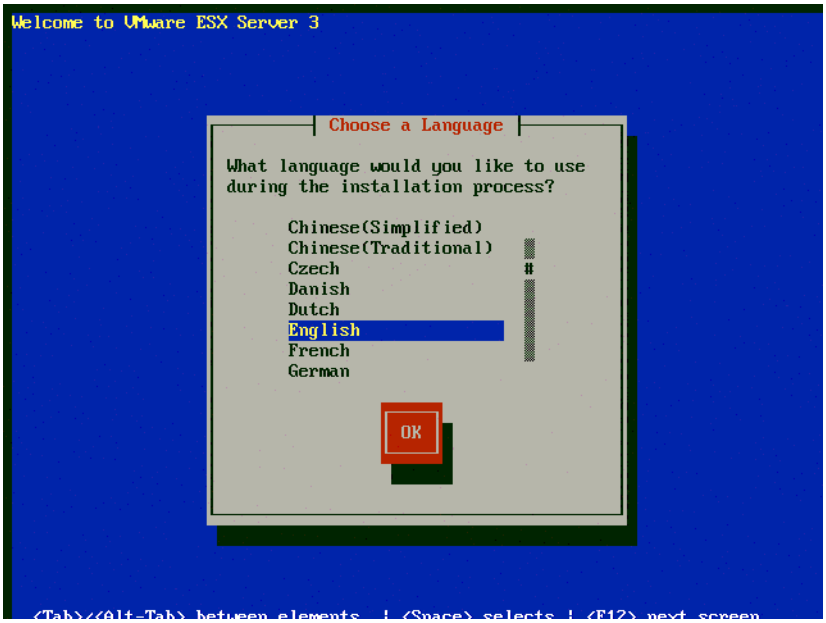
Installing and Configuring VMware ESX Server 3.5

This chapter provides instructions on installing and configuring VMware ESX Server 3.5.

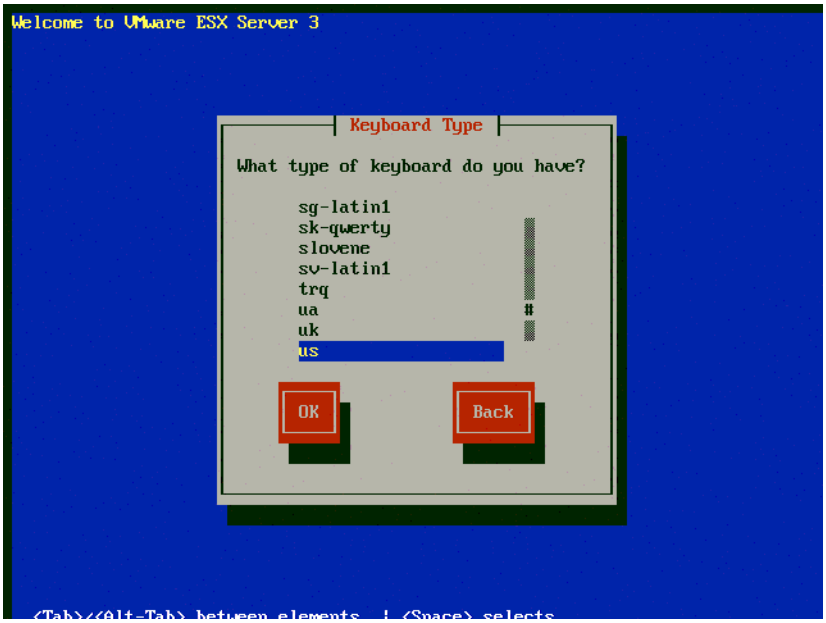
This chapter includes the following sections:

Step I. Installing VMware ESX Server 3.5

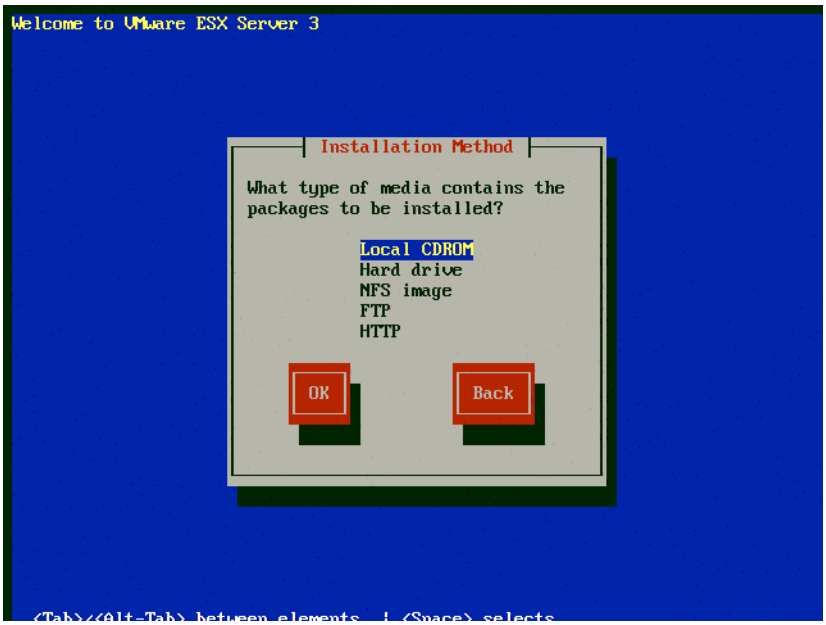
1. Select a language and click **OK**.



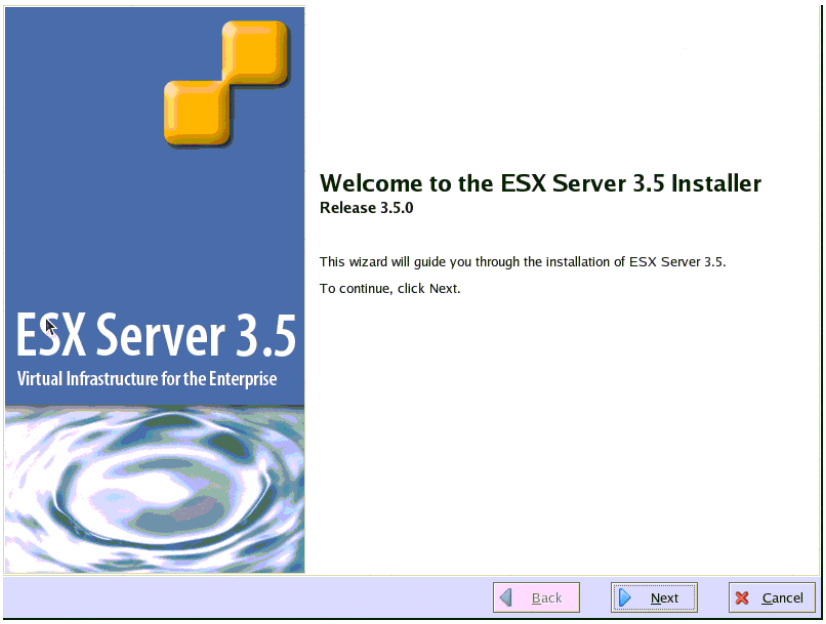
2. Select a keyboard type and click **OK**.



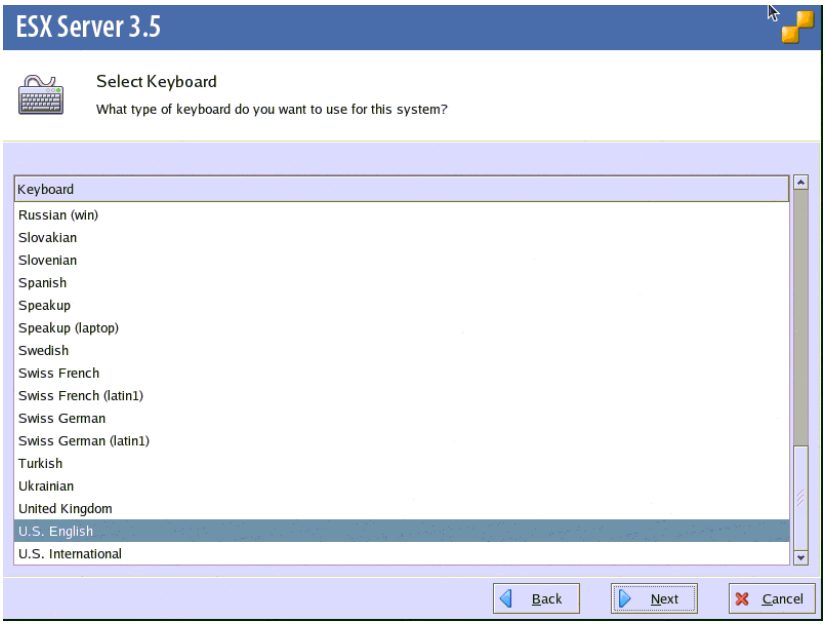
3. Select the installation media type and click **OK**.



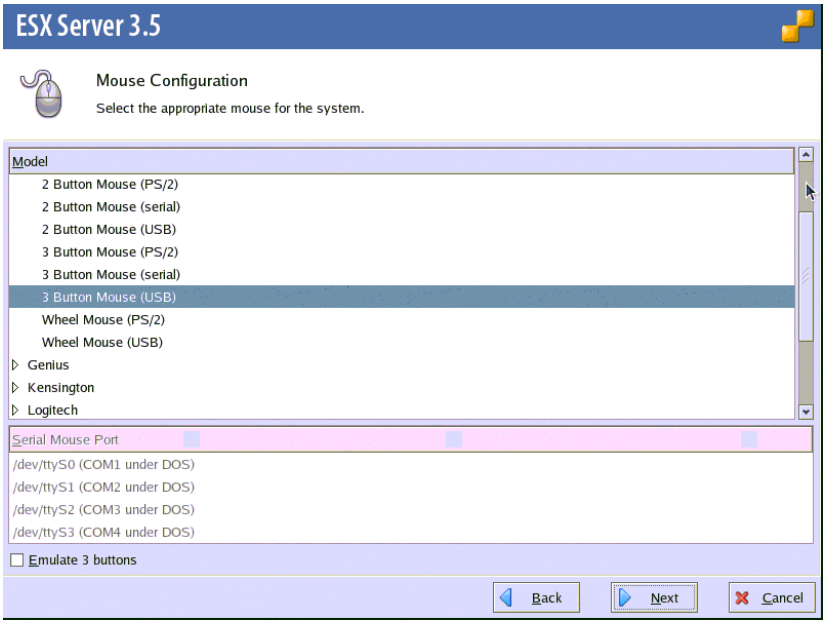
4. Click **Next**.



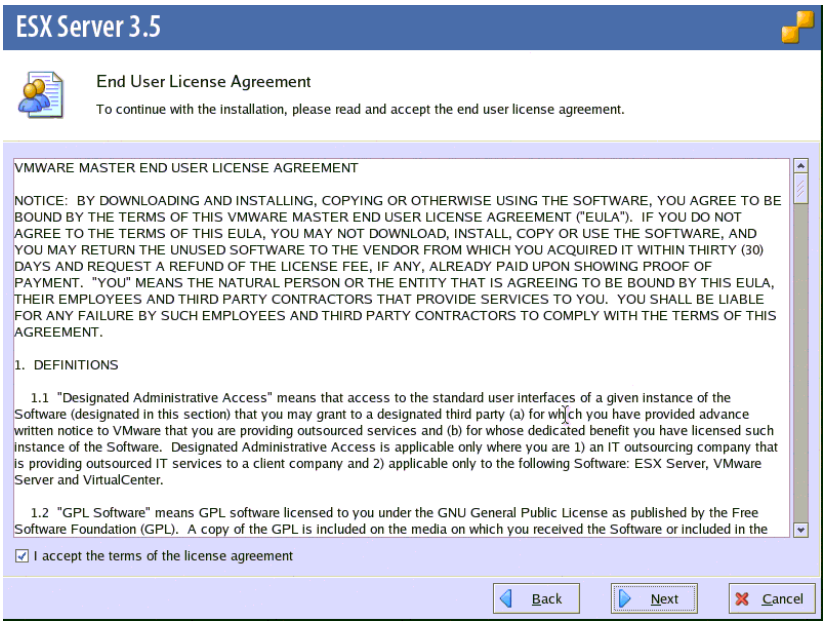
5. Select a keyboard type and click **Next**.



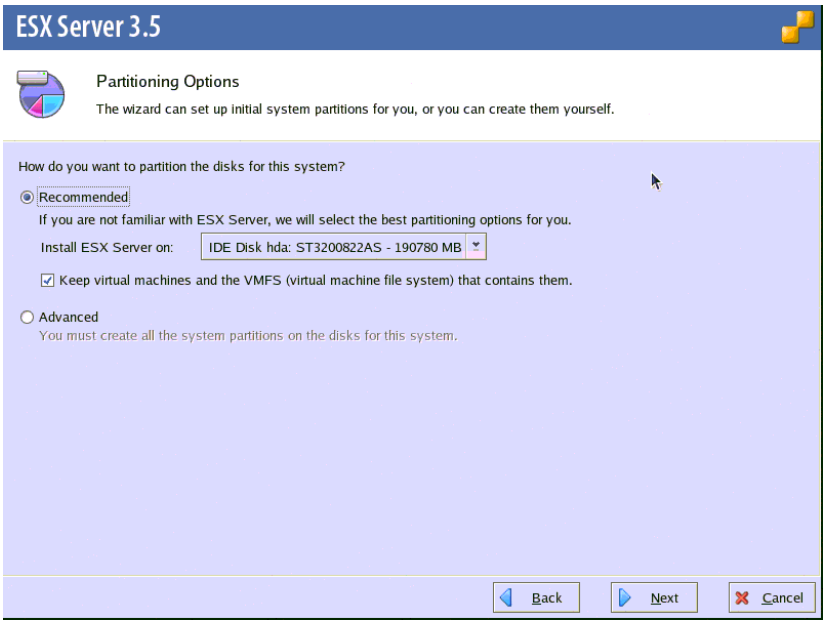
6. Select a mouse configuration and click **Next**.



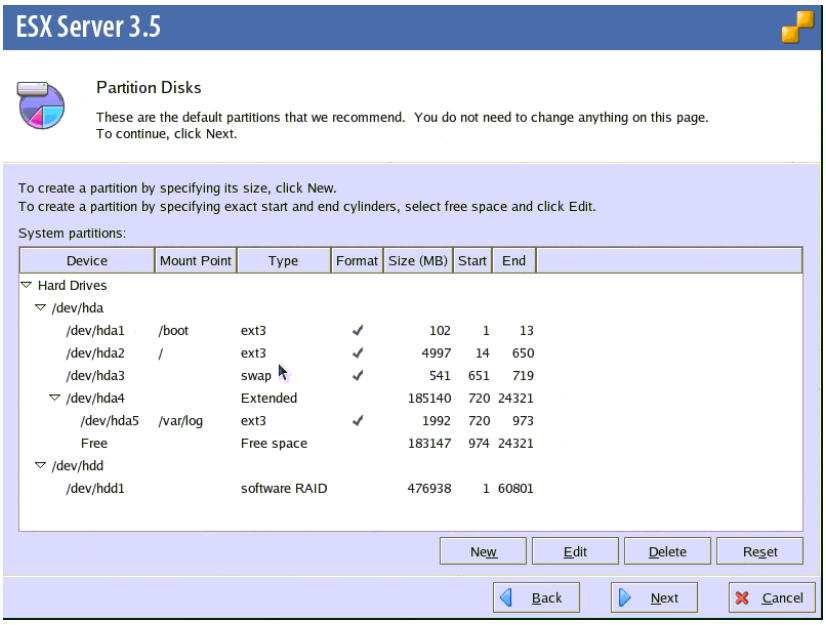
7. Select **I accept the terms of the license agreement**. Click **Next**.



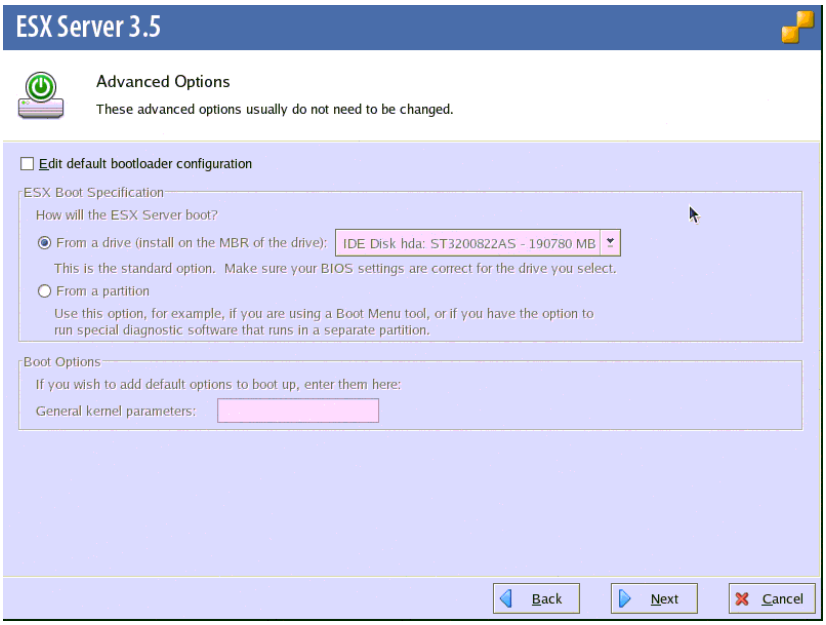
8. Select **Recommended** and select the hard disk you will be installing on. Select **Keep virtual machines and the VMFS that contains them**. You will still be able to make changes on the next screen. Click **Next**.



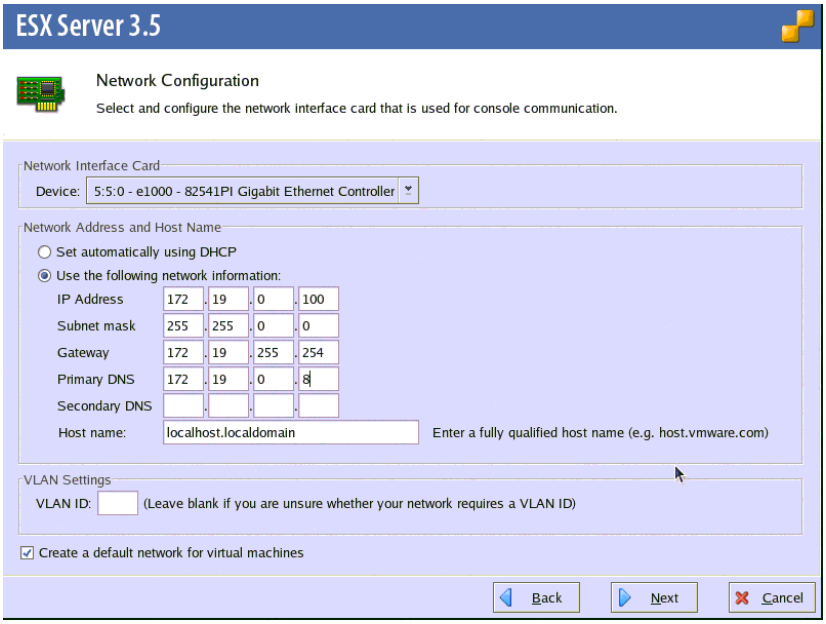
9. Review the partitions to the hard disk and make any desired changes. Click **Next**.



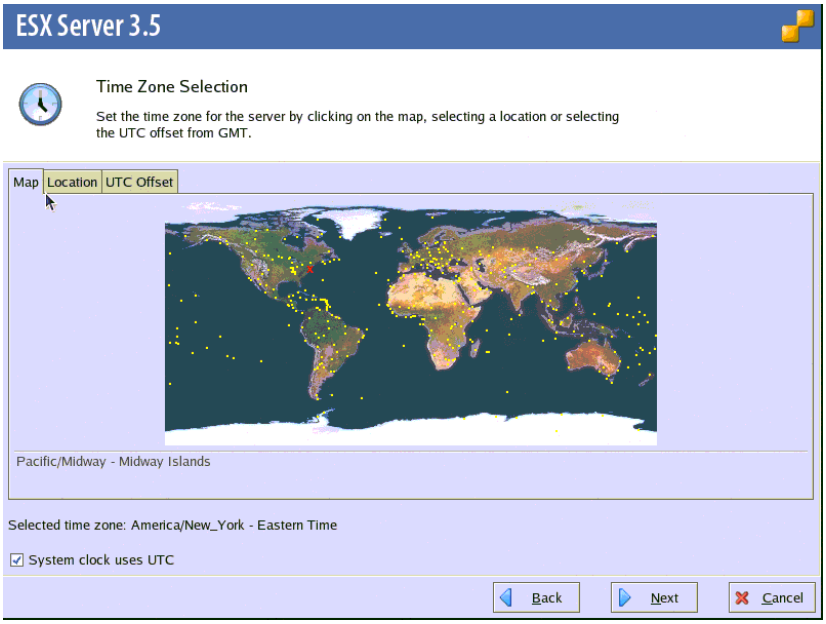
10. Click **Next**.



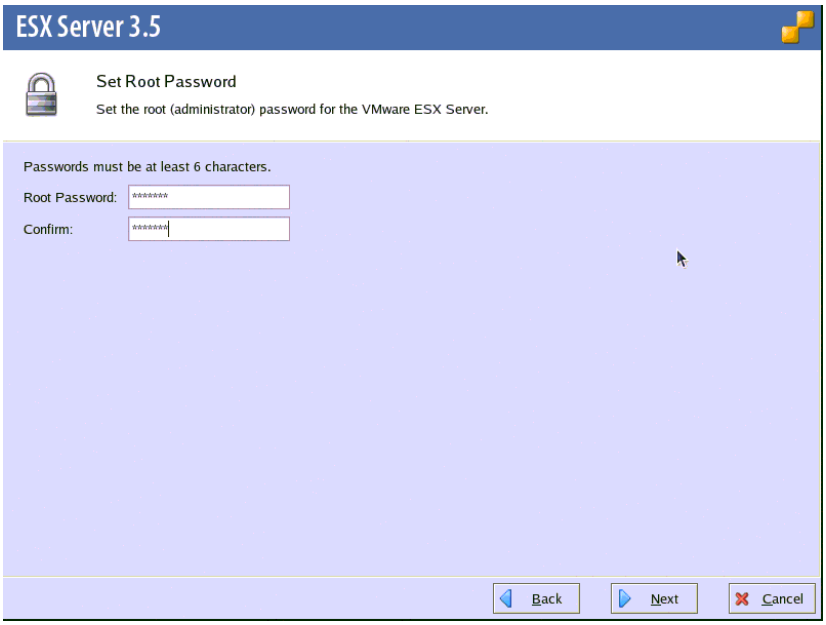
11. Enter network configuration information. Select **Create a default network for virtual machines** and click **Next**.



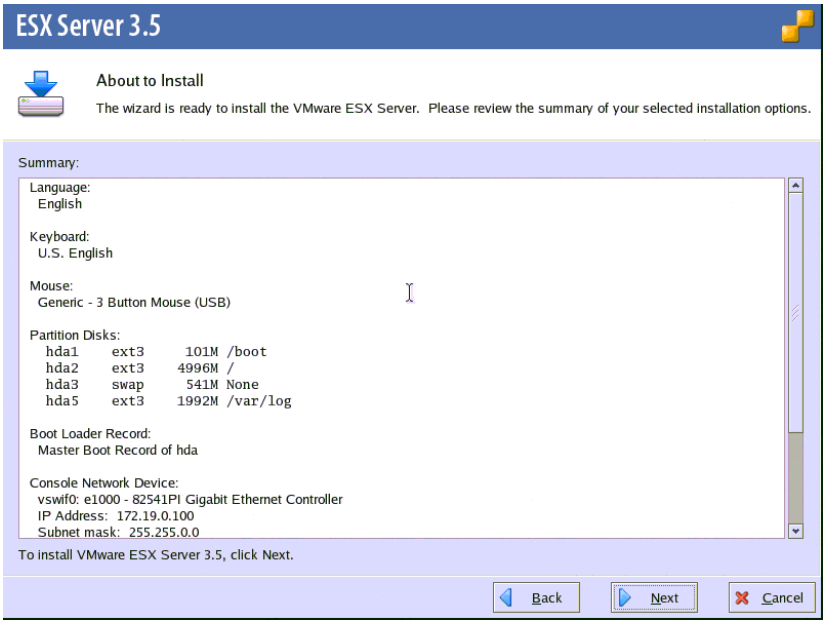
12. Select a time zone and click **Next**.



13. Enter a root password, and re-enter the password for confirmation. Click **Next**.

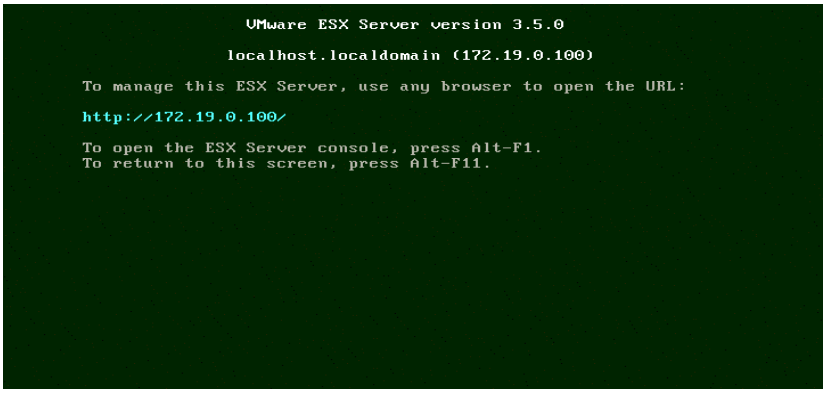


14. Review the installation options. Click **Next**.



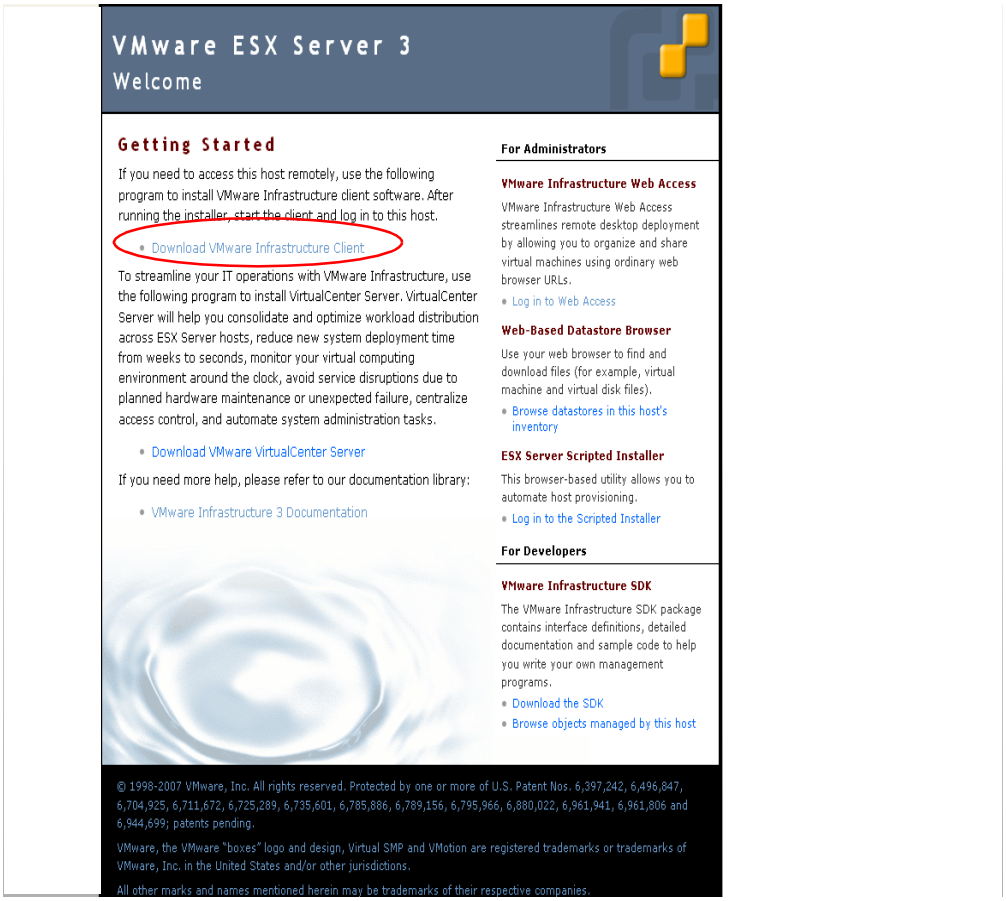
15. When the installation completes, click **Finish**.

16. After the machine has rebooted, you can access the console and log in to the machine by pressing **Alt-F1**. Take note of the URL, as it is used for VMware Infrastructure Web Access.



Step II. Installing VMware Infrastructure Client

1. From a Windows machine, open the URL noted in step 16 on page 325 of the previous section.

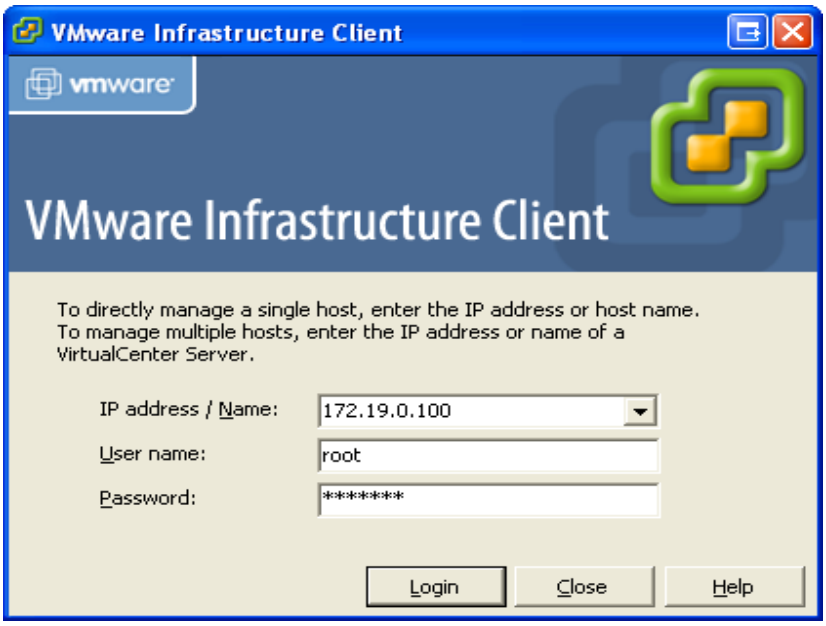


2. From the "VMware ESX Server 3" welcome page, click **Download VMware Infrastructure Client**.
3. Install the VMware Infrastructure Client.

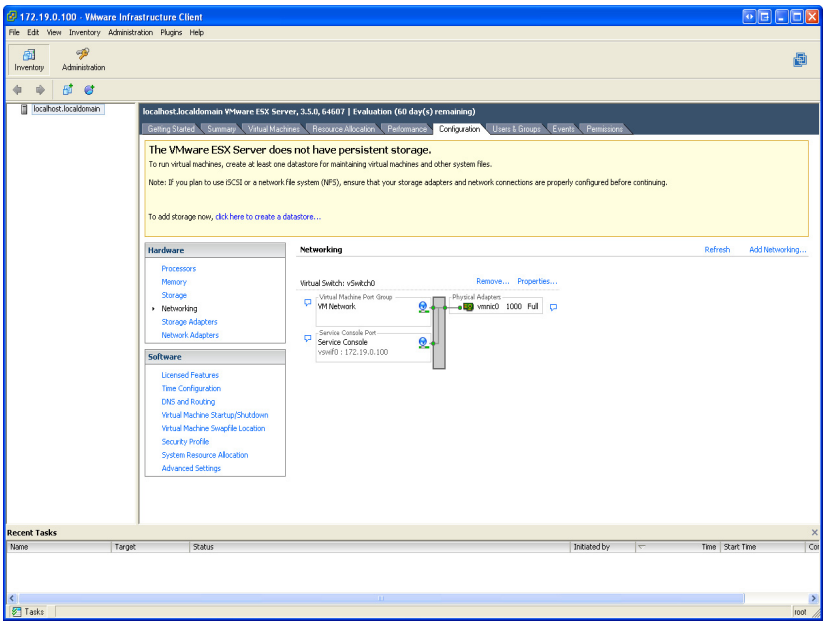
Step III. Configure VMware ESX Server 3.5

Create a VMkernel

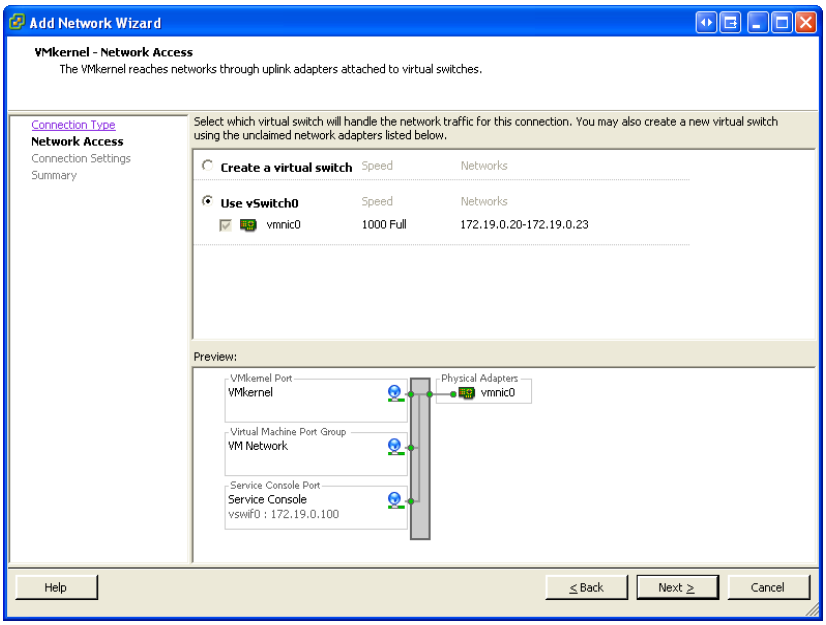
1. Run the VMware Infrastructure Client.
2. Select the IP of the VMware ESX Server. Use the root login with the password entered during the VMware ESX Server installation.



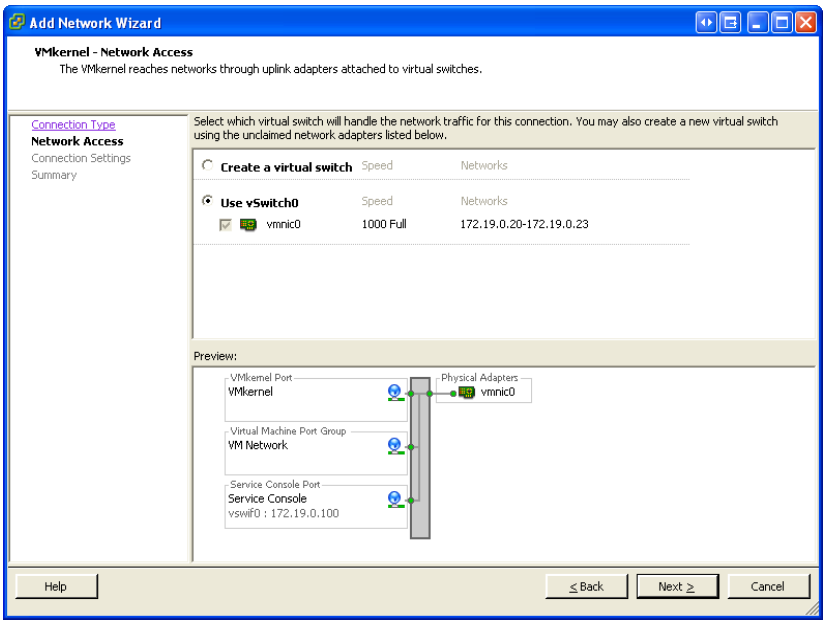
3. Select the **Configuration** tab. Click: **Hardware** > **Networking** > **Add Networking**.



4. Select **VMkernel** and click **Next**.



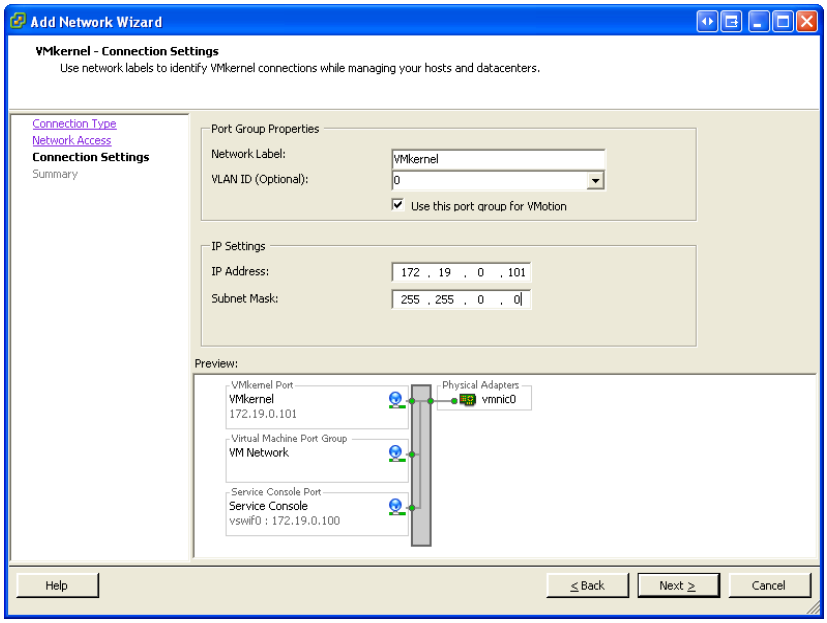
5. Select **Use vSwitch0** and click **Next**.



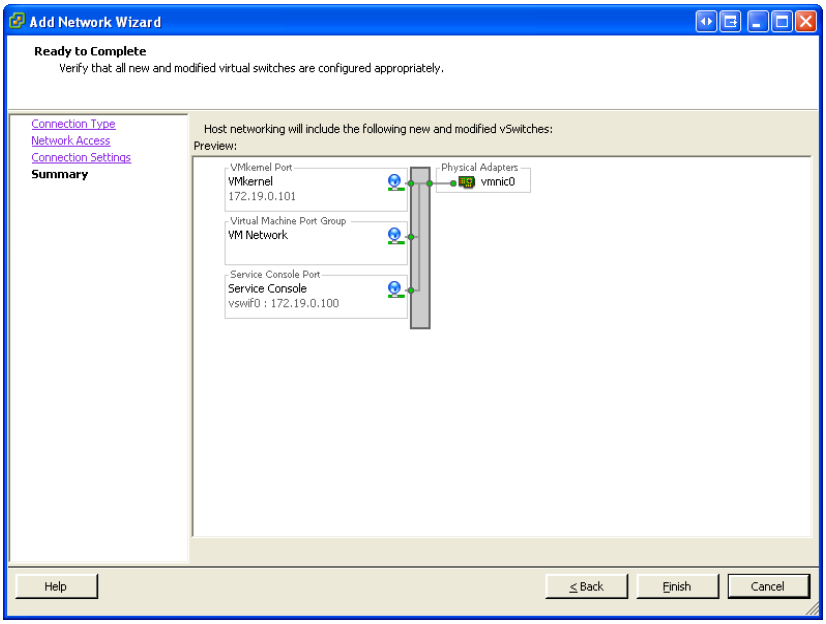
6. In the "Add Network Wizard" fill in the fields provided:

- Under **Port Group Properties**:
  - **Network Label**: Enter a network label.
  - **VLAN ID**: Select a VLAN ID,
  - Select **Use this port group for VMotion**.
- Under **IP Settings**:
  - **IP Address**: Enter an IP address
  - **Subnet mask**: Enter a subnet mask.

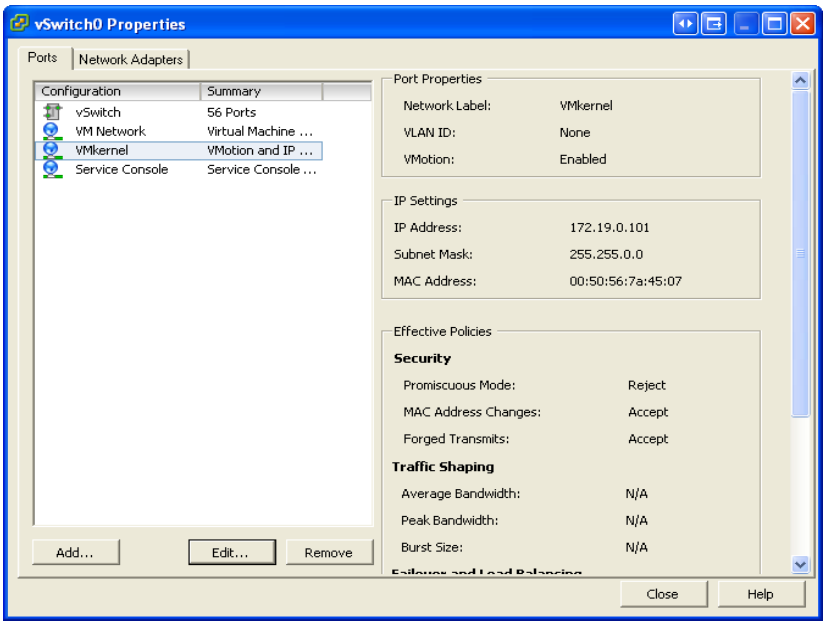
a. Click **Next**.



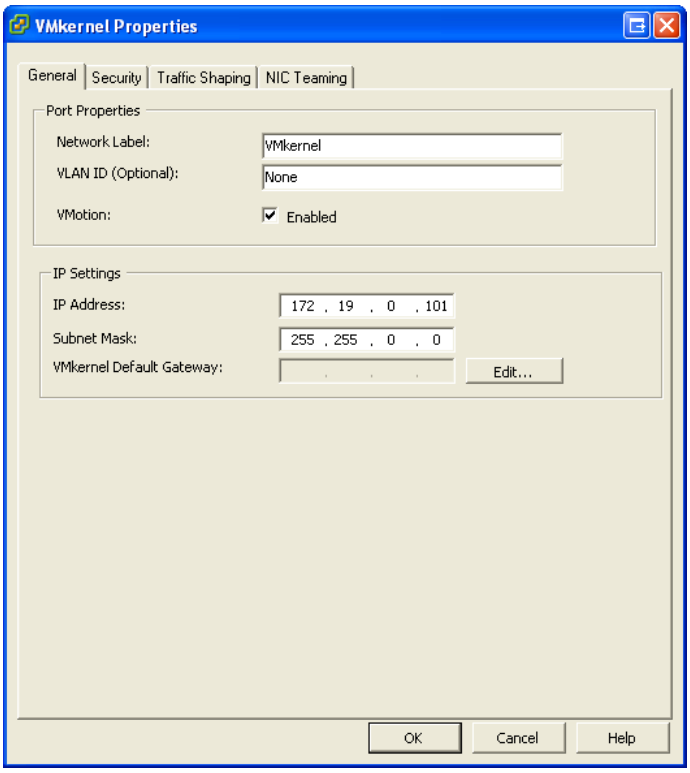
7. Click **Finish**.



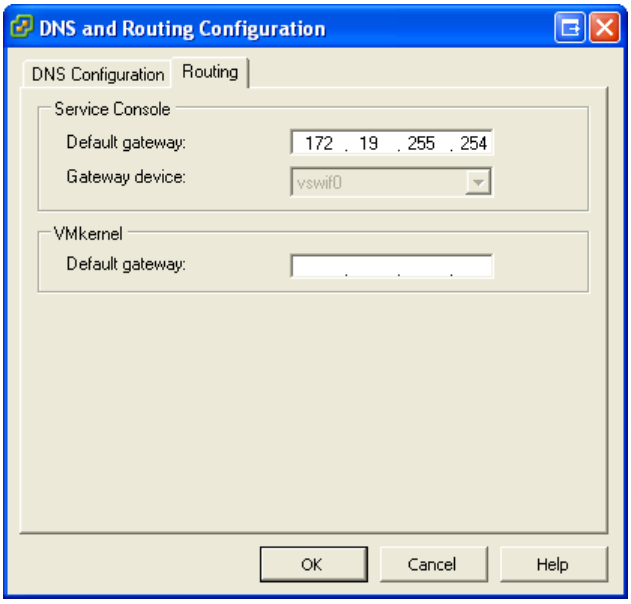
8. To make changes to the VMkernel, select the VMkernel and click **Edit**.



9. To add a default gateway to the VMkernel, click the **General** tab and click **Edit**.

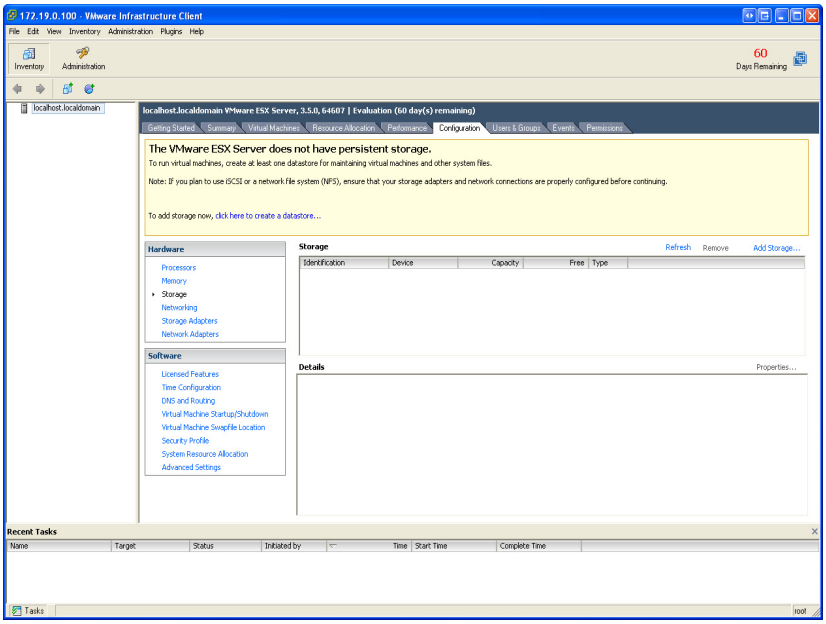


10. Enter a valid IP address for the default gateway. Click **OK**.

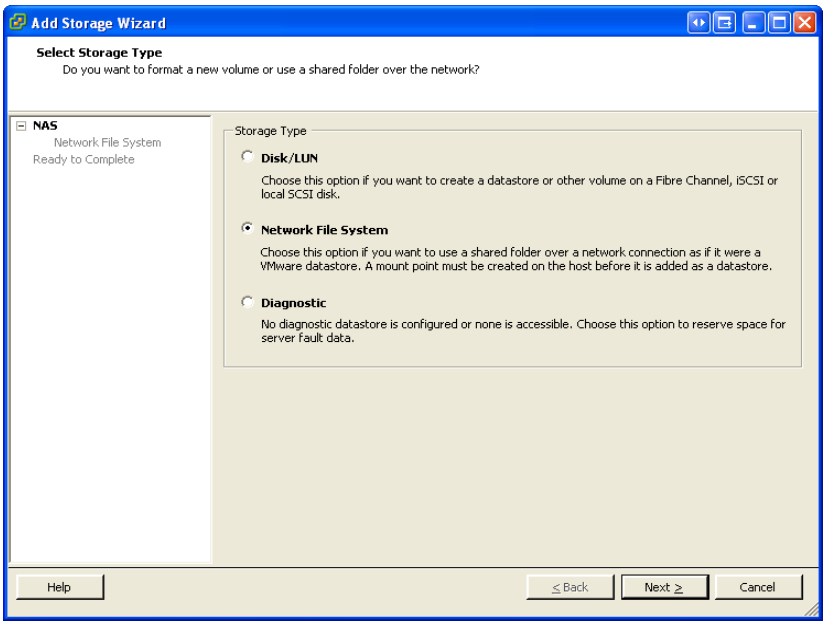


Create a Datastore

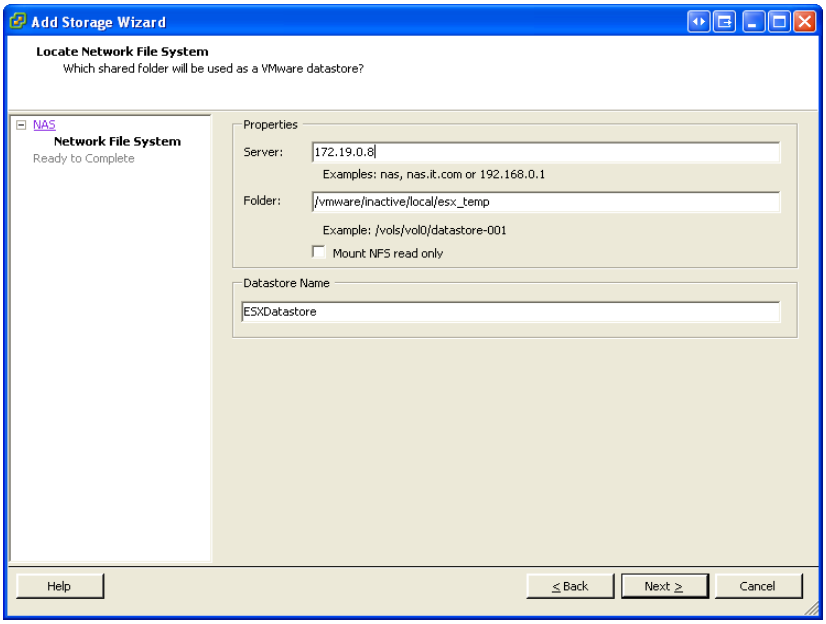
1. From the VMware Infrastructure Client, click the **Configuration** tab. Under **Hardware**, click: **Storage > Add Storage**.



2. Select a storage type. If you will be storing the virtual machines on a Fibre Channel, iSCSI, or local SCSI disk, select **Disk/LUN**. If you will be storing the virtual machines on a network shared folder, select **Network File System**. Click **Next**.

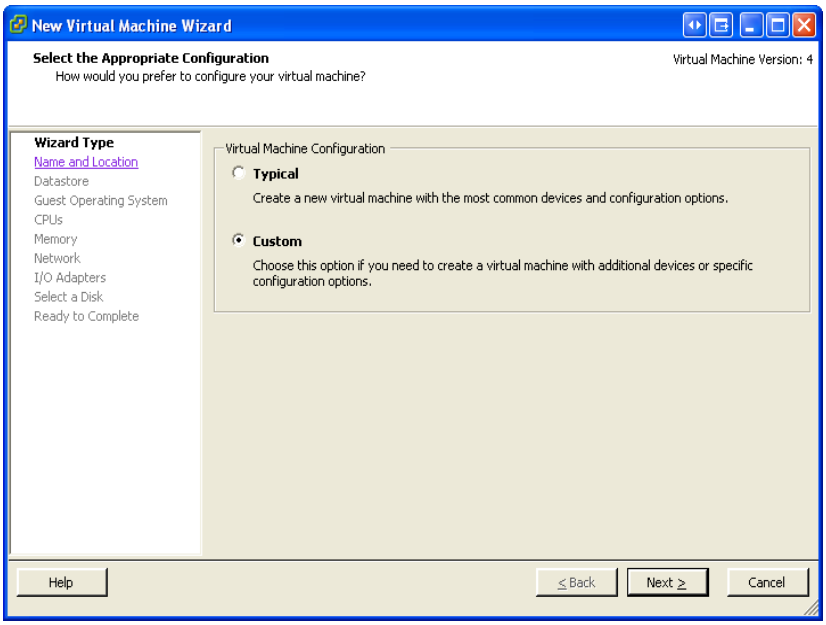


3. Enter storage location information.
   a. If you selected **Disk/LUN** in the previous step, select the SCSI device to use for your datastore and click **Next**. If the drive is not blank and you do not want these files to be overwritten, select **User free space**, otherwise select **Use the entire device**.
      1) Click **Next**.
      2) Enter a datastore name and click **Next**.
      3) Click **Next**.
      4) Click **Finish**.
   b. If you selected **Network File System** in the previous step, enter the IP address or hostname of the server with the network file system.
      1) Enter the path of the directory of the network shared folder.
      2) Enter a datastore name.
      3) Click **Next**.
      4) Click **Finish**.

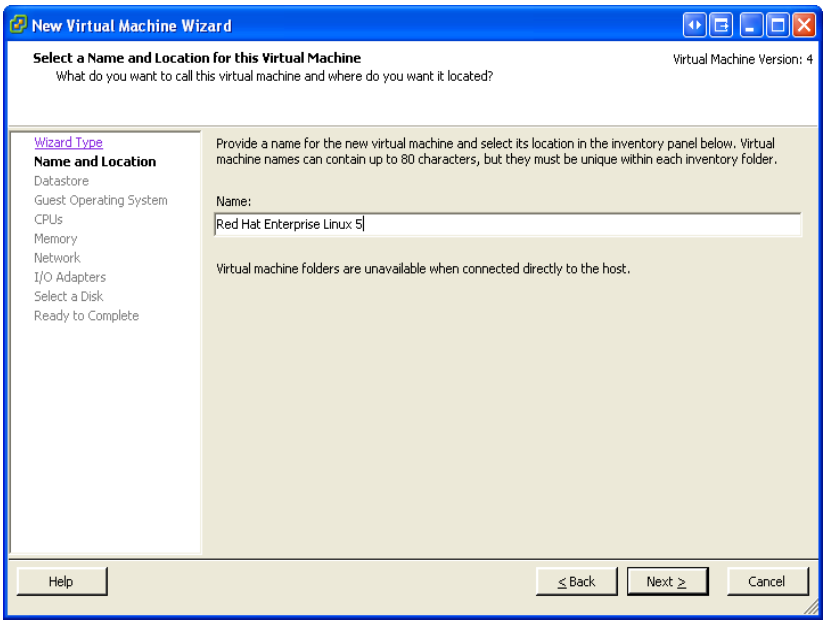


Step IV. Create a Virtual Machine

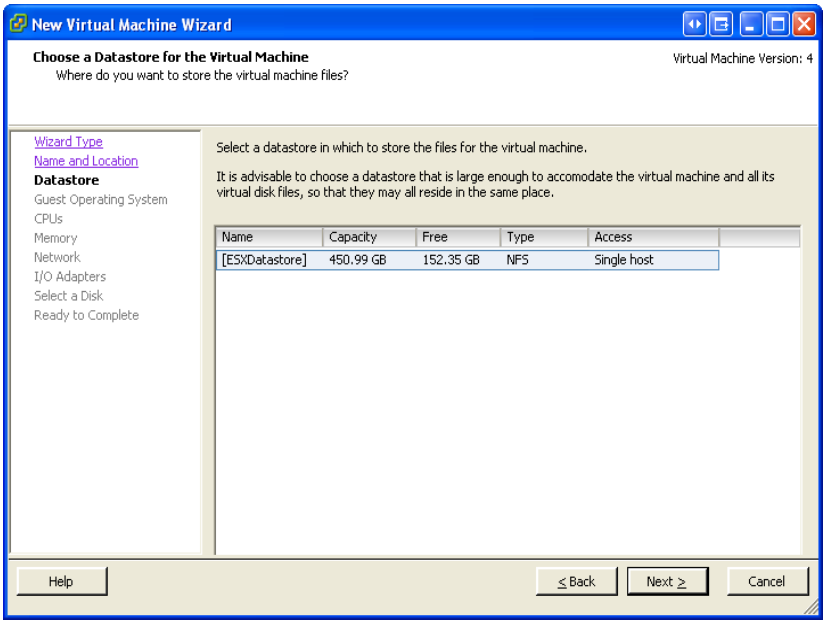
1. From the VMware Infrastructure Client, right-click the VMware ESX Server on the left side, and select **New Virtual Machine**.
2. Select **Custom** and click **Next**.



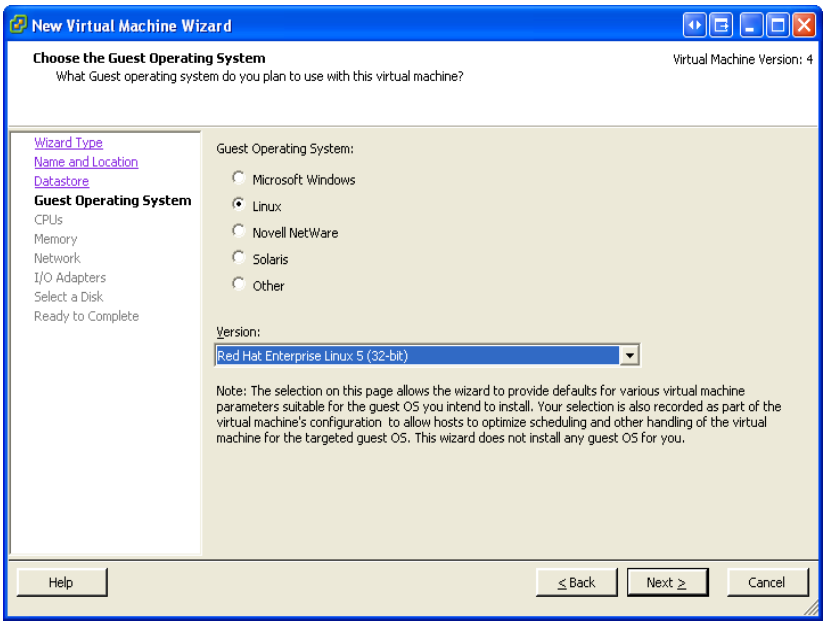
3. Enter a name for the virtual machine and click **Next**.



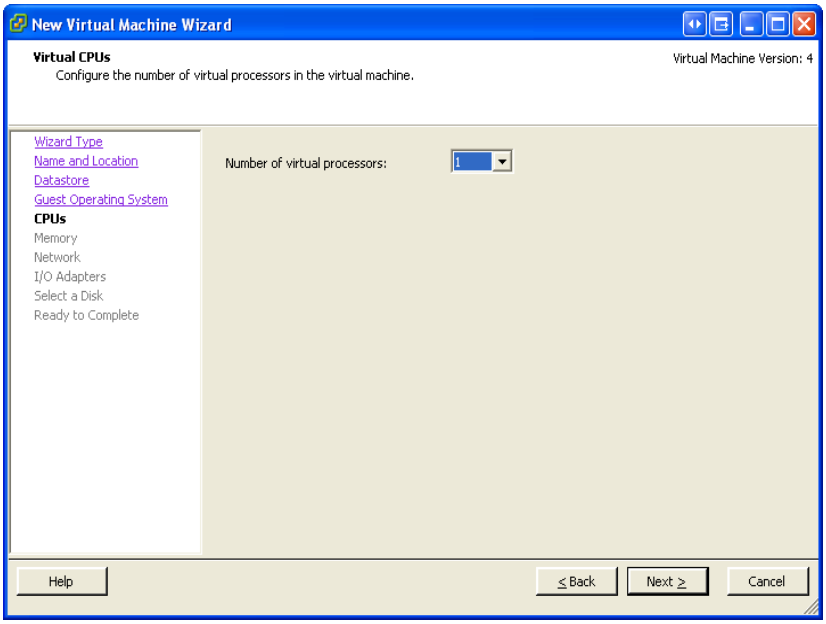
4. Select the datastore that was created in the previous section: "Create a Datastore," on page 332.



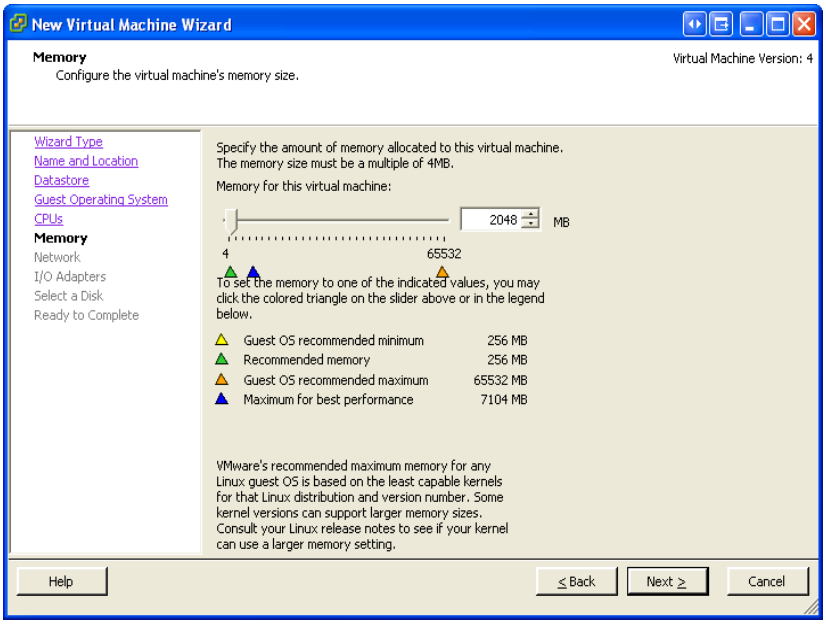
5. Select the guest operating system type and version. Click **Next**.



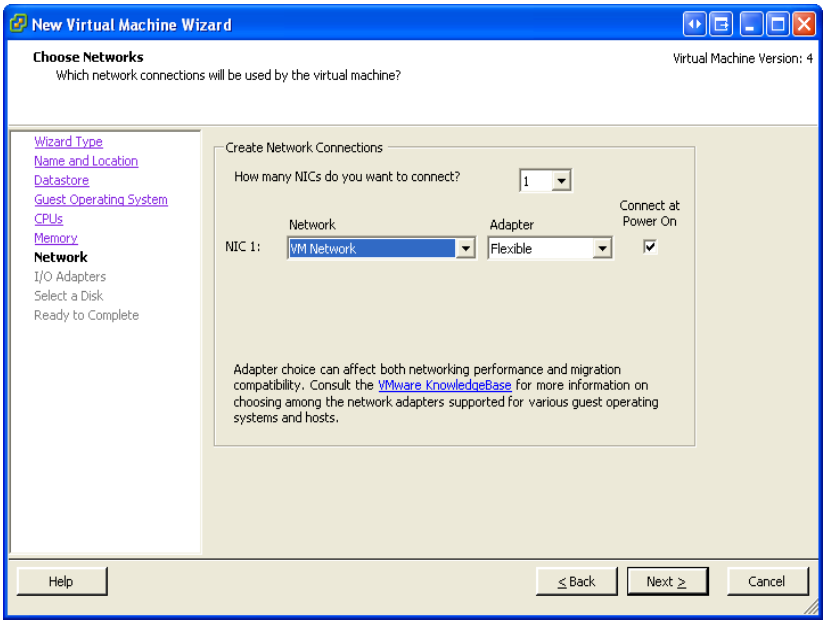
6. Select the **Number of virtual processors** to allocate to the virtual machine. Click **Next**.



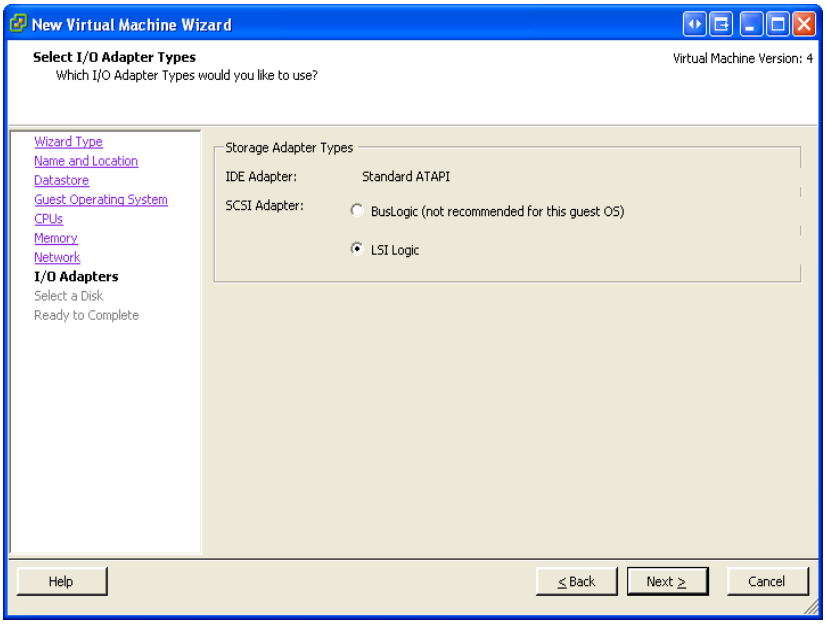
7. Select the amount of memory to allocate to the virtual machine. Click **Next**.



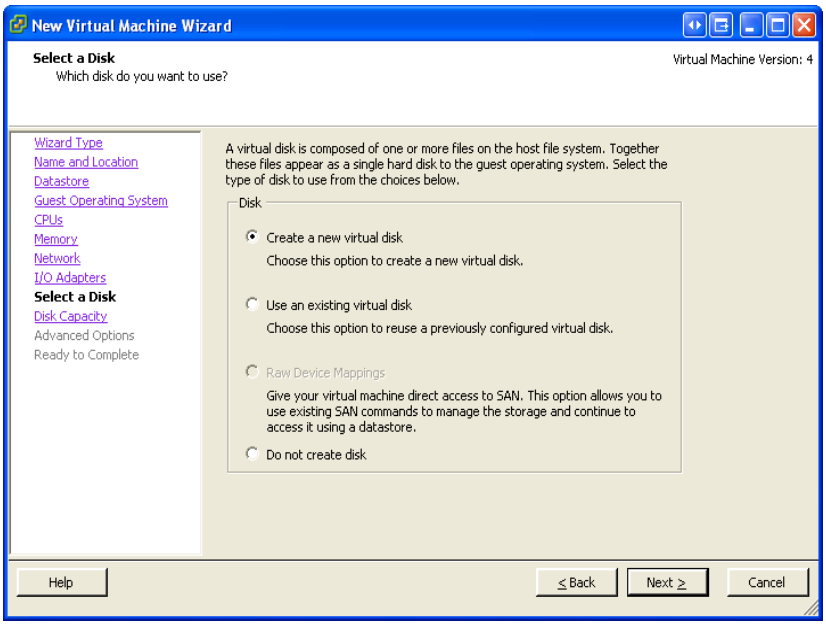
8. Select the number of physical network interface cards to allocate to the virtual machine. Select **Connect at Power On** for each network interface card. Click **Next**.



9. Select a storage adapter type. Click **Next**.

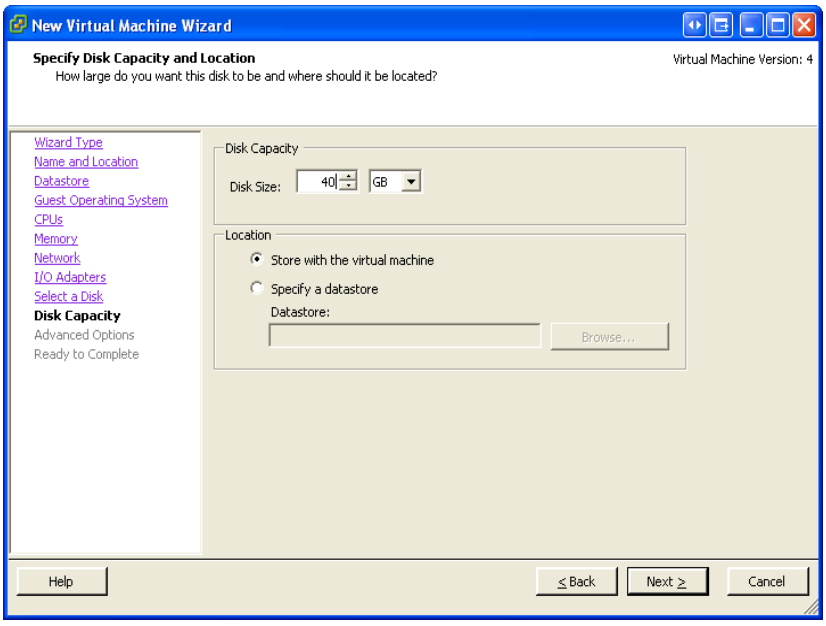


10. Select **Create a new virtual disk** and click **Next**.

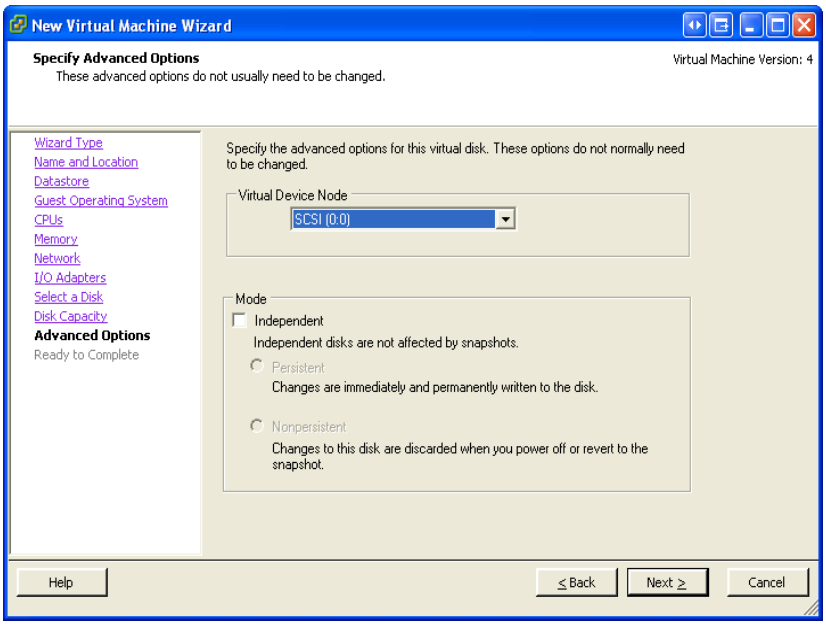


11. Select the disk size for the virtual machine.

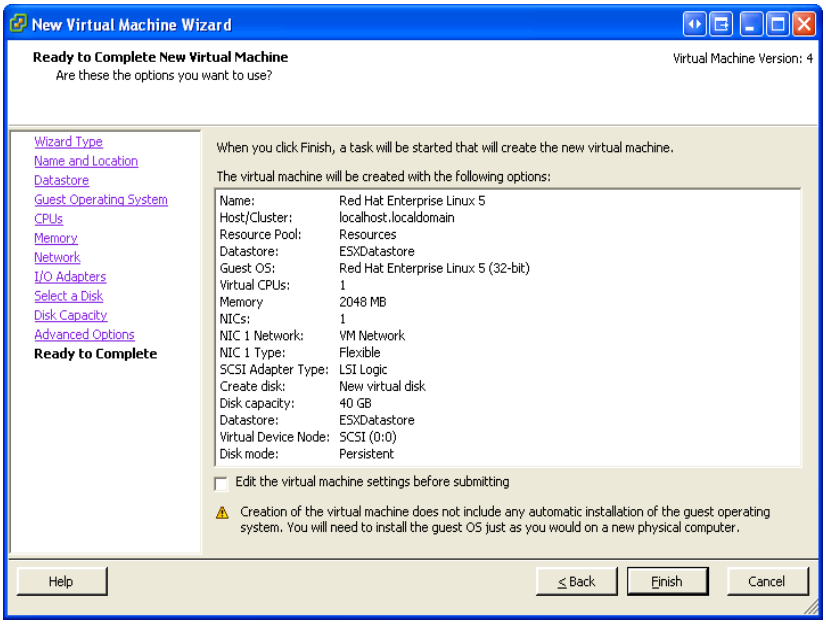
- If you want the virtual machine stored on the VMware ESX Server machine, select **Store with the virtual machine**.
- If you want the virtual machine stored in the datastore, select **Specify a datastore** and select the datastore location.



12. Select a virtual device node and click **Next**.



13. Review the virtual machine settings. Click **Finish**.

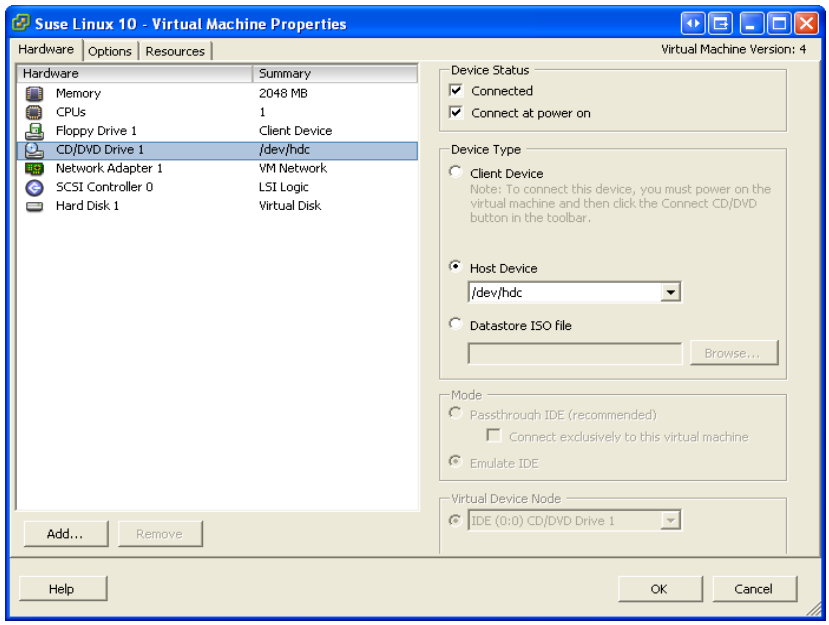


14. If you are installing the guest operating system from a CD or DVD, enter the disc into either the CD/DVD drive of the machine with VMware ESX Server 3.5 installed, or the machine with VMware Infrastructure Client installed. If you are installing the guest operating system from `.ISO files`, copy the files to the datastore created in the previous section.

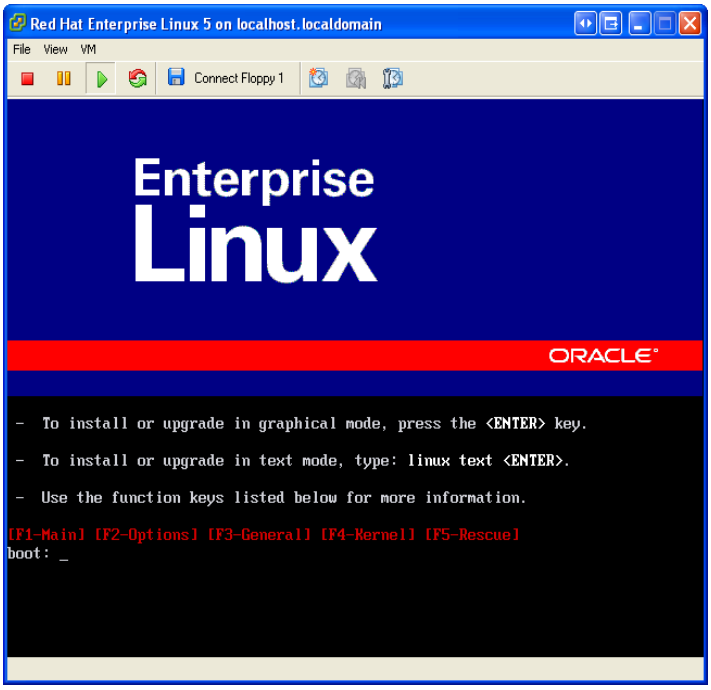
15. Click the **Virtual Machines** tab. Right-click the newly created virtual machine and click **Edit Settings**. Click **CD/DVD Drive 1**.

    a. Depending on where you put your installation media in the previous step, map the virtual CD/DVD drive to that location.

    - If your installation media is in the drive of the machine with VMware Infrastructure Client, select **Client Device**. You will not be able to connect this device until after the machine is started. To start the machine click **Connect CD/DVD** from the console.
    - If your installation media is in the drive of the machine with VMware ESX Server 3.5, select **Host Device** and the location of the device. Make sure you also select **Connected** and **Connect at power on**.
    - If your installation media is located in the datastore, select **Datastore ISO file** and select the path to the file. Click **OK**.



16. Right-click on the virtual machine name on the left side and click **Open Console**.

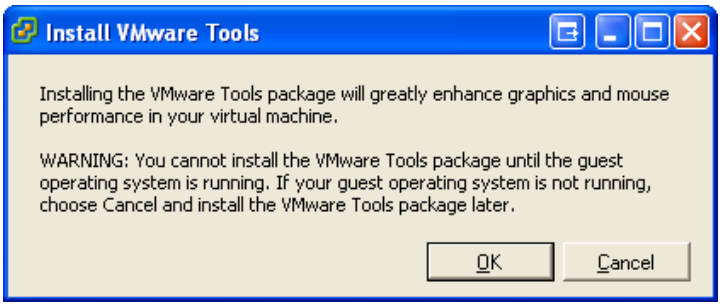


17. Click the **Virtual Machines** tab. Right-click the newly created virtual machine and click **Power On**. If your installation media is located on the client machine, click **Connect CD/DVD** from the console.

Step V. Install VM Tools

On a Windows Guest

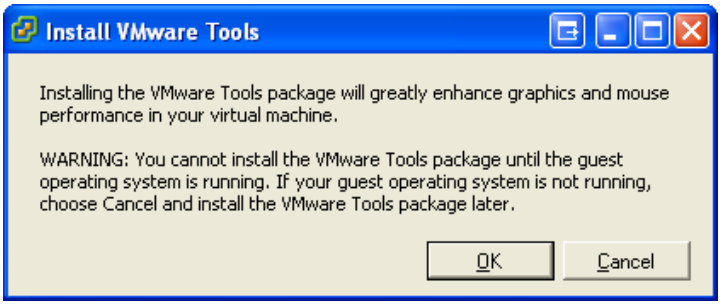
1. Open a console to the virtual machine.
2. Power on the virtual machine.
3. In the console, click **VM** and click **Install/Upgrade VMware Tools**.
4. When the dialog box opens, click **OK**.



5. From inside the virtual machine, click **OK**.
6. Click **Start** > **Run** and enter `D:\setup.exe`, where `D:` is the first CD-ROM drive on the machine, to start the InstallShield wizard.
7. After the installation has been completed, if you are using a Windows 2000 or Windows XP guest operating system, reboot the virtual machine.

On a Unix Guest

1. Open a console to the virtual machine.
2. Power on the virtual machine.
3. In the console, click **VM** and click **Install/Upgrade VMware Tools**.
4. When the dialog box opens, click **OK**.



5. From inside the virtual machine, when you're logged in as the root user, mount the VMware Tools virtual CD-ROM image and change to a working directory (`/tmp`).

- On Linux:

  mount: `/dev/cdrom /mnt/cdrom`

  `cd /tmp`

- On Solaris:

  `cd /tmp`

  If the CD-ROM was not already mounted as `/cdrom/vmwaretools`, restart the volume manager using the following commands:

  `/etc/init.d/volmgt stop`
  `/etc/init.d/volmgt start`

6. Uncompress the installer and unmount the CD-ROM image.

- On Linux:

  `tar zxpf /mnt/cdrom/VMwareTools-3.5.0-64607.tar.gz`
  `umount /dev/cdrom`

- On Solaris:

  `gunzip -c /cdrom/vmwaretools/vmware-solaris-tools.tar.gz | tar xf -`

7. Run the VMware Tools tar installer:

   ```
   cd vmware-tools-distrib
   ./vmware-install.pl
   ```

   a. Respond to the questions the installer displays.

8. Start your graphical environment.

9. Start VMware Tools

   `vmware-toolbox` `&`