

Content Server

Version: 7.0

Configuring Third-Party Software

Document Revision Date: Mar. 26, 2007



FATWIRE CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall FatWire be liable for any loss of profits, loss of business, loss of use of data, interruption of business, or for indirect, special, incidental, or consequential damages of any kind, even if FatWire has been advised of the possibility of such damages arising from this publication. FatWire may revise this publication from time to time without notice. Some states or jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

Copyright © 2007 FatWire Corporation. All rights reserved.

This product may be covered under one or more of the following U.S. patents: 4477698, 4540855, 4720853, 4742538, 4742539, 4782510, 4797911, 4894857, 5070525, RE36416, 5309505, 5511112, 5581602, 5594791, 5675637, 5708780, 5715314, 5724424, 5812776, 5828731, 5909492, 5924090, 5963635, 6012071, 6049785, 6055522, 6118763, 6195649, 6199051, 6205437, 6212634, 6279112 and 6314089. Additional patents pending.

FatWire, Content Server, Content Server Bridge Enterprise, Content Server Bridge XML, Content Server COM Interfaces, Content Server Desktop, Content Server Direct, Content Server Direct Advantage, Content Server DocLink, Content Server Engage, Content Server InSite Editor, Content Server Satellite, and Transact are trademarks or registered trademarks of FatWire, Inc. in the United States and other countries.

iPlanet, Java, J2EE, Solaris, Sun, and other Sun products referenced herein are trademarks or registered trademarks of Sun Microsystems, Inc. *AIX, IBM, WebSphere*, and other IBM products referenced herein are trademarks or registered trademarks of IBM Corporation. *WebLogic* is a registered trademark of BEA Systems, Inc. *Microsoft, Windows* and other Microsoft products referenced herein are trademarks or registered trademarks of Microsoft Corporation. *UNIX* is a registered trademark of The Open Group. Any other trademarks and product names used herein may be the trademarks of their respective owners.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>) and software developed by Sun Microsystems, Inc. This product contains encryption technology from Phaos Technology Corporation.

You may not download or otherwise export or reexport this Program, its Documentation, or any underlying information or technology except in full compliance with all United States and other applicable laws and regulations, including without limitation the United States Export Administration Act, the Trading with the Enemy Act, the International Emergency Economic Powers Act and any regulations thereunder. Any transfer of technical data outside the United States by any means, including the Internet, is an export control requirement under U.S. law. In particular, but without limitation, none of the Program, its Documentation, or underlying information of technology may be downloaded or otherwise exported or reexported (i) into (or to a national or resident, wherever located, of) Cuba, Libya, North Korea, Iran, Iraq, Sudan, Syria, or any other country to which the U.S. prohibits exports of goods or technical data; or (ii) to anyone on the U.S. Treasury Department's Specially Designated Nationals List or the Table of Denial Orders issued by the Department of Commerce. By downloading or using the Program or its Documentation, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list or table. In addition, if the Program or Documentation is identified as Domestic Only or Not-for-Export (for example, on the box, media, in the installation process, during the download process, or in the Documentation), then except for export to Canada for use in Canada by Canadian citizens, the Program, Documentation, and any underlying information or technology may not be exported outside the United States or to any foreign entity or “foreign person” as defined by U.S. Government regulations, including without limitation, anyone who is not a citizen, national, or lawful permanent resident of the United States. By using this Program and Documentation, you are agreeing to the foregoing and you are representing and warranting that you are not a “foreign person” or under the control of a “foreign person.”

Configuring Third-Party Software

Document Revision Date: Mar. 26, 2007

Product Version: 7.0

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

About This Guide	7
Who Should Use This Guide	7
Graphics in This Guide	7
Technical Support	7

Part 1. Creating and Configuring a Database

1 Creating and Configuring an Oracle 9.2.0.x Database	11
Step I. Create an Oracle 9.2.0.x Database	12
Step II. Configure the Database for Content Server	15
Next Step	19
2 Creating and Configuring an Oracle 10g Database	21
Step I. Create an Oracle 10g Database	22
Step II. Create a New User for Content Server	37
Next Step	44
3 Creating and Configuring an MS SQL Server Database.	45
Creating a Database on MS SQL Server 2000 SP3+	46
Creating a Database on MS SQL Server 2005	46
4 Creating and Configuring an IBM DB2 8.x Database	49
Creating and Configuring DB2 8.x for Content Server	50
5 Creating and Configuring an IBM DB2 9.1 Database	53
Installing and Configuring DB2 9.1 for Content Server	54
A. Install DB2	54
B. Create a New DB2 Database.	68
C. Create a User for the New Database	74

D. Configure the Database.	77
---------------------------------	----

Part 2. Installing a Web Server

6 Worksheets for Documenting the Web Server Installation	83
Key to Sample Values	84
Web Server Parameters	84
7 Installing IIS on Windows	87
Step I. Install IIS	88
Step II. Document Your IIS Installation	88
Step III. Verify the Installation	88
A. Start IIS	88
B. Verify that IIS is Serving Pages	89
Next Step	89
8 Installing Apache on Solaris and Linux	91
Step I. Install Apache.	92
Step II. Document Your Apache Parameters.	92
Step III. Verify that Apache Contains the Correct Module.	93
Step IV. Verify that Apache Runs Properly	93
Next Step	93

Part 3. Install and Configuring LDAP

9 Setting Up Sun Java Systems Access Manager 7.0	97
Start/Stop Commands	98
Creating CS Users in Sun Access Manager.	98
10 Setting Up Sun Java Systems Directory Server 5.2	107
Start/Stop Commands	108
Starting and Stopping Sun Directory Server	108
Starting and Stopping the Sun Directory Server Admin Interface	108
Installing Sun Directory Server	109
Verifying Your LDAP Configuration	119
Modifying User Passwords	122
11 Setting Up OpenLDAP 2.3.x	125
OpenLDAP Commands	126
Starting OpenLDAP.	126
Searching an OpenLDAP Server.	126

Adding an LDIF File to an OpenLDAP Server	127
Installing OpenLDAP	128
Configuring OpenLDAP	130
Adding Content Server Schema to OpenLDAP	133
Modifying User Passwords	135
Modifying User Passwords Using an LDAP Browser	135
Modifying User Passwords Using the ldapmodify Command	138
12 Setting Up the WebLogic 9.x Embedded LDAP Server	139
Enabling the WebLogic Embedded LDAP Server	140
Modifying User Passwords	142

About This Guide

This guide contains information about installing and configuring third-party software specifically for use by Content Server. Instructions in this guide supplement the instructions in the Content Server installation guides. The steps you will follow show you how to create and configure the supported databases, install supported web servers, and integrate Content Server with LDAP servers.

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/contact_info.html

Part 1

Creating and Configuring a Database

Content Server requires access to a supported database that is specifically configured for the product. Supported databases include:

- Oracle 9, 10g
- Microsoft SQL Server 2000 SP3+, 2005
- DB2 8.2, 9.1

The databases listed above are not configured for production, but are set up with full permissions. In practice, the permissions can be curtailed 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.

Instructions on creating and configuring the databases for Content Server are given in the chapters of this guide. Because database configuration is identical across different application servers, refer to the correct chapter to set up the database of your choice.

This part contains the following chapters:

- [Chapter 1, “Creating and Configuring an Oracle 9.2.0.x Database”](#)
- [Chapter 2, “Creating and Configuring an Oracle 10g 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”](#)

Chapter 1

Creating and Configuring an Oracle 9.2.0.x Database

Use this chapter to set up an Oracle 9.2.0.x database for your Content Server installation. For background information regarding database configuration and users' permissions, see [“Creating and Configuring a Database,” on page 9](#).

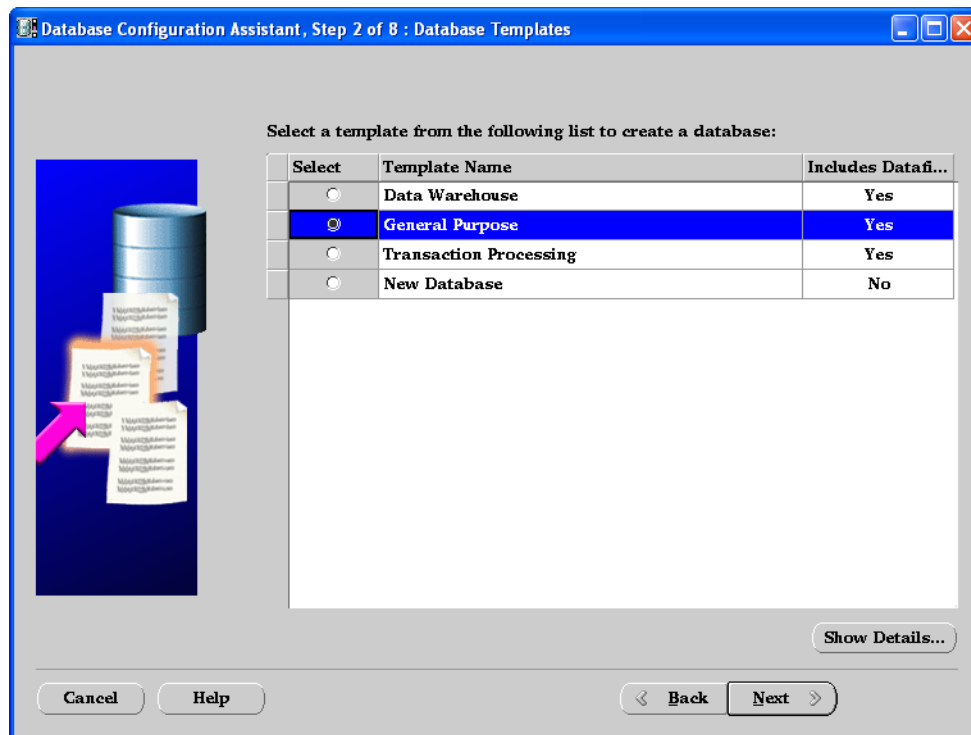
This chapter contains the following sections:

[Step I. Create an Oracle 9.2.0.x Database](#)

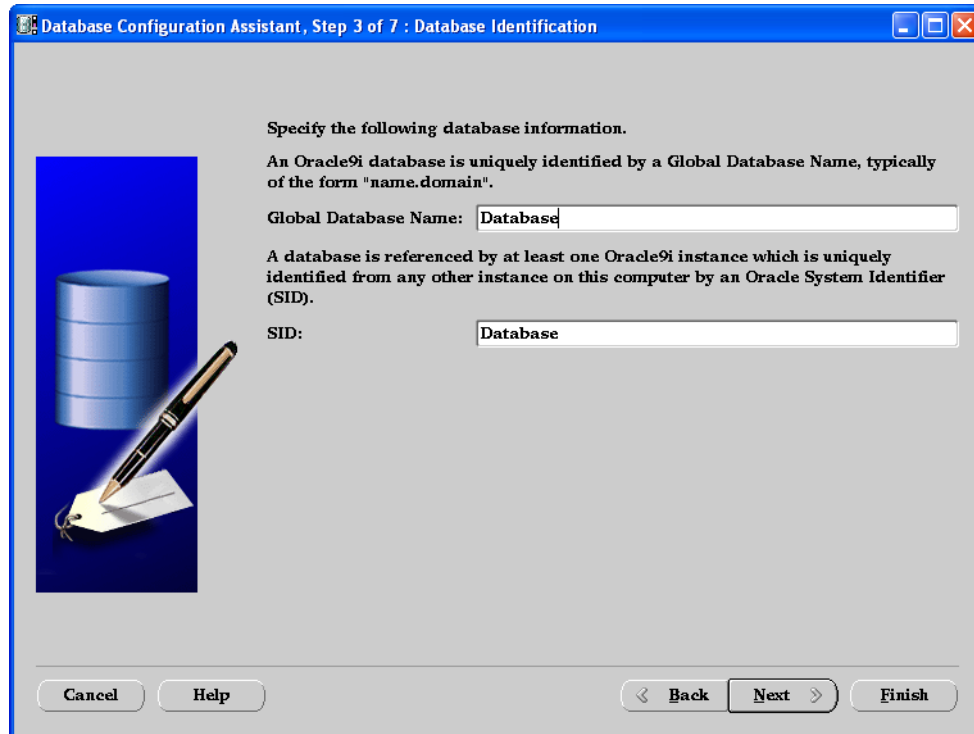
[Step II. Configure the Database for Content Server](#)

Step I. Create an Oracle 9.2.0.x Database

1. Go to the `$ORACLE9_HOME/bin` directory:
`cd $ORACLE9_HOME/bin`
2. Run the Database Configuration Assistant:
`dbca`
3. In the welcome screen, click **Next**.
4. Fill in the following screens as shown below:
 - a. On the “Step 1 of 8: Operations” screen, leave **Create a database** selected and click **Next**.
 - b. On the “Step 2 of 8: Database Templates” screen, select **General Purpose** and click **Next**.



- c. On the “Step 3 of 7: Database Identification” screen, enter the database name in the Global Database Name field. The SID will be automatically set to the first eight characters of the Database Name. Each SID must be unique. Click **Next**.



Specify the following database information.

An Oracle9i database is uniquely identified by a Global Database Name, typically of the form "name.domain".

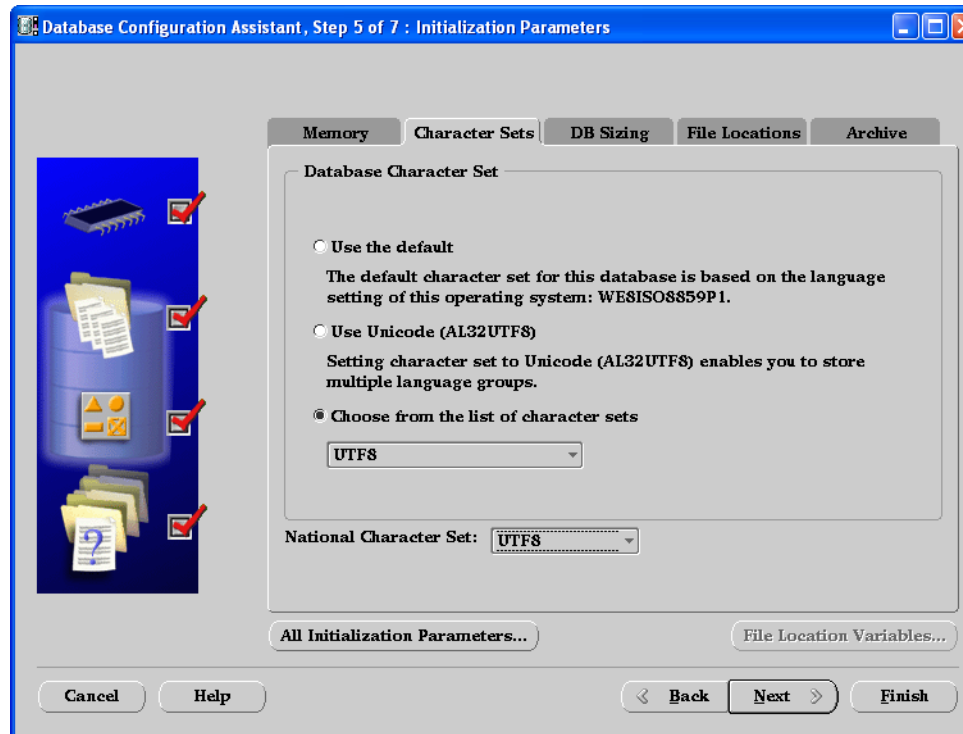
Global Database Name:

A database is referenced by at least one Oracle9i instance which is uniquely identified from any other instance on this computer by an Oracle System Identifier (SID).

SID:

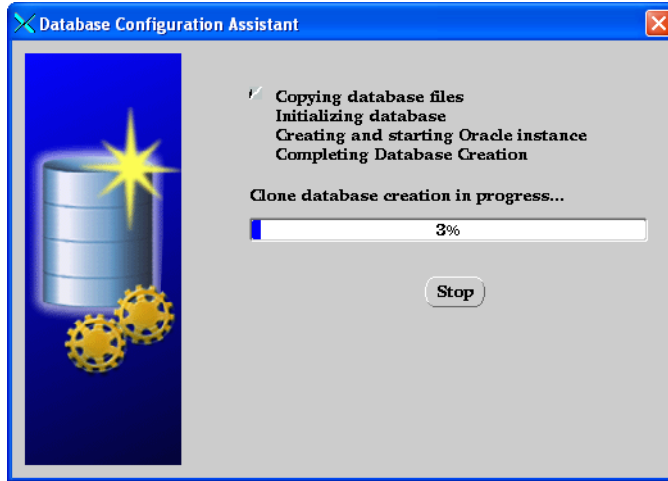
Buttons: Cancel, Help, < Back, Next >, Finish

- d. On the “Step 4 of 7: Database Connection Options” screen, leave **Dedicated Server mode** selected and click **Next**.
- e. On the “Step 5 of 7: Initialization Parameters” screen:
 - 1) Select the tab **Character Sets**.
 - 2) On the character sets screen, select **Choose from the list of character sets** and **UTF8** from the drop-down menu. For the National Character Set select **UTF8** and click **Next**.



- f. On the “Step 6 of 7: Database Storage” screen, click **Next**.
- g. On the “Step 7 of 7: Creation Options” screen, click **Finish**.

5. When the summary screen appears, click **OK**.
6. When the “Installation Progress Screen” appears, wait for the installation to be completed.



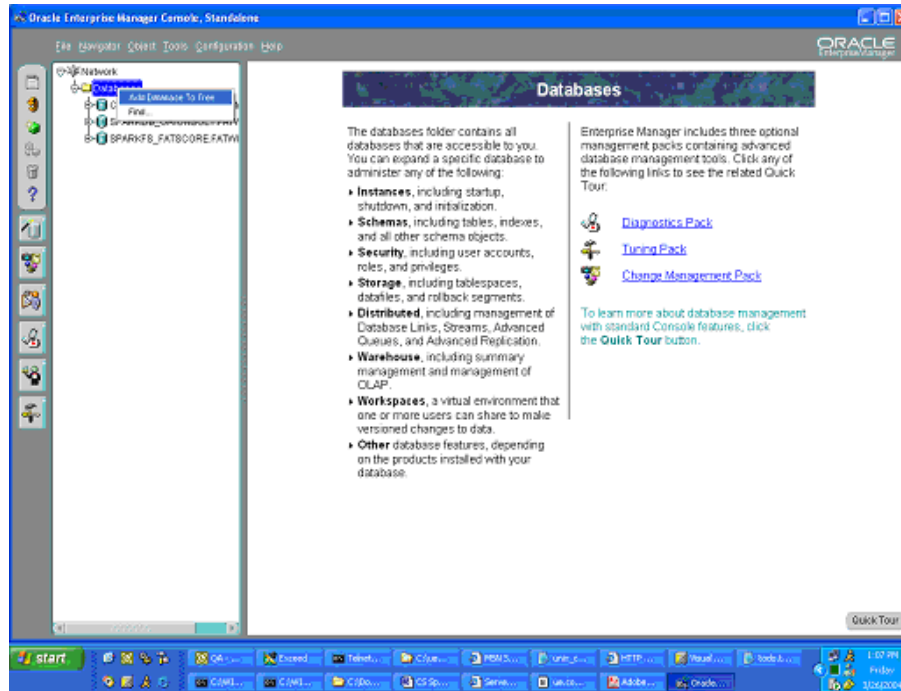
7. After the installation has been completed, the database information screen will appear, listing information about how to connect to this database using the enterprise management console. Click **OK**.

Step II. Configure the Database for Content Server

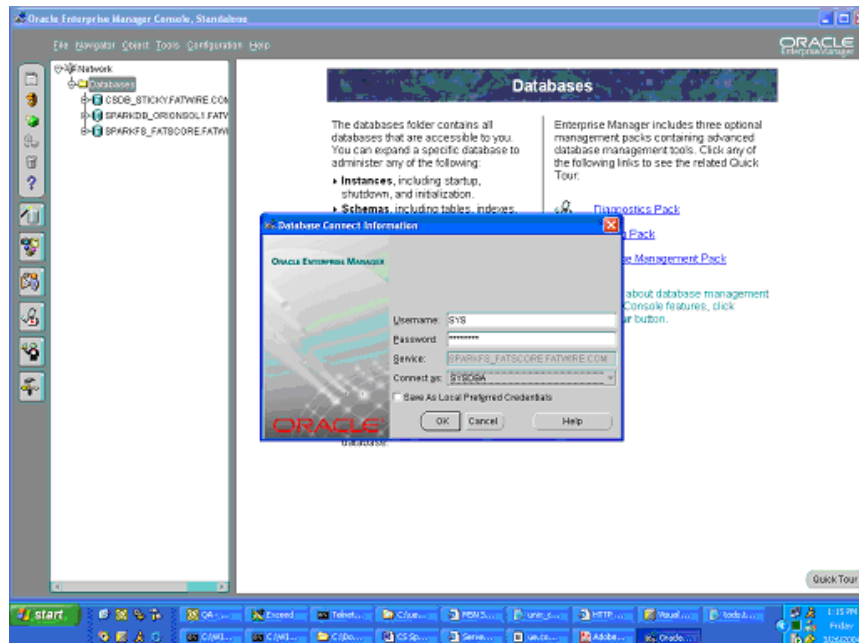
1. Start Oracle Enterprise Manage Console. Click **OK**.



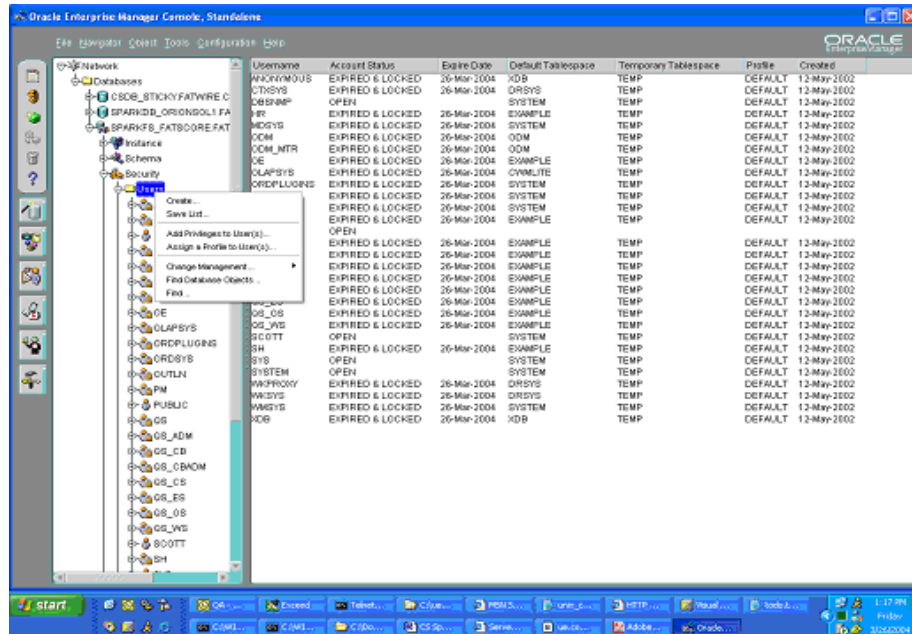
2. Expand **Network > Databases**. Select the database you have created.



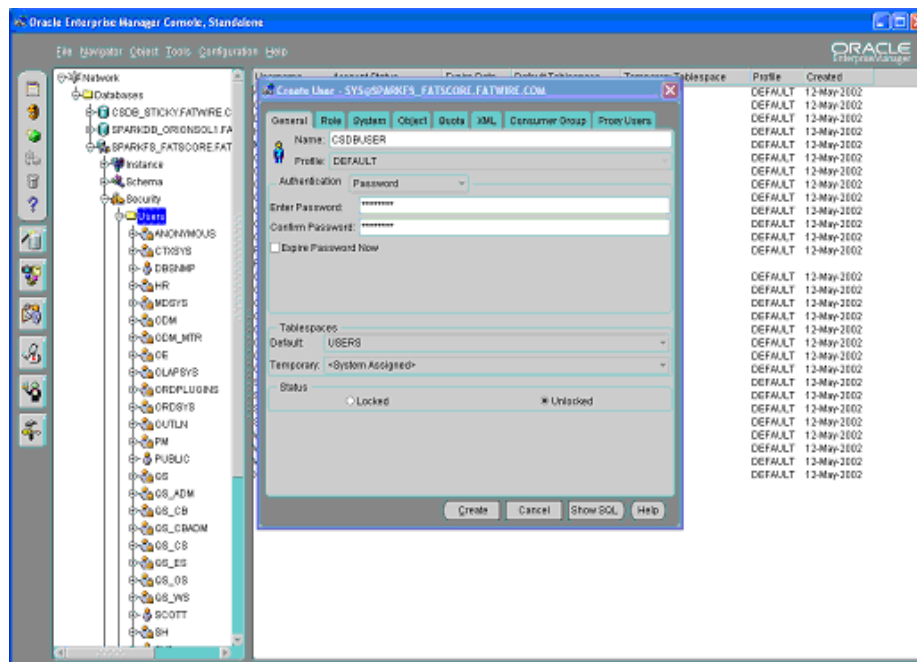
3. In the database login screen, log in as **SYS** and enter the password you specified earlier while creating the database. Click **OK**.



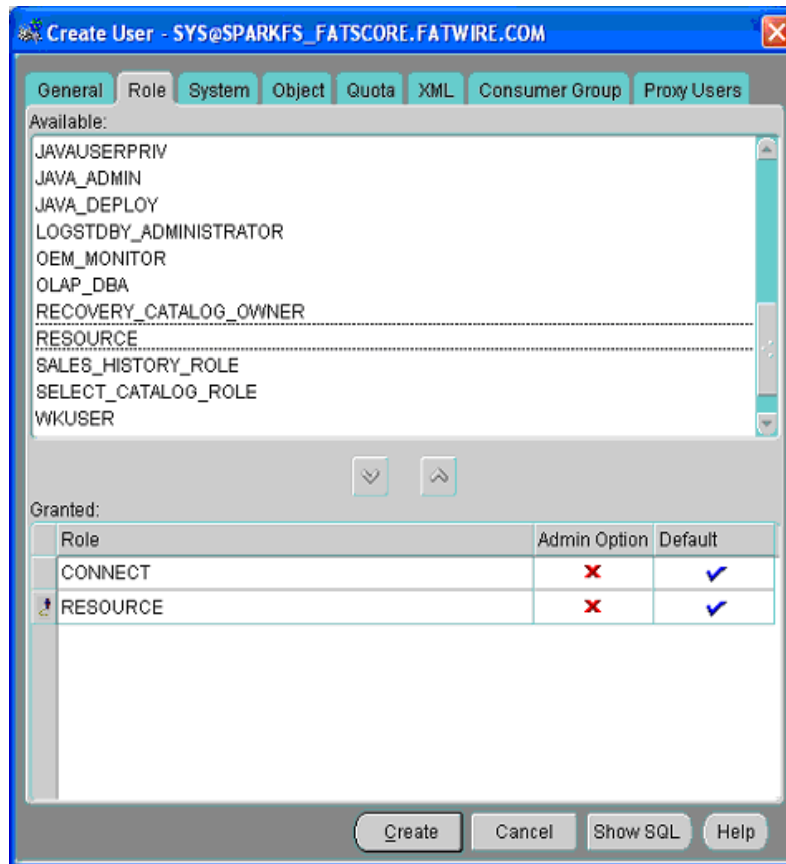
4. Expand **Security > Users**. Right-click and select **Create**.



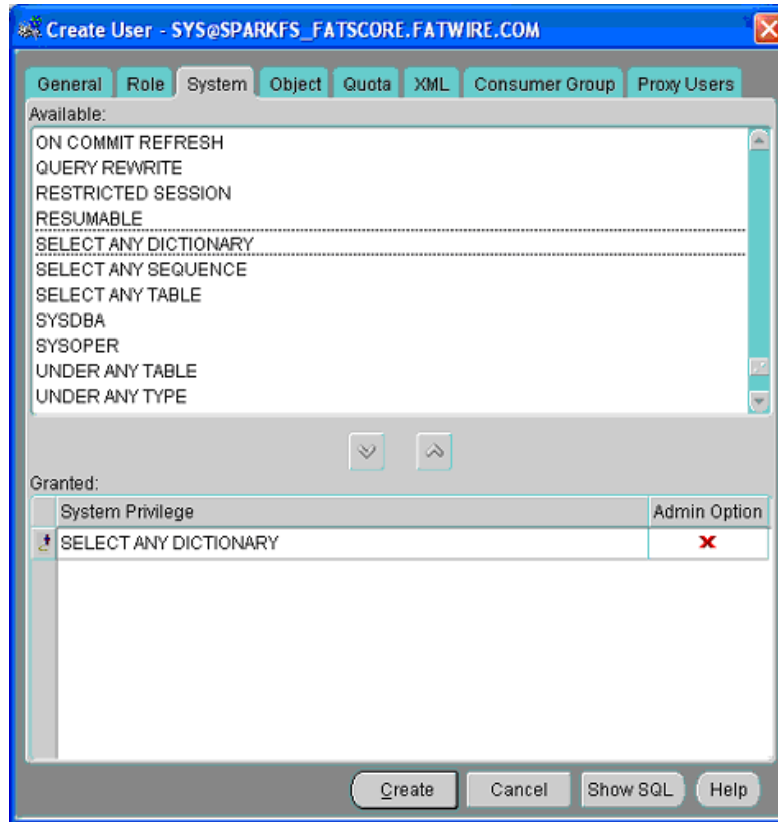
5. On the **General** tab, enter a username and password.



6. On the **Role** tab, select **Connect** and **Resource**.



7. On the **System** tab, choose **Select Any Dictionary**. Click **Create**.



Database configuration is complete.

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 10g Database

Use this chapter to set up an Oracle 10g 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:

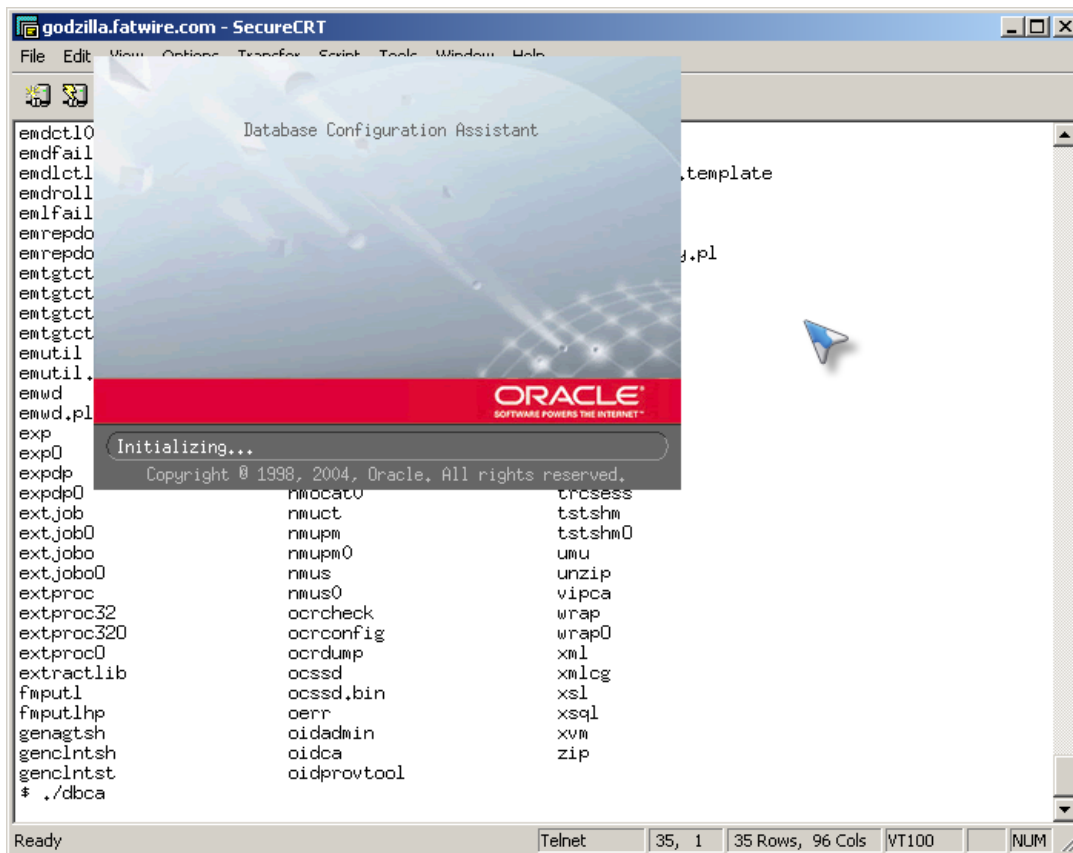
- [Step I. Create an Oracle 10g Database](#)
- [Step II. Create a New User for Content Server](#)

Step I. Create an Oracle 10g Database

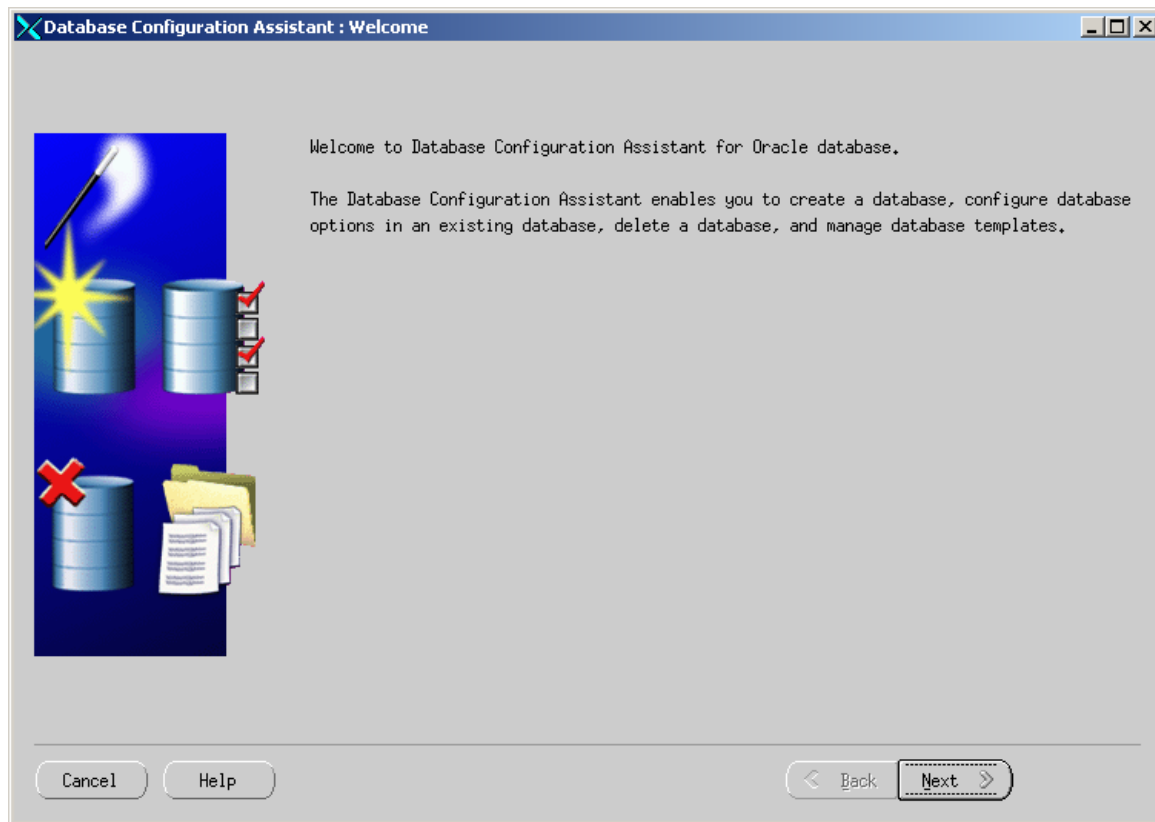
1. Execute the “Oracle Database Configuration Assistant” by doing one of the following:
 - In Unix, execute the command: **dbca**
 - In Windows, go to the “Oracle Programs” group and select **Database Configuration Assistant**.

Note

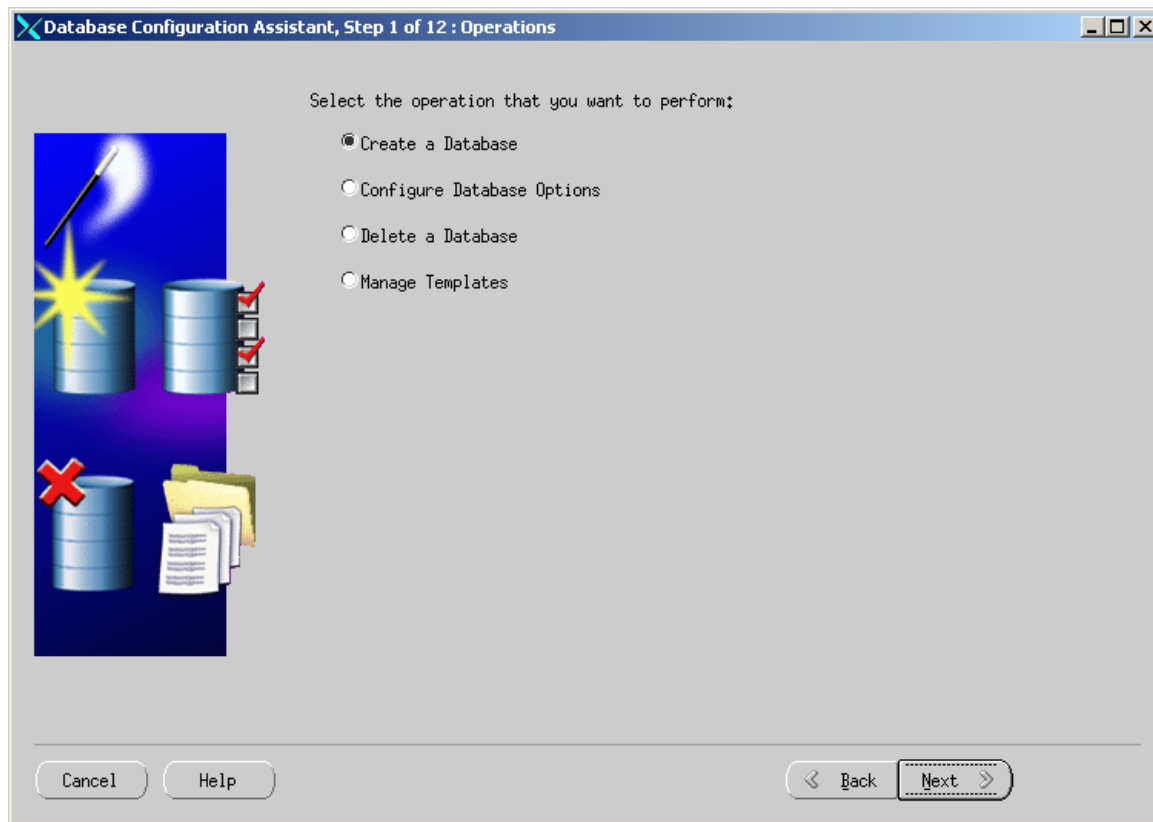
This step displays a load screen that can take some time to complete. Be patient.



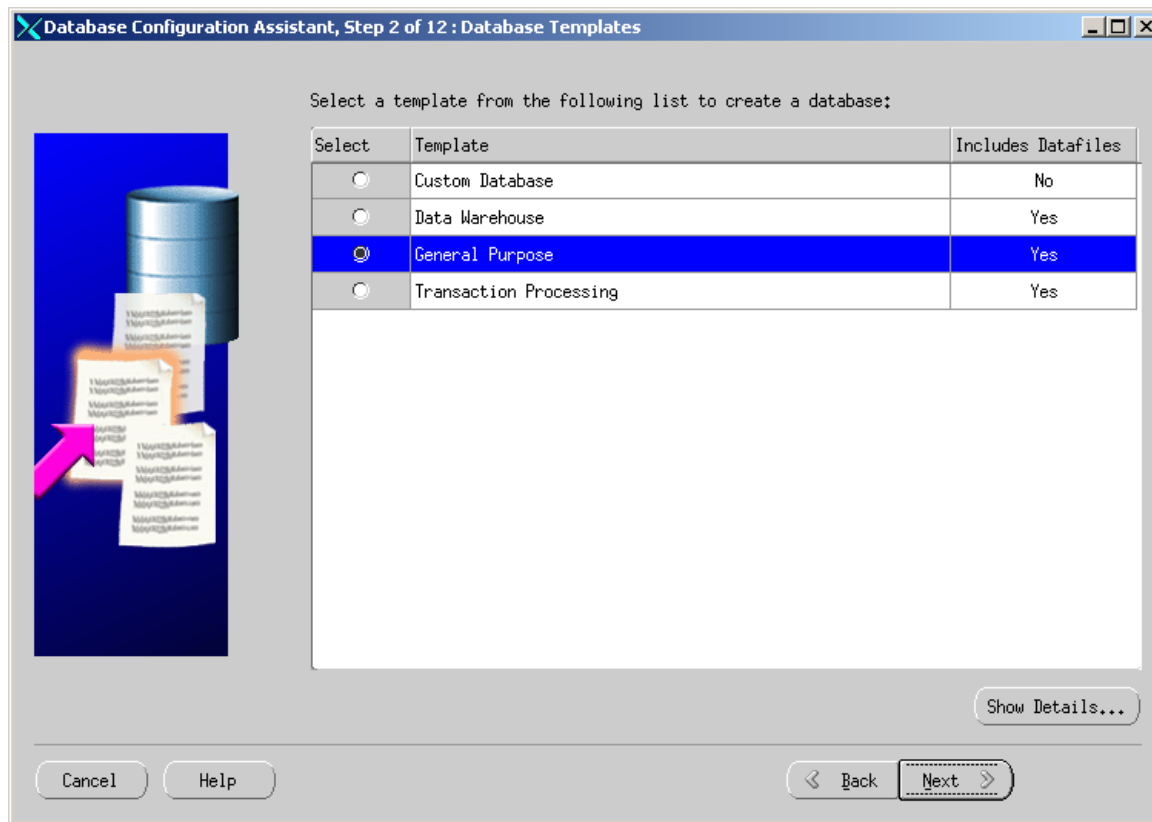
2. On the first screen that is displayed, click **Next**. In the following screen, click **Next**.



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




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



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

Database Configuration Assistant, Step 3 of 12 : Database Identification



An Oracle database is uniquely identified by a Global Database Name, typically of the form "name.domain".

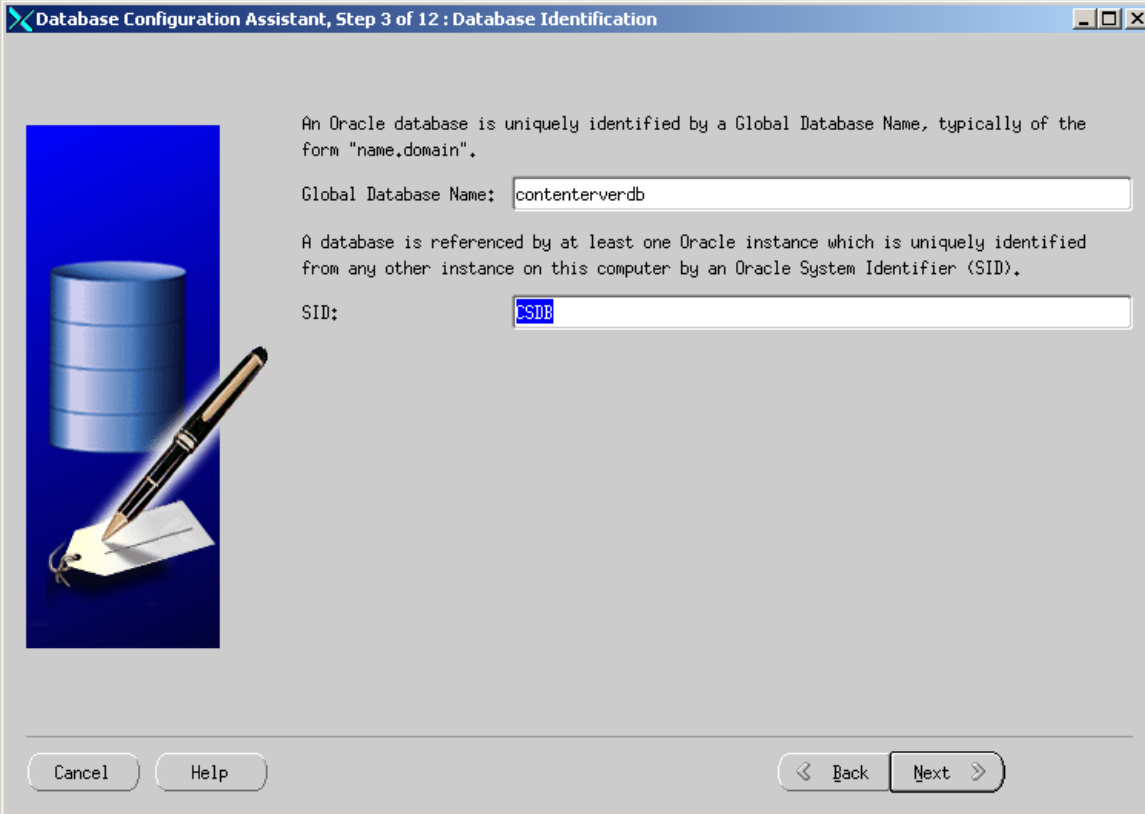
Global Database Name:

A database is referenced by at least one Oracle instance which is uniquely identified from any other instance on this computer by an Oracle System Identifier (SID).

SID:

Cancel Help < Back Next >

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



The screenshot shows the 'Database Configuration Assistant, Step 3 of 12: Database Identification' window. On the left is a graphic of a blue database cylinder and a pen writing on a tag. The main text explains that an Oracle database is uniquely identified by a Global Database Name (typically 'name.domain') and is referenced by at least one Oracle instance uniquely identified by an Oracle System Identifier (SID). There are two input fields: 'Global Database Name:' with the value 'contenterverdb' and 'SID:' with the value 'CSDB'. At the bottom are buttons for 'Cancel', 'Help', '< Back', and 'Next >'.

Database Configuration Assistant, Step 3 of 12 : Database Identification

An Oracle database is uniquely identified by a Global Database Name, typically of the form "name.domain".

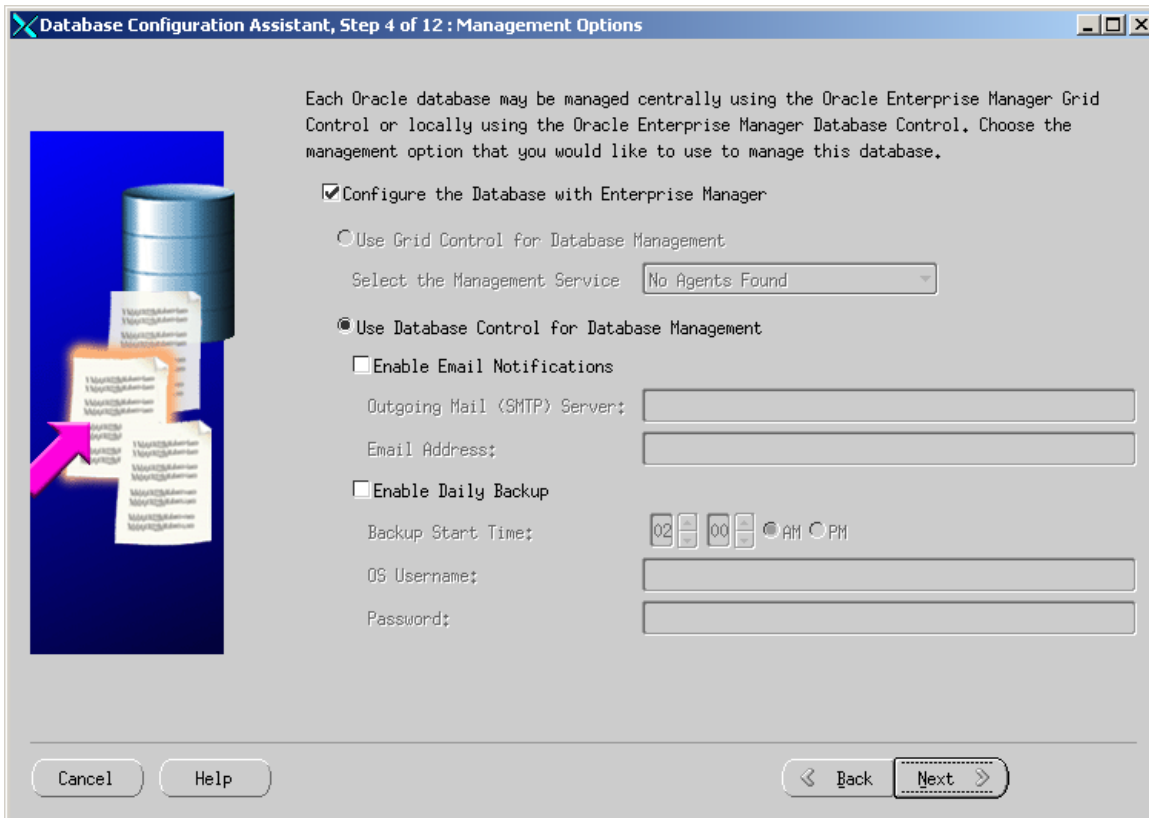
Global Database Name: contenterverdb

A database is referenced by at least one Oracle instance which is uniquely identified from any other instance on this computer by an Oracle System Identifier (SID).

SID: CSDB

Cancel Help < Back Next >

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



Database Configuration Assistant, Step 4 of 12 : Management Options

Each Oracle database may be managed centrally using the Oracle Enterprise Manager Grid Control or locally using the Oracle Enterprise Manager Database Control. Choose the management option that you would like to use to manage this database.

☒ Configure the Database with Enterprise Manager

☐ Use Grid Control for Database Management

Select the Management Service:

☒ Use Database Control for Database Management

☐ Enable Email Notifications

Outgoing Mail (SMTP) Server:

Email Address:

☐ Enable Daily Backup

Backup Start Time: ☒ AM ☐ PM

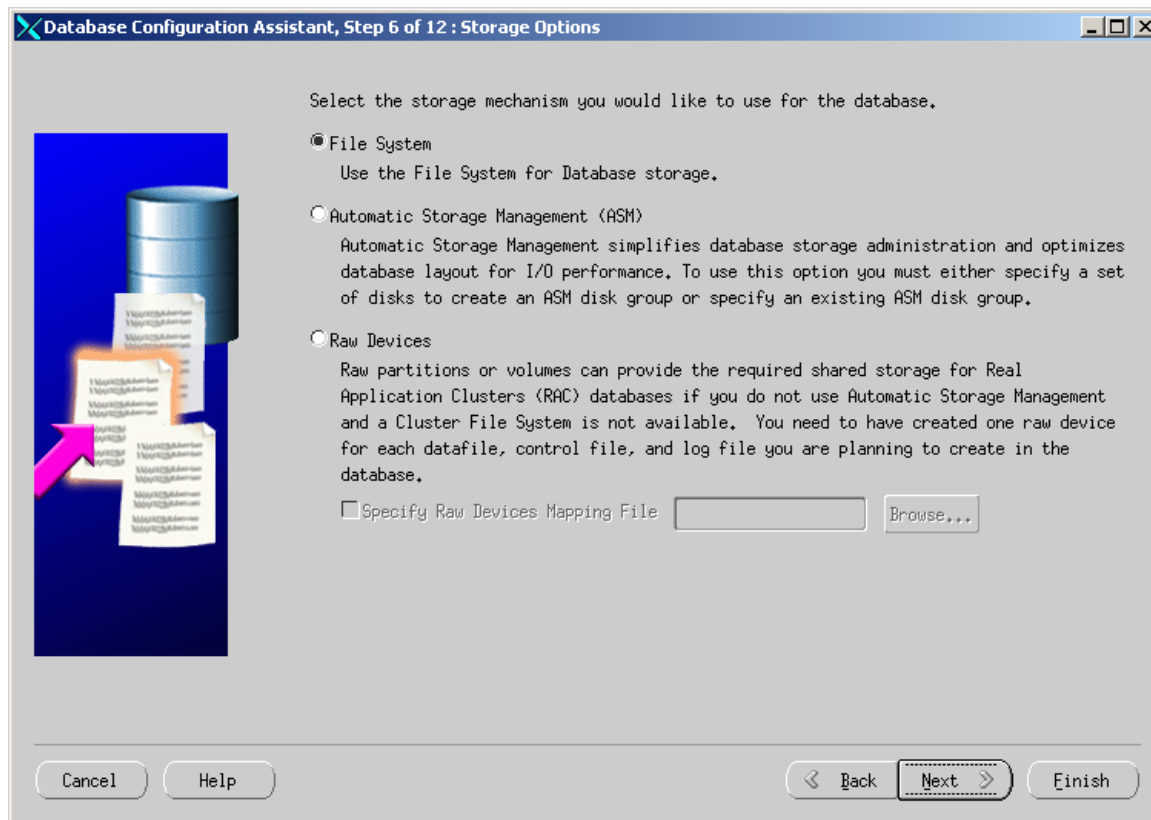
OS Username:

Password:

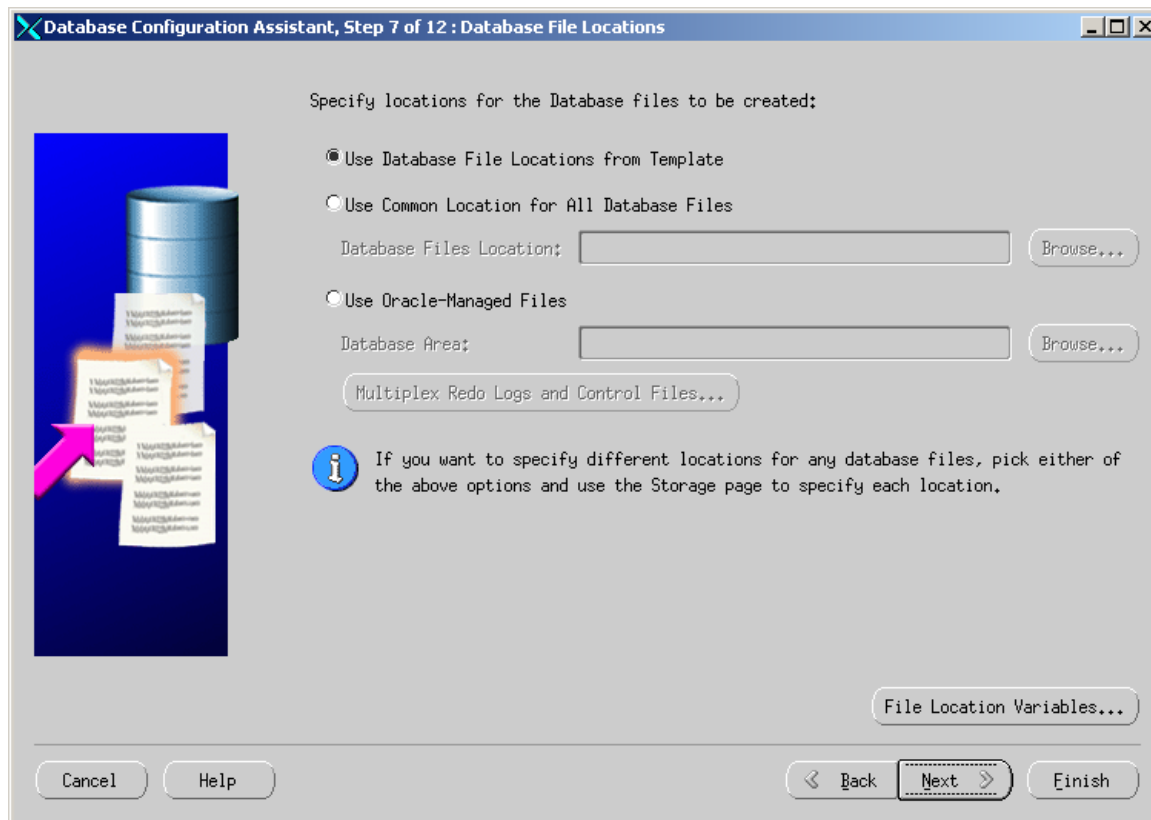
Cancel Help Back Next

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.

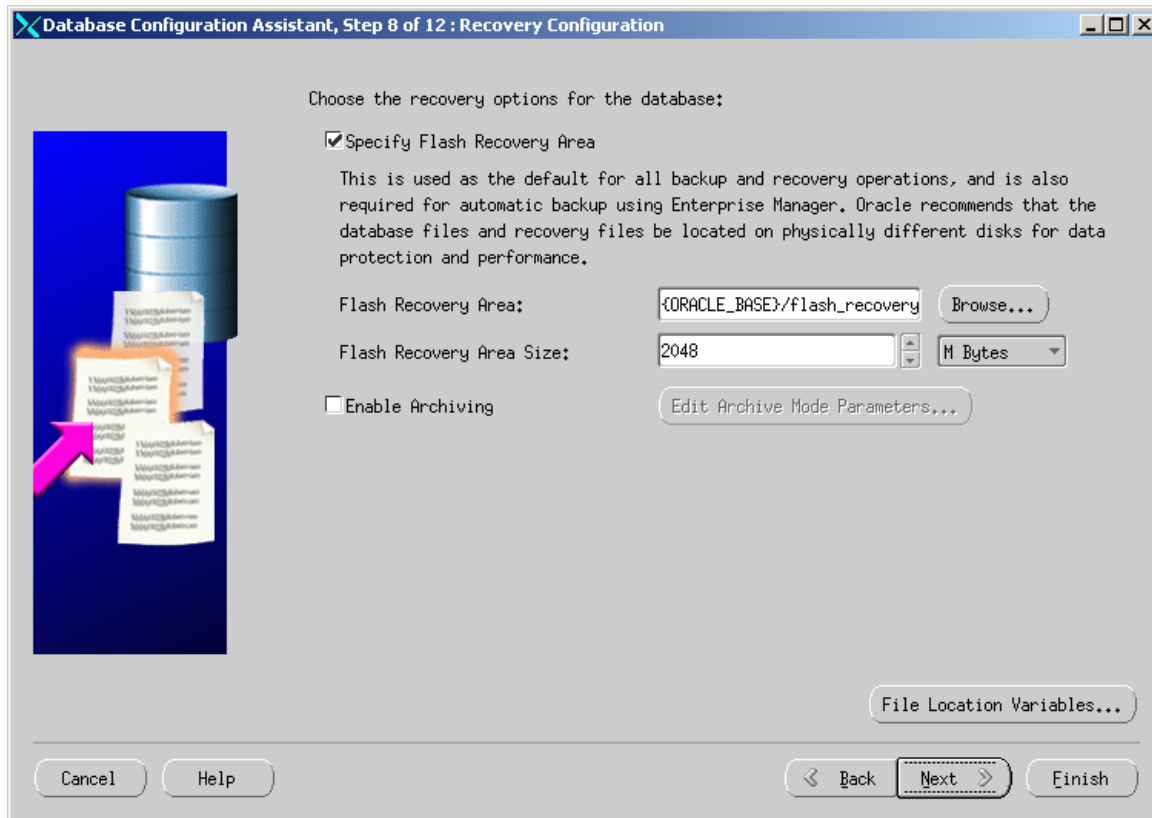
10. Do not change any options. Click **Next**.



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



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



Database Configuration Assistant, Step 8 of 12 : Recovery Configuration

Choose the recovery options for the database:

☒ Specify Flash Recovery Area

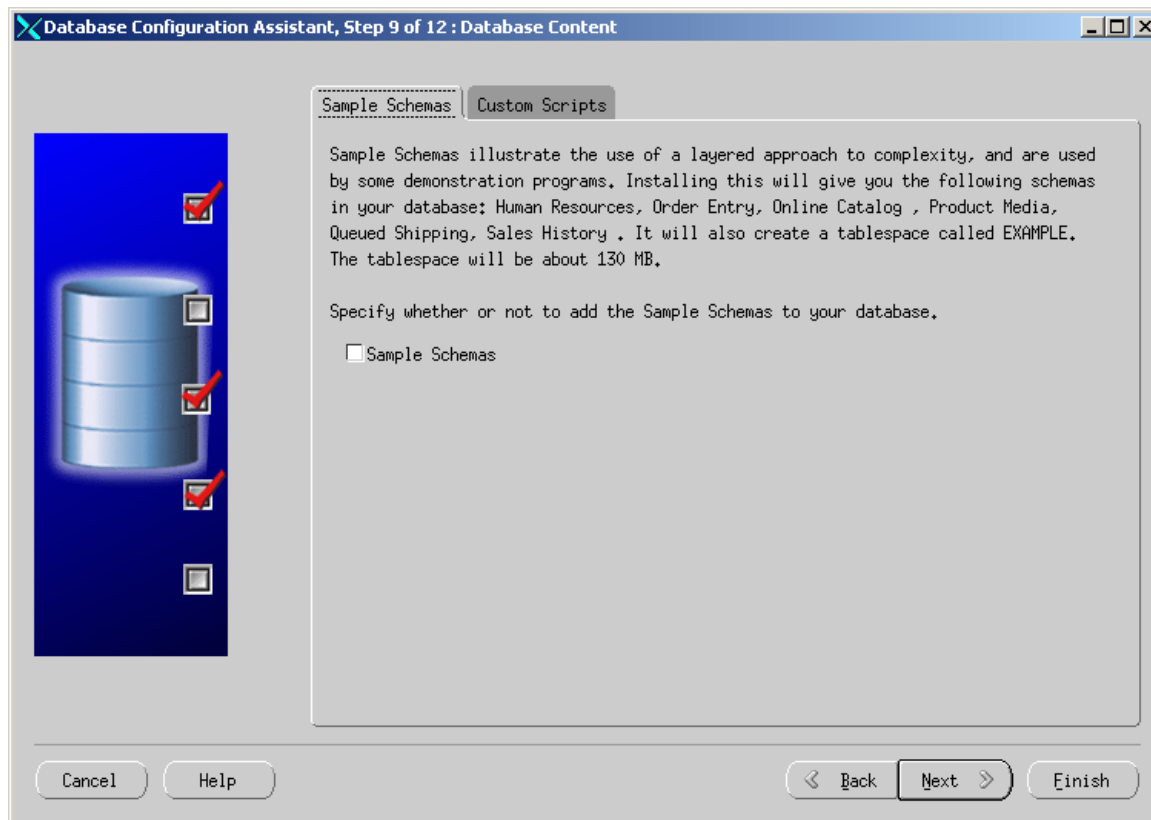
This is used as the default for all backup and recovery operations, and is also required for automatic backup using Enterprise Manager. Oracle recommends that the database files and recovery files be located on physically different disks for data protection and performance.

Flash Recovery Area:

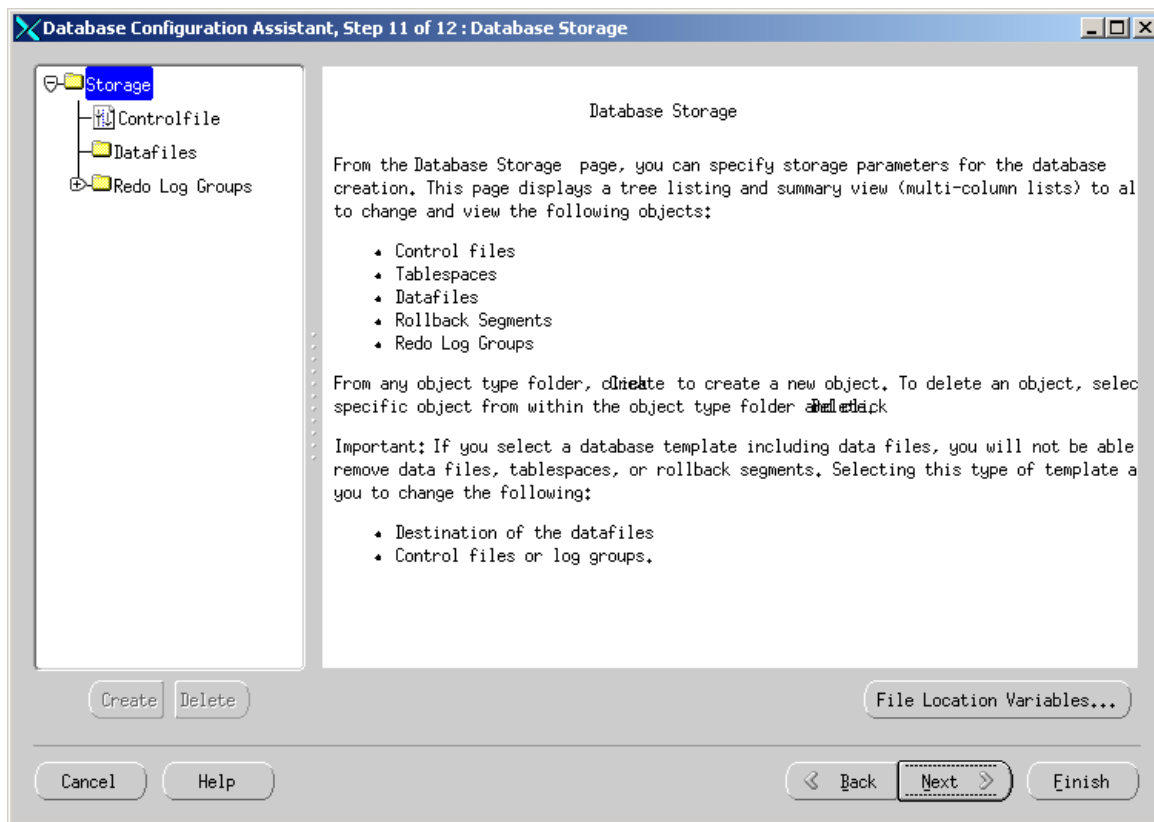
Flash Recovery Area Size:

☐ Enable Archiving

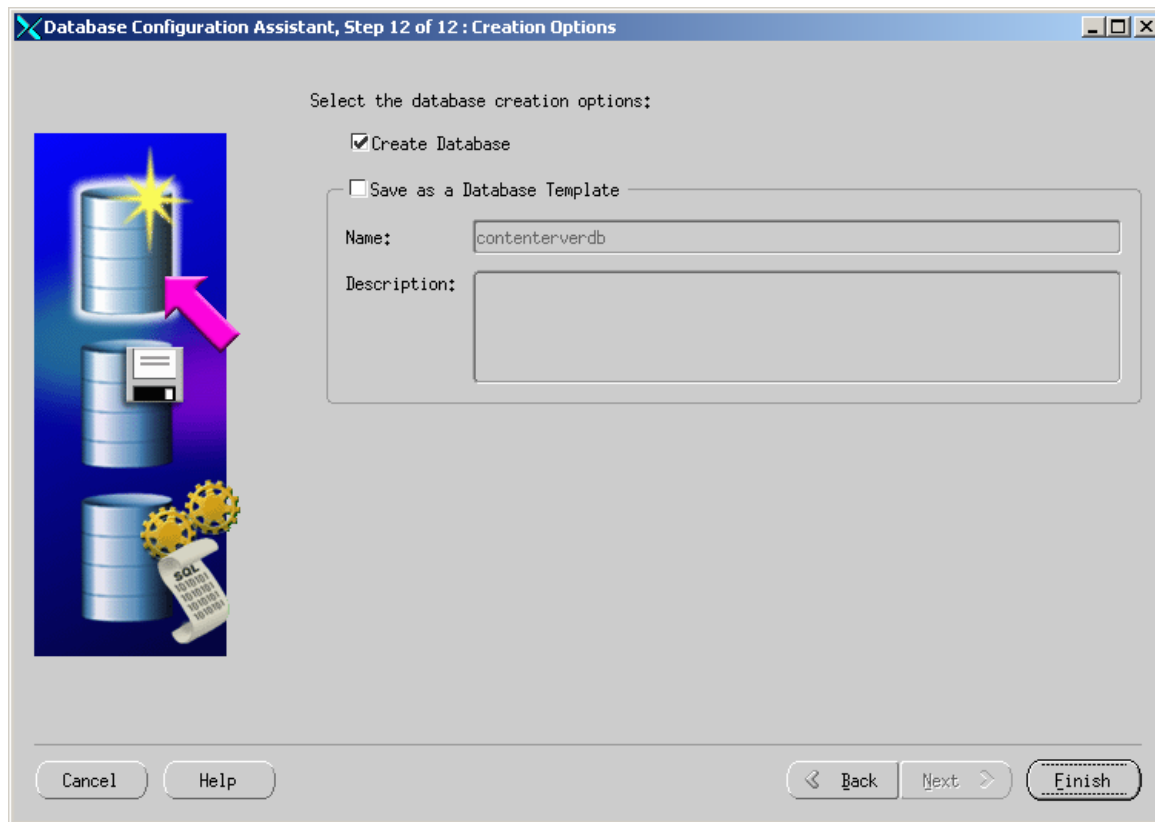
13. Do not change any options. Click **Next**.



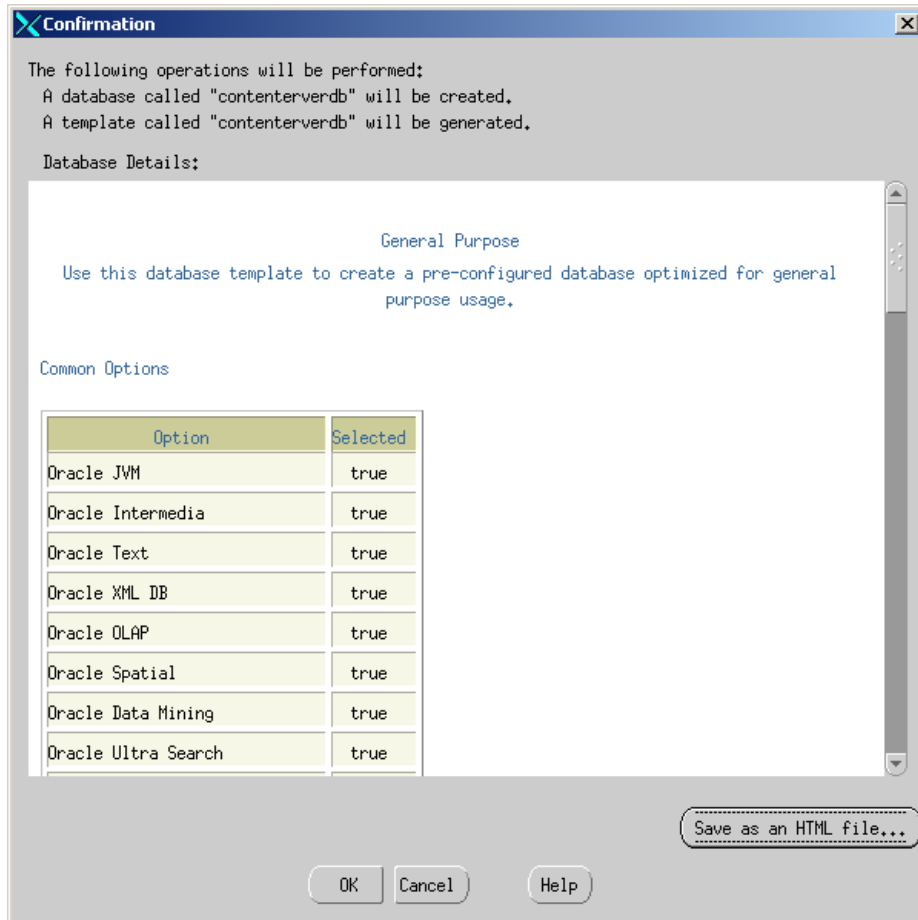
14. Click the **Character Sets** tab and do the following:
 - a. Select **Choose from the list of character sets** and select **UTF-8** from the drop-down menu.
 - b. Click the **National Character Set** drop down-menu and select **UTF8**.
15. Leave all other options on the different tabs as is and click **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**.



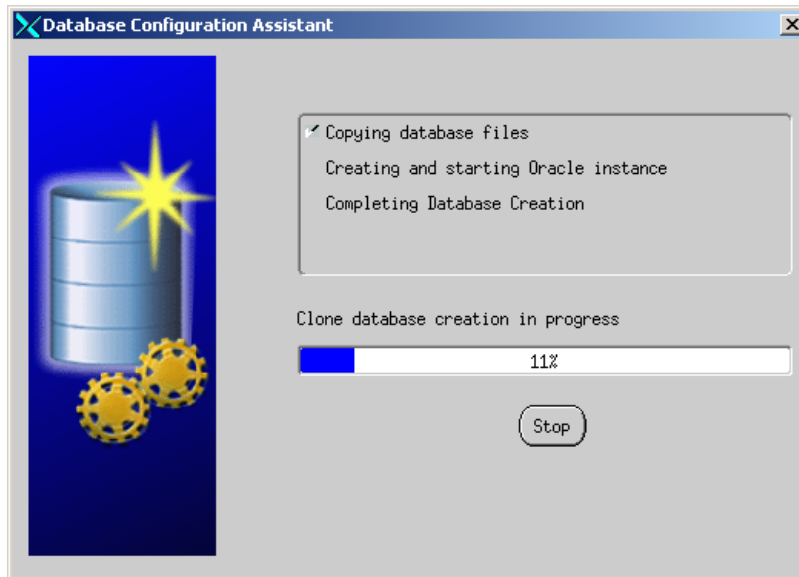
18. In the “Configuration” window, review the choices that you made on the previous screens. If you need to modify your choices, click **Cancel** and make the modifications. Otherwise, click **OK** to continue.



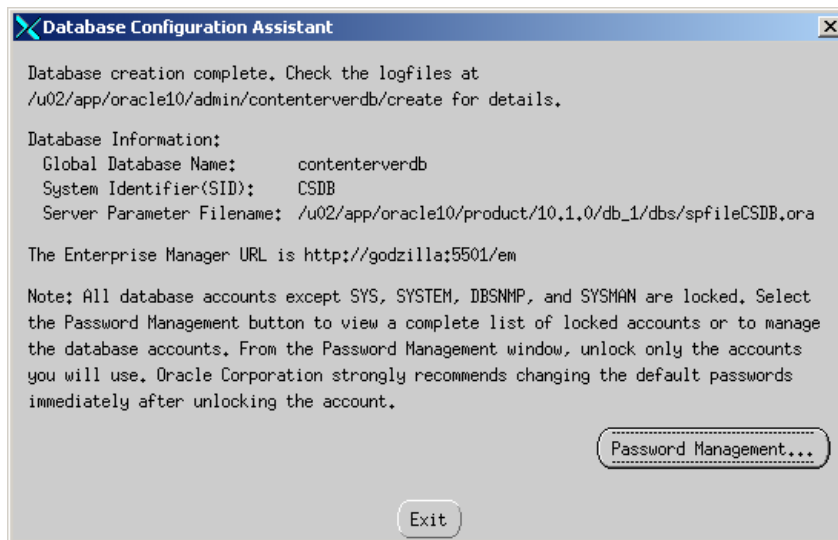
Note

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.
```

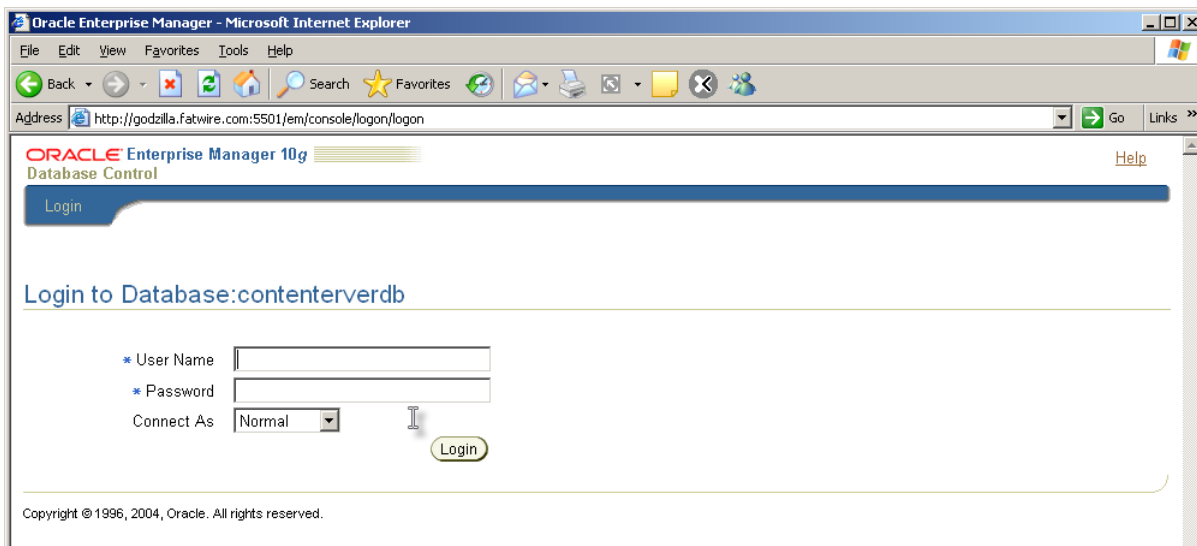
```
http://godzilla:5500/em/console/aboutApplication
Oracle Enterprise Manager 10g is running.
```

```
-----
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`**

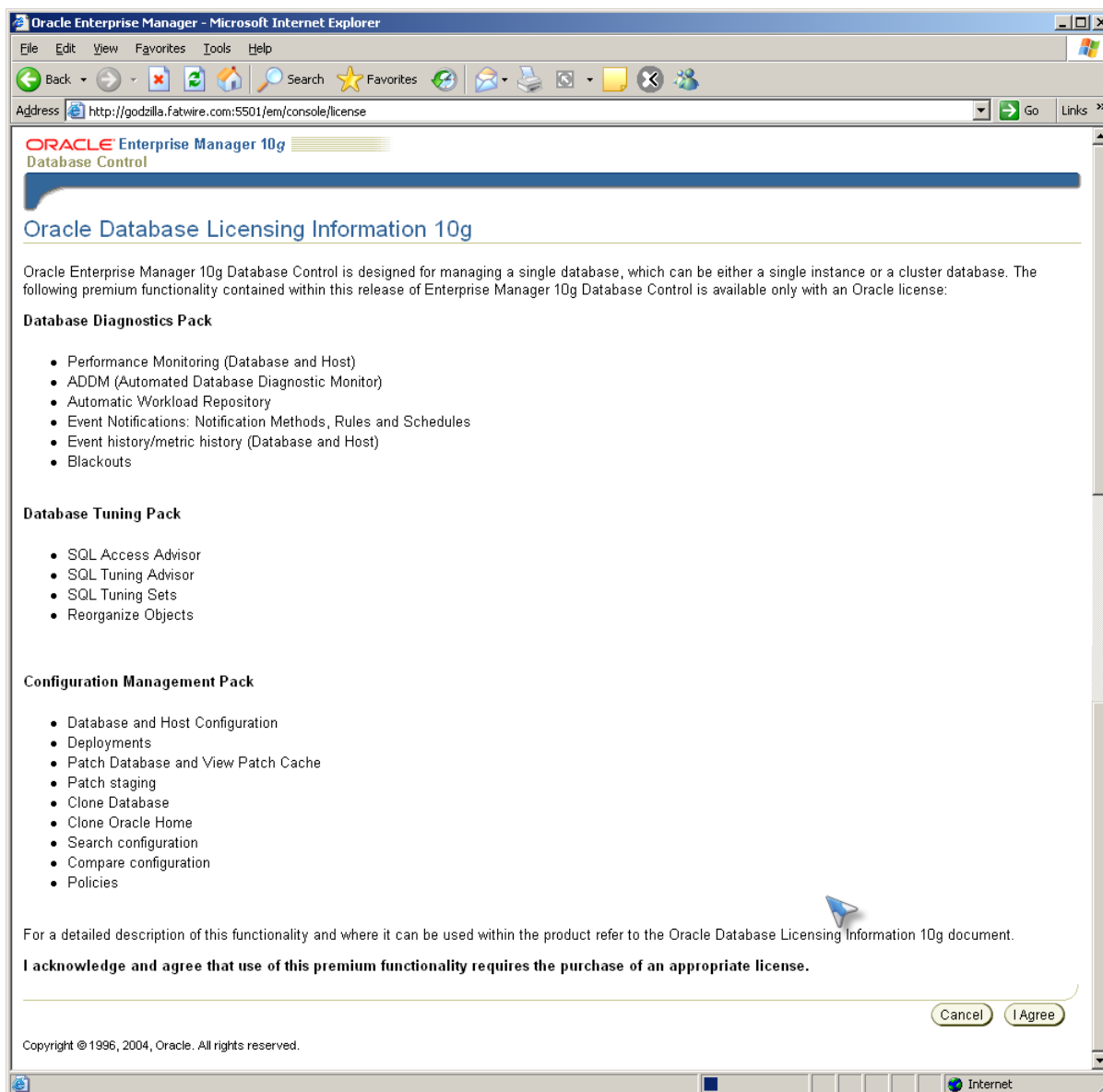
3. Open a browser and do the following:
 - a. Browse to the URL `http://<hostname>:<port>/em` (from [step 2](#)).



- 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.

The screenshot displays the Oracle Enterprise Manager 10g console in a Microsoft Internet Explorer browser window. The address bar shows the URL: `http://godzilla.fatwire.com:5501/em/console/database/instance/sitemap?event=doLoad&target=contenterverdb&type=oracle_database`. The page title is "ORACLE Enterprise Manager 10g Database Control". The user is logged in as "SYS".

The "Database: contenterverdb" page has a navigation bar with tabs: Home, Performance, Administration (selected), and Maintenance. A "Page Refreshed" message indicates the page was updated on May 26, 2005, at 10:28:11 AM. A "View Data" dropdown menu is set to "Manually".

The main content area is divided into several sections:

- General:** Displays the database status as "Up" with a "Shutdown" button. Other details include: Up Since (May 26, 2005 9:01:04 AM), Time Zone (EDT), Availability (%) (100), Instance Name (CSDB), Version (10.1.0.2.0), Read Only (No), Oracle Home (`/u02/app/oracle10/product/10.1.0/db_1`), Listener (`LISTENER_godzilla`), and Host (`godzilla`).
- Host CPU:** A line graph showing CPU usage over time, with a legend for "Other" and "CSDB".
- Active Sessions:** A pie chart showing session distribution, with a legend for "CPU", "I/O", and "Wait".
- High Availability:** Displays "Instance Recovery Time (seconds)" as 9.
- Space Usage:** Displays "Database Size (GB)" as 1.
- Diagnostic Summary:** Shows "Performance" and "No ADDM run".

The bottom of the page shows the browser's status bar with the URL and an "Internet" icon.

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

Oracle Enterprise Manager 10g
Database Control

Database: contenterverdb > Users > Create User

Logged in As SYS

Create User

General Roles System Privileges Object Privileges Quotas Consumer Groups Proxy Users

* Name: csuser

Profile: DEFAULT

Authentication: Password

* Enter Password: [masked]

* Confirm Password: [masked]

☐ Expire Password now

Default Tablespace: [empty]

Temporary Tablespace: [empty]

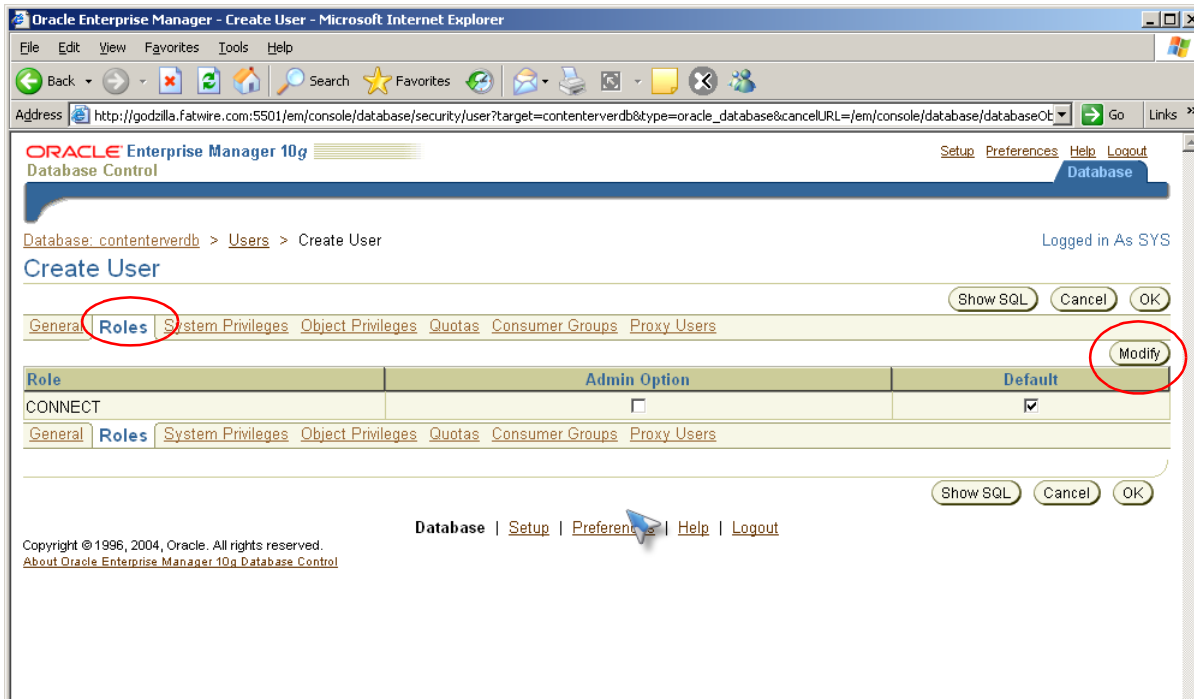
Status: ☐ Locked ☒ Unlocked

General Roles System Privileges Object Privileges Quotas Consumer Groups Proxy Users

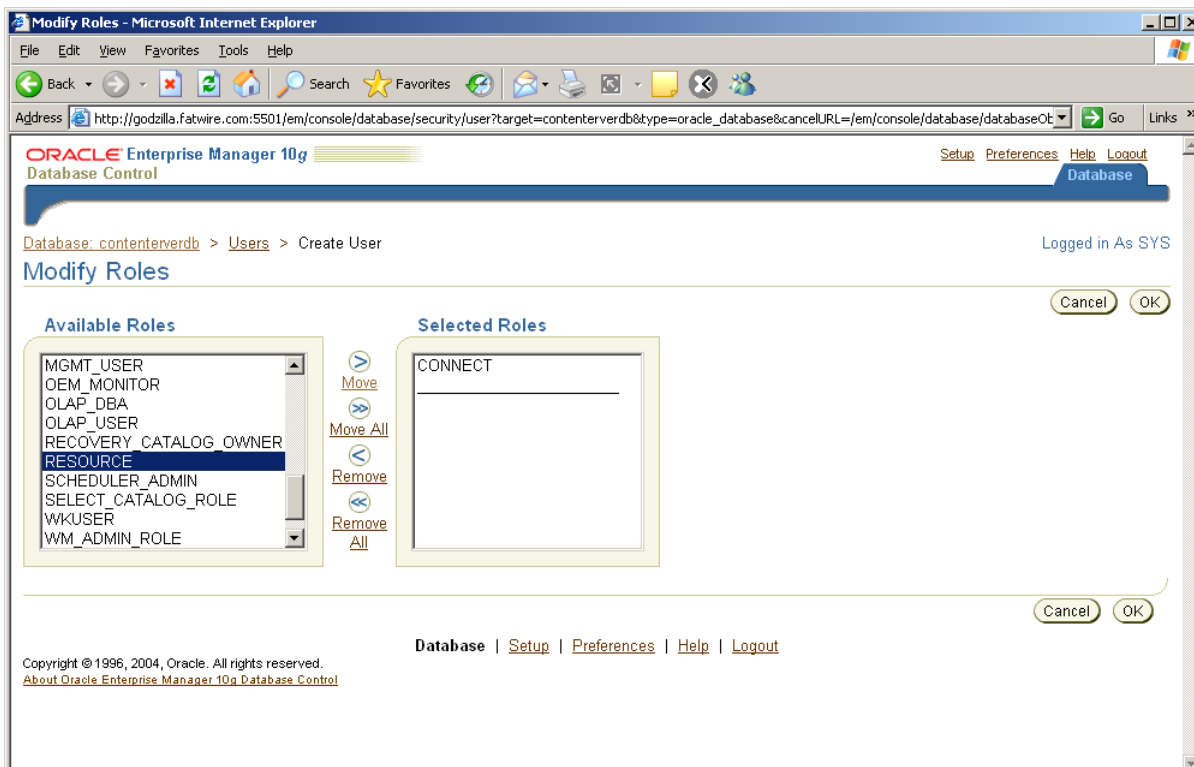
Show SQL Cancel OK

Database | Setup | Preferences | Help | Logout

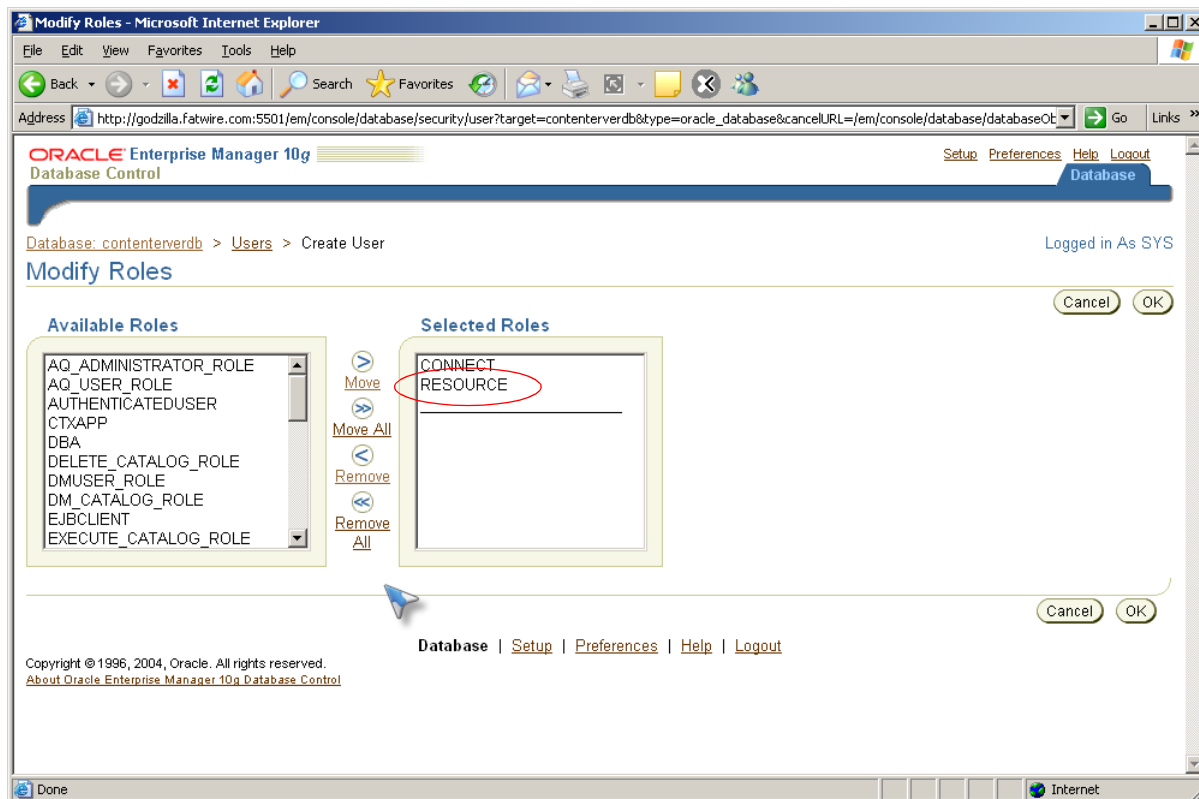
5. Click the **Roles** tab.
 - a. Click the **Modify** button.



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

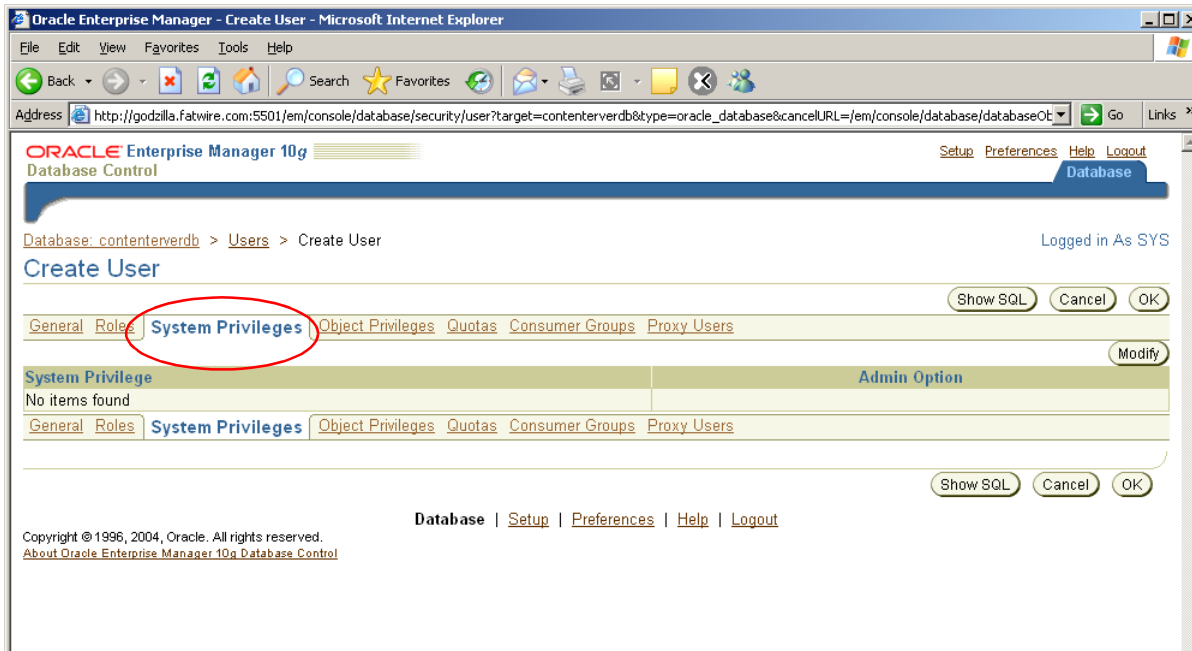


Resource is moved to the “Selected Roles” list.

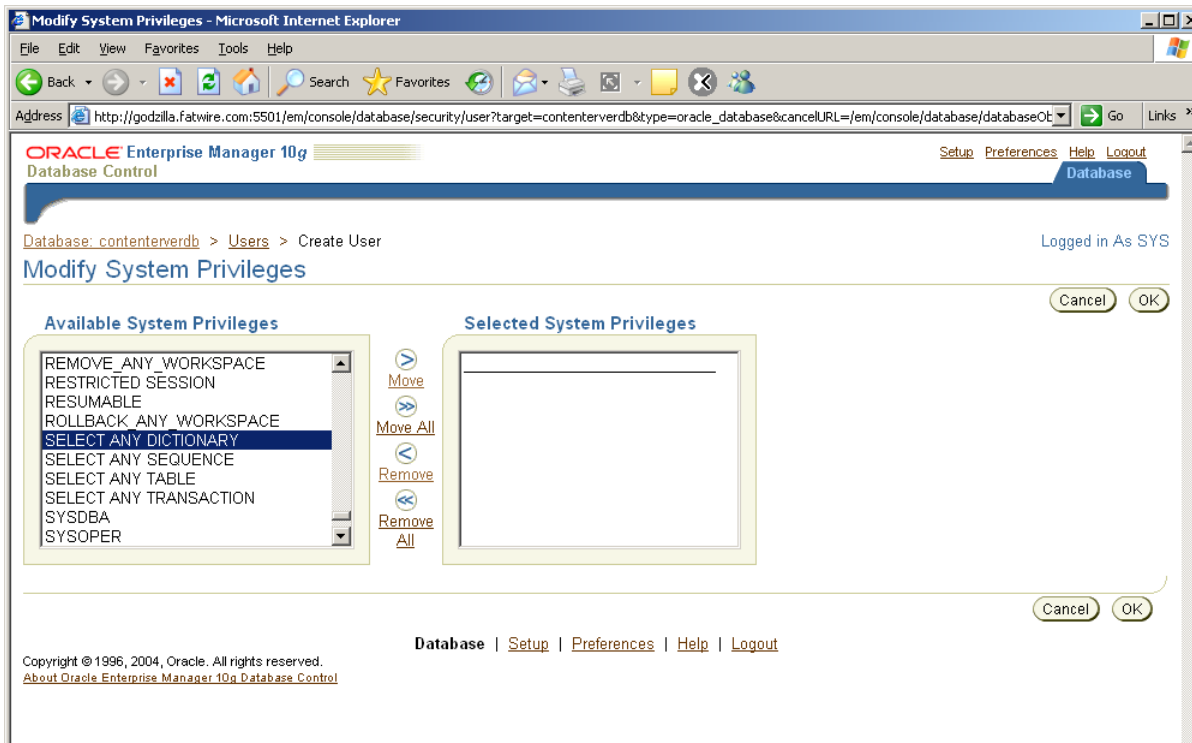


c. Click **OK**.

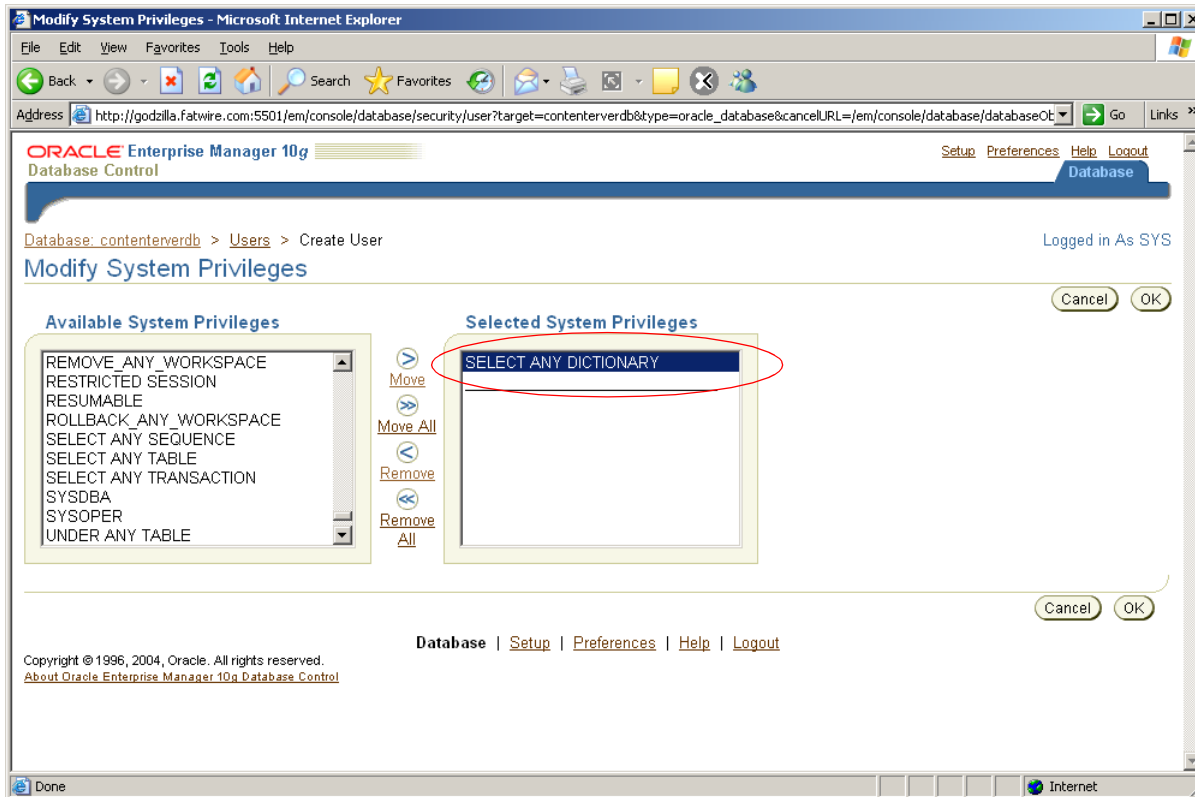
6. Click the **System Privileges** tab.
 - a. Click the **Modify** button.



- 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 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 sections:

- [Creating a Database on MS SQL Server 2000 SP3+](#)
- [Creating a Database on MS SQL Server 2005](#)

Creating a Database on MS SQL Server 2000 SP3+

To create and configure a database on MS SQL Server 2000 SP3+

1. Create the database login:
 - a. Open “Enterprise Manager.”
 - b. In the left-hand tree, select **Microsoft SQL Servers > SQL Server Group > (Local) > Security**.
 - c. Right-click on **Logins** and select **New Login...**
 - 1) Create a user (such as `csuser`), and select the proper authentication method.
 - 2) Save this user.
2. Create the database:
 - a. In the left-hand tree, select **Microsoft SQL Servers > SQL Server Group > (Local) > Databases**.
 - b. Right-click on **Databases** and select **New Database...**
 - 1) Enter a name (such as `csDB`), then modify the other fields as needed for your installation.
 - 2) Finish creating this database.
3. Assign account privileges:
 - a. Select the newly created database in the left-hand tree and click **Open**.
 - b. Right-click on **Users** and select **Add new Database User...**
 - c. In the drop-down list, choose the user created in [step c](#) of this procedure. In the **Permit role membership** list, check the box next to **db_owner**.
 - d. Save the new user.

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

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](#)

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 Group Objects** 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 Ø 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](#)

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

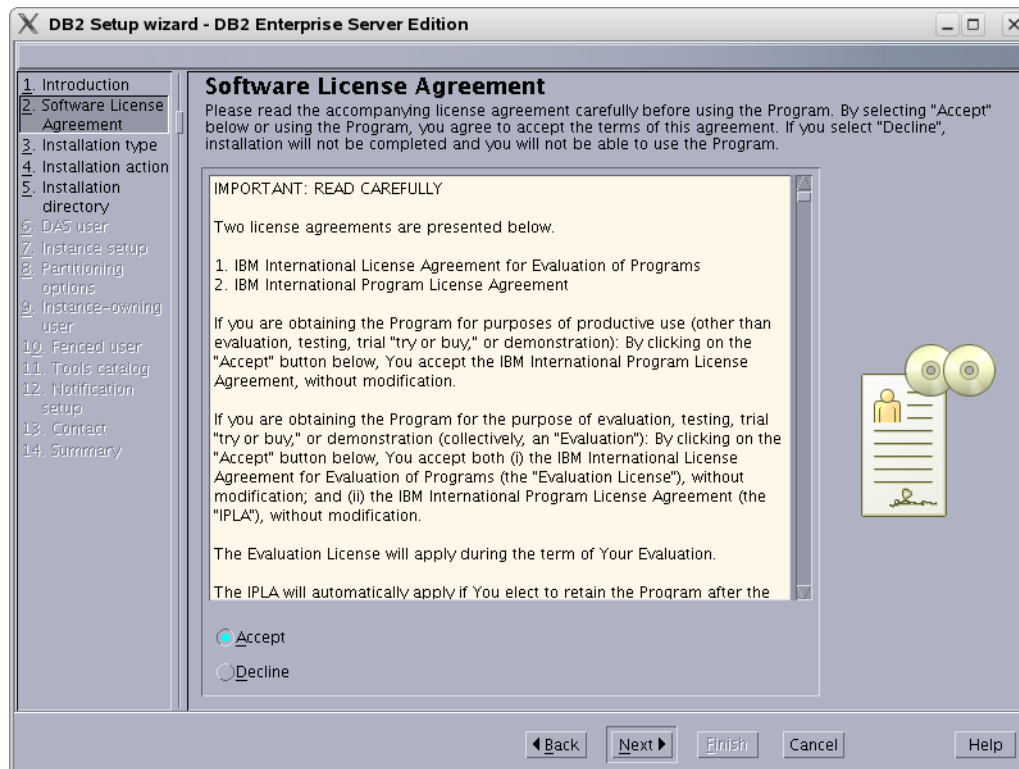
1. Uncompress the correct installation file for your distribution.
2. Run `./db2setup`
3. In the “Information Management Software” screen, select **Install a Product**.



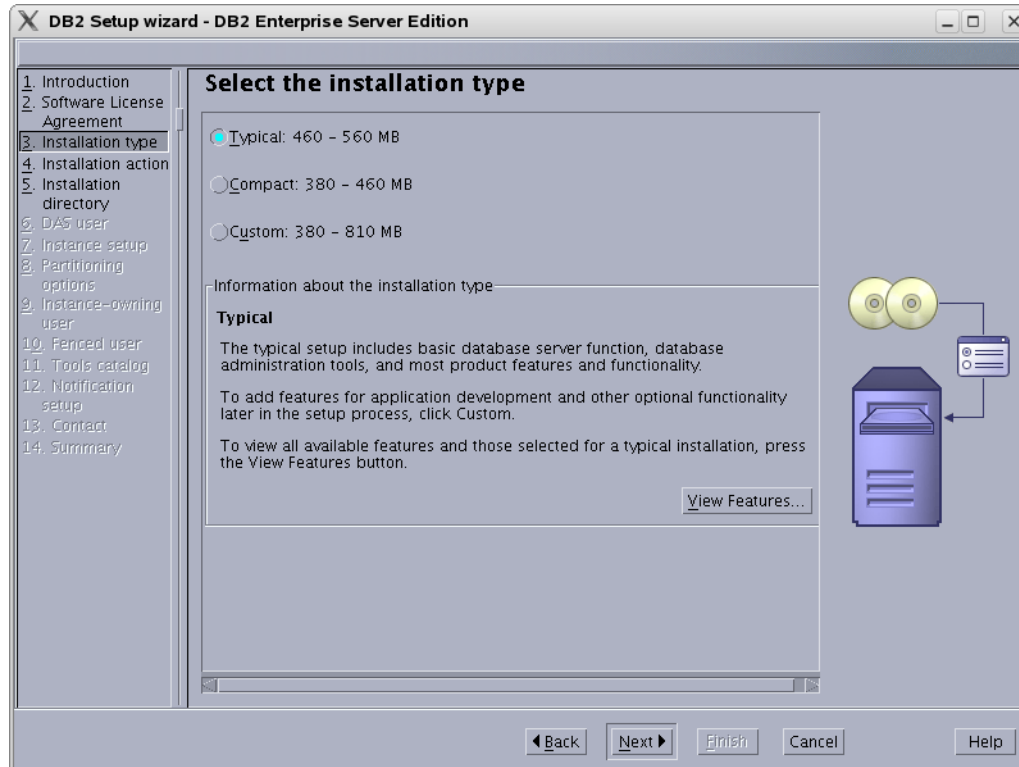
4. Under “DB2 Enterprise Server Edition,” select **Install New**.



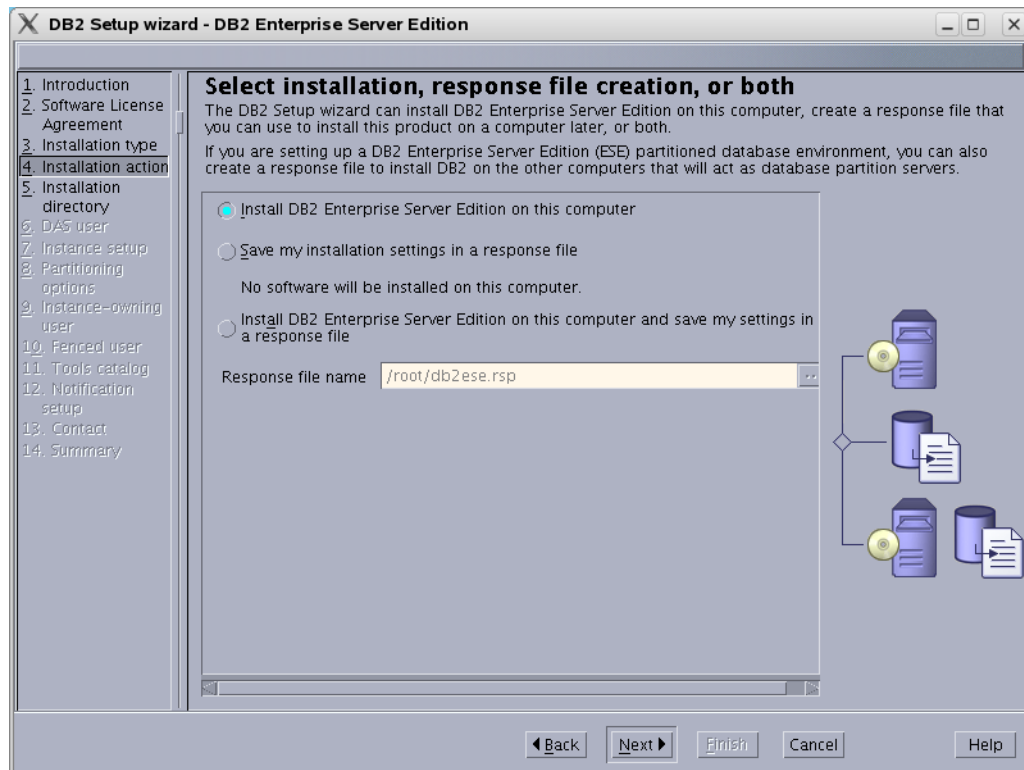
5. In the “Welcome to the DB2 Setup Wizard,” click **Next**.
6. In the “Software License Agreement” screen, click **Accept**, then click **Next**.



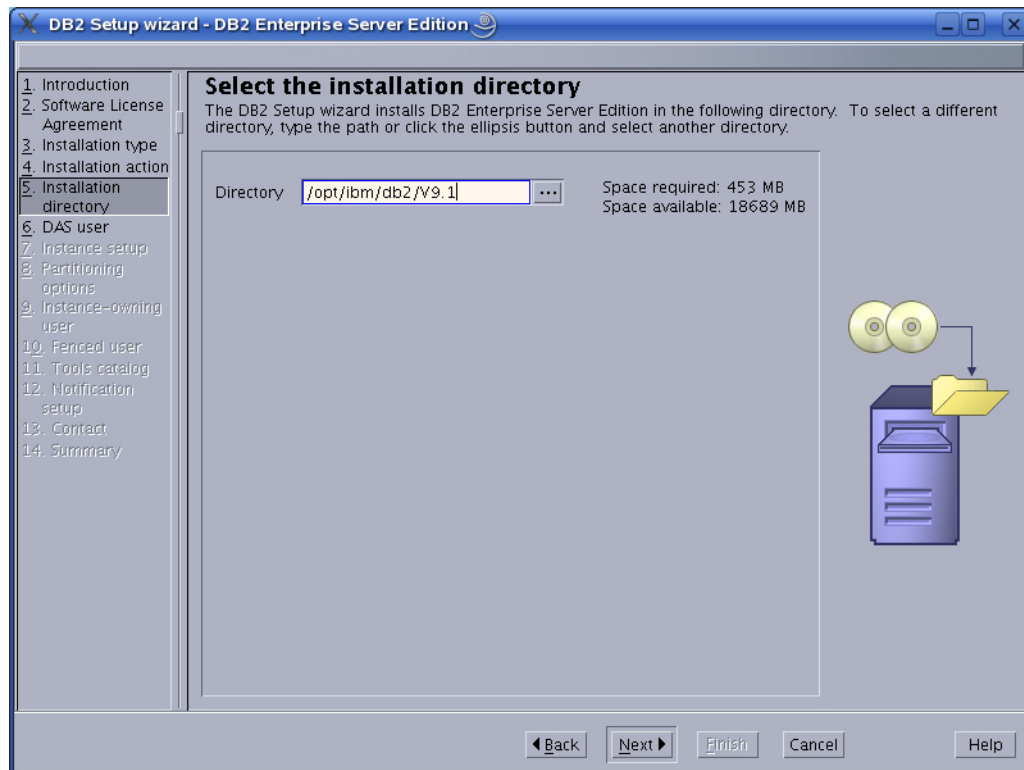
7. In “Select the Installation Type,” select **Typical** and click **Next**.



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**.

DB2 Setup wizard - DB2 Enterprise Server Edition

1. Introduction
2. Software License Agreement
3. Installation type
4. Installation action
5. Installation directory
6. DAS user
7. Instance setup
8. Partitioning options
9. Instance-owning user
10. Fenced user
11. Tools catalog
12. Notification setup
13. Contact
14. Summary

Set user information for the DB2 Administration Server

The DB2 Administration Server (DAS) runs on your computer to provide support required by the DB2 tools. A user with a minimal set of privileges is required to run the DAS. Specify the required user information for the DAS.

☒ **New user**

User name:

UID: ☒ Use default UID

Group name:

GID: ☒ Use default GID

Password:

Confirm password:

Home directory:

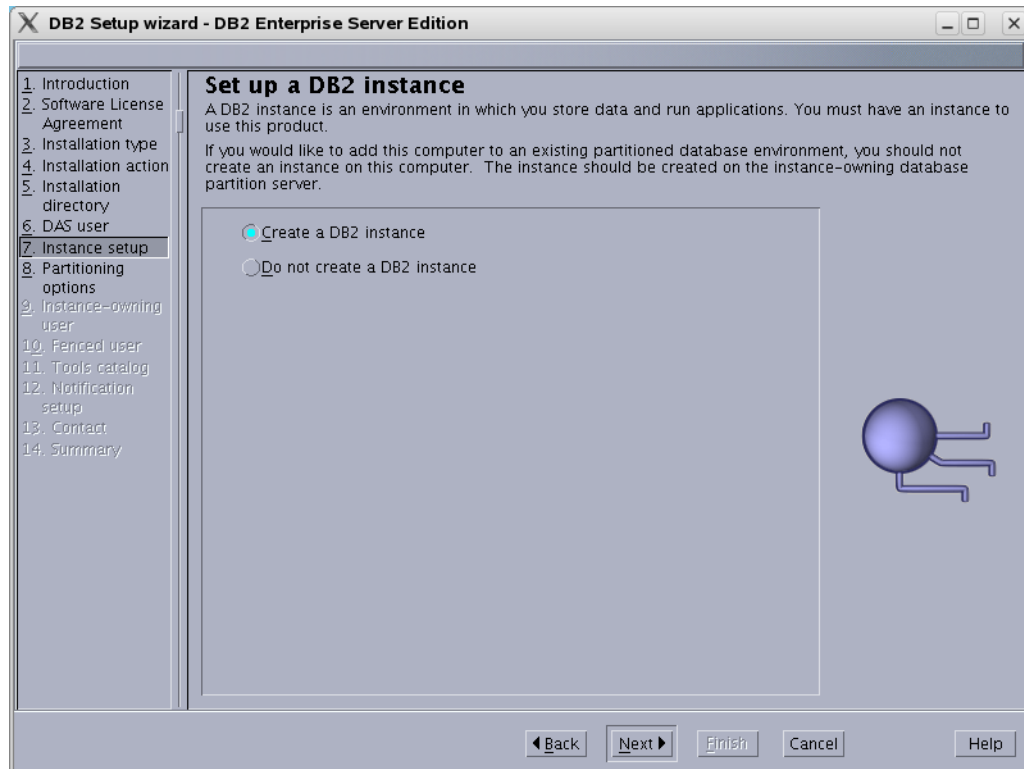
☐ **Existing user**

User name:

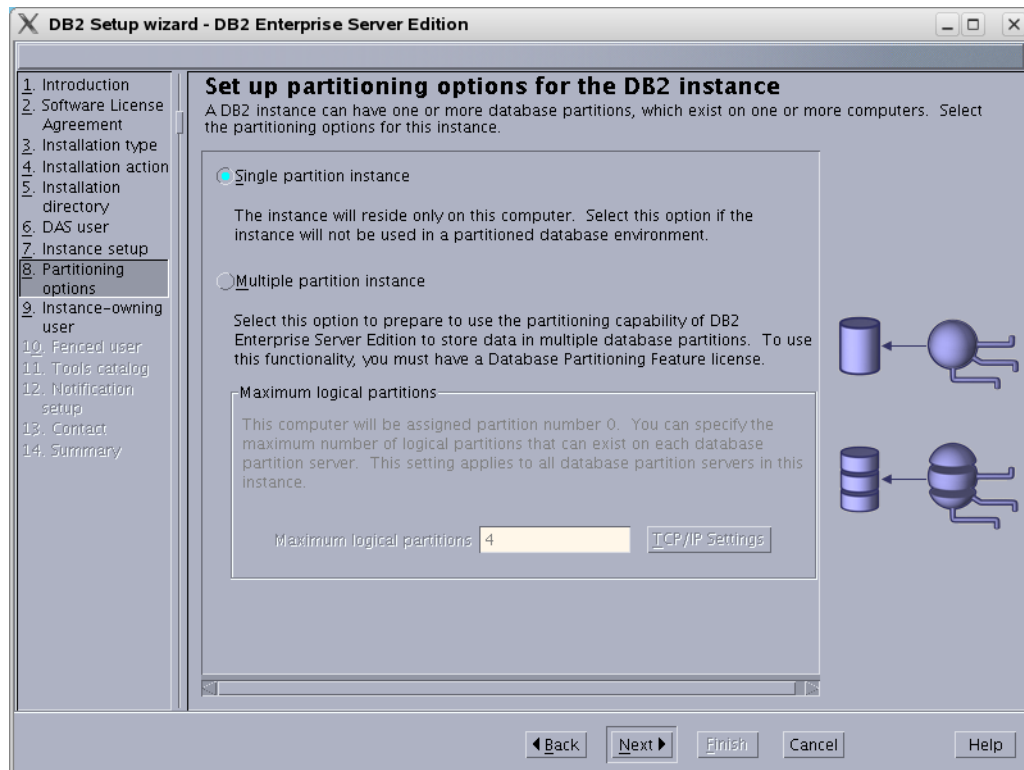
Password
• You must specify a value.

Back Next Finish Cancel Help

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**.

The screenshot shows the 'DB2 Setup wizard - DB2 Enterprise Server Edition' window. The left sidebar lists steps 1 through 14, with step 9, 'Instance-owning user', highlighted. The main panel is titled 'Set user information for the DB2 instance owner' and contains the following text: 'Specify the instance-owning user information for the DB2 instance. DB2 will use this user to perform instance functions, and will store instance information in the user's home directory. The name of the instance will be the same as the user name.'

Under the 'New user' radio button, the following fields are present:

- User name:
- UID: ☒ Use default UID
- Group name:
- GID: ☒ Use default GID
- Password: (highlighted with a red border)
- Confirm password: (highlighted with a red border)
- Home directory: ...

Under the 'Existing user' radio button, there is a 'User name' field with a dropdown arrow.

A tooltip is visible over the Password field with the text: 'Password • You must specify a value.'

At the bottom of the window are buttons for 'Back', 'Next', 'Finish', 'Cancel', and 'Help'.

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**.

DB2 Setup wizard - DB2 Enterprise Server Edition

Set user information for the fenced user
Specify the required information for the fenced user. Fenced user defined functions (UDFs) and stored procedures will execute under this user and group.

☒ **New user**

User name:

UID: ☒ Use default UID

Group name:

GID: ☒ Use default GID

Password: **Password**
• You must specify a value.

Confirm password:

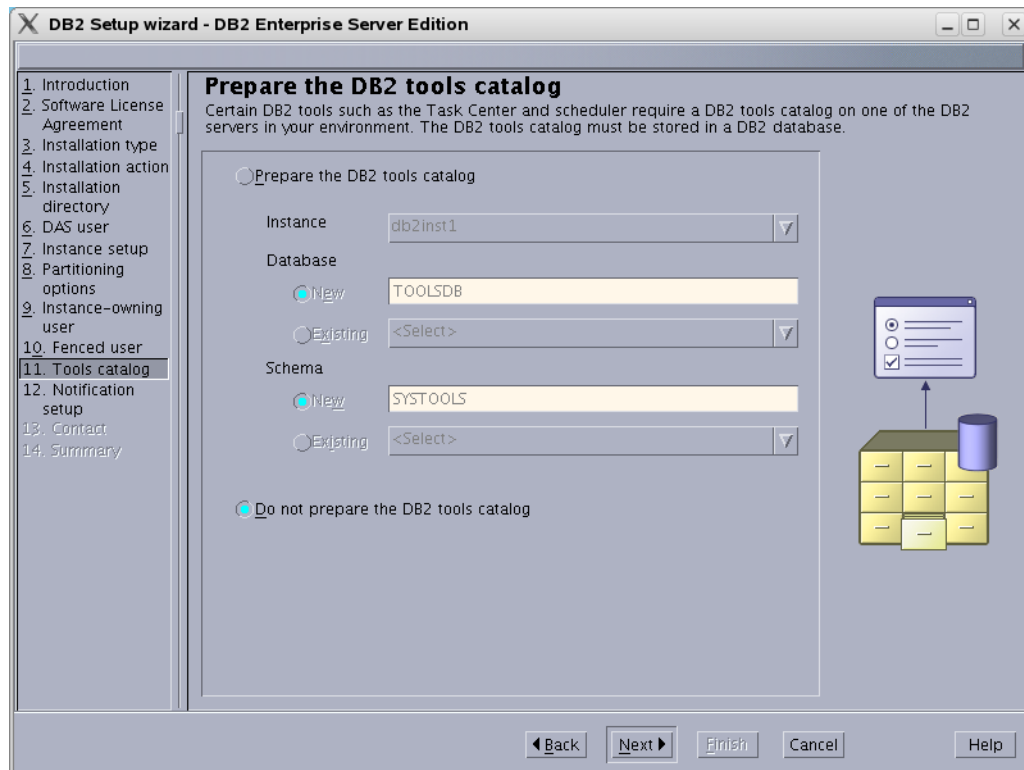
Home directory:

☐ **Existing user**

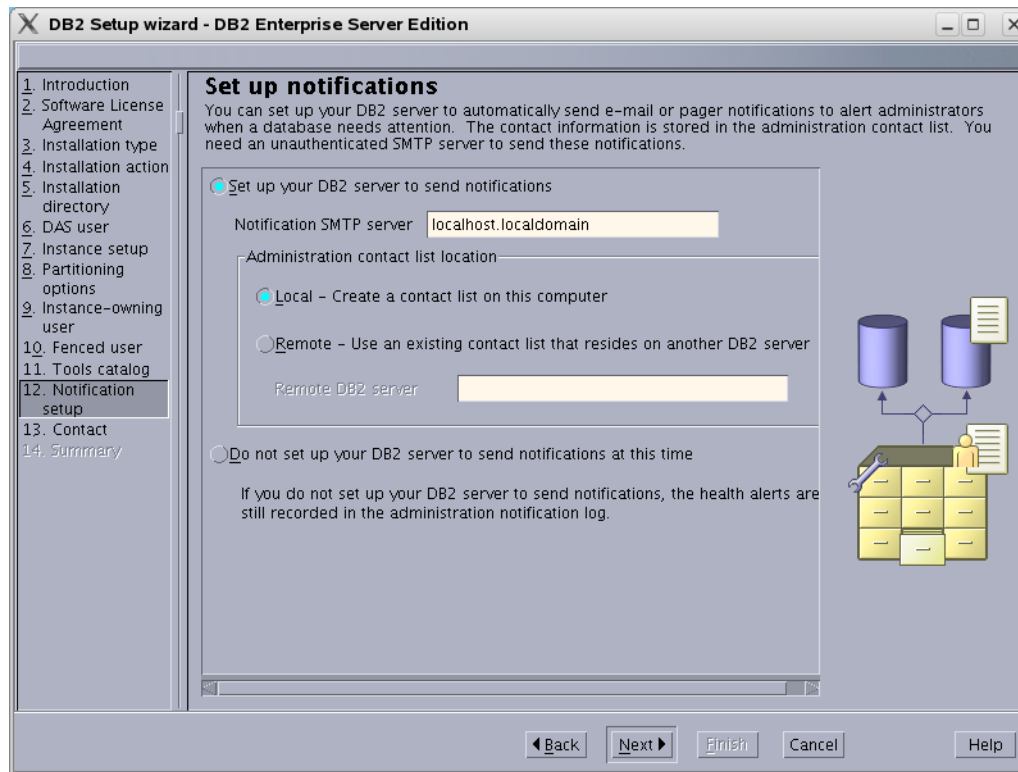
User name:

Navigation:

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

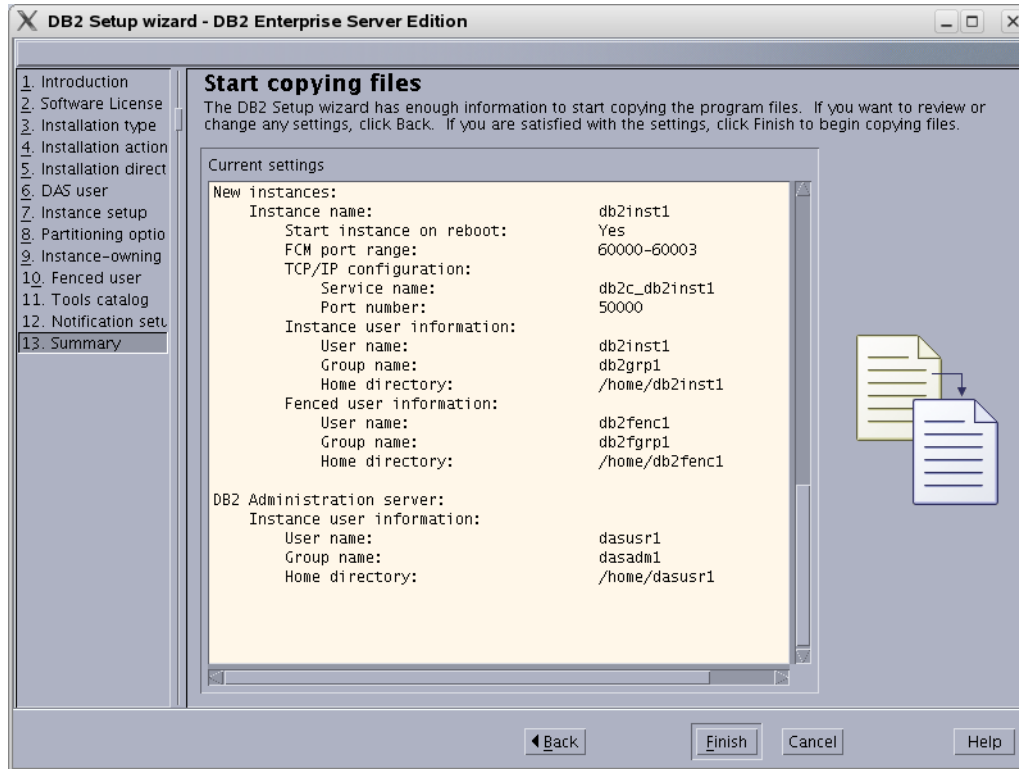


16. In “Set up notifications,” do one of the following:

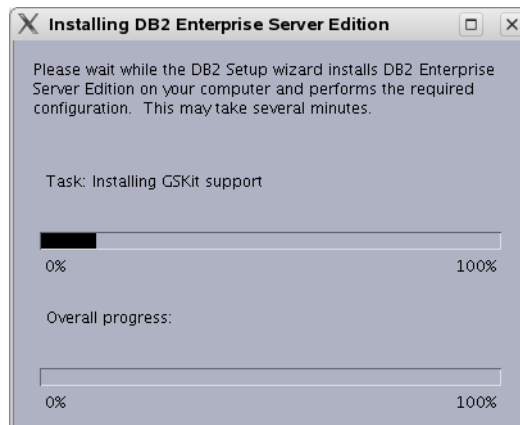


- If your system is a production server, select **Set up your DB2 server to send notifications**, enter a correct address for the local host, and click **Next**.
- If your system is not a production server, you can select **Do not set up your DB2 server to send notifications at this time**, and click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

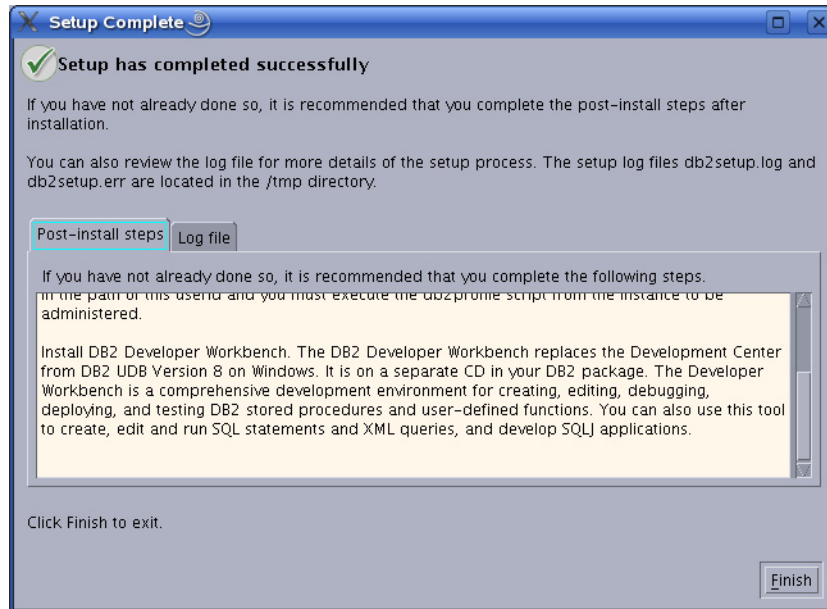
17. In “Start copying files,” check that your options are correct and click **Finish**.



18. Allow the installation to proceed.



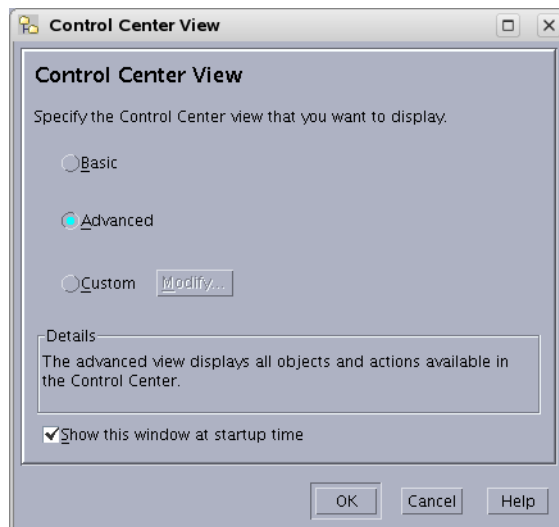
19. In “Setup has completed successfully,” read the notes, check the log tab, and click **Finish**.



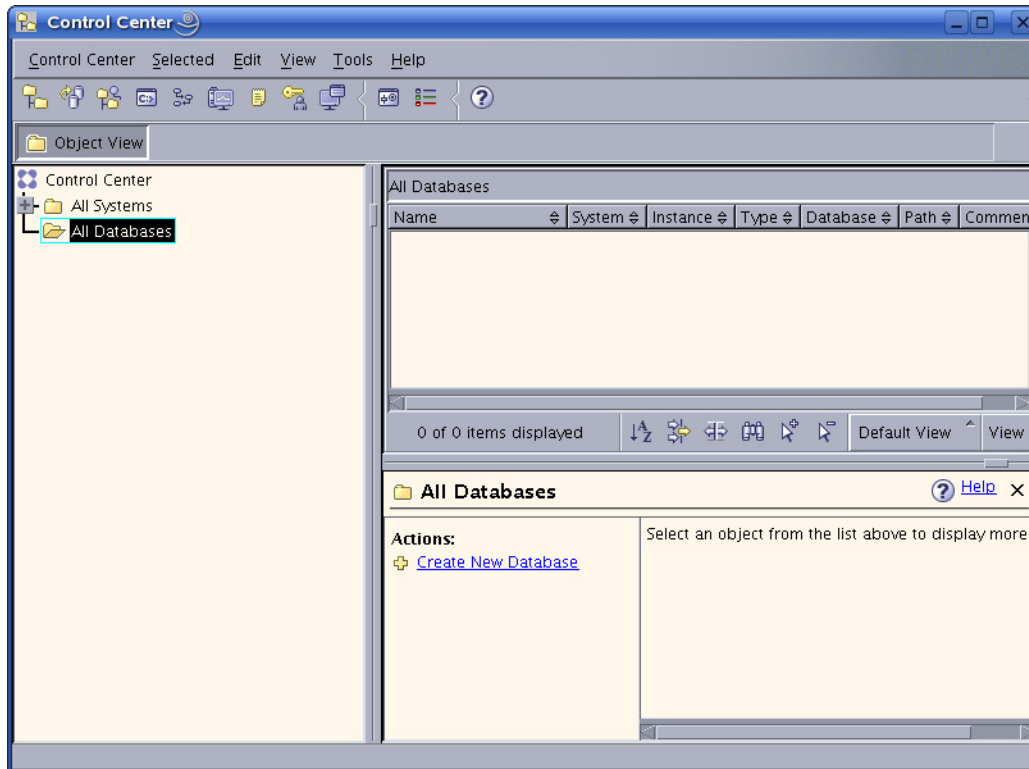
20. The installation of DB2 9.1 is now complete.

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**.

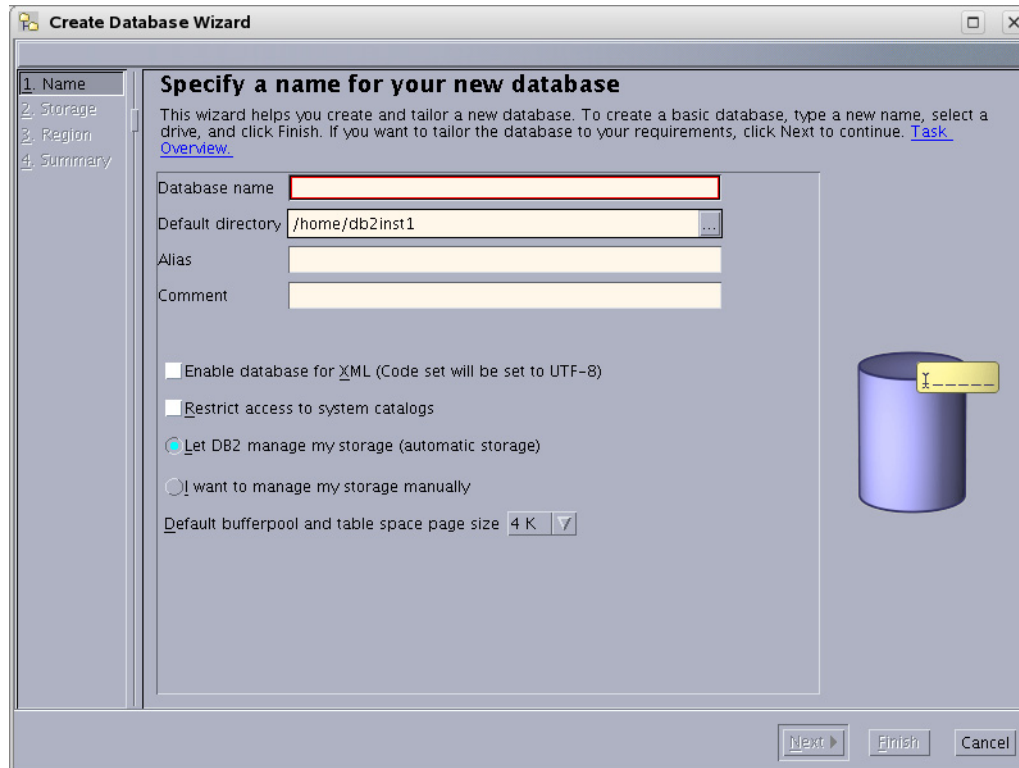


4. In the “Control Center,” open the application for creating a database:
 - a. Click the plus sign next to the tree option **All Systems**.

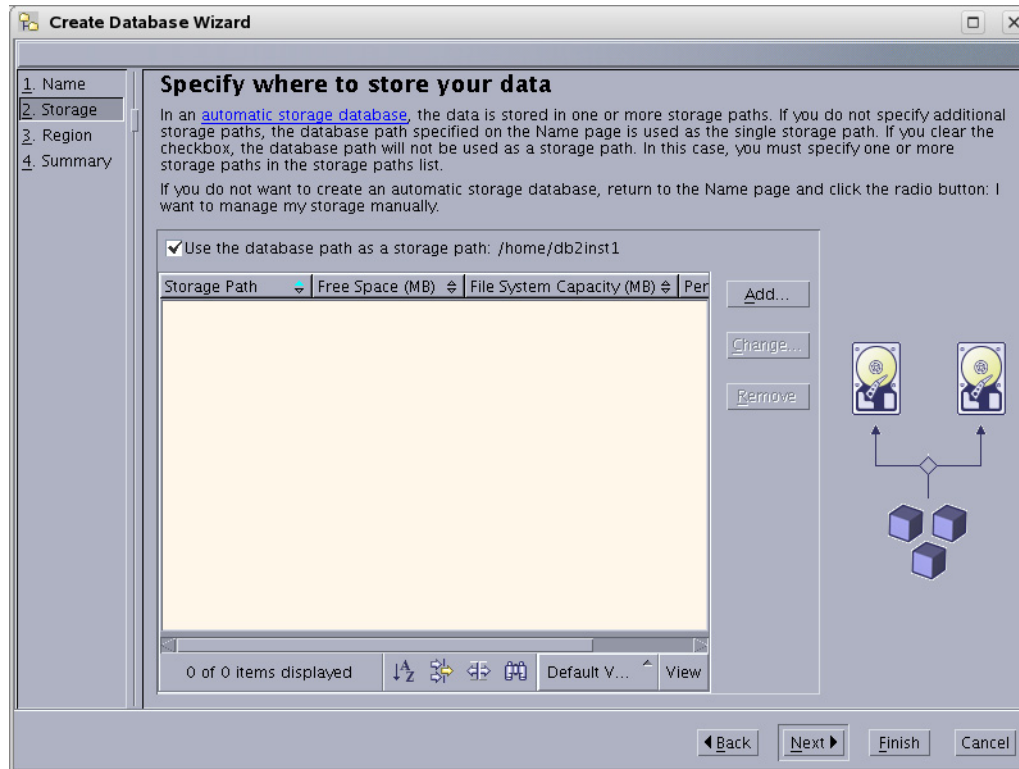


- b. Click on the expanded branch **All Databases**. (If you have not created a database previously, this branch is empty.)
 - c. Right-click on the branch **All Databases** and select **Create Database > Standard**.

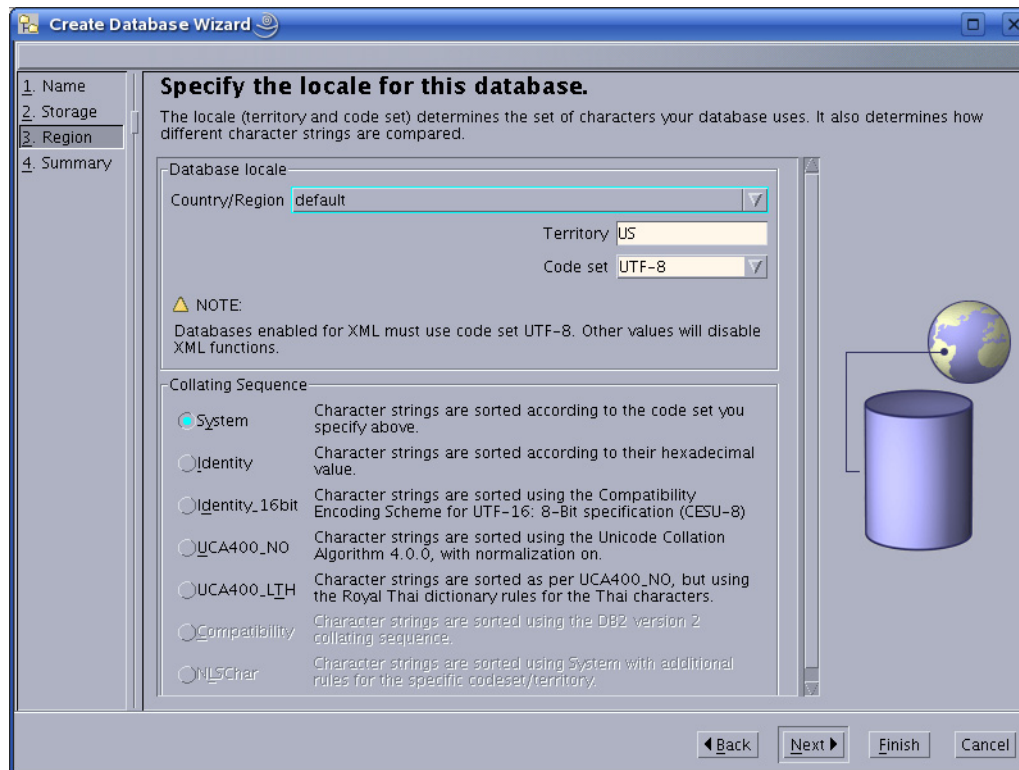
5. In “Specify a name for your new database”:
 - a. Enter a name for this database.
 - b. Select the check box **Enable database for XML**.
 - c. In the drop-down “Default bufferpool and table space page size,” select **32** and click **Next**.



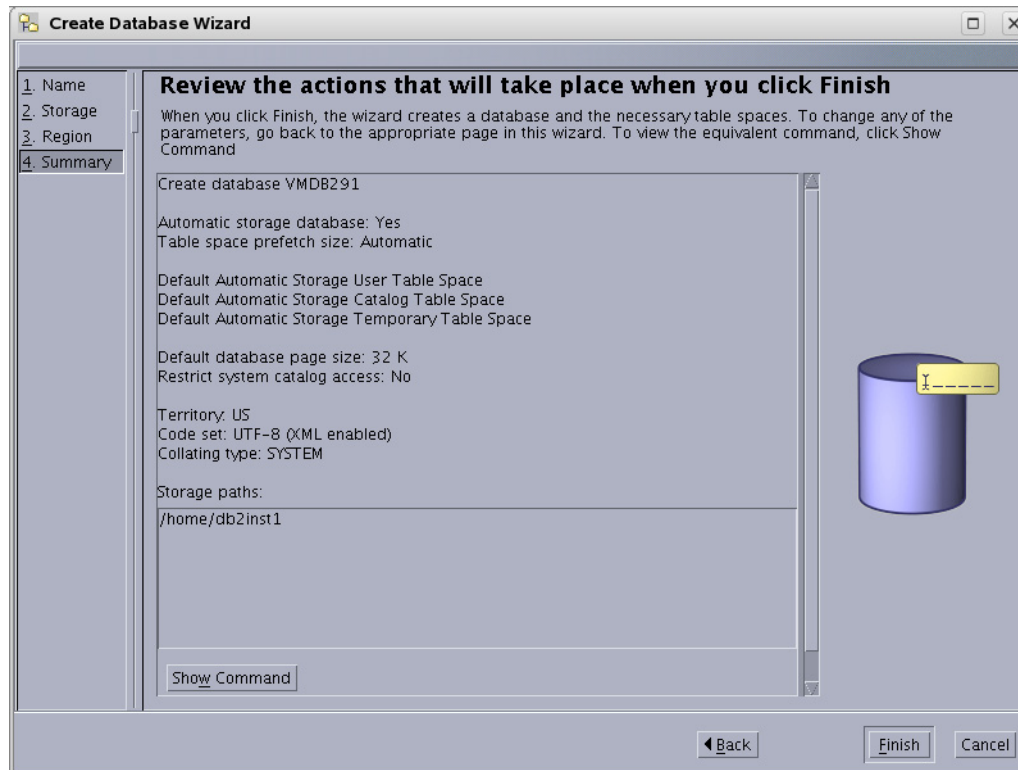
6. In “Specify where to store your data,” click **Next** (a value is unnecessary, as we kept the default option of **Let DB2 manage my storage (automatic storage)**, on the previous page).



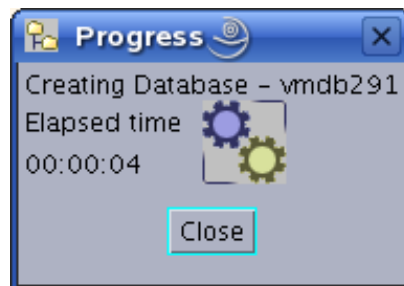
7. In “Specify the locale for this database,” ensure that the drop-down “Code set” displays UTF-8 and click **Next**.



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

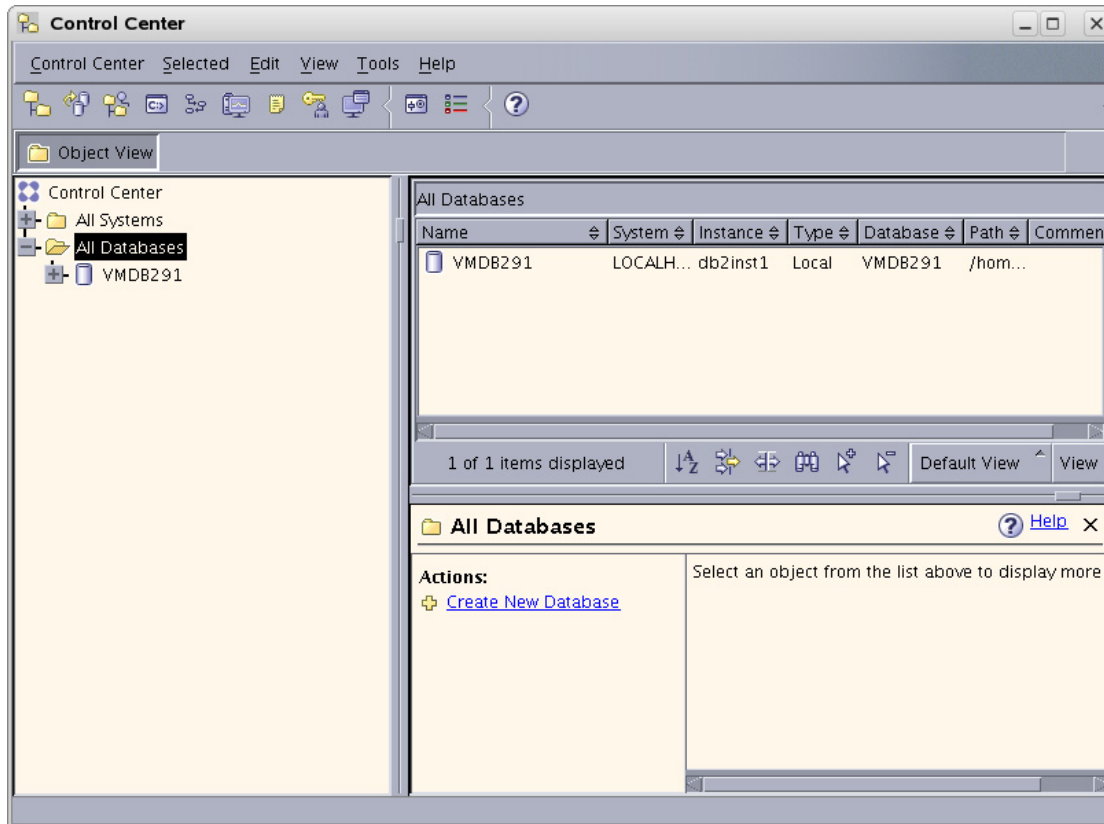


9. Allow the “Progress” window to complete creating the database. The window will close automatically when the database has been created.



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



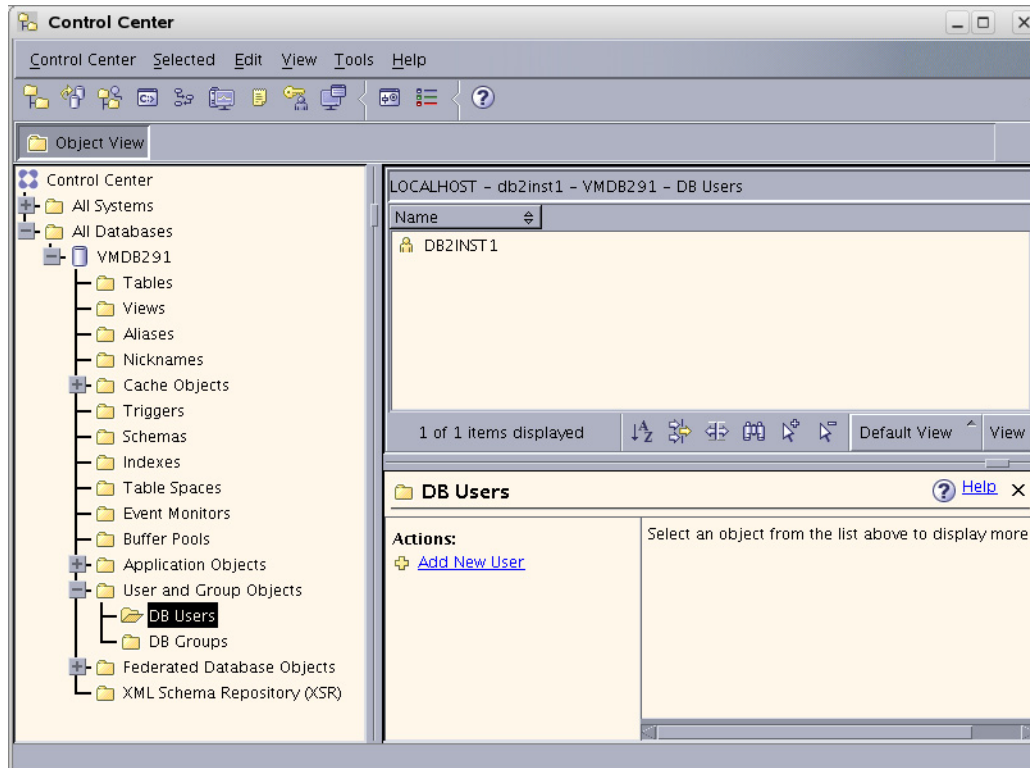
C. Create a User for the New Database

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.

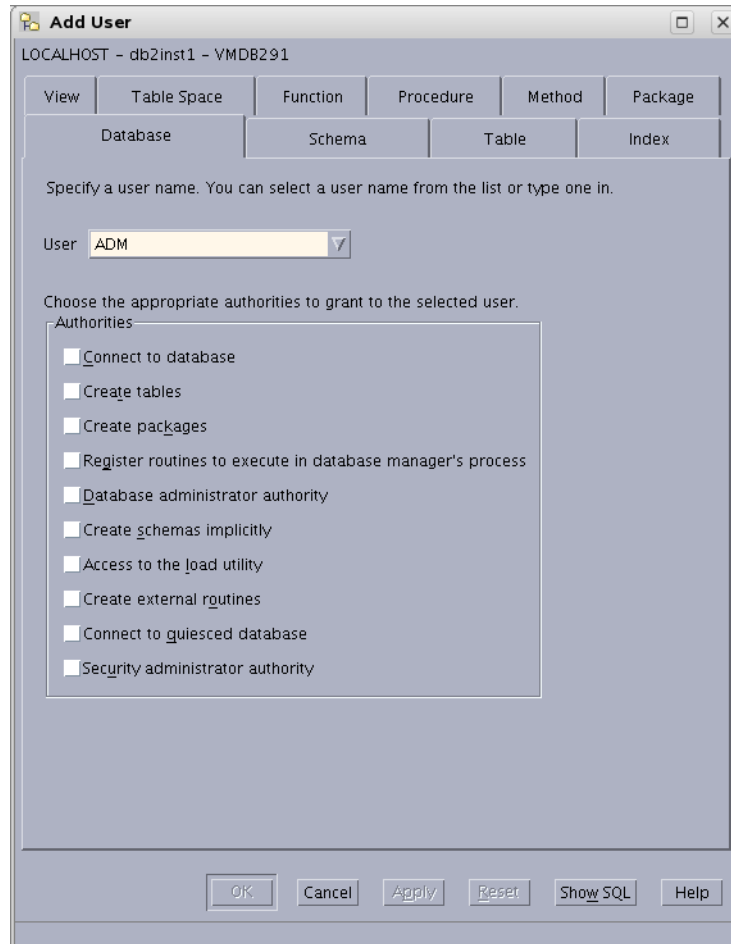
Example of how to create a user named `csuser` on Linux:

```
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 on 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 74](#).
 - b. Under “Authorities,” select all check boxes.
 - c. Click **OK**.

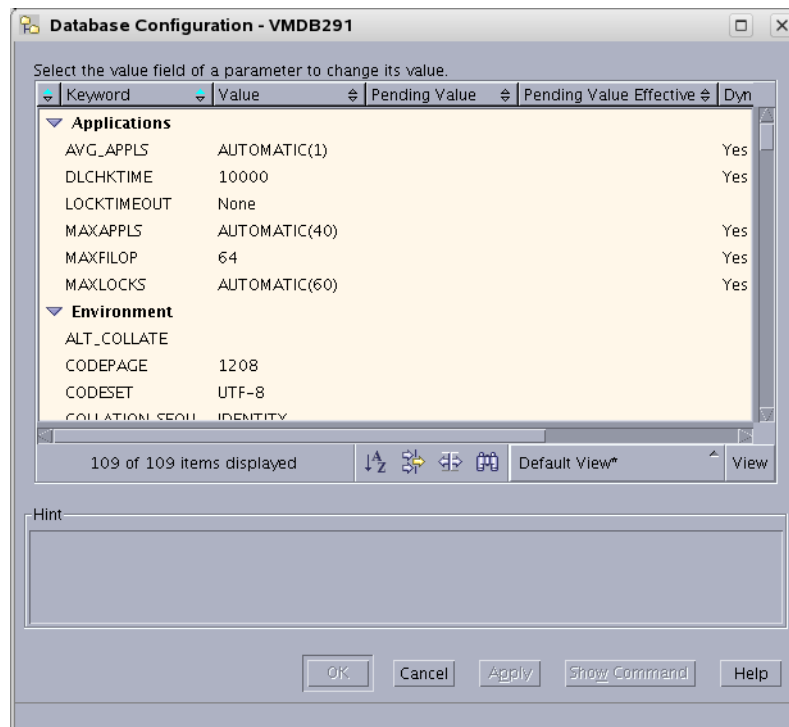


D. Configure the Database

1. Right-click on 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

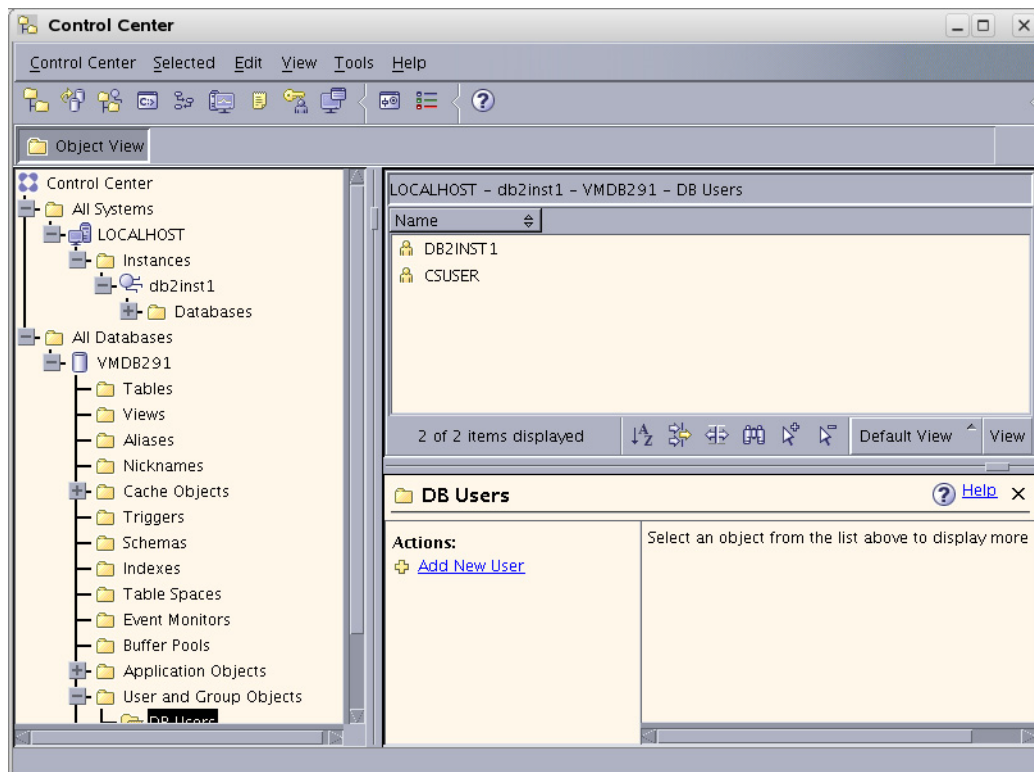
- b. Click **OK**.



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

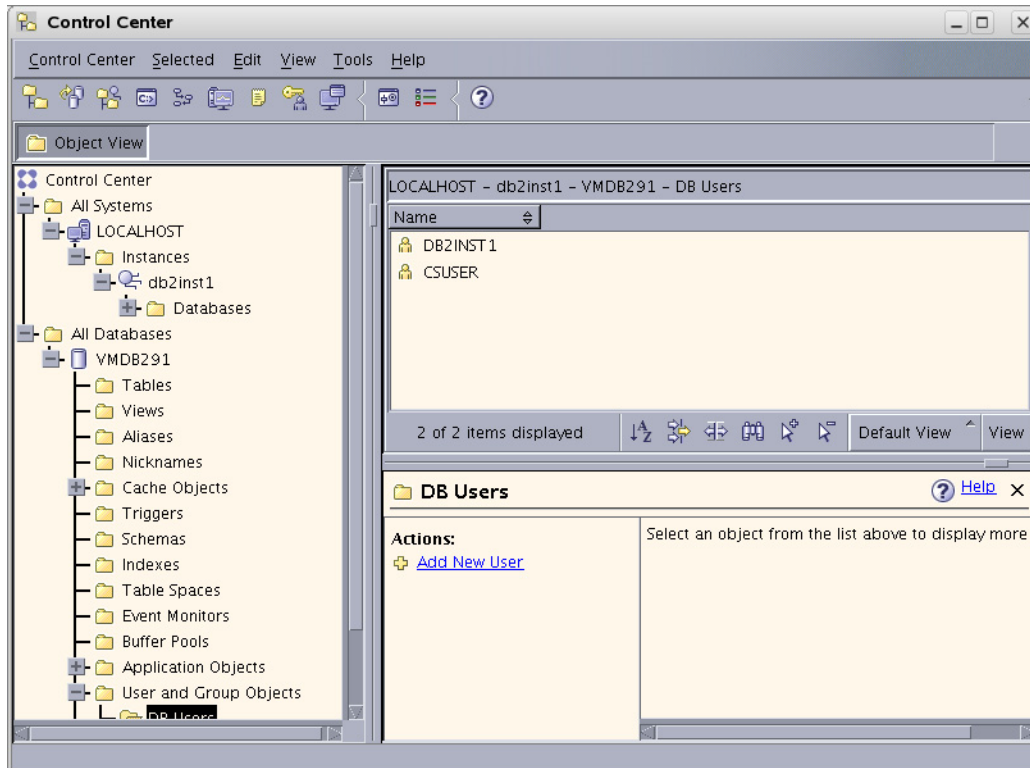
A status window flashes. ***This does not mean that the operation has been completed.*** Typically, you will need to wait 2 to 3 minutes for the system to restart.

4. Stop the instance:
 - a. Expand the following “Control Center” tree branch: **All Systems > LOCALHOST > Instances > name_of_your_instance**
 - b. Right-click on 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 on 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”](#)
- [Chapter 7, “Installing IIS on Windows”](#)
- [Chapter 8, “Installing Apache on Solaris and Linux”](#)

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	<i>WebVersion</i>	Example: Apache 1.3.37	
Web Host Name	<i>WebHost</i>	Example: jeeves	
Web Host IP Address	<i>WebIP</i>	Example: 104.222.111.155	
Web Server Port	<i>WebPort</i>	Default: 80	
IIS Only: Filter Name (ISAPI plug-in name)	<i>FilterName</i>	Suggested: iisforwardfilter	
Apache Only: Apache Root Directory	<i>ApacheRoot</i>	Example: /usr/apache	

Table 2: Apache Web Server Parameters

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

Chapter 7

Installing IIS on Windows

This chapter explains how to install and test Microsoft's Internet Information Services (IIS). It contains the following sections:

- [Step I. Install IIS](#)
- [Step II. Document Your IIS Installation](#)
- [Step III. Verify the Installation](#)
- [Next Step](#)

Note

Typically, IIS is either partially or fully installed on most Windows 2000 machines.

- If IIS is only partially installed or not installed, start with the first section, "[Step I. Install IIS](#)," on page 88.
- If IIS is fully installed, start with the section "[Step II. Document Your IIS Installation](#)," on page 88.

Step I. Install IIS

If IIS is not installed or is only partially installed, follow Microsoft's instruction for installing IIS on a Windows 2000 system.

As a convenience, here is a quick synopsis of the instructions:

1. Select **Start > Settings > Control Panel**.
2. Select **Add/Remove Programs**.
3. Select the **Add/Remove Windows Components** tab on the left.
The **Add/Remove Windows Components Wizard** appears.
4. Select **Internet Information Services (IIS)** and then follow the instructions for installing it.

Step II. Document Your IIS Installation

We strongly recommend that you document the details of your IIS installation in [Table 3](#), “[IIS Parameters](#).”

Table 3: IIS Parameters

Parameter	What It Holds	Your Value
Web Version (<i>WebVersion</i>)	The version number of the IIS software that you installed.	
Web Host Name (<i>WebHost</i>)	The name by which the installation machine is known on the network.	
Web Host IP Address (<i>WebIP</i>)	The numeric Internet Protocol address assigned to the web server host machine.	
Web Server Port (<i>WebPort</i>)	The port number assigned for web server communications. By default, it has the value 80.	

Step III. Verify the Installation

After you have installed IIS, you start it and then browse to it in a web browser to determine whether it is serving pages as it should.

A. Start IIS

You can start the various IIS services in various ways. To be sure that all the necessary services are running, start IIS from the **Services** node.

To start IIS services

1. Right-click on the **My Computer** icon.

2. Select **Manage** from the right-mouse menu.
3. In the **Computer Management** dialog box, expand the **Services and Applications** node in the tree.
4. Select **Services**.
5. In the list of services on the right, right click **IIS Admin Service**.
6. Select **Start** from the right mouse menu.

To start or stop the default web site only

1. Right-click on the **MyComputer** icon.
2. Select **Manage** from the right mouse menu.
3. In the **Computer Management** window, expand the **Services and Applications** node in the tree.
4. Expand the **Internet Information Services** node.
5. Right-click on **Default Web Site**.
6. Select **Start** or **Stop**, as appropriate, from the right mouse menu.

B. Verify that IIS is Serving Pages

To verify that IIS can serve pages, test it from both the server that is hosting it and from another browser on the network.

To verify that IIS can serve pages

1. Start a browser on the host on which IIS is running.
2. From the browser, go to the following URL:
`http://WebHost:WebPort`
3. Do one of the following:
 - If the browser displays the IIS home page, then IIS is installed and running properly. Continue to step 4.
 - If the browser returns an error, consult Microsoft's documentation, determine what went wrong, and fix it before you continue.
4. Start a browser on another machine on your network (a host other than the machine hosting IIS).
5. From the browser, go to the following URL:
`http://WebHost:WebPort`

If the browser displays the IIS "Under Construction" page, then IIS is installed and running and the network naming service appears to be working properly.

Next Step

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

Chapter 8

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](#)
- [Step II. Document Your Apache Parameters](#)
- [Step III. Verify that Apache Contains the Correct Module](#)
- [Step IV. Verify that Apache Runs Properly](#)
- [Next Step](#)

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 92.
 - 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 4](#), “[Apache Parameters.](#)”

Table 4: Apache Parameters

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

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 93](#).
- 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 92](#).

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 92](#)).

Next Step

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

Part 3

Install and Configuring LDAP

This part describes how to install and configure a supported LDAP server for integration with your Content Server application.

This part contains the following chapters:

- [Chapter 9, “Setting Up Sun Java Systems Access Manager 7.0”](#)
- [Chapter 10, “Setting Up Sun Java Systems Directory Server 5.2”](#)
- [Chapter 11, “Setting Up OpenLDAP 2.3.x”](#)
- [Chapter 12, “Setting Up the WebLogic 9.x Embedded LDAP Server”](#)

Chapter 9

Setting Up Sun Java Systems Access Manager 7.0

This chapter provides instructions for setting up the currently supported Sun Java Systems 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.

This chapter contains the following sections:

- [Start/Stop Commands](#)
- [Creating CS Users in Sun Access Manager](#)

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:

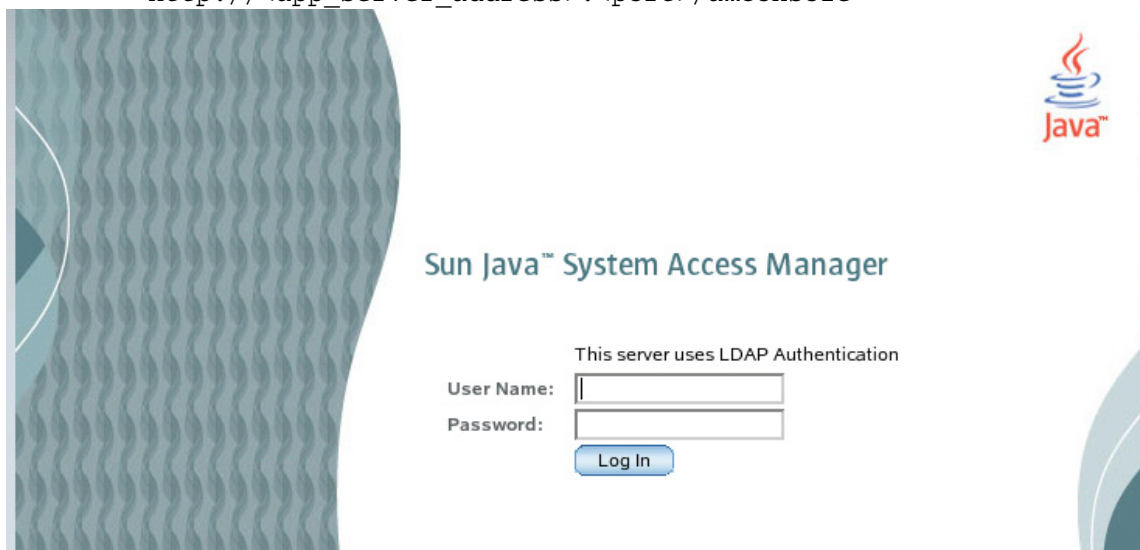
- On Solaris:
`./usr/sbin/amserver stop`
- On Unix (except Solaris):
`<sun_portal_home>/identity/bin/amserver stop`
- On Windows:
Start --> Programs --> Sun Microsystems --> Sun One Identity --> Stop Sun One Identity Servers --> Stop

Creating CS Users in Sun Access Manager

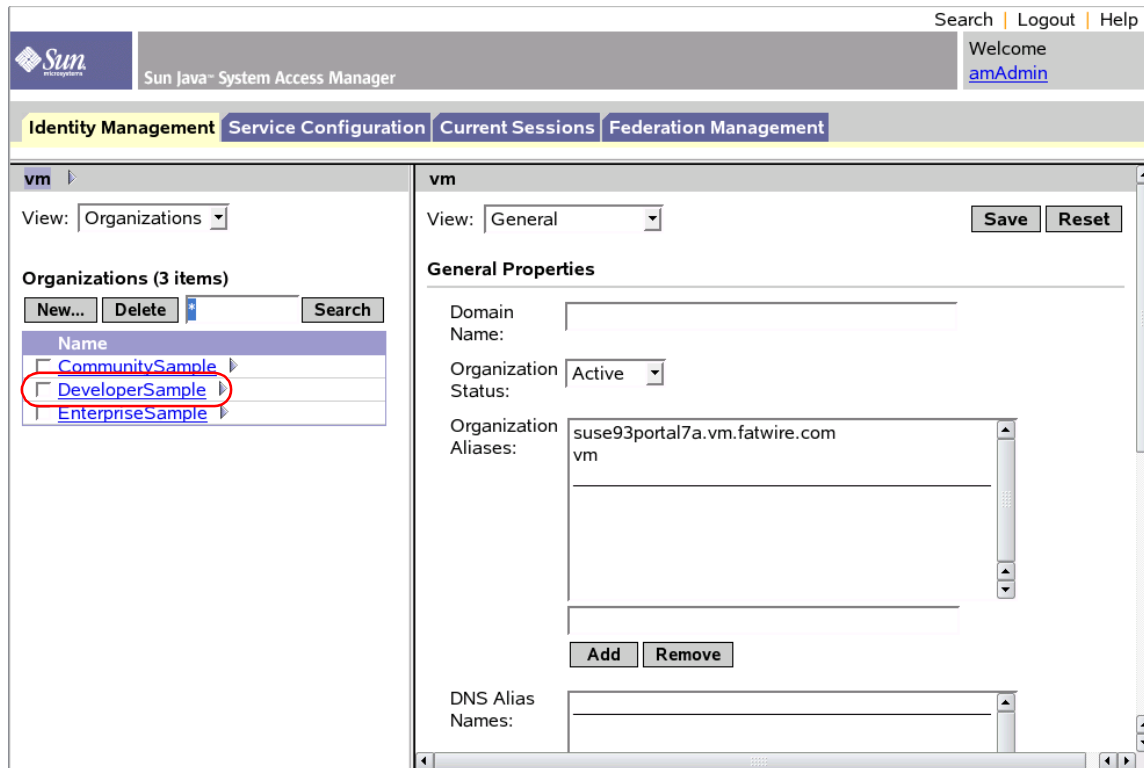
In this section, you will use the Sun Access Manager console to create Content Server users in the backend LDAP server that is associated with Sun Access Manager.

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).

- 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**.

The screenshot shows the Sun Java System Access Manager 7.0 interface. The top navigation bar includes 'Search', 'Logout', and 'Help'. The main navigation tabs are 'Identity Management', 'Service Configuration', 'Current Sessions', and 'Federation Management'. The left pane shows the 'vm > DeveloperSample' breadcrumb. The 'View' dropdown menu is open, showing options: Organizations, Groups, Users, Services, Roles, Policies, and Agents. The 'Users' option is highlighted. The right pane shows the 'DeveloperSample' configuration page with a 'View' dropdown set to 'General'. The 'General Properties' section includes fields for 'Domain Name', 'Organization Status' (set to 'Active'), 'Organization Aliases' (containing 'DeveloperSample'), and 'DNS Alias Names'. There are 'Save' and 'Reset' buttons at the top right of the configuration pane.

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

The screenshot shows the Sun Java System Access Manager 7.0 interface. The top navigation bar includes 'Search', 'Logout', and 'Help'. The main navigation tabs are 'Identity Management', 'Service Configuration', 'Current Sessions', and 'Federation Management'. The left pane shows the 'vm > DeveloperSample' breadcrumb. The 'View' dropdown menu is open, showing options: Organizations, Groups, Users, Services, Roles, Policies, and Agents. The 'Users' option is highlighted. The right pane shows the 'fwadmin' configuration page with a 'View' dropdown set to 'General'. The 'General Properties' section includes fields for 'First Name', '* Last Name' (set to 'default'), '* Full Name' (set to 'fwadmin'), 'Password' (with a 'Change...' link), 'Email Address', 'Employee Number', 'Telephone Number', 'Home Address', '* User Status' (set to 'Active'), and 'Account Expiration Date'. There are 'Save' and 'Reset' buttons at the top right of the configuration pane. A note '* Indicates required field' is present.

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**.

Search | Logout | Help

Welcome
[amAdmin](#)

Identity Management Service Configuration Current Sessions Federation Management

vm > DeveloperSample ▾

View: Users ▾

Users (1 item)

New... Delete fwadmin Search

[Advanced Search...](#)

User ID	Full Name
fwadmin	fwadmin ▾

New User - Step 1 of 2

Select the services to be assigned to the user.

Available Services

<input type="checkbox"/>	Access List
<input type="checkbox"/>	Authentication Configuration
<input checked="" type="checkbox"/>	Mobile Address Book
<input checked="" type="checkbox"/>	Mobile Calendar
<input checked="" type="checkbox"/>	Mobile Mail
<input type="checkbox"/>	NetFile
<input type="checkbox"/>	Netlet
<input checked="" type="checkbox"/>	portal1 Desktop
<input checked="" type="checkbox"/>	portal1 Subscriptions
<input type="checkbox"/>	Proxylet
<input checked="" type="checkbox"/>	SSO Adapter

Back Next Cancel

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**.

Search | Logout | Help

Welcome
[amAdmin](#)

Identity Management | Service Configuration | Current Sessions | Federation Management

vm > DeveloperSample ▾

View: Users ▾

Users (1 item)

New... Delete fwadmin Search

[Advanced Search...](#)

User ID	Full Name
<input type="checkbox"/> fwadmin	fwadmin ▾

New User - Step 2 of 2

Enter Required User Attributes

* Indicates required field

User

* User ID: demouser

First Name:

* Last Name: demo

* Full Name: user

* Password: *****

* Password (confirm): *****

* User Status: Active ▾

Back Finish Cancel

9. Assign Groups to the user:
 - a. Locate the newly created user (the fastest way is to use the **Search** function).

The screenshot displays the Sun Java System Access Manager web interface. The top navigation bar includes links for Search, Logout, and Help, along with a welcome message for 'amAdmin'. The main menu features tabs for Identity Management, Service Configuration, Current Sessions, and Federation Management. The left pane shows the 'vm > DeveloperSample' view with a 'Users' filter. A table lists one user, 'demouser', with a red circle highlighting the selection checkbox. The right pane shows the 'demouser' user details in the 'General' tab, with fields for First Name, Last Name, Full Name, Password, Email Address, Employee Number, Telephone Number, Home Address, User Status, and Account Expiration Date. The 'User Status' is set to 'Active'. A red asterisk indicates required fields.

User ID	Full Name
<input type="checkbox"/> demouser	user

demouser

View: General

Save Reset

* Indicates required field

First Name:

* Last Name:

* Full Name:

Password: [Change...](#)

Email Address:

Employee Number:

Telephone Number:

Home Address:

* User Status:

Account Expiration Date:

Format: mm/dd/yyyy hh:mm

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

The screenshot displays the Sun Java System Access Manager web interface. The top navigation bar includes links for Search, Logout, and Help, along with a welcome message for 'amAdmin'. The main navigation tabs are Identity Management, Service Configuration, Current Sessions, and Federation Management. The left pane shows the 'vm > DeveloperSample' hierarchy with a 'View: Users' dropdown. The right pane is titled 'demouser' and has a 'View: Groups' dropdown, which is circled in red. Below this, a message states: 'The Selected list contains the groups associated with this user. Use Search to find a specific group.' A search box with a '*' placeholder and a 'Search' button is provided. The 'Available:' list contains the following groups: PageEditor, GE Lighting-GeneralAdmin, BurlingtonFinancial-Designer, GE Lighting-WorkflowAdmin, FirstSiteII-ProductEditor, GE Lighting-Designer, BurlingtonFinancial-Checker, and FirstSiteII-ProductAuthor. At the bottom of the available list are buttons for 'Add', 'Add All', 'Remove', and 'Remove All'. The 'Selected:' list is currently empty.

User ID	Full Name
<input type="checkbox"/> demouser	user ▶
<input type="checkbox"/> user_analyst	user_analyst ▶
<input type="checkbox"/> user_approver	user_approver ▶
<input type="checkbox"/> user_author	user_author ▶
<input type="checkbox"/> user_checker	user_checker ▶
<input type="checkbox"/> user_designer	user_designer ▶
<input type="checkbox"/> user_editor	user_editor ▶
<input type="checkbox"/> user_expert	user_expert ▶
<input type="checkbox"/> user_marketer	user_marketer ▶
<input type="checkbox"/> user_pricer	user_pricer ▶

- 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**.

The screenshot shows the Sun Java System Access Manager web interface. The top navigation bar includes 'Search', 'Logout', and 'Help'. The main header displays the Sun logo and 'Sun Java System Access Manager'. Below this, there are tabs for 'Identity Management', 'Service Configuration', 'Current Sessions', and 'Federation Management'. The 'Identity Management' tab is selected, and the 'Users' sub-tab is active. On the left, a 'View: Users' dropdown is shown. Below it, a 'Users (10 items)' section contains a search bar with 'user*' and a 'Search' button. A table lists users with columns 'User ID' and 'Full Name'. On the right, a 'Use Search to find a specific group.' section has a search bar. Below it, an 'Available:' list contains roles like PageEditor, GE Lighting-GeneralAdmin, etc. At the bottom of this list are buttons: 'Add', 'Add All', 'Remove', and 'Remove All'. A 'Selected:' list below shows 'Spark-SiteAdmin', 'Spark-SparkContentUser', and 'Spark-GeneralAdmin'. At the bottom right are 'Save' and 'Reset' buttons.

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 10

Setting Up Sun Java Systems Directory Server 5.2

This chapter how to set up the currently supported Sun Java Systems Directory Server for use with Content Server on Sun Portal Server 7. This chapter contains the following sections:

- [Start/Stop Commands](#)
- [Installing Sun Directory Server](#)
- [Verifying Your LDAP Configuration](#)
- [Modifying User Passwords](#)

Start/Stop Commands

This section contains commands for starting and stopping Sun Directory Server and its administration interface.

Starting and Stopping Sun Directory Server

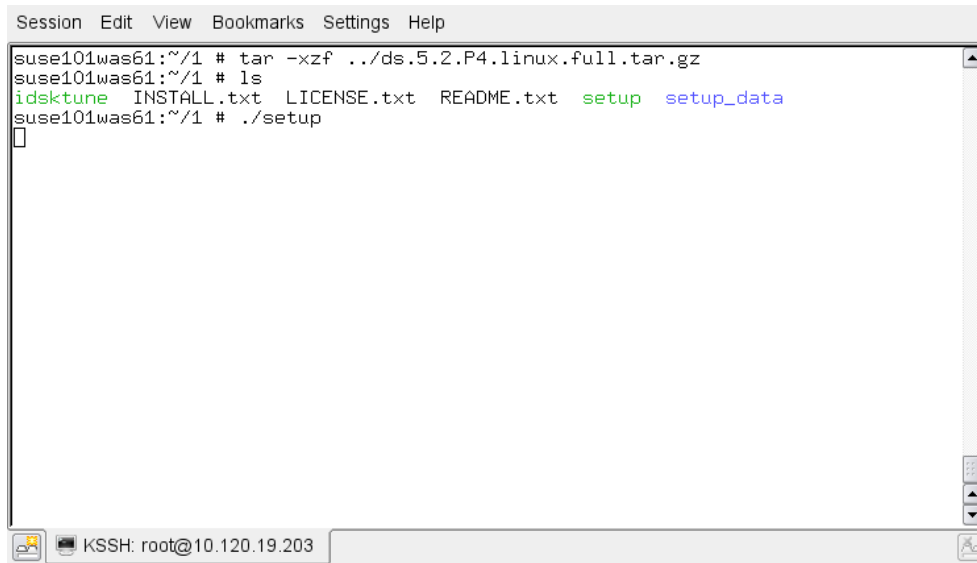
- To start:
 - On Solaris:
`/usr/sbin/directoryserver start`
 - On Unix (except Solaris):
`<dirserv_home>/slapd-<hostname>/start-slapd`
 - On Windows:
Start the following service: Sun ONE Directory Server 5.2 <hostname>
- To stop:
 - On Solaris:
`/usr/sbin/directoryserver stop`
 - On Unix (except Solaris):
`<dirserv_home>/slapd-<hostname>/stop-slapd`
 - On Windows:
Stop the following service: Sun ONE Directory Server 5.2 <hostname>

Starting and Stopping the Sun Directory Server Admin Interface

- To start:
 - On Solaris:
`/usr/sbin/directoryserver start-admin`
 - On Unix (except Solaris):
`<dirserv_home>/start-admin`
- To stop:
 - On Solaris:
`/usr/sbin/directoryserver stop-admin`
 - On Unix (except Solaris):
`<dirserv_home>/stop-admin`

Installing Sun Directory Server

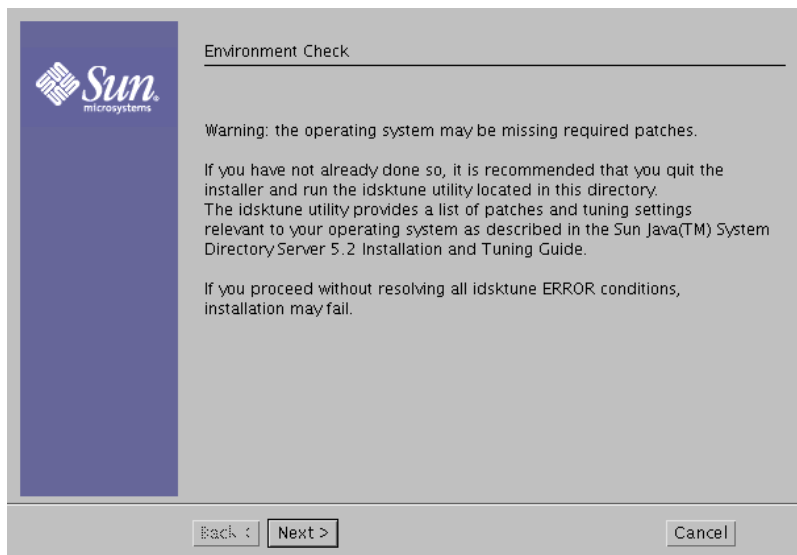
11. Download the Directory Server installation file (`ds.5.2.P4.linux.full.tar.gz`) from Sun's web site.
12. Decompress the file into a temporary directory and change to that directory.
13. Start the Directory Server installer using the following command: `./setup`



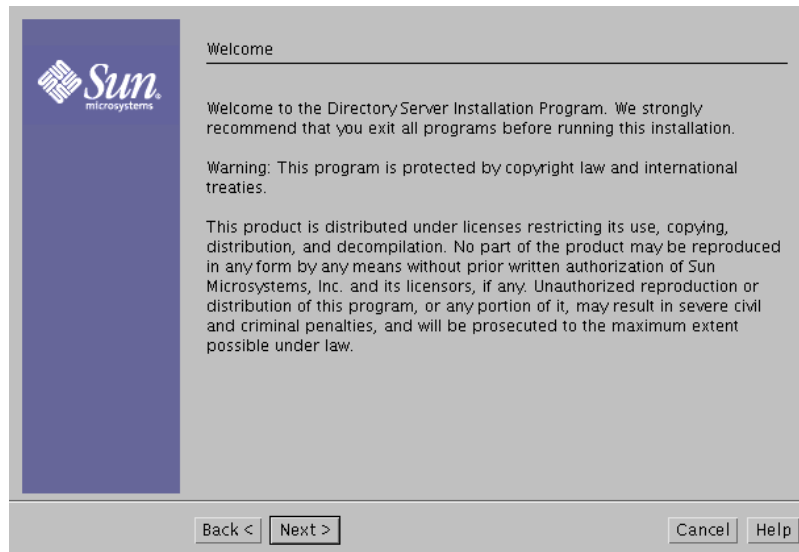
A terminal window with a menu bar (Session, Edit, View, Bookmarks, Settings, Help) and a title bar (KSSH: root@10.120.19.203). The terminal shows the following commands and output:

```
suse101was61:~/1 # tar -xzf ../ds.5.2.P4.linux.full.tar.gz
suse101was61:~/1 # ls
idsktune  INSTALL.txt  LICENSE.txt  README.txt  setup  setup_data
suse101was61:~/1 # ./setup
```

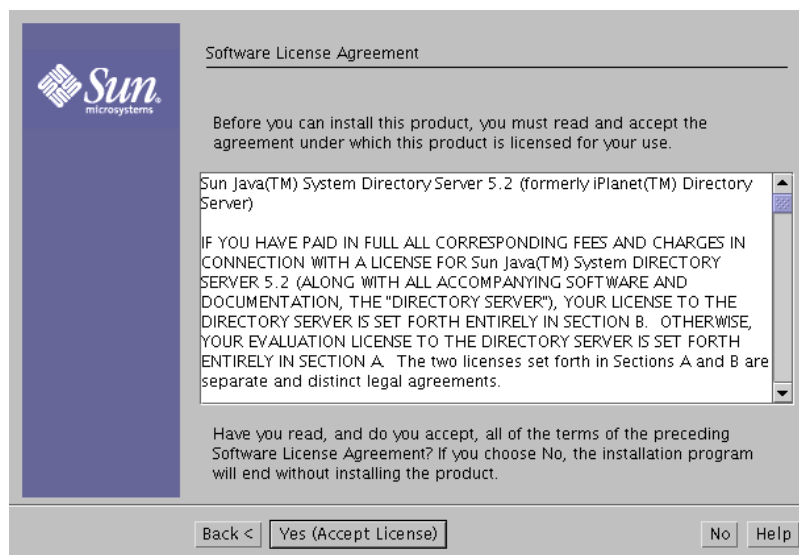
14. In the “Environment Check” screen, click **Next**.



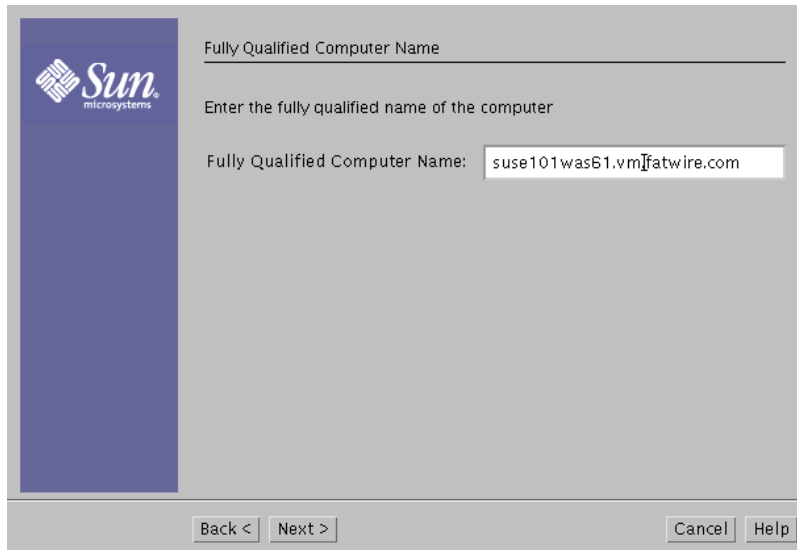
15. In the “Welcome” screen, click **Next**.



16. In the “Software License Agreement” screen, click **Yes (Accept License)**.

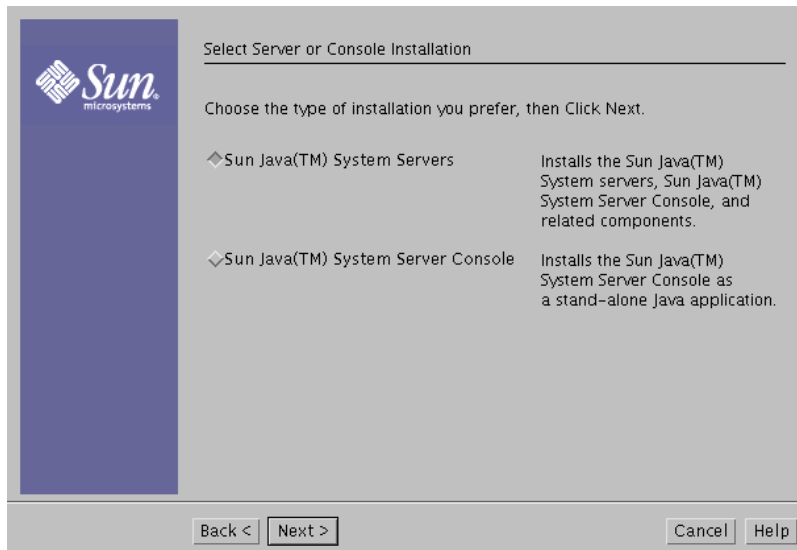


17. In the “Fully Qualified Computer Name” screen, ensure that the displayed DNS name is valid for this server and click **Next**.



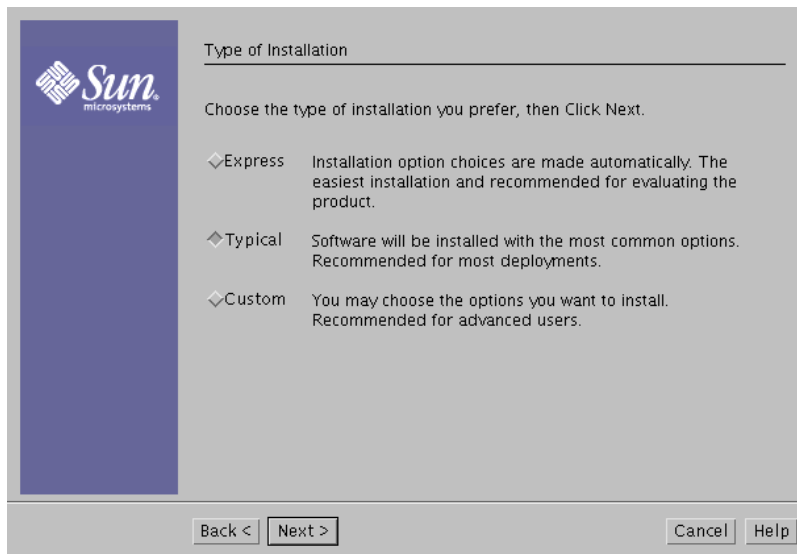
The screenshot shows a window titled "Fully Qualified Computer Name" with the Sun Microsystems logo on the left. The main area contains the text "Enter the fully qualified name of the computer" and a text box labeled "Fully Qualified Computer Name:" containing the value "suse101was61.vm.fatwire.com". At the bottom, there are four buttons: "Back <", "Next >", "Cancel", and "Help".

18. In the “Select Server or Console Installation” screen, select **Sun Java(TM) System Servers** (default selection) and click **Next**.

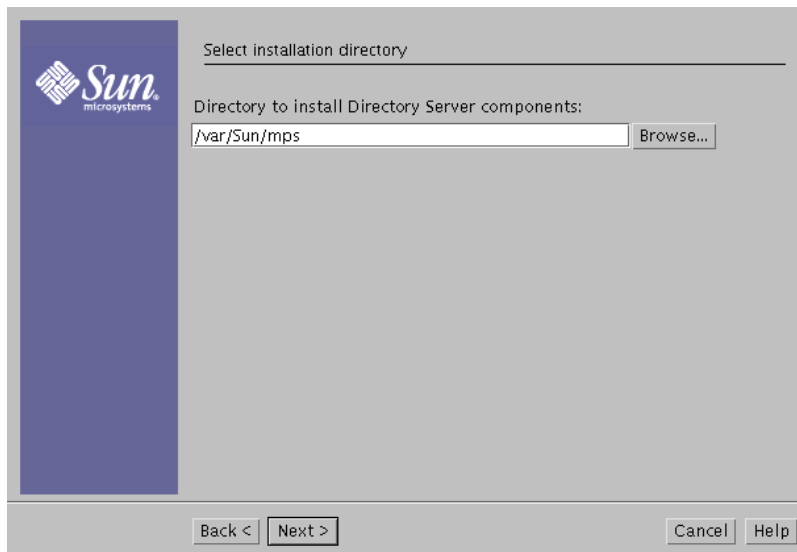


The screenshot shows a window titled "Select Server or Console Installation" with the Sun Microsystems logo on the left. The main area contains the text "Choose the type of installation you prefer, then Click Next." and two radio button options. The first option, "Sun Java(TM) System Servers", is selected and described as "Installs the Sun Java(TM) System servers, Sun Java(TM) System Server Console, and related components." The second option, "Sun Java(TM) System Server Console", is described as "Installs the Sun Java(TM) System Server Console as a stand-alone Java application." At the bottom, there are four buttons: "Back <", "Next >", "Cancel", and "Help".

19. In the “Type of Installation” screen, select **Typical** (default selection).



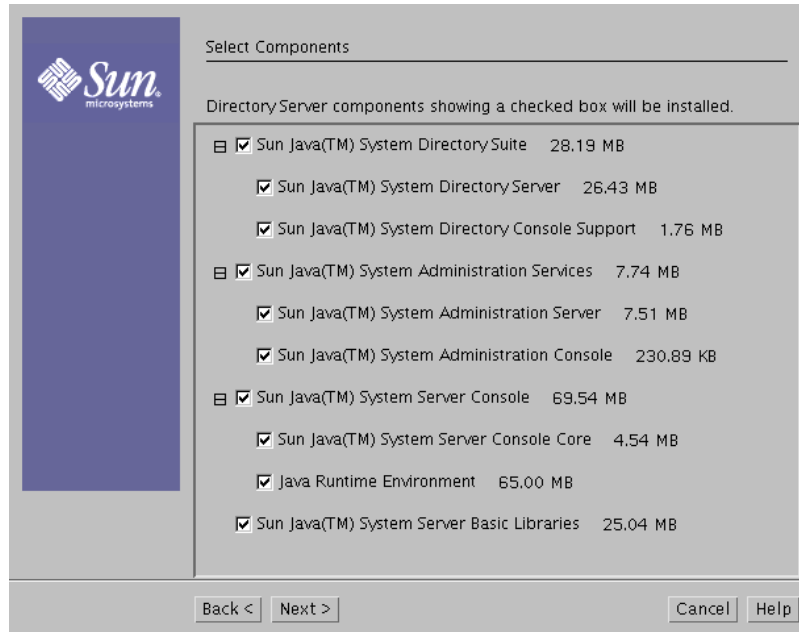
20. In the “Select Installation Directory” screen, enter the path and directory where you want Directory Server installed. (This path is referred to later in this chapter as `<dirserv_home>`.) Typically, it is safe to use the default, unless your installation requires you to install Directory Server in a different location. Make a record of the path you enter here. When you are finished, click **Next**.



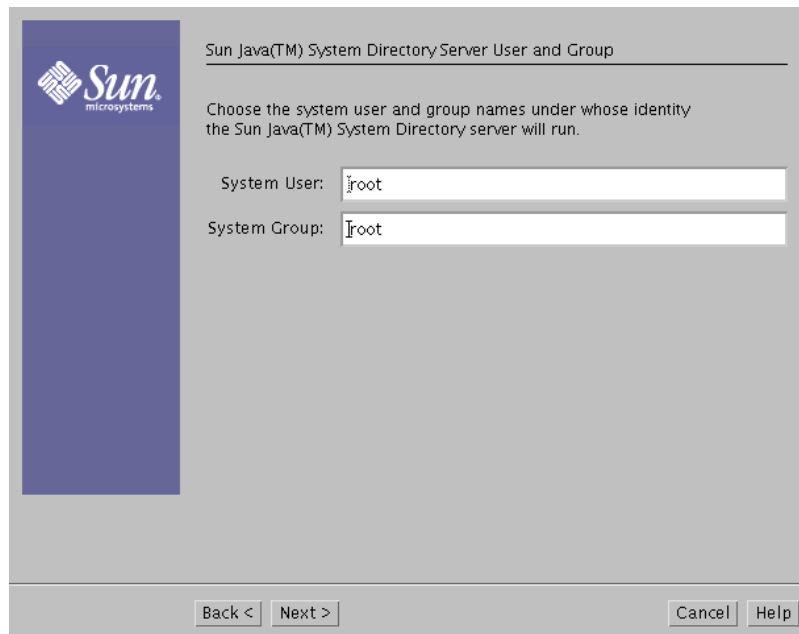
21. In the pop-up dialog, click **Create Directory**.



22. In the “Select Components” screen, select all options and click **Next**.



23. In the “Sun JAVA(TM) Systems Directory Server User Group” screen, enter the user name and group under which Directory Server will run. The default values are acceptable, but if you need to change them for security reasons, you may do so. When you are finished, click **Next**.



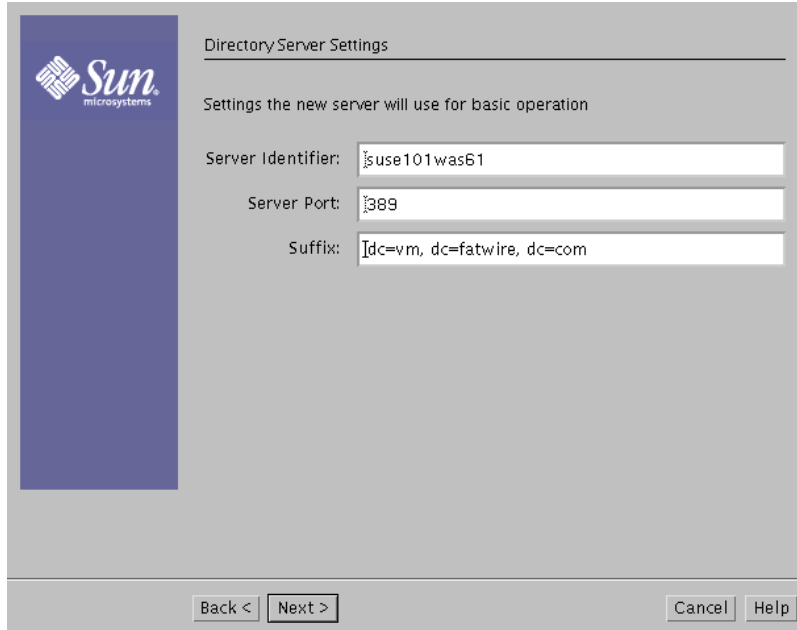
24. In the “Configuration Directory Server” screen, select **The new instance will be the configuration Directory Server** (default selection) and click **Next**.

The screenshot shows the 'Configuration Directory Server' window. On the left is the Sun Microsystems logo. The main text reads: 'You may store Sun Java(TM) System server configuration information in another Sun Java(TM) System Directory Server. If you have already prepared a configuration server, you may configure the new server to use it.' There are two radio button options: 'The new instance will be the configuration Directory Server' (which is selected) and 'Use existing configuration Directory Server'. Below these are input fields for 'Host', 'Port' (set to 389), 'Bind As' (set to admin), and 'Password'. At the bottom are 'Back <', 'Next >', 'Cancel', and 'Help' buttons.

25. In the “Data Storage Location” screen, select **Store data in the new Directory Server** (default selection) and click **Next**.

The screenshot shows the 'Data Storage Location' window. On the left is the Sun Microsystems logo. The main text reads: 'You may already have a Directory Server where you store user and group information.' There are two radio button options: 'Store data in the new Directory Server' (which is selected) and 'Store data in an existing Directory Server'. Below these are input fields for 'Host', 'Port' (set to 389), 'Bind As' (set to cn=Directory Manager), 'Password', and 'Suffix' (set to dc=vm, dc=fatwire, dc=com). At the bottom are 'Back <', 'Next >', 'Cancel', and 'Help' buttons.

26. In the “Directory Server Settings” screen, all values should be properly detected by the installer. Confirm that they are as follows, and make changes if necessary:
- “Server Identifier” is the Directory Server host name
 - “Server Port” is the Directory Server port. This must be set to **389**.
 - “Suffix” is the Directory Server domain. This is also the LDAP base DN.



Directory Server Settings

Settings the new server will use for basic operation

Server Identifier: jsuse101was61

Server Port: 389

Suffix: ldc=vm, dc=fatwire, dc=com

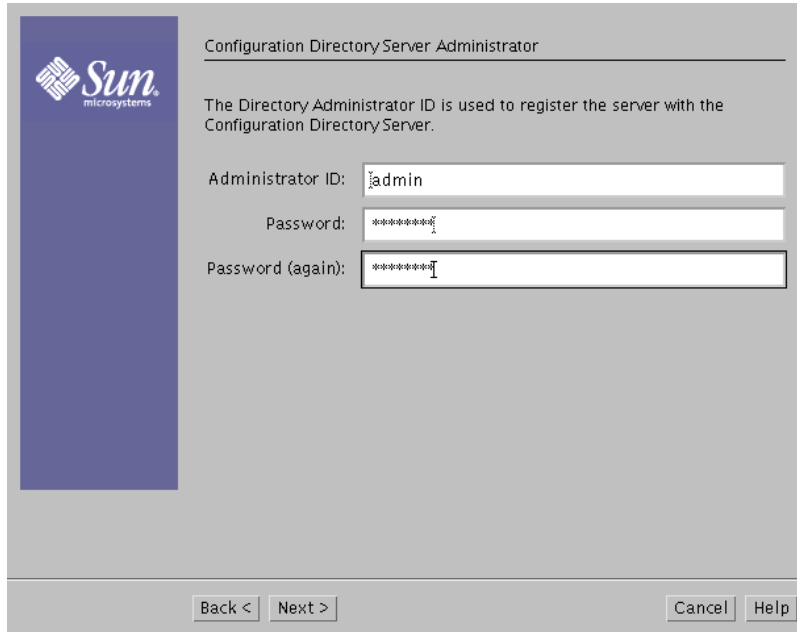
Back < Next > Cancel Help

Note

Make a record of the information you enter in this screen. You will need this information when running the Content Server LDAP integration program.

When you are finished, click **Next**.

27. In the “Configuration Directory Server Administrator” screen, enter a password in the appropriate fields. Make a record of the password you enter here. When you are finished, click **Next**.



Configuration Directory Server Administrator

The Directory Administrator ID is used to register the server with the Configuration Directory Server.

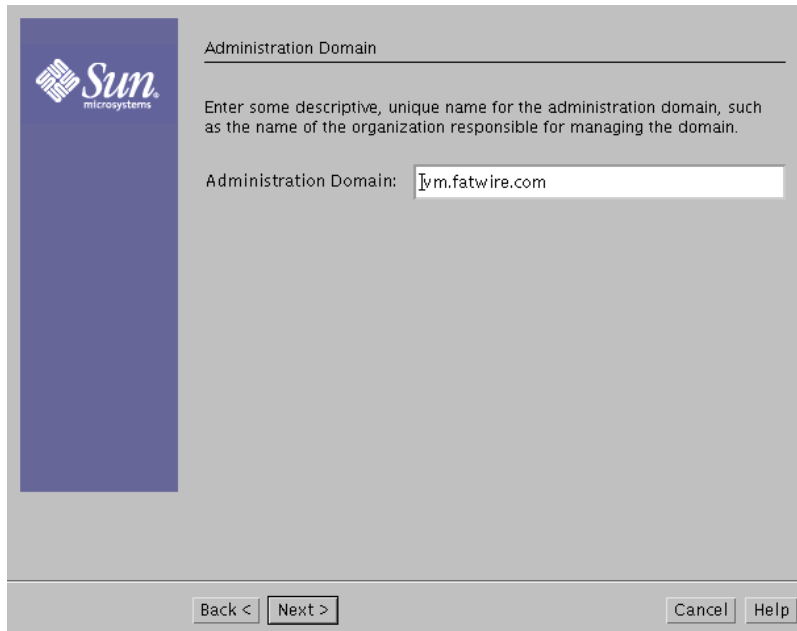
Administrator ID:

Password:

Password (again):

Back < Next > Cancel Help

28. In the “Administration Domain” screen, click **Next**.



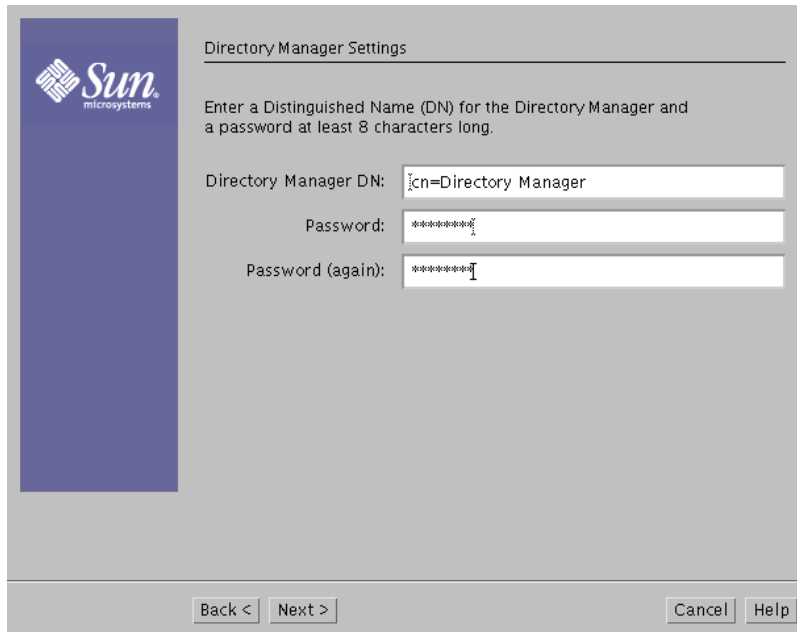
Administration Domain

Enter some descriptive, unique name for the administration domain, such as the name of the organization responsible for managing the domain.

Administration Domain:

Back < Next > Cancel Help

29. In the “Directory Manager Settings” screen, enter a password in the appropriate fields. Make a record of the password you enter here. When you are finished, click **Next**.



Directory Manager Settings

Enter a Distinguished Name (DN) for the Directory Manager and a password at least 8 characters long.

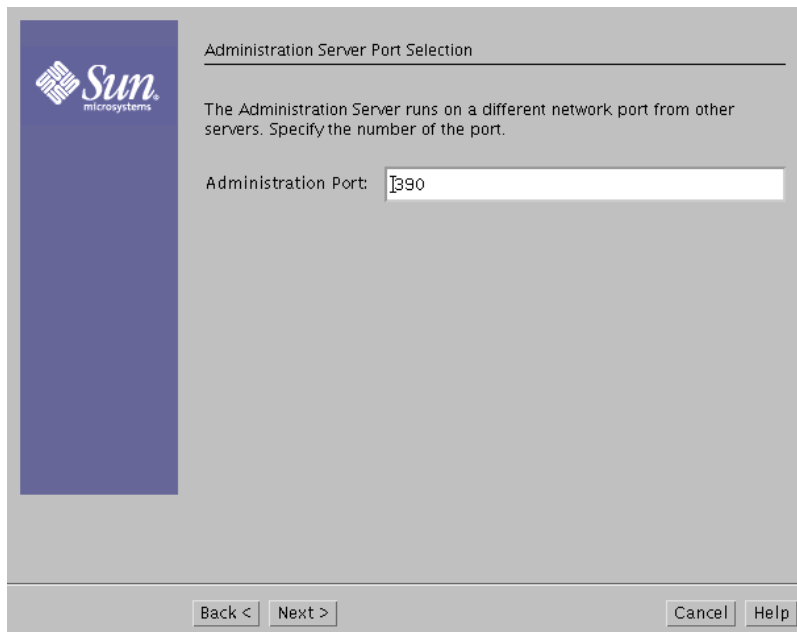
Directory Manager DN:

Password:

Password (again):

Back < Next > Cancel Help

30. In the “Administration Server Port Selection” screen, click **Next**.



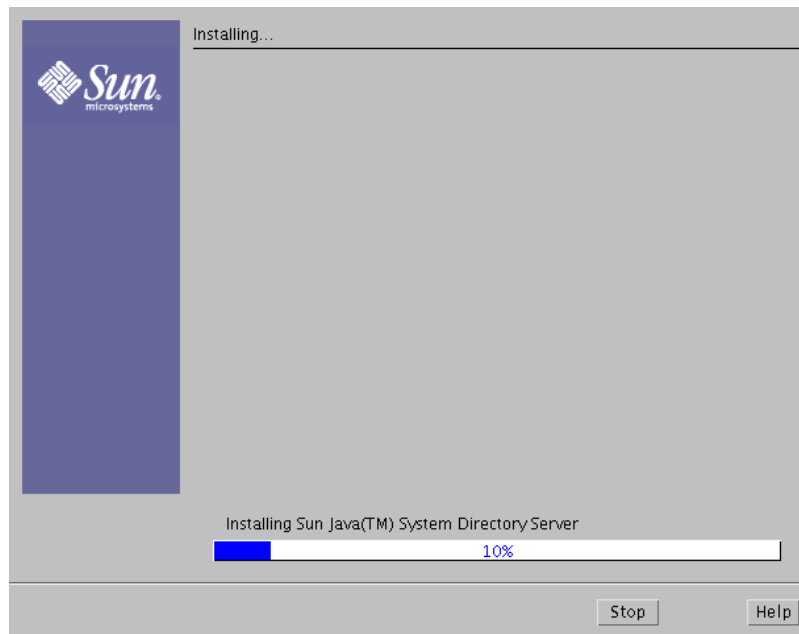
Administration Server Port Selection

The Administration Server runs on a different network port from other servers. Specify the number of the port.

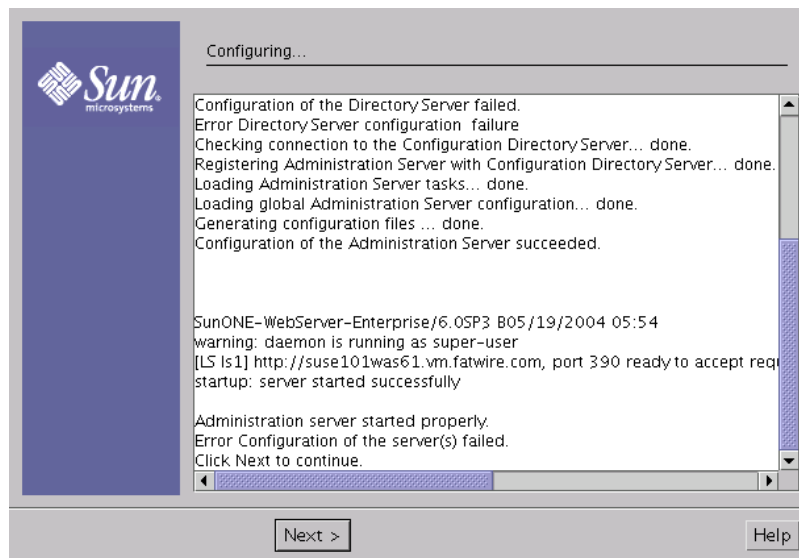
Administration Port:

Back < Next > Cancel Help

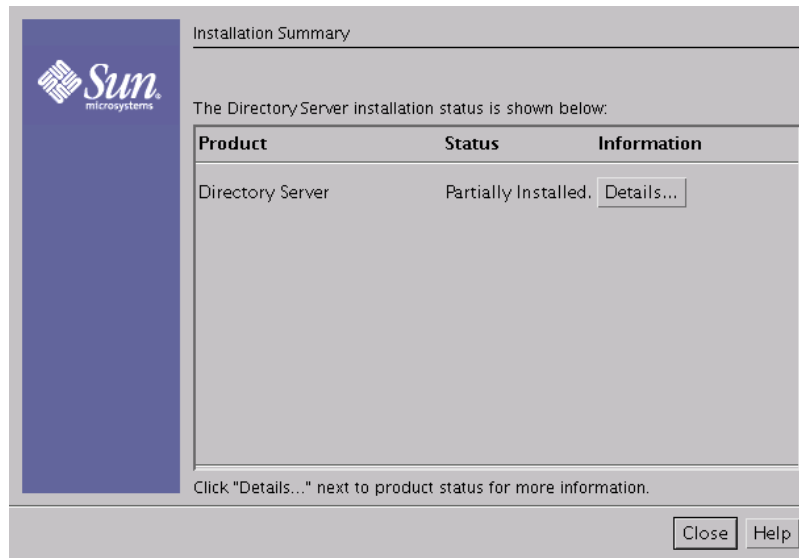
31. In the “Ready to Install” screen, click **Install Now** and wait until the installation is complete.



32. In the “Configuring” screen, click **Next**.



33. In the “Installation Summary” screen, click **Close**.



Verifying Your LDAP Configuration

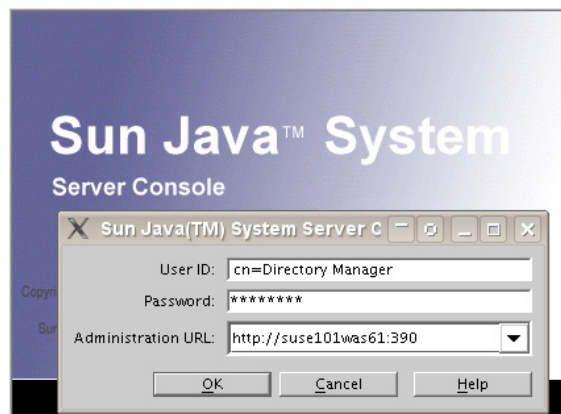
This section shows you how to verify your LDAP configuration through the Sun JES Server Console. You will also use the console to administer Sun Directory Server.

1. Start the JES Server Console:
 - On Solaris:

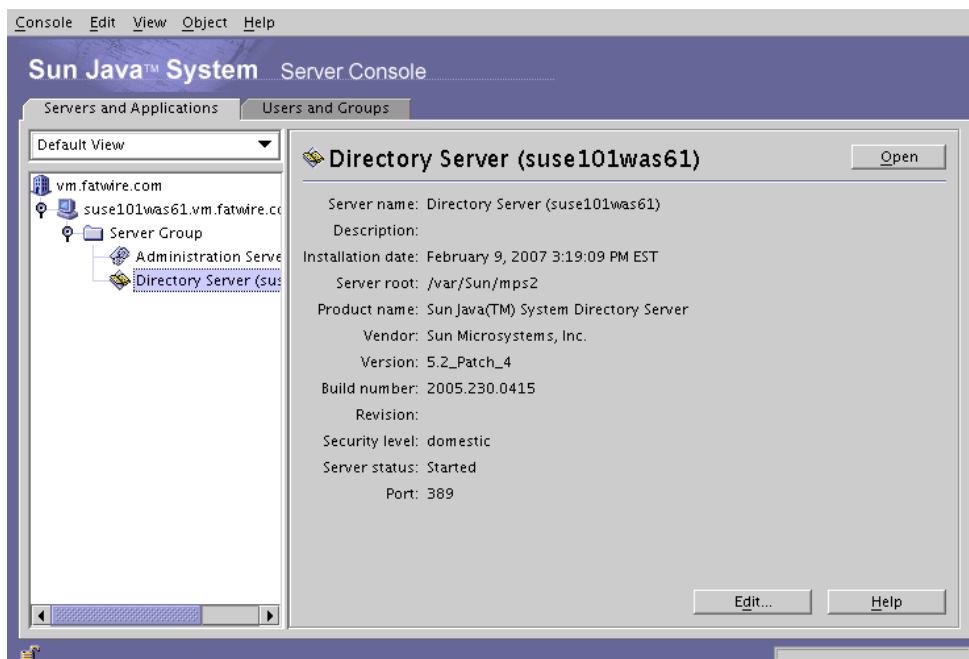

```
/usr/sbin/directoryserver startconsole
```
 - On Unix (except Solaris):


```
<dirserv_home>/startconsole
```
2. In the “Server Console” dialog box, do the following:
 - a. In the **User ID** field, enter **cn=Directory Manager**.
 - b. In the **Password** field, enter the Directory Manager password you entered in [step 29 on page 117](#).

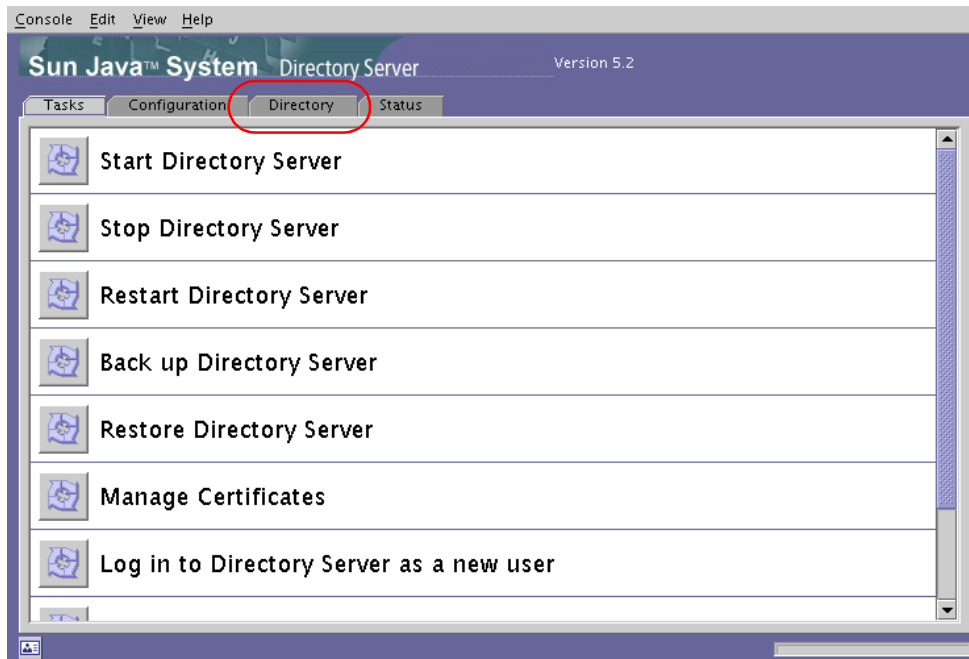
- c. Click **OK**.



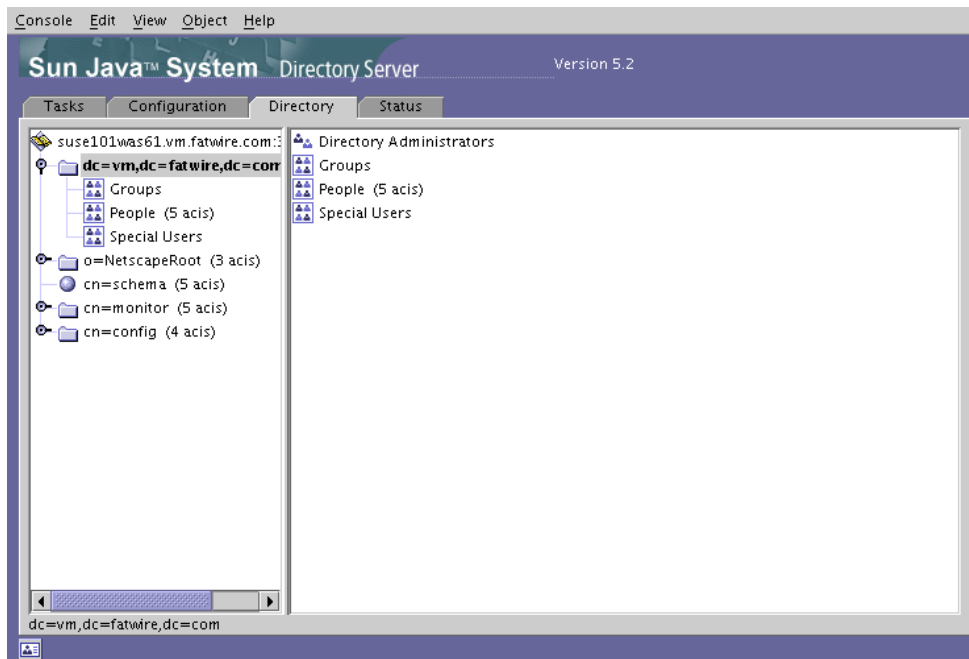
3. In the "System Server Console," drill down the left-hand tree and double-click the **Directory Server** node.



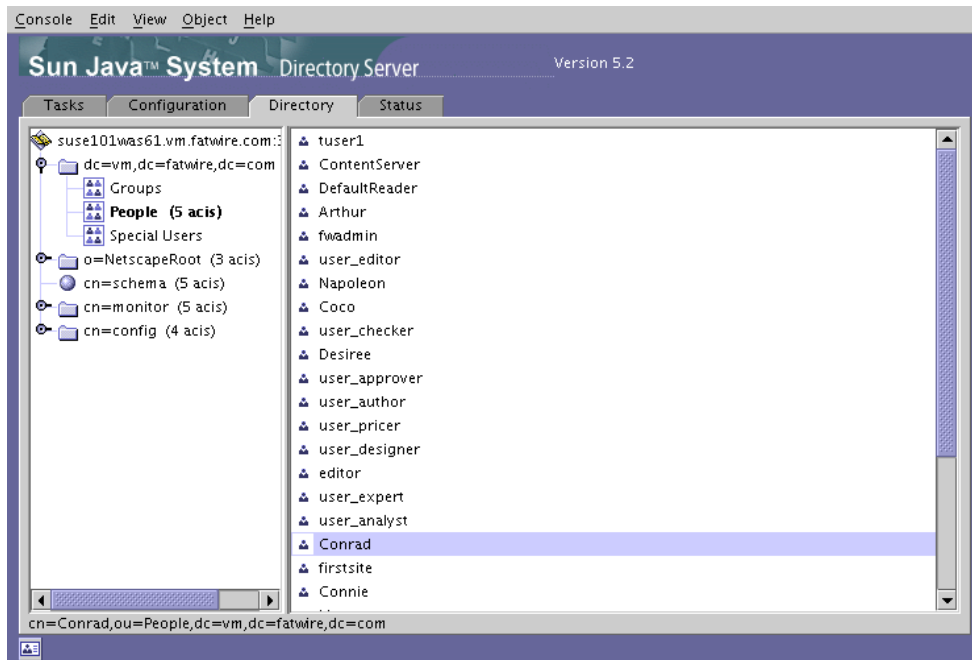
4. In the pop-up window that appears, click the **Directory** tab.



5. In the left-hand tree, locate the base DN for this instance of Directory Server. The base DN is the value you entered in the **Suffix** field in [step 26 on page 115](#). (In the example below, the base DN is `dc=vm,dc=fatwire,dc=com`.)



6. In the left hand tree, click the **People** node and browse the directory in order to confirm that the Content Server users were added correctly.



7. (Optional) If you want to change user passwords, continue on to the next section, [“Modifying User Passwords,” on page 122.](#)

Modifying User Passwords

When you run the Content Server LDAP integrator, all Content Server users (except for fwadmin, ContentServer, and DefaultReader) are assigned the default password that you enter in the “Content Server Configuration” screen of the integrator. For security reasons, you might want to manually change the passwords for these users.

Note

User passwords can be changed from the CS interface or through the JES Server Console. Because it is faster to use the Server Console, we provide the steps in this chapter. To change passwords through Content Server, see the *Content Server Administrator's Guide*.

To modify user passwords through the JES Server Console

1. Perform the steps in [“Verifying Your LDAP Configuration,” on page 119.](#)
2. In the list of users, double-click the user whose password you want to change.

3. In the window that appears, enter the new user password into the appropriate fields, then click **OK**.

Martha

Phone:
Fax:

User
Account

* Last Name: Martha

* Common Name(s): Martha

Password: *****

Confirm Password: *****

Phone: _____

Fax: _____

* Indicates a required field

Access Permissions Help OK Cancel Help

Chapter 11

Setting Up OpenLDAP 2.3.x

This chapter explains how to set up OpenLDAP for use with Content Server. It contains the following sections:

- [OpenLDAP Commands](#)
- [Installing OpenLDAP](#)
- [Configuring OpenLDAP](#)
- [Adding Content Server Schema to OpenLDAP](#)
- [Modifying User Passwords](#)

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 130](#).

2. When prompted for a password, enter the Root DN user password you specified in [step d on page 131](#).

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 130](#).
- <root_dn_password> is the Root DN user password you specified in [step d on page 131](#).
- <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`

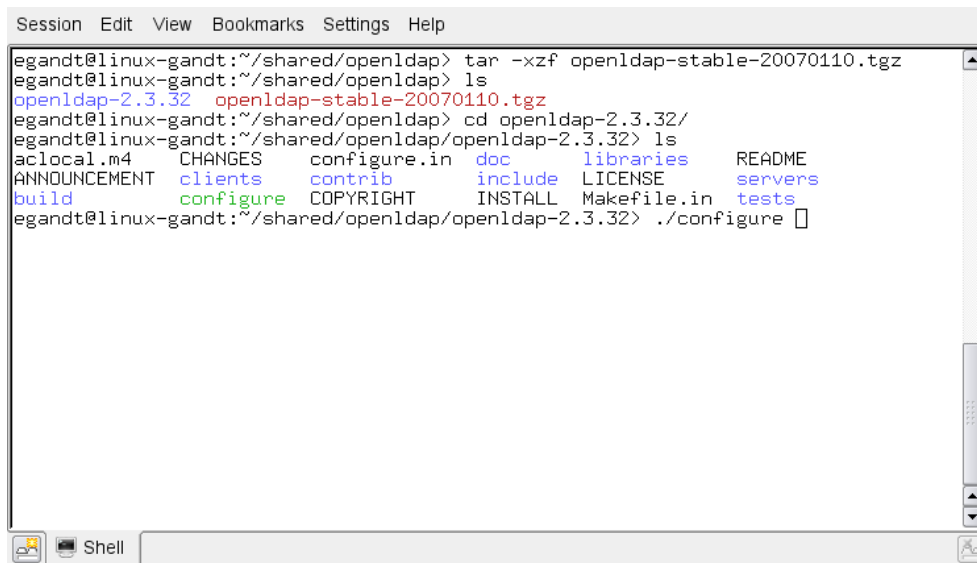
2. Decompress the archive:

- 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:

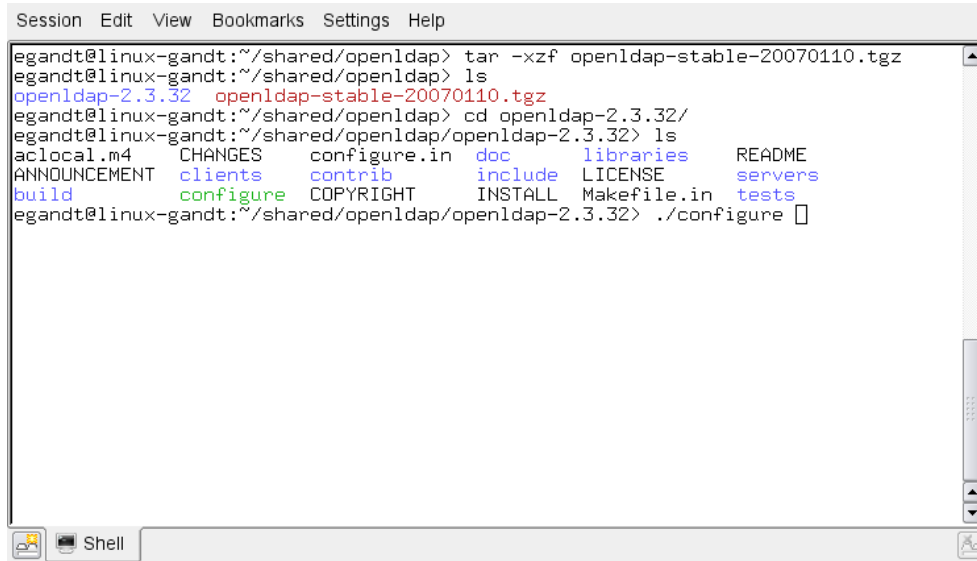
```
gzip -d openldap-stable-20070110.tgz ; tar -xvf openldap-stable-20070110.tar
```



```
Session Edit View Bookmarks Settings Help
egandt@linux-gandt:~/shared/openldap> tar -xzf openldap-stable-20070110.tgz
egandt@linux-gandt:~/shared/openldap> ls
openldap-2.3.32  openldap-stable-20070110.tgz
egandt@linux-gandt:~/shared/openldap> cd openldap-2.3.32/
egandt@linux-gandt:~/shared/openldap/openldap-2.3.32> ls
aclocal.m4  CHANGES  configure.in  doc  libraries  README
ANNOUNCEMENT  clients  contrib  include  LICENSE  servers
build  configure  COPYRIGHT  INSTALL  Makefile.in  tests
egandt@linux-gandt:~/shared/openldap/openldap-2.3.32> ./configure
```


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

```
cd openldap-2.3.32
```



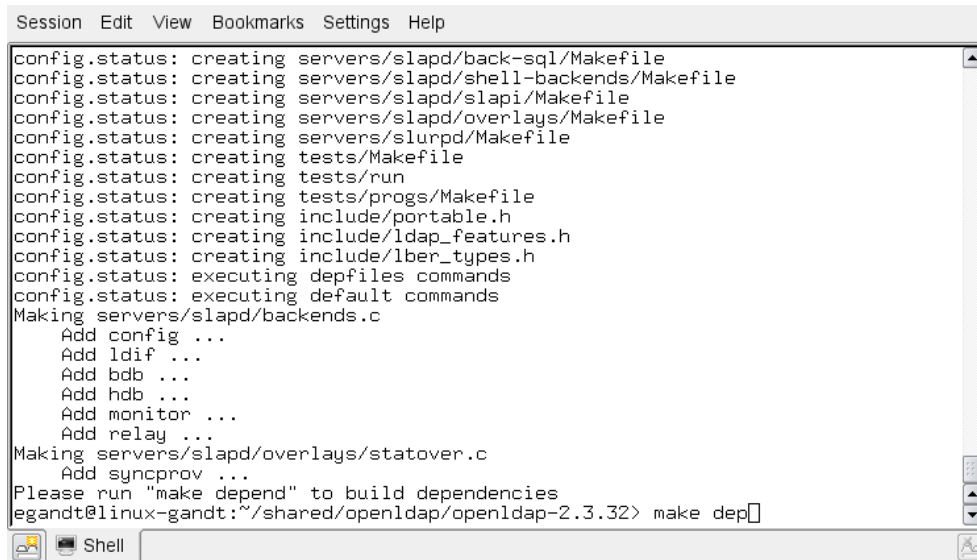
```

Session Edit View Bookmarks Settings Help
egandt@linux-gandt:~/shared/openldap> tar -xzf openldap-stable-20070110.tgz
egandt@linux-gandt:~/shared/openldap> ls
openldap-2.3.32  openldap-stable-20070110.tgz
egandt@linux-gandt:~/shared/openldap> cd openldap-2.3.32/
egandt@linux-gandt:~/shared/openldap/openldap-2.3.32> ls
aclocal.m4  CHANGES  configure.in  doc  libraries  README
ANNOUNCEMENT  clients  contrib  include  LICENSE  servers
build  configure  COPYRIGHT  INSTALL  Makefile.in  tests
egandt@linux-gandt:~/shared/openldap/openldap-2.3.32> ./configure

```

4. Configure the OpenLDAP source as follows:

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



```

Session Edit View Bookmarks Settings Help
config.status: creating servers/slapd/back-sql/Makefile
config.status: creating servers/slapd/shell-backends/Makefile
config.status: creating servers/slapd/slapi/Makefile
config.status: creating servers/slapd/overlays/Makefile
config.status: creating servers/slurpd/Makefile
config.status: creating tests/Makefile
config.status: creating tests/run
config.status: creating tests/progs/Makefile
config.status: creating include/portable.h
config.status: creating include/ldap_features.h
config.status: creating include/lber_types.h
config.status: executing depfiles commands
config.status: executing default commands
Making servers/slapd/backends.c
Add config ...
Add ldif ...
Add bdb ...
Add hdb ...
Add monitor ...
Add relay ...
Making servers/slapd/overlays/statover.c
Add syncprov ...
Please run "make depend" to build dependencies
egandt@linux-gandt:~/shared/openldap/openldap-2.3.32> make dep

```

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://<hostname_or_IP> ldap://<hostname_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 `slapd.conf` file as follows:

Note

If you installed OpenLDAP manually by following the steps in the previous section, `slapd.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 )
```

Comment the section out by placing a # character 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.

To configure OpenLDAP for Content Server

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

```
version: 1
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 130](#).

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 130](#).
- `<root_dn_password>` is the Root DN user password you specified in [step d on page 131](#).

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 130](#).

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 *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](#)

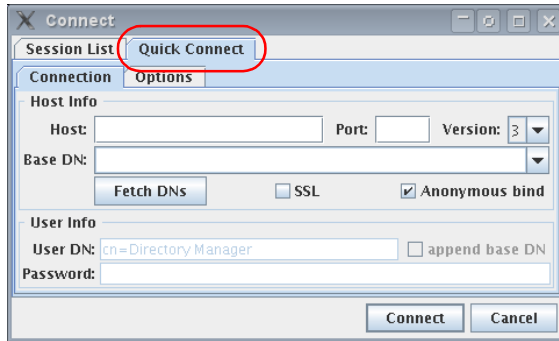
Modifying User Passwords Using an LDAP Browser

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.

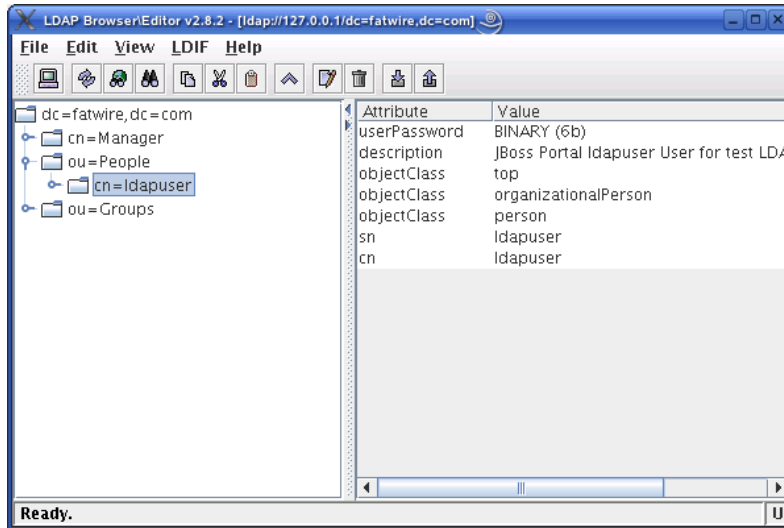


4. Fill out the fields as follows:

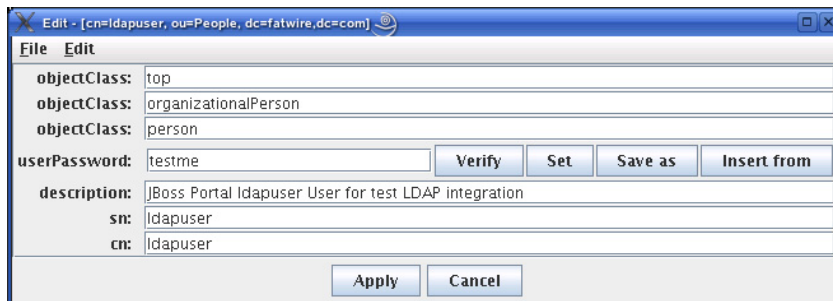
Field	Value
Hostname	The host name of your OpenLDAP server.
Port	389
Version	3
Base DN	The Base DN you specified in step a on page 130 .
Anonymous bind	Yes (select check box)
User DN	cn=Manager
Append base DN	Yes (select check box)
Password	The Root DN user password you specified in step d on page 131 .

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**.

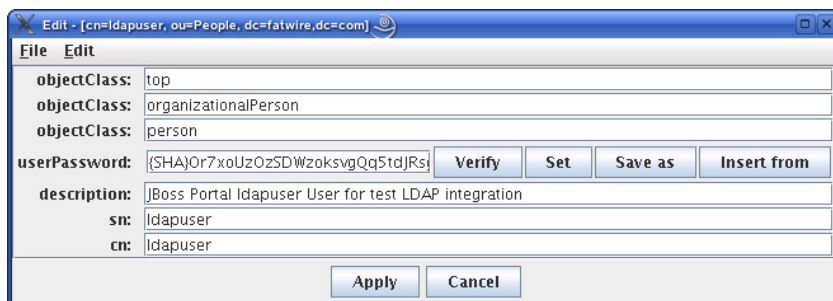


9. In the pop-up window, enter the user's password and click **Set**.



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}yDUT5RCpBAU80P0PW8gaHnsmYmL1mUL8
```

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 130](#).
- `<root_dn_password>` is the Root DN user password you specified in [step d on page 131](#).

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 130](#).
 - 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 12

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.

This chapter contains the following sections:

- [Enabling the WebLogic Embedded LDAP Server](#)
- [Modifying User Passwords](#)

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**.

The screenshot displays the WebLogic Server Administration Console interface. On the left, the 'Domain Structure' tree shows 'portalDomain' selected. The 'Change Center' pane on the far left indicates that the configuration is locked and edited. The main workspace shows the 'Settings for portalDomain' page, with the 'Security' tab and 'Embedded LDAP' sub-tab selected. The page contains several configuration fields: 'Credential' and 'Confirm Credential' (password fields), 'Backup Hour' (23), 'Backup Minute' (5), 'Backup Copies' (7), 'Cache Enabled' (checked), 'Cache Size' (32), 'Cache TTL' (60), 'Refresh Replica At Startup' (unchecked), and 'Master First' (unchecked). Each field has a corresponding description and a 'More Info...' link.

WEBLOGIC SERVER ADMINISTRATION CONSOLE

Welcome, weblogic Connected to: portalDomain Home Log Out Preferences Help AskBEA

Home > portalDomain

Settings for portalDomain

Configuration Monitoring Control Security Web Service Security Notes

General Filter Unlock User **Embedded LDAP** Roles Policies

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

This page allows you to configure the embedded LDAP server for this WebLogic Server domain.

Credential: [password field] The credential (usually a password) used to connect to the embedded LDAP server. [More Info...](#)

Confirm Credential: [password field] Enter the credential again. [More Info...](#)

Backup Hour: 23 The hour at which the embedded LDAP server should be backed up. [More Info...](#)

Backup Minute: 5 The minute at which the embedded LDAP server should be backed up. [More Info...](#)

Backup Copies: 7 The maximum number of backup copies that should be made for the embedded LDAP server. [More Info...](#)

☒ **Cache Enabled** Specifies whether a cache is used with the embedded LDAP server. [More Info...](#)

Cache Size: 32 The size of the cache (in kilobytes) that is used with the embedded LDAP server. [More Info...](#)

Cache TTL: 60 The time-to-live of the cache (in seconds) that is used with the embedded LDAP server. [More Info...](#)

☐ **Refresh Replica At Startup** Specifies whether a Managed Server should refresh all replicated data at boot time. (This is useful if you have made a large amount of changes when the Managed Server was not active, and you want to download the entire replica instead of having the Administration Server push each change to the Managed Server.) [More Info...](#)

☐ **Master First** Specifies whether a Managed Server should always connect to the master LDAP server (contained in the Administration Server), instead of connecting to the local replicated LDAP server (contained in the Managed Server). [More Info...](#)

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.

WEBLOGIC SERVER ADMINISTRATION CONSOLE

Welcome, weblogic Connected to: portalDomain Home Log Out Preferences Help AskBEA

Home > portalDomain > Summary of Security Realms > myrealm > Providers

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings Providers Migration

Authentication Authorization Adjudication Role Mapping Auditing Credential Mapping Certification Path Keystores

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

Customize this table

Authentication Providers

New Delete Reorder Showing 1 - 5 of 5 Previous | Next

<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	SQLAuthenticator	Provider that performs DBMS authentication	1.0
<input type="checkbox"/>	WSRPIdentityAsserter	WSRP 8.1 Compatibility, Identity Asserter Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
<input type="checkbox"/>	SAMLIdentityAsserter	WebLogic SAML Identity Assertion Provider. Supports Security Assertion Markup Language v1.1.	2.0
<input type="checkbox"/>	SAMLAuthenticator	WebLogic SAML Authentication Provider.	1.0

New Delete Reorder Showing 1 - 5 of 5 Previous | Next

- 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.

The screenshot shows the WebLogic Server Administration Console interface. On the left, the 'Domain Structure' tree is expanded to 'Security Realms' > 'myrealm' > 'Users and Groups'. The main workspace displays the 'Settings for myrealm' page with the 'Users and Groups' tab selected. Below the tabs, a message states: 'This page displays information about each user that has been configured in this security realm.' A link 'Customize this table' is present. Below that, a table lists users. The user 'firstsite' is highlighted with a red circle. The table has columns for Name, Description, and Provider. The 'firstsite' user has an empty description and is provided by 'LDAPProvider'.

Name	Description	Provider
Arthur		LDAPProvider
Connie		LDAPProvider
Conrad		LDAPProvider
ContentServer		LDAPProvider
DefaultReader		LDAPProvider
Desiree		LDAPProvider
firstsite		LDAPProvider
fwadmin		LDAPProvider
Mark		LDAPProvider
Martha		LDAPProvider

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

The workspace displays the “Settings for *user name*” screen:

The screenshot shows the 'Settings for firstsite' window with the 'General' tab selected. At the top, there are three tabs: 'General', 'Passwords', and 'Groups'. Below the tabs is a 'Save' button. The main content area contains the instruction: 'Use this page to change the description for the selected user.' Below this, there are two rows of information. The first row is labeled 'Name:' and shows 'firstsite' with a description: 'The login name of this user. [More Info...](#)'. The second row is labeled 'Description:' and has an empty text input field with a description: 'A short description of this user. For example, the user's full name. [More Info...](#)'. At the bottom of the form is another 'Save' button.

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

The screenshot shows the 'Settings for firstsite' window with the 'Passwords' tab selected. At the top, there are three tabs: 'General', 'Passwords', and 'Groups'. Below the tabs is a 'Save' button. The main content area contains the instruction: 'Use this page to change a user's password.' Below this, there are two rows of information. The first row is labeled 'New Password:' and has a text input field filled with asterisks, with a description: 'The new password of this user. [More Info...](#)'. The second row is labeled 'Confirm New Password:' and has a text input field filled with asterisks, with a description: 'The confirmed new password of this user. [More Info...](#)'. At the bottom of the form is another 'Save' button.

6. Click **Save**.

A confirmation message appears.

The screenshot shows a 'Messages' section with a green checkmark icon and the text: 'Settings updated successfully.'

