Oracle® Fusion Middleware

Upgrade Guide for Oracle Identity Management

11*g* Release 1 (11.1.1)

E10129-02

October 2009

ORACLE®

Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management, 11*g* Release 1 (11.1.1)

E10129-02

Primary Author: Peter LaQuerre

Contributors: Pradeep Bhat, Paul Dickson, Robert Donat, Stuart Duggan, Pramodini Gattu, Pratima Gogineni , Atika Jain , Ajay Keni , Ari Kermaier , Stephen Lee , Sophia Maler, William Norcott, Bharath Reddy, Michael Rubino, Reza Shafii, Olaf Stullich, Sitaraman Swaminathan, Mark Wilcox

Contents

4 Upgrading Your Oracle Internet Directory Environment

5 Upgrading Your Oracle Virtual Directory Environment

6 Upgrading Your Oracle Identity Federation Environment

Part III   Upgrading Oracle Identity Management High Availability Environments

7   Upgrading Oracle Internet Directory High Availability Environments

8   Upgrading an Oracle Identity Management Cold Failover Cluster Environment

11 Upgrading an Oracle Identity Federation High Availability Environment

Index

x

Preface

This preface contains the following sections:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

Audience

This manual is intended for Oracle Fusion Middleware system administrators who are responsible for installing and upgrading Oracle Fusion Middleware instances. It is assumed that the readers of this manual have knowledge of the following:

- Oracle Application Server 10*g* system administration and configuration
- The configuration and expected behavior of the system being upgraded

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at `http://www.fcc.gov/cgb/consumerfacts/trs.html`, and a list of phone numbers is available at `http://www.fcc.gov/cgb/dro/trsphonebk.html`.

Related Documents

For more information, see the following documents in the Oracle Other Product One Release 7.0 documentation set or in the Oracle Other Product Two Release 6.1 documentation set:

- *Oracle Fusion Middleware Upgrade Planning Guide*

- *Oracle Fusion Middleware Installation Planning Guide*

- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*

- *Oracle Fusion Middleware Administrator's Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Summary of the Oracle Identity Management Upgrade Process

This chapter provides a high-level overview of the Oracle SOA Suite, WebCenter, and ADF upgrade process. Refer to the following sections for more information:

- Flow Chart of the Oracle Identity Management Upgrade Process
- Table Describing the Steps in the Oracle Application Server Upgrade Process

1.1 Flow Chart of the Oracle Identity Management Upgrade Process

Figure 1–1 provides a flow chart of the Oracle Identity Management upgrade process. Review this chart to get familiar with the steps you will be required to take, based on your existing version of Oracle Identity Management.

Figure 1–1   Flow Chart of the Oracle Identity Management Upgrade Process
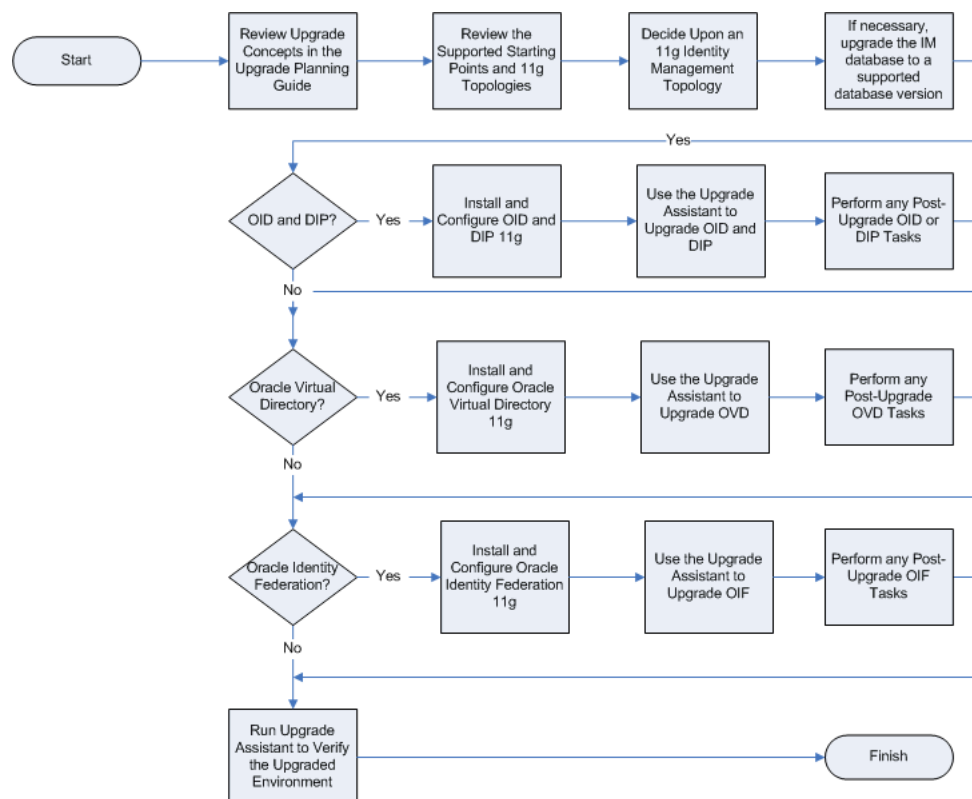
1.2 Table Describing the Steps in the Oracle Application Server Upgrade Process

Table 1–1 describes each of the steps in the upgrade process flow chart, which is shown in Figure 1–1. The table also provides information on where to get more information on each step in the process.

Table 1–1   Table Describing the Steps in the Oracle Application Server Upgrade Process

Step	Description	More Information
Review Upgrade Concepts in the Upgrade Planning Guide	The *Oracle Fusion Middleware Upgrade Planning Guide* provides a high-level overview of how to upgrade your entire Oracle Application Server environment to Oracle Fusion Middleware. It includes compatibility information and instructions for upgrading any databases that support your middleware components.	*Oracle Fusion Middleware Upgrade Planning Guide*
Review the Supported Starting Points and 11g Topologies	Before starting your upgrade, you should be familiar with the new features, supported started points, and recommended topologies for Oracle Fusion Middleware 11g. Based this knowledge, you can later decide upon an 11g topology.	Chapter 2, "Supported Starting Points for Oracle Identity Management Upgrade" Chapter 3, "Types of Oracle Identity Management Environments"
Decide Upon an 11g Identity Management Topology	Oracle Fusion Middleware 11g introduces a new architecture, based on Oracle WebLogic Server. As a result, you should review your current Oracle Application Server topology and decide upon an equivalent Oracle Fusion Middleware topology before you begin the upgrade process.	Chapter 3, "Types of Oracle Identity Management Environments"
If necessary, upgrade the IM database to a supported database version	When you upgrade to Oracle Fusion Middleware 11*g*, the OracleAS Identity Management schemas are upgraded to 11*g*. As a result, before you upgrade, you must be sure the database that hosts the schemas is a supported verison.	*Oracle Fusion Middleware Upgrade Planning Guide*
OID and DIP?	If you are upgrading Oracle Internet Directory or the Oracle Directory Integration Platform, then be sure to follow the appropriate instructions in this guide.	Chapter 4, "Upgrading Your Oracle Internet Directory Environment"

Table 1–1   (Cont.) Table Describing the Steps in the Oracle Application Server Upgrade Process

Step	Description	More Information
Install and Configure OID and DIP 11g	Install and configure an instance of Oracle Internet Directory 11*g* and Oracle Directory Integration Platform 11*g* on the same host as the Oracle Application Server 10*g* installation. Note that in preparation for upgrade, Oracle Universal Installer provides some specific installation screens when it detects that your database contains the 10*g* version of your OracleAS Identity Management schemas.	Section 4.3, "Task 3: Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11g Components"
Use the Upgrade Assistant to Upgrade OID and DIP	Run the Upgrade Assistant from your new 11*g* Oracle home and upgrade the Oracle Internet Directory schemas and middle tiers.	Section 4.4, "Task 4: Use the Upgrade Assistant to Upgrade Oracle Internet Directory"
Perform any Post-Upgrade OID or DIP Tasks	The Upgrade Assistant automates many of the upgrade procedures, but in many cases, there are additional, manual tasks that you might have to perform in some cases.	Section 4.5, "Task 5: Perform Any Required Oracle Internet Directory and Oracle Directory Integration Platform Post-Upgrade Tasks"
Oracle Virtual Directory?	If you are upgrading Oracle Internet Directory or the Oracle Directory Integration Platform, then be sure to follow the appropriate instructions in this guide.	Chapter 5, "Upgrading Your Oracle Virtual Directory Environment"
Install and Configure OVD 11*g*	Install and configure an instance of Oracle Virtual Directory 11*g* on the same host as the Oracle Application Server 10*g* installation. Note that in preparation for upgrade, Oracle Universal Installer provides some specific installation screens when it detects that your database contains the 10*g* version of your OracleAS Identity Management schemas.	Section 5.2, "Task 2: Install and Configure Oracle Virtual Directory 11g"
Use the Upgrade Assistant to Upgrade OVD	Run the Upgrade Assistant from your new 11*g* Oracle home and upgrade the Oracle Virtual Directory schema and middle tier.	Section 5.3, "Task 3: Use the Upgrade Assistant to Upgrade Oracle Virtual Directory"
Perform any Post-Upgrade OVD Tasks	The Upgrade Assistant automates many of the upgrade procedures, but in many cases, there are additional, manual tasks that you might have to perform in some cases.	Section 5.4, "Task 4: Perform Any Required Oracle Virtual Directory Post-Upgrade Tasks"
Oracle Identity Federation?	If you are upgrading Oracle Identity Federation, then be sure to follow the appropriate instructions in this guide.	Chapter 6, "Upgrading Your Oracle Identity Federation Environment"

Table 1–1 (Cont.) Table Describing the Steps in the Oracle Application Server Upgrade Process

Step	Description	More Information
Install and Configure OIF 11g	Install and configure an instance of Oracle Identity Federation 11*g* on the same host as the Oracle Application Server 10*g* installation. Note that in preparation for upgrade, Oracle Universal Installer provides some specific installation screens when it detects that your database contains the 10*g* version of your OracleAS Identity Management schemas.	Section 6.3, "Task 3: Install and Configure Oracle Identity Federation 11g"
Use the Upgrade Assistant to Upgrade OIF	Run the Upgrade Assistant from your new 11*g* Oracle home and upgrade the Oracle Identity Federation schemas and middle tiers.	Section 6.4, "Task 4: Use the Upgrade Assistant to Upgrade Oracle Identity Federation"
Perform any Post-Upgrade OIF Tasks	The Upgrade Assistant automates many of the upgrade procedures, but in many cases, there are additional, manual tasks that you might have to perform in some cases.	Section 6.5, "Task 5: Perform Any Required Oracle Identity Federation Post-Upgrade Tasks"
Run Upgrade Assistant to Verify the Upgraded Environment	You can use the Upgrade Assistant, as well other techniques to validate the upgrade and verify that the upgraded environment is up and running successfully.	Section 4.6, "Task 6: Verify that the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade Was Successful" Section 5.5, "Task 5: Verify that the Oracle Virtual Directory Upgrade Was Successful" Section 6.6, "Task 6: Verify that the Oracle Identity Federation Upgrade Was Successful"

Part I

Preparing for an Oracle Identity Management Upgrade

Part I contains the following chapters:

2

Supported Starting Points for Oracle Identity Management Upgrade

This chapter describes the supported starting points for Oracle Identity Management upgrade. This chapter contains the following sections:

- Supported Starting Points for Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

- Supported Starting Points for Oracle Virtual Directory Upgrade

- Supported Starting Points for Oracle Identity Federation Upgrade

> **Note:** The starting point patchsets listed in in this chapter were the latest patchsets available at the time this guide was published.
>
> For a list of the latest patchsets available for your installation, refer to Oracle*MetaLink*:
>
> `http://metalink.oracle.com/`

2.1 Supported Starting Points for Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

This guide provides instructions for upgrading from Oracle Internet Directory and Oracle Directory Integration Platform this is installed as part of the Oracle Application Server 10*g* releases and installation types described in Table 2–1.

> **Note:** Note that there is no upgrade path supported for Oracle Single Sign-On or Oracle Delegated Administration Services 10*g*.
>
> For more information, see Section 4.1, "Task 1: Understand Your Upgrade Options for SSO and Oracle Delegated Administration Services".

Table 2–1   Oracle Internet Directory and Oracle Directory Integration Platform Releases Supported By This Guide

Release	Installation Type	Description or Notes	Latest Patchset
10*g* Release 2 (10.1.2)	Oracle Identity Management and OracleAS Metadata Repository	This installation type includes the Identity Management software, as well as a database populated with the required Oracle Application Server Identity Management schemas.	10*g* Release 2 (10.1.2.3.0)
10*g* Release 2 (10.1.2)	Oracle Identity Management	This installation type installed only the Oracle Internet Directory software. It assumed you installed the required Identity Management schemas in an existing database by using the Repository Creation Utility (repca).	10*g* Release 2 (10.1.2.3.0)
10*g* (10.1.4.0.1)	Oracle Identity Management and OracleAS Metadata Repository	This installation type includes the Identity Management software, as well as a database populated with the required Oracle Application Server Identity Management schemas.	10*g* (10.1.4.3)
10*g* (10.1.4.0.1)	Oracle Identity Management	This installation type installed only the Oracle Internet Directory software. It assumed you installed the required Identity Management schemas in an existing database by using the Repository Creation Utility (repca).	10*g* (10.1.4.3)

2.2 Supported Starting Points for Oracle Virtual Directory Upgrade

This guide provides instructions for upgrading from the Oracle Virtual Directory releases described in Table 2–2.

Table 2–2   Oracle Virtual Directory Releases Supported By This Guide

Release	Description or Notes	Latest Patchset
10*g* (10.1.4.0.1)	This version of Oracle Identity Federation was available as part of Oracle Application Server 10*g* (10.1.4.0.1). It was installed using a separate isntallation procedure and installation guide.	10*g* (10.1.4.3)

2.3 Supported Starting Points for Oracle Identity Federation Upgrade

This guide provides instructions for upgrading from the Oracle Identity Federation releases described in Table 2–3.

Table 2–3   Oracle Identity Federation Releases Supported By This Guide

Release	Description or Notes	Latest Patchset
10*g* (10.1.4.0.1)	This version of Oracle Identity Federation was available as part of Oracle Application Server 10*g* (10.1.4.0.1).	10*g* (10.1.4.3)

3

Types of Oracle Identity Management Environments

This chapter describes the most common topologies for Oracle Identity Management 10*g* and how they compare with equivalent topologies in Oracle Fusion Middleware 11*g*.

This chapter contains the following sections:

- Oracle Internet Directory and Oracle Directory Integration Platform Topology
- Oracle Virtual Directory Topologies
- Oracle Identity Federation Topologies

3.1 Summary of the Oracle Identity Management 10*g* and 11*g* Components

The following sections describe the Oracle Identity Management components that were included in the Oracle Application Server 10*g* Release 2 (10.1.2) and Oracle Identity Management 10*g* (10.1.4.0.1) releases:

- Identity Management Components Available in Oracle Application Server 10g Release 2 (10.1.2)
- Identity Management Components Available in Oracle Identity Management 10g (10.1.4.0.1)
- Identity Management Components Available in Oracle Fusion Middleware 11g

3.1.1 Identity Management Components Available in Oracle Application Server 10*g* Release 2 (10.1.2)

In Oracle Application Server 10*g* Release 2 (10.1.2), the Oracle Identity Management components consists of the following:

- Oracle Internet Directory
- Oracle Directory Integration Platform
- Oracle Single Sign-On
- Oracle Delegated Administration Services

When you install and configure these 10*g* Release 2 (10.1.2) components, you can install them all into the same Oracle home (a colocated environment), or you can distribute them in separate Oracle homes (a distributed environment).

For the distributed environment, users typically intall the Oracle Internet Directory and Oracle Directory Integration Platform components into one Oracle home and the Oracle Single Sign-On and Oracle Delegated Administration Services componetns into a second Oracle home.

3.1.2 Identity Management Components Available in Oracle Identity Management 10*g* (10.1.4.0.1)

Oracle Identity Management 10*g* (10.1.4.0.1) provided the following Oracle Identity Management components:

- Oracle Internet Directory

- Oracle Directory Integration Platform

- Oracle Single Sign-On

- Oracle Delegated Administration Services

- Oracle Virtual Directory

- Oracle Identity Federation

- Oracle Access Manager

As shown in the previous list, Oracle Identity Management 10*g* (10.1.4.0.1) introduced the Oracle Virtual Directory and Oracle Identity Federation components.

In a typical environment, Oracle Virtual Directory and Oracle Identity Federation are separately from the colocated or distributed installations of the other Oracle Identity Management components.

3.1.3 Identity Management Components Available in Oracle Fusion Middleware 11*g*

Oracle Fusion Middleware 11*g* provides new versions of the following Oracle Identity Management 10*g* components:

- Oracle Internet Directory

- Oracle Directory Integration Platform

- Oracle Virtual Directory

- Oracle Identity Federation

Note that Oracle Fusion Middleware 11*g* does not include Oracle Single Sign-On or Oracle Delegated Administration Services. It also does not include Oracle Access Manager.

For more information about the Oracle Identity Management components available with 11*g*, refer to the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*.

3.2 Oracle Internet Directory and Oracle Directory Integration Platform Topology

Oracle Identity Management 10*g* Release 2 (10.1.2) and 10*g* (10.1.4.0.1) supported two main types of Oracle Identity Management environments. The following sections describe these environments and compare them with an equivalent environment in Oracle Fusion Middleware 11*g*:

- Upgrading a Colocated Identity Management Environment

■   Upgrading a Non-Colocated Identity Management Environment

3.2.1 Upgrading a Colocated Identity Management Environment

Figure 3–1 compares a typical colocated Oracle Identity Management environment in 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) with a similar topology in Oracle Fusion Middleware 11*g*.

Figure 3–1   Upgrading an Oracle Identity Management 10g Colocated Installation to Oracle Fusion Middleware 11g
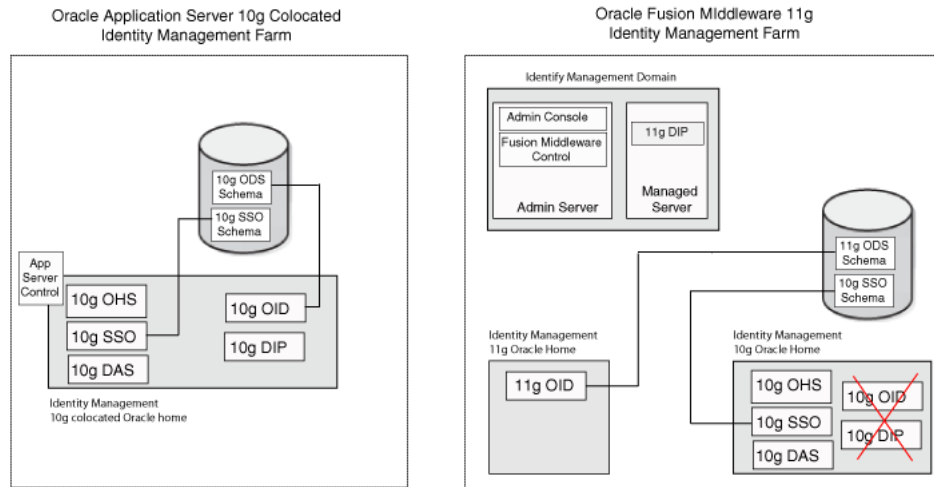
3.2.2 Upgrading a Non-Colocated Identity Management Environment

Figure 3–2 compares a typical non-colocated Oracle Identity Management environment in Oracle Application Server 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) with a similar topology in 11*g*.

Figure 3–2   Upgrading an Oracle Identity Management 10g Non-Colocated Installation to Oracle Fusion Middleware 11g
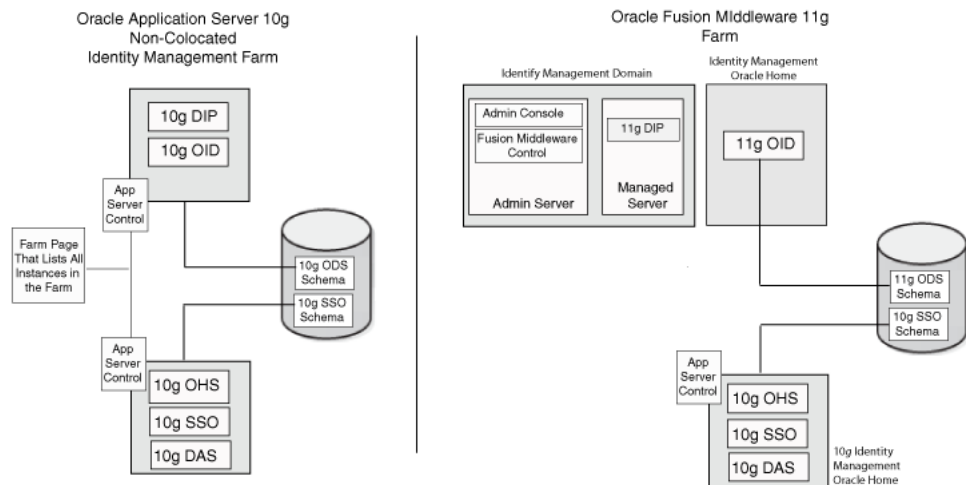
3.3 Oracle Virtual Directory Topologies

Oracle Virtual Directory 10*g* could be installed and configured with Oracle Internet Directory 10*g* or without Oracle Internet Directory 10*g*.

Figure 3–3 compares the Oracle Virtual Directory 10*g* and Oracle Virtual Directory 11*g* topologies when you are not using Oracle Internet Directory.

Figure 3–3   Upgrading Oracle Virtual Directory
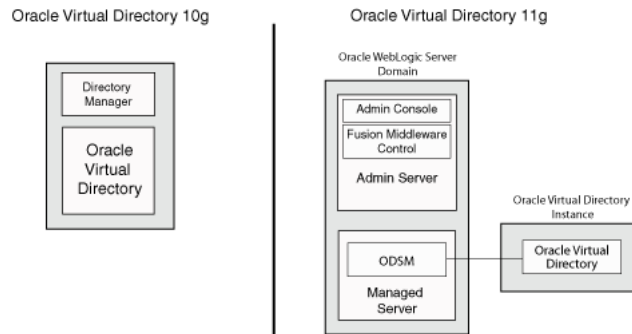
3.4 Oracle Identity Federation Topologies

Figure 3–4 compares a typical Oracle Identity Federation topology in Oracle Application Server 10*g* (10.1.4.0.1) with a similar topology in Oracle Fusion Middleware 11*g*.

Figure 3–4   Comparison of Typical Oracle Identity Federation Topologies in Oracle Application Server 10g (10.1.4.0.1) and Oracle Fusion Middleware 11g
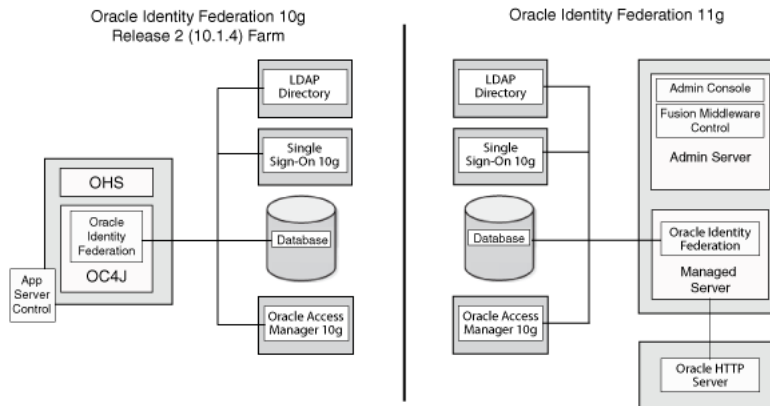
Part II

Upgrading Your Oracle Identity Management Environment

Part II contains the following chapters:

4

Upgrading Your Oracle Internet Directory Environment

This chapter describes how to upgrade your existing 10*g* Release 2 (10.1.2) or 10*g* (10.1.4) Oracle Identity Management to Oracle Identity Management Release 11.

This chapter contains the following sections:

- Task 1: Understand Your Upgrade Options for SSO and Oracle Delegated Administration Services

- Task 2: If Necessary, Upgrade the Database That Contains the 10g Identity Management Schemas

- Task 3: Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11g Components

- Task 4: Use the Upgrade Assistant to Upgrade Oracle Internet Directory

- Task 5: Perform Any Required Oracle Internet Directory and Oracle Directory Integration Platform Post-Upgrade Tasks

- Task 6: Verify that the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade Was Successful

4.1 Task 1: Understand Your Upgrade Options for SSO and Oracle Delegated Administration Services

If you are using Oracle Single Sign-On or Oracle Delegated Administration Services, then you should be aware that there is no upgrade path to Oracle Fusion Middleware 11*g* for these components.

Instead, if you are using Oracle Single Sign-On with Oracle Portal, Forms, Reports, and Discoverer, then you should maintain your existing 10*g* Release 2 (10.1.2) or 10*g* (10.1.4) Oracle Single Sign-On instance.

For more information, see Section 3.1, "Summary of the Oracle Identity Management 10g and 11g Components".

Oracle Fusion Middleware offers a new version of Oracle Internet Directory and the Oracle Directory Integration Platform. Oracle recommends that you upgrade your Oracle Internet Directory and Oracle Directory Integration Platform instances to Oracle Fusion Middleware 11*g*.

4.2 Task 2: If Necessary, Upgrade the Database That Contains the 10*g* Identity Management Schemas

When you upgrade your Oracle Identity Management components, the Oracle Identity Management schemas in the metadata repository are upgraded "in-place." This means that you do not install the Oracle Fusion Middleware 11*g* schemas; instead, you upgrade the existing 10*g* schemas to 11*g*, using the Upgrade Assistant.

However, you must ensure that the version of the database that will contain the upgraded Oracle Identity Management schemas is supported by Oracle Fusion Middleware 11*g*.

For instructions on verifying that your database meets the requirements of Oracle Fusion Middleware 11*g*, as well as instructions for upgrading the database, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*

4.3 Task 3: Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11*g* Components

The following sections describe how to install and configure your new Oracle Fusion Middleware 11*g* environment in preparation for upgrading from Oracle Application Server 10*g*:

- Understanding the Implications of Installing Oracle Internet Directory 11g Against the Oracle Internet Directory 10g Schema

- Installing the Oracle WebLogic Server Software and Creating the Middleware Home

- Installing and Configuring Oracle Internet Directory and Oracle Directory Integration Platform 11g in Preparation for Upgrade

---

Note: If you are upgrading your Oracle Application Server 10*g* Oracle Internet Directory and Oracle Directory Integration Platform components to 11*g*, then you must install the new 11*g* software on the same host as the Oracle Application Server 10*g* components.

4.3.1 Understanding the Implications of Installing Oracle Internet Directory 11*g* Against the Oracle Internet Directory 10*g* Schema

To upgrade Oracle Internet Directory to 11*g*, you must install the new Oracle Internet Directory 11*g* instance against the existing Oracle Internet Directory 10*g* (ODS) schema. Then, you can you run the Upgrade Assistant to upgrade the Oracle Internet Directory 10*g* schema to 11*g*.

Note, however, that until you upgrade the Oracle Internet Directory 10*g* schema to 11*g*, the Oracle Internet Directory instance will be in read-only mode. As a result, be sure you have planned for enough time to not only install the new Oracle Internet Directory instance, but to upgrade the ODS schema, as described in "Task 4: Use the Upgrade Assistant to Upgrade Oracle Internet Directory".

4.3.2 Installing the Oracle WebLogic Server Software and Creating the Middleware Home

The following sections provide information about installing Oracle WebLogic Server and creating the Middleware home in preparation for an Oracle Identity Management upgrade:

- When is Oracle WebLogic Server Required?

- Installing the Oracle WebLogic Server Software and Create the Middleware Home

4.3.2.1 When is Oracle WebLogic Server Required?

Before you install Oracle Internet Directory and Oracle Directory Integration Platform 11*g*, note the following:

- Oracle Directory Integration Platform 11*g* requires an existing Oracle WebLogic Server domain.

- Oracle Internet Directory does not require a domain. However, if you install Oracle Internet Directory without specifying a domain, then you will not be able to manage the Oracle Internet Directory instance with Fusion Middleware Control or Oracle Directory Services Manager.

  Note that you can later use an OPMN command to register the standalone Oracle Internet Directory instance with a domain where Oracle Directory Services Manager is configured. For more information, see "Registering an Oracle Instance or Component with the WebLogic Server" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

When you install the Oracle WebLogic Server software on disk, you create a directory called the Middleware home, which contains the Oracle WebLogic Server software files. Later, you also install an Oracle Identity Management Oracle home inside the Middleware home.

4.3.2.2 Installing the Oracle WebLogic Server Software and Create the Middleware Home

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

4.3.3 Installing and Configuring Oracle Internet Directory and Oracle Directory Integration Platform 11*g* in Preparation for Upgrade

The following sections provide information about installing Oracle Internet Directory and Oracle Directory Integration Platform in preparation for upgrade:

- Before You Begin Installing Oracle Internet Directory and Oracle Directory Integration Platform

- Procedure for Installing Oracle Internet Directory and Oracle Directory Integration Platform Before Upgrade

4.3.3.1 Before You Begin Installing Oracle Internet Directory and Oracle Directory Integration Platform

Before you begin installing and configuring Oracle Internet Directory and Oracle Directory Integration Platform in preparation for an upgrade, consider the following:

- When you install Oracle Internet Directory and Oracle Directory Integration Platform in preparation for upgrade, the installation is similar to any other 11*g* installation, except that in this case, you install the Oracle Internet Directory 11*g* instance against the existing Oracle Internet Directory 10*g* (ODS) schema.

  Immediately after the installation, you then use the Oracle Fusion Middleware Upgrade Assistant to upgrade the ODS schema to 11*g*. During the time between the installation and running the Upgrade Assistant, the Oracle Internet Directory instance is in read-only mode. As a result, it is not fully operational until after you run the Upgrade Assistant.

- When you make your selections while installing Oracle Internet Directory and Oracle Directory Integration Platform, you should configure the new 11*g* environment so it matches the topology you configured for Oracle Application Server 10*g*.

  For example, if you were running both Oracle Internet Directory and Oracle Directory Integration Platform out of the same 10*g* Oracle home, you should install and configure both components in the same Oracle Fusion Middleware 11*g* Oracle home.

- If you recently upgraded the database that contains your Oracle Identity Management schemas, be sure check for invalid objects in the databae before proceeding with the upgrade.

  For more information, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

4.3.3.2 Procedure for Installing Oracle Internet Directory and Oracle Directory Integration Platform Before Upgrade

To install and configure Oracle Internet Directory and Oracle Directory Integration Platform, in preparation for upgrade:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network (OTN):

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Use the instructions in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* to start the Oracle Identity Management installation and configuration tool.

4. Follow the instructions in the installer to install and configure the Oracle Internet Directory and Oracle Directory Integration Platform components.

Refer to Table 4–1 for information about the configuration screens that are specific to the upgrade of Oracle Internet Directory and Oracle Directory Integration Platform.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

Note: At the end of the installation (when you are preparing for an Oracle Identity Management upgrade), the port values shown on the Installation Summary screen might not reflect the actual port values used by the new Oracle Internet Directory 11*g* instance.

To verify the port numbers in use by Oracle Internet Directory 11*g*, use the `opmnctl status` command, as described in the *Oracle Fusion Middleware Oracle Process Manager and Notification Server Administrator's Guide*.

Table 4–1   Installation Screens Specific to Oracle Internet Directory and Oracle Directory Integration Platform

Installer Screen	Description
Specify Schema Database	In an upgrade scenario, use this screen (Figure 4–1) to select the database that contains the 10*g* ODS schema, as follows:
	1. Select **Use Existing Schema**.
	2. In the **Connect String** field, enter the connection information for the database where the 10*g* ODS schema is installed.
	3. In the **Password** field, enter the password for the ODS schema.
	The ODS schema is used by Oracle Internet Directory. By default, the password for the ODS schema is the `ias_admin` password you provided when you installed Oracle Internet Directory 10g. However, the password might have been changed using the `oidpasswd` utility, which is documented in the *Oracle Identity Management 10g User Reference*.
Warning Dialog Box	The Upgrade Scenario Detected warning dialog box (Figure 4–2) indicates that you are installing Oracle Internet Directory as part of an upgrade scenario. The installer displays this dialog box when it recognizes that the database contains an Oracle Internet Directory (ODS) 10g schema.
	Click **Yes** to continue installing Oracle Identity Management in preparation for an upgrade to Oracle Identity Management 11*g*.
	Note that from this point on, the Oracle Internet Directory instance is in read-only mode until you run the Upgrade Assistant and upgrade the Oracle Internet Directory schema (ODS) to 11*g*.

Figure 4–1   Specify Schema Database Screen in the Oracle Identity Management Installer
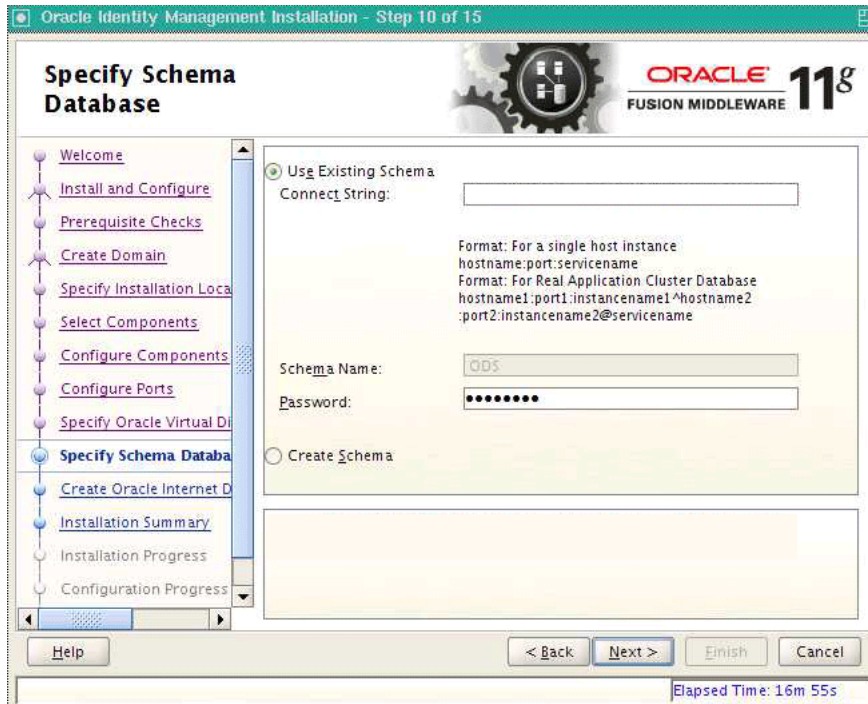
Figure 4–2   Upgrade Scenario Detected Dialog Box During an Oracle Identity Management Installation
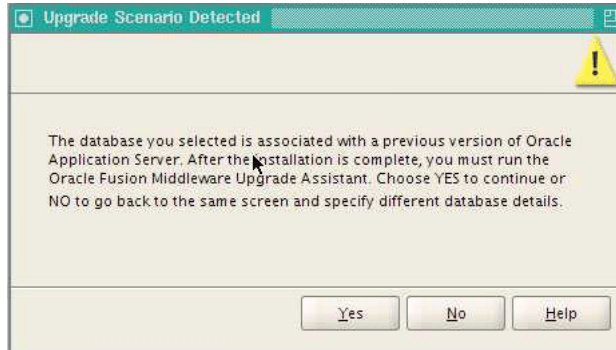
4.4 Task 4: Use the Upgrade Assistant to Upgrade Oracle Internet Directory

After you install Oracle Internet Directory and Oracle Directory Integration Platform and point the installation to the existing Oracle Identity Management 10*g* schemas, you can then run the Oracle Fusion Middleware Upgrade Assistant.

The Upgrade Assistant automates the upgrade of the Oracle Internet Directory schema and your Oracle Identity Management 10*g* middle tier.

The Upgrade Assistant is installed automatically into the `bin` directory of your Oracle Fusion Middleware Oracle home.

The following sections provide more information:

■   Task 4a: Perform Required Pre-Upgrade Tasks

- Task 4b: Start the Upgrade Assistant for an Oracle Identity Management Upgrade
- Task 4c: Upgrade the Oracle Internet Directory and Oracle Directory Integration Platform Instance

4.4.1 Task 4a: Perform Required Pre-Upgrade Tasks

Before you start the Upgrade Assistant, perform the following pre-Upgrade tasks that apply to your installation:

- Verifying the Status of the Oracle Identity Management 10g Schemas
- Modifying the SSL Port Configuration When Using SSL Authentication Mode on the Windows Operating System

4.4.1.1 Verifying the Status of the Oracle Identity Management 10*g* Schemas

Before you start the Upgrade Assistant to upgrade your Oracle Identity Management components to Oracle Identity Management 11*g*, verify that the existing Oracle Identity Management 10*g* schemas in the database are valid:

> **Note:** This procedure is especially important to perform after you apply the 10*g* Release 2 (10.1.2.3) patch set to your 10*g* Release 2 (10.1.2) environment and before you upgrade our 10*g* Release 2 (10.1.2.3) components to 11*g*.

1. Connect to the database that contains the Oracle Identity Management 10*g* component schemas using SQLPlus.

2. Use the following SQL SELECT statement to view the status of the schemas:

   ```
   SQL> SELECT comp_id,version,status FROM app_registry;
   ```

3. Verify that the status of the schemas is set to VALID.

   If the output from the SELECT command identifies the OID schema as INVALID, perform the following steps to fix the issue:

   a. Use a text editor to open the following file in the Oracle Internet Directory 10*g* Oradle home:

      ```
      ORACLE_HOME/ldap/admin/oidi10121.sql
      ```

   b. Insert the following at the top of the `oidi10121.sql` file so that it is run as the ODS schema user:

      ```
      alter session set current_schema = ODS;
      ```

   c. Run `patchcfg.sql` as the SYS user.

      For example:

      ```
      cd ORACLE_HOME/ldap/admin/oidi10121.sql
      sqlplus "connect / as sysdba"
      SQL> @patchcfg.sql
      ```

   d. Identify the objects in the database that are owned by SYS and are also owned by ODS.

      The list of objects you should drop from the database are shown in Example 4–1.

    e. For each of the objects in Example 4–1, enter a DROP PACKAGE statement.

    For example:

```
drop package OIDMETRICINFO;
```

Example 4–1   Invalid Objects to Drop from the Oracle Identity Management Schema Database

```
select owner, object_name, object_type from dba_objects
      where status = 'INVALID' order by owner, object_name;

OWNER       OBJECT_NAME        OBJECT_TYPE
----------  ------------------ ------------
SYS         LDAPBLKMOD         PACKAGE BODY
SYS         LDAPUPGUTLS        PACKAGE BODY
SYS         MODIFYDN           PACKAGE
SYS         MODIFYDN           PACKAGE BODY
SYS         ODIGETDIPINFO      PACKAGE BODY
SYS         OIDCONFIGINFO      PACKAGE BODY
SYS         OIDMETRICINFO      PACKAGE BODY
SYS         OIDPORTINFO        PACKAGE BODY
SYS         OIDREPLSTATUSINFO  PACKAGE BODY
SYS         OIDSTATUSINFO      PACKAGE BODY
SYS         OID_STATS          PACKAGE
SYS         OID_STATS          PACKAGE BODY
SYS         OLADD              PACKAGE BODY
SYS         PURGEADMIN         PACKAGE BODY
SYS         TSPURGE            PACKAGE BODY
```

4.4.1.2 Modifying the SSL Port Configuration When Using SSL Authentication Mode on the Windows Operating System

If you are running Oracle Identity Management components on the Windows operating system, and you have configured Authentication Mode for the SSL port for Oracle Internet Directory 10*g*, then you must change this configuration to SSL No Authentication Mode prior to the upgrade to 11*g*.

Simarly, if Oracle Directory Integration Platform 10*g* is connected to the Oracle Internet Directory SSL port using SSL Server Authentication Mode, then you must also reconfigure Oracle Directory Integration Platform to connect to Oracle Internet Directory using SSL No Authentication Mode mode prior to the upgrade to 11*g*.

For more information, see *Oracle Internet Directory Administrator's Guide* and *Oracle Identity Management Integration Guide* in the 10*g* (10.1.4.0.1) documentation library.

After the upgrade, reconfigure both Oracle Internet Directory and Oracle Directory Integration Platform for SSL Server Authentication Mode mode using wallets.

For more information, see the following:

■ "Configuring Secure Sockets Layer (SSL)" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

■ "Managing the Oracle Directory Integration Platform" in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*

These changes are not required on Linux or UNIX-based operating systems.

4.4.2 Task 4b: Start the Upgrade Assistant for an Oracle Identity Management Upgrade

To start the Upgrade Assistant using the graphical user interface:

> **Note:** You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

1. Change directory the `ORACLE_HOME`/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

    On UNIX system:

    `./ua`

    On Windows systems:

    `ua.bat`

    The Upgrade Assistant displays the Welcome screen as shown in Figure 4–3

Figure 4–3   Upgrade Assistant Welcome Screen
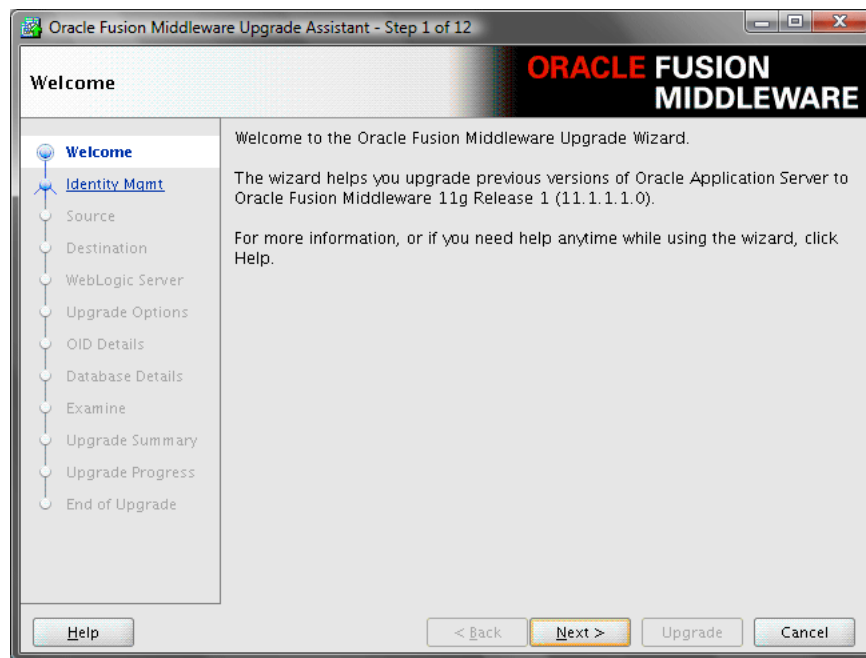
3. Click **Next** to display the Select Operation screen (Figure 4–3).

    The options available in the Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Identity Management Oracle home, the options shown on the Select Operation screen are the valid options for an Oracle Identity Management Oracle home.

Figure 4–4   Upgrade Assistant Select Operation Screen for an Oracle Identity Management Upgrade
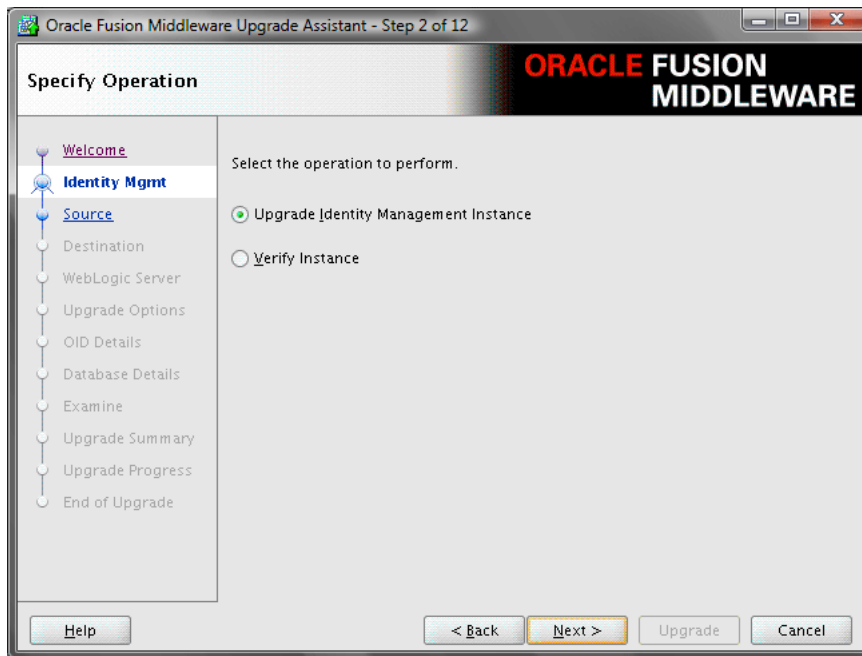
4.4.3 Task 4c: Upgrade the Oracle Internet Directory and Oracle Directory Integration Platform Instance

When you upgrade Oracle Internet Directory and Oracle Directory Integration Platform, the Upgrade Assistant upgrades the Oracle Identity Management schemas in the Metadata Repository and the configuration files in the Oracle Internet Directory and Oracle Directory Integration Platform middle tier.

Refer to the following sections for more information:

- Using the Upgrade Assistant to Upgrade Oracle Internet Directory and Oracle Directory Integration Platform

- About Specifying Real Application Clusters (RAC) Database Details on the Specify Database Details Screen

- Recovering From an Oracle Internet Directory Error During the Upgrade Assistant Examine Phase

4.4.3.1 Using the Upgrade Assistant to Upgrade Oracle Internet Directory and Oracle Directory Integration Platform

> **Note:** This example assumes you have installed Oracle Internet Directory and Oracle Directory Integration Platform in the same Oracle Fusion Middleware 11*g* Oracle instance. You can also install Oracle Internet Directory and Oracle Directory Integration Platform in separate Oracle instances.
>
> For more information, see Section 3.2, "Oracle Internet Directory and Oracle Directory Integration Platform Topology".

To upgrade Oracle Internet Directory and Oracle Directory Integration Platform when they reside in the same Oracle instance:

1. Backup the database that contains the Oracle Identity Management schemas.

   For more information, see "Backup Strategies Before Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

2. Make sure that both the Oracle Internet Directory 10*g* instance and the new 11*g* instance are up and running before you start the Upgrade Assistant.

3. Start the Upgrade Assistant as described in Task 4b: Start the Upgrade Assistant for an Oracle Identity Management Upgrade.

4. Select **Upgrade Identity Management Instance** on the Select Operation screen (Figure 4–4).

5. Refer to Table 4–2 for a description of the Upgrade Assistant screens that require input from you during an Oracle Internet Directory and Oracle Directory Integration Platform upgrade.

6. After the Target Database Details screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

     See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

   - Displays the End of Upgrade screen, which confirms that the upgrade was complete.

   - Sets the ODSSM schema password to match the existing ODS schema password.

7. Exit the Upgrade Assistant.

Table 4–2 Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* Release 2 (10.1.2) or 10*g* (10.1.4) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the 11*g* Oracle instance, or click **Browse** to locate the instance directory.

Table 4–2   (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify WebLogic Server	Enter the host and Administration Server port for the Oracle WebLogic Server you configured in Section 4.3.2, "Installing the Oracle WebLogic Server Software and Creating the Middleware Home".
	Note this information is required if you are upgrading Oracle Directory Integration Platform. It is also required if you associated your Oracle Internet Directory 11*g* installation with Oracle WebLogic Server.
	For more information, see Section 4.3.2.1, "When is Oracle WebLogic Server Required?".
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	Select the upgrade options you want to apply to the Oracle Identity Management upgrade: ■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance. Note if you select this option, you will not be able to run both the 10*g* and 11*g* middle tiers at the same time; otherwise, port conflicts will occur. ■ **Start destination components after successful upgrade :** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade. Click **Help** to display more information about the upgrade options on this screen.
Specify OID Details	Use this screen to enter the details required to connect to the Oracle Internet Directory 10*g* instance, including the password to the Oracle Internet Directory super user account (`cn=orcladmin`). For more information, click **Help**.

Table 4–2   (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Database Details	Use this screen to enter the details required to connect to the database where the Oracle Identity Management schemas reside, including the host, service name, port, and SYS password for the database.
	Note the following important information about this screen:
	■ You must enter the password for the ODS schema password. The default ODS password is the same as the Oracle Application Server administrator password, but this password can be changed after installation, using the OID Database Password Utility.
	■ The instructions for identifying a Real Application Clusters (RAC) database are different, depending upon whether you are identifying the RAC database that contains the Oracle Internet Directory (ODS) schema or a RAC database that is being used for Oracle Directory Integration Platform.
	For more information, see Section 4.4.3.2, "About Specifying Real Application Clusters (RAC) Database Details on the Specify Database Details Screen".

4.4.3.2 About Specifying Real Application Clusters (RAC) Database Details on the Specify Database Details Screen

If you are upgrading the Oracle Internet Directory or Oracle Directory Integration Platform schemas that are stored in a RAC database, then you must consider the following important steps when entering the database connection details in the Specify Database Details screen in the Upgrade Assistant:

■ If you are upgrading the Oracle Internet Directory (ODS) schema in a RAC database, enter the details about only one node of the RAC database in the **Database Host**, **Database Port**, and **Database Service** fields. Do not enter any information about the OID schema database in the **Clustered Database Specification** field.

■ If you are upgrading Oracle Directory Integration Platform in a RAC database, then you must select the **Clustered Database** check box and enter the database connection details for each and every node in the cluster in the **Database Cluster Specification** field, using the syntax shown in Example 4–2.

Be sure to use the caret character (^) as a separator between each RAC node in the list.

Example 4–3 shows an example of how you would use the syntax to connect to a RAC database.

Example 4–2   Syntax for the Database Connection Details for a RAC Database

```
host_name:port:first_instance_name^host_name:port:second_instance_name@db_service_name
```

Example 4–3   Example of the Database Connection Details for a RAC Database

```
host1.example.com:1521:inst1^host3.example.com:1522:inst2@db_service.example.com
```

4.4.3.3 Recovering From an Oracle Internet Directory Error During the Upgrade Assistant Examine Phase

The Upgrade Assistant always examines the components in your source and target environments before performing an upgrade to Oracle Fusion Middleware 11g. After this examination phase, you can then proceed with the upgrade of the selected components.

However, if an error occurs while the Upgrade Assistant is examining an Oracle Internet Directory instance, you might have a problem using Upgrade Assistant to examine the Oracle Internet Directory instance again later.

Specifically, during the examine phase, the Upgrade Assistant checks to see if the Oracle Internet Directory instance is up and running. If the instance is not running, then the examine phase reports the problem. You must start the instance before proceeding to the upgrade phase.

After starting the instance, if you then click the **Back** button or restart the Upgrade Assistant, then the Upgrade Assistant skips the Oracle Internet Directory instance during the examination phase and does not report on its state.

To remedy this problem and to re-examine the Oracle Internet Directory instance after a previous examination error, do the following:

1. Stop the Upgrade Assistant.

2. Locate and delete the following temporary file:

   ORACLE_INSTANCE/OID/temp/oidretry.dat

3. Restart the Upgrade Assistant and re-examine the components you want to upgrade.

4.5 Task 5: Perform Any Required Oracle Internet Directory and Oracle Directory Integration Platform Post-Upgrade Tasks

After you upgrade Oracle Internet Directory and Oracle Directory Integration Platform, perform the following post-upgrade tasks:

- Recreating Any Non-Default Oracle Internet Directory Instances

- Disabling the Oracle Internet Directory and Oracle Directory Integration Platform 10g Components

- Configuring OPMN in the 10g Oracle Home After Upgrading Oracle Internet Directory to 11g

- Enabling Oracle Internet Directory Referential Integrity After Upgrade

- Reviewing Configuration Attributes That Are Not Upgraded to Oracle Internet Directory 11g

- Removing Oracle Internet Directory and Oracle Directory Integration Platform 10g from Application Server Control

- Removing Unneeded Oracle Directory Integration Platform Template Profiles After Upgrade

4.5.1 Recreating Any Non-Default Oracle Internet Directory Instances

When you upgrade Oracle Internet Directory, only the default Oracle Internet Directory instance is upgraded.

If you have additional, non-default Oracle Internet Directory instances in your 10*g* environment, you must create those manually in the 11*g* environment, as follows:

1. Perform the following ldapsearch command to locate the additional Oracle Internet Directory instances:

```
ldapsearch
    -p oidPort
    -h oidHost
    -D cn=orcladmin
    -w adminPasswd
    -b "cn=osdldapd, cn=subconfigsubentry"
    -s one "cn=config*" dn orclsslport orclnonsslport orclmaxcc orclserverprocs
```

2. Verify the following before you create the additional Oracle Internet Directory instances:

   - That the following files, which are created during the installation, exist in the *ORACLE_INSTANCE*/config directory:

     ```
     tnsnames.ora
     tnsnames_copy.ora
     ```

   - Verify that OIDDB appears as an entry in the tnsnames.ora file.

3. Create each additional Oracle Internet Directory instance with the following command:

```
opmnctl createcomponent
   -adminRegistration OFF
   -componentType OID
   -componentName componentName
   -Db_info "DBHostName:Port:DBSvcName"
     [-Ods_Password_File 'File_with_DB_ODS_USER_PASSWORD']
     [-Sm_Password_File 'File_with_DB_ODSSM_USER_PASSWD']
     [-Admin_Password_File 'File_with_OID_Admin_Passwd']
   -Namespace "dc=domain_component1,dc=domain_component2..."
   [-Port nonSSLPortFromAboveSearchCommand]
   [-Sport SSLPortFromAboveSearchCommand]
```

4. After the new instance of Oracle Internet Directory is created, update the orclmaxcc and orclserverprocs using either Fusion Middleware Control or, as follows, using ldapmodify command:

```
ldapmodify -p <oidPort> -D cn=orcladmin -w <adminPaswd> << eof
dn: cn=<componentName>,cn=osdldapd,cn=subconfigsubentry
changetype: modify
replace: orclmaxcc
orclmaxcc: <orclMaxxCCValueFrom#1>
-
replace: orclserverprocs
orclserverProcs: <orclServerProcsValueFrom#1>
eof
```

5. Start new instances:

```
opmnctl startproc ias-component=componentName
```

4.5.2 Disabling the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* Components

If you are using Oracle Single Sign-On and Oracle Delegated Administration Services, and then you upgrade the Oracle Internet Directory and Oracle Directory Integration Platform components in that environment, then you must disable the Oracle Internet Directory and Oracle Directory Integration Platform components in the Oracle Application Server 10*g* Oracle home.

This step is necessary because in most cases, you will want to maintain your Oracle Single Sign-On and Oracle Delegated Administration Services 10*g* components, but not the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* components. For more information, see Section 3.2, "Oracle Internet Directory and Oracle Directory Integration Platform Topology".

To de-associate the existing 10*g* Oracle Single Sign-On from Oracle Internet Directory:

1. Modify the Oracle Internet Directory entry in the OPMN configuration file:

   a. Locate the following file in the Oracle Application Server 10*g* Oracle home:

      ```
      $ORACLE_HOME/opmn/conf/opmn.xml
      ```

   b. Make a backup copy of the file so you can easily revert to the original version if necessary.

   c. Locate the following entry in the opmn.xml file:

      ```
      <ias-component id="OID" status="enabled">
      ```

   d. Modify the entry so that the OID component is disabled:

      ```
      <ias-component id="OID" status="disabled">
      ```

2. Modify the Oracle Internet Directory and Oracle Directory Integration Platform settings in the ias.properties file:

   a. Locate the following file in the Oracle Application Server 10*g* Oracle home:

      ```
      ORACLE_HOME/config/ias.properties
      ```

   b. Make a backup copy of the file so you can easily revert to the original version if necessary.

   c. Locate the following entries in the ias.properties file and change them from true to false:

      ```
      OID.LaunchSuccess=false
      DIP.LaunchSuccess=false
      ```

3. Restart Oracle Single Sign-On in the Oracle Application Server 10*g* Oracle home.

4.5.3 Configuring OPMN in the 10*g* Oracle Home After Upgrading Oracle Internet Directory to 11*g*

Use the information in this section if you are upgrading a distributed Oracle Identity Management environment, where the Oracle Internet Directory instance is on a different host from the Oracle Single Sign-On 10*g* instance.

In such a distributed environment, after you upgrade Oracle Internet Directory to 11*g*, you must reconfigure the oc4j_security OC4J instance so it does not continue to attempt to connect to OPMN on the Oracle Internet Directory 10*g* host. Otherwise,

errors will appear in the `ons.log` file and the `oc4j_security` instance on the Oracle Single Sign-On host will fail to start.

To reconfigure the `oc4j_security` instance on the Oracle Single Sign-On host:

1. Locate the following configuration file in the Oracle Identity Management 10*g* Oracle home on the Oracle Single Sign-On host:

   ```
   ORACLE_HOME/opmn/conf/ons.conf
   ```

2. Edit the `ons.conf` file and remove any references to the Oracle Internet Directory host.

   In the following example, OPMN is using the information in the `ons.conf` file to communicate with OPMN on both SSOHOST1 and OIDHOST1. To stop OPMN from attempting to connect to the OIDHOST1, remove the OIDHOST1 and post from the file:

   ```
   nodes=SSOHOST1.example.com:6200,OIDHOST1.example.com:6200
   ```

4.5.4 Enabling Oracle Internet Directory Referential Integrity After Upgrade

When you upgrade Oracle Internet Directory to 11*g*, the referential integrity feature of Oracle Internet Directory is not enabled by default. As a result, if you were using referential integrity in Oracle Internet Directory 10*g*, perform the following steps after the upgrade to 11*g*:

1. Use the Oracle Internet Directory Server Diagnostic command-line tool (oiddiag) to identify and fix any referential integrity violations.

   For more information, see "oiddiag" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management*.

2. Enable referential integrity for the upgraded Oracle Internet Directory 11*g*.

   For more information, see "Configuring Referential Integrity" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

4.5.5 Reviewing Configuration Attributes That Are Not Upgraded to Oracle Internet Directory 11*g*

When you upgrade your Oracle Internet Directory 11*g* instance to Oracle Internet Directory 11*g*, the following configuration parameter values are not upgraded to the 11*g* instance.

- `MinConnectionsInPool`: The value of this attribute will not be saved if it is zero.

- `PluginName`: This attribute identifies the authentication plug-in name; after upgrade, the 11*g* default values will be used for a particular authentication level.

- `ConnectionIdleTimeout`: This parameter is obsolete for Oracle Identity Management 11*g*.

For more information about the configuration parameters supported in Oracle Internet Directory 11*g*, see "Attribute Reference" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management*.

4.5.6 Removing Oracle Internet Directory and Oracle Directory Integration Platform 10*g* from Application Server Control

After you upgrade to Oracle Internet Directory 11*g* and Oracle Directory Integration Platform 11*g*, the 10*g* versions of these components will still appear in the Oracle Enterprise Manager Application Server Control that is running out of the Oracle Single Sign-On 10*g* Oracle home.

To remove the Oracle Internet Directory and Oracle Directory Integration Platform targets from 10*g* Application Server Control:

1. Locate the following file in the Oracle Single Sign-On 10*g* Oracle home:

    ORACLE_HOME/sysman/emd/targets.xml

2. Delete the entry that represents the Oracle Internet Directory 10*g* instance from the targets.xml file.

    Note that the target element is formatted differently in the targets.xml file, depending on whether you are upgrading a 10*g* Release 2 (10.1.2) or 10*g* (10.1.4) Identity Management environment:

    - If you are upgrading from Oracle Identity Management 10*g* Release 2 (10.1.2), refer to Example 4–4 for an example of an entry in the targets.xml file that defines an Oracle Internet Directory target called oid10g.

    - If you are upgrading from Oracle Identity Management 10*g* (10.1.4), refer to Example 4–5 for an example of an entry in the targets.xml file that defines an Oracle Internet Directory target called oid10g.

    Note that Oracle Directory Integration Platform could not be managed by Oracle Enterprise Manager in 10*g* Release 2 (10.1.2), so you will not see a Oracle Directory Integration Platform entry in the 10*g* Release 2 (10.1.2) entry.

3. If necessary, do the same for the Oracle Directory Integration Platform target in the Oracle Single Sign-On 10*g* Oracle home.

    Refer to Example 4–6 for an example of any entry in targets.xml that defines an Oracle Directory Integration Platform target. When searching for the target, searchy for the target type, "oracle_eps_server".

4. Start Application Server Control.

    Refer to the Oracle Application Server 10*g* documentation for instructions on stopping and starting Application Server Control.

    Note that these changes require a restart of Application Server Control before they take affect. However, in this case, the Oracle Application Server 10*g* environment will be down immediately after the upgraded, so there is no need to stop Application Server before starting it in this case.

Example 4–4   Oracle Internet Directory Target Entry in a 10g Release 2 (10.1.2) targets.xml File

```
<Target TYPE="oracle_ldap" NAME="oid10g.myhost.example.com_LDAP"
        DISPLAY_NAME="Internet Directory" VERSION="2.5"
        ON_HOST="myhost.example.com">
        <Property NAME="OracleHome" VALUE="/oracle/product/inst/ias10g"/>
                     .
                     .
                     .
</Target>
```

Example 4–5 Oracle Internet Directory Target Entry in a 10g (10.1.4) targets.xml File

```
<Target TYPE="oracle_ldap" NAME="oid10g.myhost.example.com_LDAP"
             DISPLAY_NAME="OID" VERSION="3.0" ON_HOST="myhost.example.com">
    <Property NAME="OracleHome"
              VALUE="/oracle/product/inst/ias10g"/>
                  .
                  .
                  .
    <CompositeMembership>
              <MemberOf TYPE="oracle_ias"
                    NAME="ias10g.myhost.example.com" ASSOCIATION=" "/>
    </CompositeMembership>
</Target>
```

Example 4–6 Oracle Directory Integration Platform Entry in a 10g (10.1.4)

```
<Target TYPE="oracle_eps_server"
       NAME="dip1014.myhost.example.com_DIP"
       DISPLAY_NAME="dip1014.myhost.example.com_DIP">
  <Property NAME="OracleHome" VALUE="C:\oracle\products\oim1014"/>
  <Property NAME="UserName" VALUE="013549bf4bf5c73c" ENCRYPTED="TRUE"/>
  <Property NAME="password" VALUE="fdfd90d00d859820" ENCRYPTED="TRUE"/>
  <Property NAME="host" VALUE="myhost"/>
  <Property NAME="ConnectDescriptor"
     VALUE="(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
     (HOST=bigip41.example.com)
     (PORT=1251))(ADDRESS=(PROTOCOL=TCP)
     (HOST=bigip42.example.com)(PORT=1251))
     (LOAD_BALANCE=yes))(CONNECT_DATA=(SERVICE_NAME=newdb.example.com)))"/>
  <Property NAME="version" VALUE="10.1.4.0.1"/>
  <AssocTargetInstance ASSOC_TARGET="epsldap"
                    TYPE="oracle_ldap"
                    NAME="oid10g.myhost.example.com_LDAP"/>
  <CompositeMembership>
     <MemberOf TYPE="oracle_ias" NAME="ias10g.myhost.example.com"/>
  </CompositeMembership>
</Target>
```

4.5.7 Removing Unneeded Oracle Directory Integration Platform Template Profiles After Upgrade

All Oracle Directory Integration Platform 10*g* template profiles are upgraded to 11*g* during the upgrade process. These profiles can be deleted using Fusion Middleware Control, depending upon the needs of your environment.

Deleting these profiles is an optional step. Be sure not to delete any profiles that were actively being used in the 10g topology.

4.6 Task 6: Verify that the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade Was Successful

To verify that your Oracle Internet Directory and Oracle Directory Integration Platform upgrade was successful:

1. Run the Upgrade Assistant again and select **Verify Instance** on the Specify Operation page.

    Follow the instructions on the screen for information on how to verify that specific Oracle Fusion Middleware components are up and running.

2. Use the Fusion Middleware Control to verify that the Oracle Internet Directory and Oracle Directory Integration Platform components are up and running.

   For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

5

Upgrading Your Oracle Virtual Directory Environment

This chapter describes how to upgrade your existing Oracle Virtual Directory 10*g* (10.1.4.3) to Oracle Virtual Directory 11*g*.

This chapter contains the following sections:

- Task 1: Decide Upon an Oracle Virtual Directory Topology
- Task 2: Install and Configure Oracle Virtual Directory 11g
- Task 3: Use the Upgrade Assistant to Upgrade Oracle Virtual Directory
- Task 4: Perform Any Required Oracle Virtual Directory Post-Upgrade Tasks
- Task 5: Verify that the Oracle Virtual Directory Upgrade Was Successful

5.1 Task 1: Decide Upon an Oracle Virtual Directory Topology

Before you install Oracle Virtual Directory 11*g*, consider the topology you currently have in Oracle Application Server 10*g* (10.1.4.3), as well as any requirements for your Oracle Fusion Middleware 11*g* environment.

Note that you can configure Oracle Virtual Directory with Oracle WebLogic Server domain or you can configure it without a domain.

For more information, refer to Chapter 3.3, "Oracle Virtual Directory Topologies".

5.2 Task 2: Install and Configure Oracle Virtual Directory 11*g*

The following sections describes how to install and configure new Oracle Fusion Middleware 11*g* middle tier instances in preparation for an upgrade to Oracle Fusion Middleware 11*g*:

- Installing the Oracle WebLogic Server Software and Creating the Middleware Home
- Installing and Configuring Oracle Virtual Directory 11g in Preparation for Upgrade

5.2.1 Installing the Oracle WebLogic Server Software and Creating the Middleware Home

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

5.2.2 Installing and Configuring Oracle Virtual Directory 11*g* in Preparation for Upgrade

Installing and configuring Oracle Virtual Directory in preparation for an upgrade is similar to any other 11*g* installation. Later, you use the Oracle Fusion Middleware Upgrade Assistant to copy configuration information from the 10*g* environment to the new 11*g* environment.

To install and configure Oracle Virtual Directory, in preparation for upgrade:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network (OTN):

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the `setup.exe` file.

4. Follow the instructions in the installer to install Oracle Virtual Directory.

   For complete details, as well as prerequisite information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

5.3 Task 3: Use the Upgrade Assistant to Upgrade Oracle Virtual Directory

The Oracle Fusion Middleware Upgrade Assistant automates the upgrade of many aspects of your Oracle Application Server 10*g* environment.

The Upgrade Assistant is installed automatically into the `bin` directory of your Oracle Fusion Middleware Oracle home.

The following sections provide more information:

- Task 3a: Stop the Oracle Virtual Directory Instances
- Task 3b: Start the Upgrade Assistant for an Oracle Virtual Directory Upgrade
- Task 3c: Upgrade Oracle Virtual Directory

5.3.1 Task 3a: Stop the Oracle Virtual Directory Instances

Before you start the Upgrade Assistant, the Oracle Virtual Directory instance that you are about to upgrade must be stopped.

On the Linux operating system, the Upgrade Assistant stops Oracle Virtual Directory automatically before it begins the upgrade process.

However, on the Windows operating system, you must stop Oracle Virtual Directory manually before you start the Upgrade Assistant.

For more information, refer to the section, "Starting & Stopping Oracle Virtual Directory" in the *Oracle Virtual Directory Installation Guide*, which is available in the Oracle Identity Management 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN):

```
http://www.oracle.com/technology/documentation/oim1014.html
```

5.3.2 Task 3b: Start the Upgrade Assistant for an Oracle Virtual Directory Upgrade

To start the Upgrade Assistant using the graphical user interface:

> **Note:** You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen as shown in Figure 5–1

Figure 5–1   Upgrade Assistant Welcome Screen
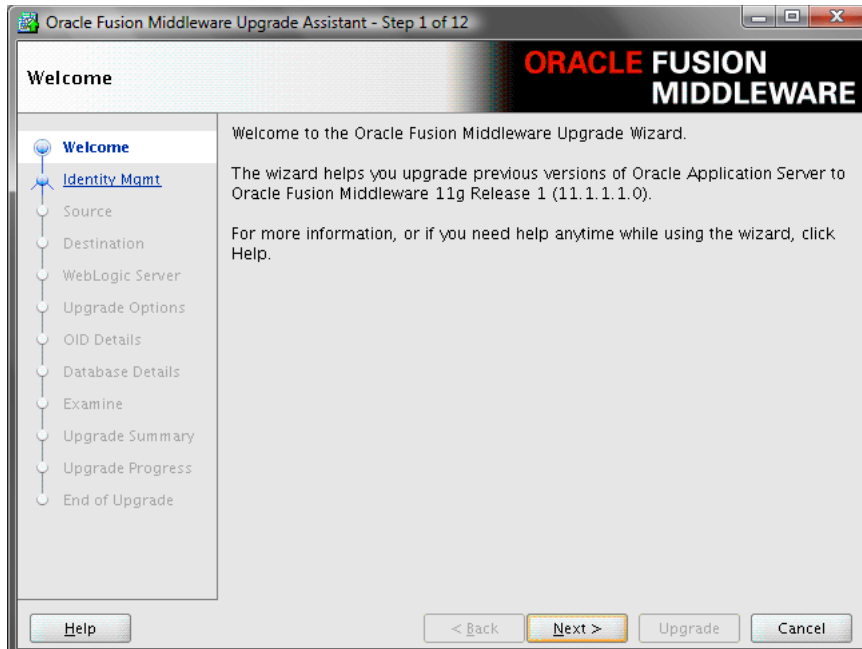
3. Click **Next** to display the Select Operation screen (Figure 5–2).

The options available in the Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Identity Management Oracle home, the options shown on the Select Operation screen are the valid options for an Oracle Identity Management Oracle home.

Figure 5–2   Upgrade Assistant Select Operation Screen for an Oracle Virtual Directory Upgrade
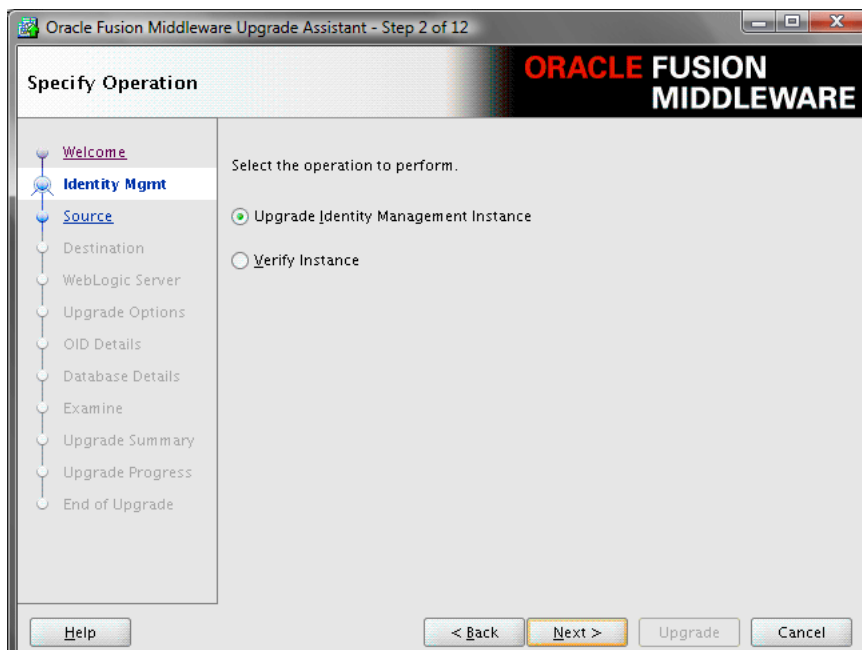
5.3.3 Task 3c: Upgrade Oracle Virtual Directory

To upgrade Oracle Virtual Directory:

1. Start the Upgrade Assistant as described in Task 3b: Start the Upgrade Assistant for an Oracle Virtual Directory Upgrade.

2. Select **Upgrade Identity Management Instance** on the Select Operation screen (Figure 5–2).

3. Refer to Table 5–1 for a description of the Upgrade Assistant screens that require input from you during an Oracle Virtual Directory upgrade.

4. After you provide all required input, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

     See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

   - Displays the End of Upgrade screen, which confirms that the upgrade was complete.

Table 5–1   Upgrade Assistant Screens That Require Input During an Oracle Virtual Directory Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* (10.1.4.3) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the destination 11*g* Oracle instance that you installed inside the middleware home. This is the Oracle instance that contains the Oracle Virtual Directory software.
	Alternatively, click **Browse** to select the Oracle instance.
Specify WebLogic Server	Enter the host, Administration Server port, and administration user credentials for the Oracle WebLogic Server domain you configured in Section 5.2.1, "Installing the Oracle WebLogic Server Software and Creating the Middleware Home".
	This screen appears only if you chose to associate the Oracle Virtual Directory 11*g* instance with Oracle WebLogic Server during the Oracle Virtual Directory installation.
	It does not appear if you selected to install Oracle Virtual Directory without an Oracle WebLogic Server domain.

Table 5–1   (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Virtual Directory Upgrade

Upgrade Assistant Screen	Description
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	This screen offers these upgrade options:
	■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance. Note if you select this option, you will not be able to run both the 10*g* and 11*g* middle tiers at the same time; otherwise, port conflicts will occur.
	■ **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade.
	Click **Help** to display more information about the upgrade options on this screen.

5.4 Task 4: Perform Any Required Oracle Virtual Directory Post-Upgrade Tasks

After you upgrade Oracle Virtual Directory by running the Upgrade Assistant, you must perform the following post-upgrade tasks:

- Configuring Anonymous Ciphers for Oracle Virtual Directory SSL Listeners

- Starting Oracle Virtual Directory After Upgrade When Using Privileged Ports

- Updating Oracle Virtual Directory Monitoring Properties in Fusion Middleware Control

- Upgrading Oracle Virtual Directory Logging Configuration Settings

5.4.1 Configuring Anonymous Ciphers for Oracle Virtual Directory SSL Listeners

Oracle Virtual Directory 10*g* (10.1.4.3) and later LDAP SSL listeners supports anonymous ciphers (in no-auth SSL mode) by default. The list of enabled cipher suites are set in OVD start-up scripts:

- `vde_start.sh` on UNIX systems

- `OViDServer.lax` on Windows systems

The list of ciphers can be modified by editing the `-D` Java system property `vde.ldap.ciphers` in these start-up scripts. This list is applicable across all LDAP

SSL listeners. There was no option to enable different cipher suites for each LDAP listener.

In Oracle Virtual Directory 11*g*, the `vde.ldap.ciphers` Java system property is no longer supported. Instead, you can enable different cipher suites for each Oracle Virtual Directory listener when configuring SSL with Oracle Enterprise Manager Fusion Middleware Control or with the WLST command-line tool.

Anonymous cipher suites are disabled on Oracle Virtual Directory SSL listeners for security, by default. For information on enabling anonymous ciphers as part of configuring SSL security for your Oracle Virtual Directory environment, see "SSL Configuration in Oracle Fusion Middleware" in the *Oracle Fusion Middleware Administrator's Guide*.

5.4.2 Starting Oracle Virtual Directory After Upgrade When Using Privileged Ports

If you select the **Use source Oracle home ports in destination** option when upgrading an Oracle Virtual Directory 10*g* instance that is configured to listen on privileged ports, then the Upgrade Assistant cannot start Oracle Virtual Directory 11*g* after the upgrade.

Instead, the following error message appears in the Oracle Virtual Directory log file:

```
Cannot start Oracle Virtual Directory server: Permission denied.
```

To start an Oracle Virtual Directory 11*g* instance that is listening on privileged ports, perform the following steps:

1. Stop Oracle Process Manager and Notification Server (OPMN) and its managed processes, by using the following command in the Oracle instance directory where Oracle Virtual Directory 11*g* is configured:

   ORACLE_INSTANCE/bin/opmnctl stopall

2. Execute following commands as root:

   To start OPMN :

   ORACLE_INSTANCE/bin/opmnctl start

   Start Oracle Virtual Directory 11*g*:

   ORACLE_INSTANCE/bin/opmnctl startproc ias-component=*OVDCompName*

   In this example, replace *OVDCompName* with the name of the Oracle Virtual Directory instance.

For more information, see "Managing Oracle Virtual Directory Server Processes" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

5.4.3 Updating Oracle Virtual Directory Monitoring Properties in Fusion Middleware Control

After upgrading Oracle Virtual Directory, you might encounter situations where the performance metrics and charts do not display properly when you are monitoring Oracle Virtual Directory in Oracle Enterprise Manager Fusion Middleware Control.

If this problem occurs, perform the following task to modify the monitoring properties in Fusion Middleware Control:

1. Login to Fusion Middleware Control.

2. From the **Farm** menu, select **Agent-Monitored Targets**.

3. Click the Configure icon for the Oracle Virtual Directory target that you just upgraded.

4. On the Configuration page, change the following fields so they match the values required for the upgraded Oracle Virtual Directory instance:

   - Machine Name

   - Virtual Directory Admin Port

   - Virtual Directory LDAP Port

5. Click **OK** to save the changes.

6. Log in to the system where Oracle Virtual Directory was installed and navigate to the Oracle Virtual Directory Oracle home:

   ```
   ORACLE_HOME/bin
   ```

7. Run the following commands to import the Oracle Virtual Directory listener keystore certificates into the Fusion Middleware Control agent wallet:

   a. Export Oracle Virtual Directory server certificate:

   ```
   keytool -exportcert
           -keystore OVD_KEYSTORE_FILE
           -storepass passwd
           -alias OVD_SERVER_CERT_ALIAS
           -rfc
           -file OVD_SERVER_CERT_FILE
   ```

   b. Add the Oracle Virtual Directory server certificate to Oracle Management Agent wallet

   ```
   ORACLE_HOME/bin/orapki wallet add
           -wallet ORACLE_INSTANCE/EMAGENT/EMAGENT/sysman/config/monwallet
           -trusted_cert
           -cert OVD_SERVER_CERT_FILE
           -pwd WALLET_PASSWD
   ```

   For example, if you're using default values configured at installation time, you would use the following values for the variables in the above example:

   Replace *OVD_KEY_STORE_FILE* with:

   ```
   ORACLE_INSTANCE/config/OVD/ovd1/keystores/keys.jks
   ```

   Replace *OVD_SERVER_CERT_ALIAS* with `serverselfsigned`.

   Replace *passwd* with the password for the Oracle Virtual Directory administrator account.

For more information about configuring Agent-monitored targets, see "Troubleshooting the Display of Performance Metrics and Charts in Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

5.4.4 Upgrading Oracle Virtual Directory Logging Configuration Settings

When you ugprade Oracle Virtual Directory, the logging settings you configured in Oracle Virtual Directory 10*g* are not upgraded.

Instead you will find that after upgrade:

- The log levels in the upgraded Oracle Virtual Directory 11*g* instance are set to "Notification", and the access log is enabled by default after upgrade, irrespective of its configuration in Oracle Virtual Directory 10*g*.

  To disable the access log, modify log level of logger name `com.octetstring.accesslog` to "ERROR:1".

  For more information, see "Managing Oracle Virtual Directory Logging and Auditing" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

- If the Oracle Virtual Directory Dump Transactions plug-in is configured, then the log level for the plug-in must be changed to one of the following values: SEVERE, WARNING, INFO, FINE, FINER, or FINEST.

  For more information, see "Using the Dump Transactions Plug-In to Gather Information About Data Transformation Errors" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

5.5 Task 5: Verify that the Oracle Virtual Directory Upgrade Was Successful

To verify that your Oracle Virtual Directory upgrade was successful:

1. Run the Upgrade Assistant again and select **Verify Instance** on the Specify Operation page.

   Follow the instructions on the screen for information on how to verify that specific Oracle Fusion Middleware components are up and running.

2. Use the Fusion Middleware Control to verify that the Oracle Virtual Directory components are up and running.

   For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

6

Upgrading Your Oracle Identity Federation Environment

This chapter describes how to upgrade your existing 10*g* (10.1.4) Oracle Identity Federation to Oracle Identity Federation 11*g*.

This chapter contains the following sections:

- Task 1: Decide Upon an Oracle Identity Federation Topology
- Task 2: Use the Repository Creation Utility to Install the Oracle Identity Federation Schema in the Database
- Task 3: Install and Configure Oracle Identity Federation 11g
- Task 4: Use the Upgrade Assistant to Upgrade Oracle Identity Federation
- Task 5: Perform Any Required Oracle Identity Federation Post-Upgrade Tasks
- Task 6: Verify that the Oracle Identity Federation Upgrade Was Successful

6.1 Task 1: Decide Upon an Oracle Identity Federation Topology

Before you install Oracle Identity Federation 11*g*, consider the topology you currently have in Oracle Application Server 10*g* (10.1.4), as well as any requirements for your Oracle Fusion Middleware 11*g* environment.

For more information, refer to Chapter 3.4, "Oracle Identity Federation Topologies".

6.2 Task 2: Use the Repository Creation Utility to Install the Oracle Identity Federation Schema in the Database

Before you can upgrade to Oracle Identity Federation 11*g*, you must first install the Oracle Identity Federation schema into a supported database.

For more information, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

For more information about installing the Oracle Identity Federation schema, refer to the following sections:

- Verifying that the Database Meets the Minimum Requirements for the Oracle Identity Federation Schema
- Running the Repository Creation Utility in Preparation for Upgrading Oracle Identity Federation

6.2.1 Verifying that the Database Meets the Minimum Requirements for the Oracle Identity Federation Schema

Before performing any installation you should read the system requirements and certification documentation to ensure that your environment meets the minimum installation requirements for the products you are installing.

For more information, refer to "System Requirements and Prerequisites" in the *Oracle Fusion Middleware Installation Planning Guide*.

6.2.2 Running the Repository Creation Utility in Preparation for Upgrading Oracle Identity Federation

To run the Repository Creation Utility to install the Oracle Identity Federation schema in the database, refer to the following resources:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*

- *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

After you start the Repository Creation Utility, follow the instructions on the Repository Creation Utility screens to connect to the database and create the required schemas.

During the installation of the schema, note the following:

- On the Select Componts screen, be sure to select the **Oracle Identity Federation** schema.

- No other schemas are required unless you plan to use this database for installing other Oracle Fusion Middleware 11*g* components.

6.3 Task 3: Install and Configure Oracle Identity Federation 11*g*

The following sections describes how to install and configure new Oracle Fusion Middleware 11*g* middle tier instances in preparation for an upgrade to Oracle Fusion Middleware 11*g*:

- Task 3a: Install the Oracle WebLogic Server Software and Create the Middleware Home

- Task 3b: Install and Configure Oracle Identity Federation 11g in Preparation for Upgrade

- Task 3c: Create an Oracle HTTP Server Instance and Link It to Oracle Identity Federation 11g

6.3.1 Task 3a: Install the Oracle WebLogic Server Software and Create the Middleware Home

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

6.3.2 Task 3b: Install and Configure Oracle Identity Federation 11*g* in Preparation for Upgrade

Installing and configuring Oracle Identity Federation in preparation for an upgrade is similar to any other 11*g* installation. Later, you use the Oracle Fusion Middleware Upgrade Assistant to copy configuration information from the 10*g* environment to the new 11*g* environment.

To install and configure Oracle Identity Federation, in preparation for upgrade:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network (OTN):

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

   On UNIX systems, enter the following command:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the `setup.exe` file.

4. Follow the instructions in the installer to install Oracle Identity Federation.

   Refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Identity Federation installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

6.3.3 Task 3c: Create an Oracle HTTP Server Instance and Link It to Oracle Identity Federation 11*g*

For specific instructions, refer to "Create and Manage Oracle HTTP Server" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

6.4 Task 4: Use the Upgrade Assistant to Upgrade Oracle Identity Federation

The Oracle Fusion Middleware Upgrade Assistant automates the upgrade of many aspects of your Oracle Application Server 10*g* environment.

The Upgrade Assistant is installed automatically into the `bin` directory of your Oracle Fusion Middleware Oracle home.

You run the Upgrade Assistant once for each Oracle Application Server 10*g* Oracle home that you are upgrading. For example, if you are upgrading upgrading two different 10*g* Release 2 (10.1.2) Oracle homes that are a part of the same 10*g* Release 2 (10.1.2) farm, then you would run the Upgrade Assistant two times, once for each of the 10*g* Release 2 (10.1.2) Oracle homes.

Similarly, if you configure multiple Oracle instances in your new Oracle Fusion Middleware 11*g* environment, you must run the Upgrade Assistant once for each Oracle instance.

> **Note:** If you have configured more than one data store, Authentication Engine, or SP Engine in your Oracle Identity Federation environment, the Upgrade Assistant will upgrade only the enabled resources to 11*g*. Any additional data stores, authentication engines, or SP engines that are are configured, but not enabled, will not be upgraded to the new Oracle Identity Federation 11*g* environment.
>
> After you upgrade, you can reconfigure the resources that were not upgraded. In addition, unlike Oracle Identity Federation 10g, you can enable more than one of these resources at a time in 11*g*.

The following sections provide more information:

- Task 4a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade
- Task 4b: Upgrade Oracle Identity Federation

6.4.1 Task 4a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade

To start the Upgrade Assistant using the graphical user interface:

> **Note:** You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

1. Change directory the `ORACLE_HOME`/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

    On UNIX system:

    ```
    ./ua
    ```

    On Windows systems:

    ```
    ua.bat
    ```

    The Upgrade Assistant displays the Welcome screen as shown in Figure 6–1

Figure 6–1 Upgrade Assistant Welcome Screen
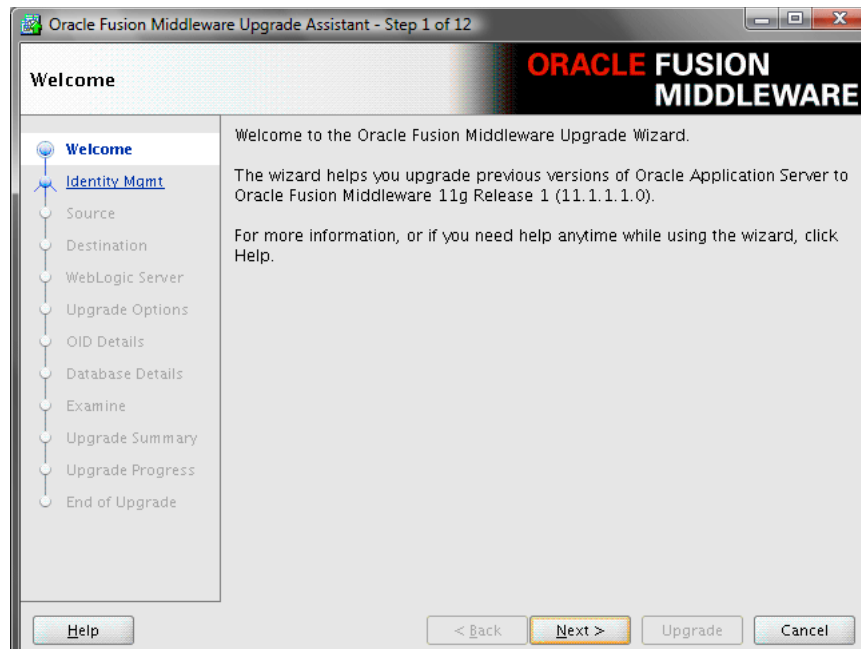
3. Click **Next** to display the Select Operation screen (Figure 6–2).

The options available in the Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Identity Management Oracle home, the options shown on the Select Operation screen are the valid options for an Oracle Identity Management Oracle home.

Figure 6–2 Upgrade Assistant Select Operation Screen for an Oracle Identity Federation Upgrade
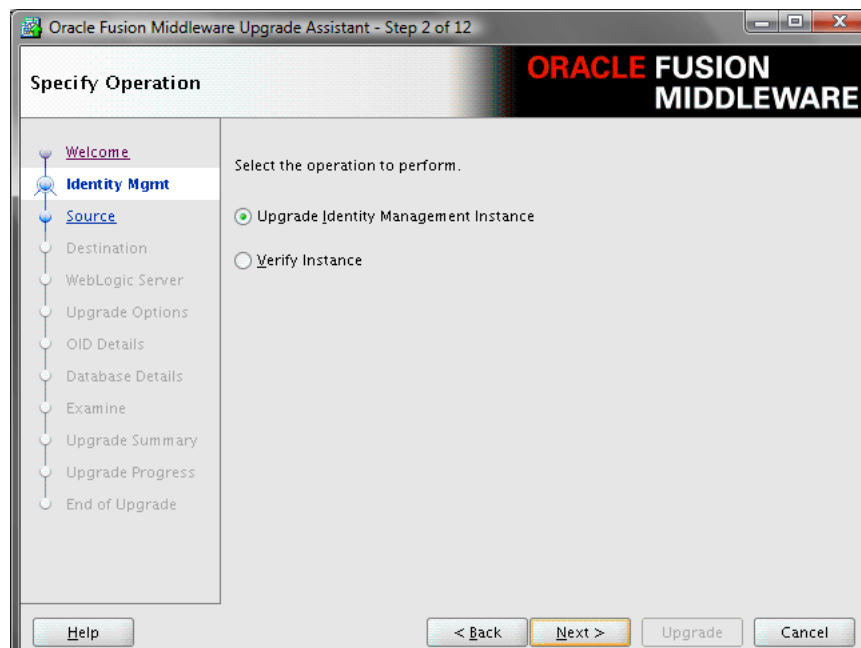
6.4.2 Task 4b: Upgrade Oracle Identity Federation

When you upgrade Oracle Identity Federation, the Upgrade Assistant upgrades the configuration files in the Oracle Identity Federation middle tier.

To upgrade Oracle Identity Federation when they reside in the same Oracle instance:

1. Start the Upgrade Assistant as described in Task 4a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade.

2. Select **Upgrade Identity Management Instance** on the Select Operation screen (Figure 6–2).

3. Refer to Table 6–1 for a description of the Upgrade Assistant screens that require input from you during an Oracle Identity Federation upgrade.

4. After the Specify Upgrade Options screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

    ■   Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

    ■   Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

    ■   Provides a progress screen so you can see the status of the upgrade as it proceeds.

    ■   Alerts you of any errors or problems that occur during the upgrade.

        See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

    ■   Displays the End of Upgrade screen, which confirms that the upgrade was complete.

5. Exit the Upgrade Assistant.

Table 6–1   Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* (10.1.4) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the destination 11*g* Oracle home that you installed inside the middleware home. This is the Oracle home that contains the Oracle Identity Federation software.
	Alternatively, click **Browse** to select the directory.
Specify WebLogic Server	Enter the host, Administration Server port, and administration user credentials for the Oracle WebLogic Server domain you configured in Section 6.3.2, "Task 3b: Install and Configure Oracle Identity Federation 11g in Preparation for Upgrade".

Table 6–1 (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	This screen offers these upgrade options:
	■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance.
	Note that Oracle recommends that you always select this option when upgrading Oracle Identity Federation.
	■ **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade.
	Click **Help** to display more information about the upgrade options on this screen.

6.5 Task 5: Perform Any Required Oracle Identity Federation Post-Upgrade Tasks

The following sections describe the manual upgrade steps required when you upgrading to Oracle Identity Federation 11*g*:

■ Integrating Oracle Identity Federation 11g with Oracle Access Manager 10g

■ Using a Custom Authentication Engine or Custom SP Engine with Oracle Identity Federation 11g

■ Reconfiguring Oracle Single Sign-On Server After Upgrade to Work with Oracle Identity Federation 11g

■ About Backwards Compatibility for ShareID Service URLs

■ Upgrading Oracle Identity Federation SSL Configuration

■ Setting Oracle Identity Federation System Properties After Upgrade

■ Additional Oracle Identity Federation Post-Upgrade Tasks

6.5.1 Integrating Oracle Identity Federation 11*g* with Oracle Access Manager 10*g*

If you were previously using Oracle Identity Federation 10*g* with Oracle Access Manager, you can use the following procedure to configure Oracle Identity Federation 11*g* so it can work successfully with your existing Oracle Access Manager 10*g* software.

Note that the steps described here are based on the instructions available in the section, "Deploying Oracle Identity Federation with Oracle Access Manager" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

To use Oracle Identity Federation 11*g* with Oracle Access Manager 10*g*:

1. Upgrade to Oracle Identity Federation 11*g* using the instructions in the previous sections of this chapter.

   Specifically, be sure you have installed and configured Oracle Identity Federation 11*g* and that you have used the Upgrade Assistant to upgrade the Oracle Identity Federation instance to 11*g*.

2. Optionally, use Oracle Access Manager 10*g* as the authentication engine for Oracle Identity Federation 11*g*.

   For specific instructions, refer to "Integrate Oracle Access Manager as an Authentication Engine" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

3. Optionally, integrate Oracle Access Manager 10*g* as an SP integration module.

   For specific instructions, refer to "Integrate Oracle Access Manager as an SP Integration Module" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

4. Optionally, configure Oracle Access Manager 10*g* so that protected resources are using the new Oracle Identity Federation 11*g* authentication schemes.

   To perform this task, use the instructions that help you verify the proper integration of Oracle Access Manager by allowing Oracle Identity Federation 11*g* to create policy objects and authentication schemes in Oracle Access Manager.

   These instructions are located in the section, "Integrate Oracle Identity Federation with Oracle Access Manager" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

5. When the integration with Oracle Access Manager is complete, delete any old access gates, authentication schemes, and policies for Oracle Identity Federation 10*g* from Oracle Access Manager 10*g*.

   For more information, refer to the Oracle Access Manager documentation in the Oracle Identity Management 10*g* (10.1.4) documentation library, which is available on the Oracle Technology Network (OTN):

   `http://www.oracle.com/technology/documentation`

6.5.2 Using a Custom Authentication Engine or Custom SP Engine with Oracle Identity Federation 11*g*

If your Oracle Identity Federation 10*g* instance is integrated with a custom authentication engine, then use the information in the following sections to configure the custom authentication engine with Oracle Identity Federation 11*g*:

- Modifying the Authentication Engine Code
- Modifying the SP Engine Code
- Changes to the Logout Service for Authentication or SP Engines
- Deploying the Authentication or SP Engine
- Creating the Authentication Engine in Oracle Identity Federation 11g
- Creating the SP Engine in Oracle Identity Federation 11g

6.5.2.1 Modifying the Authentication Engine Code

The `HTTPServletRequestAttributes` available to the authentication engines Oracle Identity Federation 11*g* are different from those in 10*g*. As a result, you must modify the authentication engine code so it can read the attribute values from their new parameter names.

Refer to the following sections for more information:

- Changes to Parameters and Attributes Received by Oracle Identity Federation 11g
- New Incoming Attributes Supported by Oracle Identity Federation 11g
- Changes to Parameters and Attributes Sent to Oracle Identity Federation 11g
- Additional Attributes to Include in a Request to Oracle Identity Federation 11g

Changes to Parameters and Attributes Received by Oracle Identity Federation 11*g*

Table 6–2 shows the new and changed parameters used for authentication engines in Oracle Identity Federation 11*g*.

Table 6–2 Parameters and Attributes received from Oracle Identity Federation

Parameter or Attribute	Changes in Oracle Identity Federation 11*g*
`doneURL` `getUsrSess`	These query parameters are not available in 11*g*. In 11g, there is no need to consult these parameters to find where the user has to be forwarded after being identified by the authentication engine. In 11g, after successful authentication, the engine must forward the user to Oracle Identity Federation. To do this use the root context, `/fed`, and the relativePath, `/user/loginsso`.

`authnMech`	This 10*g* query parameter has been changed to the following attribute in 11*g*:
	
	`oracle.security.fed.authn.authnmech`
	
	As a result, any occurences of `request.getParameter("authnMech")` in the custom engine will have to be changed to the folowing:
	
	`request.getAttribute("oracle.security.fed.authn.authnmech")`
	
	In 10g, the value of the the `authnMech` parameter was always as follows:
	
	`oracle:fed:authentication:password-protected`
	
	In 11g, the `oracle.security.fed.authn.authnmech` attribute can have other values. For more information, see "Configuring Authentication Mechanisms" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

`refID`	This 10*g* query parameter has been changed to the following attribute in 11*g*:
	
	`oracle.security.fed.authn.refid`
	
	As a result, any occurrences of `request.getParameter("refID")` in the custom engine will have to be changed to the following:
	
	`request.getAttribute("oracle.security.fed.authn.refid")`

New Incoming Attributes Supported by Oracle Identity Federation 11*g*

In addition to the changes described in Table 6–2, the following new incoming attributes are available in Oracle Identity Federation 11*g*; these attributes have no equivalents in Oracle Identity Federation 10*g*, but are available to the authentication engine in 11g:

- oracle.security.fed.authn.providerid
- oracle.security.fed.authn.providerdescription
- oracle.security.fed.authn.engineid

- oracle.security.fed.authn.userid

- oracle.security.fed.authn.forceauthn

- oracle.security.fed.authn.passive

- oracle.security.fed.authn.attributes

- oracle.security.fed.sessionid

For more information about these new attributes, see "Implementing the Service" the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

Changes to Parameters and Attributes Sent to Oracle Identity Federation 11*g*

The following attribute names must be changed after you upgrade to Oracle Identity Federation 11*g*:

- Change `oracle.security.sso.sasso.uid` to `oracle.security.fed.authn.userid`

- Change `oracle.security.sso.sasso.refID` to `oracle.security.fed.authn.refid`

- Change `oracle.security.sso.sasso.authnMech` to `oracle.security.fed.authn.authnmech`

- Change `oracle.security.sso.sasso.authnInst` to `oracle.security.fed.authn.authntime`

For example, suppose you have the following attribute in Oracle Identity Federation 11*g*:

```
request.setAttribute("oracle.security.sso.sasso.uid", userID)
```

For Oracle Identity Federation 11*g*, you must change this attribute as follows:

```
request.setAttribute("oracle.security.fed.authn.userid". userID);
```

For more information about the values that must be set by the authentication engine before doing an internal forward to Oracle Identity Federation 11*g*, see "Implementing the Service" the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

Additional Attributes to Include in a Request to Oracle Identity Federation 11*g*

In addition to the existing 10*g* attributes, Oracle Identity Federation 11*g* expects the additional attributes shown in Table 6–3 in each request.

Table 6–3   Additional Attributes to Include in a Request to Oracle Identity Federation 11g

Attribute	Description
oracle.security.fed.authn.expirationtime	Expiration time of the authenticated session as a Date Object

Table 6–3   (Cont.) Additional Attributes to Include in a Request to Oracle Identity Federation 11g

Attribute	Description
oracle.security.fed.authn.engineid	The identifier referencing the engine used to authenticate the user.
	The engine is created in the configuration of Oracle Identity Federation 11*g*. For more information, see Section 6.5.2.5, "Creating the Authentication Engine in Oracle Identity Federation 11g".
oracle.security.fed.authn.attributes	This optional map of attributes is stored in the user session. It will have String objects as the keys and Set of Objects as values.
oracle.security.fed.sessionid	This optional string contains the Oracle Identity Federation session identifier that Oracle Identity Federation will need to use to reference the user session.
	This allows the engine and the Oracle Identity Federation server to share the same identifier to reference the user session. Later, when the logout flow is being executed, Oracle Identity Federation will pass the sessionID that is being logged out to the engine, so that the engine can delete the data that was used for this user session.

6.5.2.2 Modifying the SP Engine Code

Similar to the its affect on authentication engines, the `HTTPServletRequestAttributes` available to the SP engines in Oracle Identity Federation 11*g* are different from those in 10*g*. As a result, you must modify the SP engine code so it can read the attribute values from their new parameter names.

Refer to the following sections for more information:

- Initiating a Federation SSO Operation

- Processing the Request from the Federation Server

Initiating a Federation SSO Operation

In Oracle Identity Federation 10*g*, if the Service Provider Engine did not find a valid user, then it initiated single sign-on by redirecting to the Oracle Identity Federation server function as the service provider. The URL it redirects to is as follows:

```
http://SP_HOST_NAME:SP_PORT/fed/sp/initiatesso
```

The following values are set to Oracle Identity Federation as query parameters:

- `providerid` – the provider ID of the IdP to use for single sign-on

- `returnurl` – the URL to which Oracle Identity Federation should send the user after single sign-on

In OIF 11g these query parameters have changed:

- The `providerId` should now be specified as the `HTTPServletRequest` attribute `oracle.security.fed.sp.providerid`

- The `returnurl` query parameter no longer exists; instead, it can be specified in the `HTTPServlet` request attribute `oracle.security.fed.sp.relaystate`.

- There are additional attributes in Oracle Identity Federation 11*g* that can be passed to the Oracle Identity Federation servers when initiating single sign-on. These additional attributes are as follows:

  - oracle.security.fed.sp.authnmech

  - oracle.security.fed.sp.federationid

- – oracle.security.fed.sp.engineid
- – oracle.security.fed.sp.localauthn
- – oracle.security.fed.sp.usedefault
- – oracle.security.fed.sp.forceauthn
- – oracle.security.fed.sp.allowfedcreation
- – oracle.security.fed.sp.passive
- – oracle.security.fed.sp.requestbinding
- – oracle.security.fed.sp.responsebinding
- – oracle.security.fed.sp.authnmechcomparison
- – oracle.security.fed.sp.nameidformat

For more information, see "Implementing the Service" the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

Processing the Request from the Federation Server

The following incoming parameter names for SP engines have changed in Oracle Identity Federation 11*g*:

- The `oracle.security.sso.sasso.uid` attribute has changed to `oracle.security.fed.sp.userid`

- `oracle.security.sso.sasso.authnInst` has changed to `oracle.security.fed.sp.authntime`

- `oracle.security.sso.sasso.expiryInst` has changed to `oracle.security.fed.sp.expirationtime`

- `oracle.security.sso.sasso.targetURL` is no longer available in Oracle Identity Federation 11*g*.

  The SP Engine can store the `targetURL` (to which the user will be forwarded) in `oracle.security.fed.sp.relaystate` before forwarding to Oracle Identity Federation to initiate an single sign-on operation. Oracle Identity Federation will pass this parameter back to the SP after doing an single sign-on.

The following additional, new parameters are available in Oracle Identity Federation 11*g* for the SP Engine to use. These new parameters include:

- oracle.security.fed.sp.authnresult
- oracle.security.fed.sp.authnmech
- oracle.security.fed.sp.attributes
- oracle.security.fed.sp.topstatus
- oracle.security.fed.sp.lowstatus
- oracle.security.fed.sp.statusmessage
- oracle.security.fed.sp.providerid
- oracle.security.fed.sp.engineid
- oracle.security.fed.sp.sessionid

For more information, see "Implementing the Service" the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

6.5.2.3 Changes to the Logout Service for Authentication or SP Engines

When using the logout service for an authentiation or SP engine with Oracle Identity Federation 11*g*, consider the information in the following sections:

- Changes When the Engine Initiates a Logout
- Changes When Oracle Identity Federation Forwards to the Engine for Logout

Changes When the Engine Initiates a Logout

In Oracle Identity Federation 11*g*, an authentication or SP engine can initiate a logout operation. For more information, see "Logout" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

Changes When Oracle Identity Federation Forwards to the Engine for Logout

The following changes need to be made to the logout service of the authentication or SP engine if it is present:

- The `invokeOSFSLogout` parameter and the `doneUrl` parameters are no longer sent to the engine. In Oracle Identity Federation 11*g*, the engine should always perform an internal forward to the `/fed web context` and `/user/logoutretsso` relative path.

- The `engineId` of the invoked engine is available to the logout service through the http request attribute `oracle.security.fed.authn.engineid`

- The `oracle.security.fed.sessionid` HTTP request attribute can optionally contain the session identifier of the session being logged out.

- In Oracle Identity Federation 11*g*, the logout service should redirect the user to `/fed/user/logoutretsso` after logout rather than to the `/fed/user/logoutsso` URL.

- Specify the `engineId` in the attribute referenced by `oracle.security.fed.authn.engineid` (if the engine is an Authentication Engine) or `oracle.security.fed.sp.engineid` (if the engine is an SP Engine).

6.5.2.4 Deploying the Authentication or SP Engine

You deploy the authentication or SP engine just the same as you deploy any Java EE aplication. For more information, refer to "Deploying Applications" in the *Oracle Fusion Middleware Administrator's Guide*.

6.5.2.5 Creating the Authentication Engine in Oracle Identity Federation 11*g*

To create an authentication engine for Oracle Identity Federation 11*g*:

1. In Oracle Enterprise Manager Fusion Middleware Control, navigate to the Oracle Identity Federation home page.

   For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

2. From the **Oracle Identity Federation** menu, select **Administration**, then **Authentication Engines**.

3. On the Custom Authentication Engines tab, click **Add** to create a new Authentication Engine, and then enter values for the following fields:

   - **Name** – a name for the engine
   - **Enabled** – selected

- **Web Context** – the root context where the engine is deployed

- **Authentication Relative Path** – the relative path to the engine

- **Logout Enabled** – select this check box if the engine needs to perform logout when a logout operation is performed.

- **Logout Relative Path** – the relative path of the engine logout service.

4. Click **Save**.

The Oracle Identity Federation server generates an Engine ID for the new engine. The Engine ID is the value of the `oracle.security.fed.authn.engineid` attribute that the custom engine needs to send to the Oracle Identity Federation server after authenticating the user.

6.5.2.6 Creating the SP Engine in Oracle Identity Federation 11*g*

To create an SP engine for Oracle Identity Federation 11*g*:

1. In Oracle Enterprise Manager Fusion Middleware Control, navigate to the Oracle Identity Federation home page.

For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

2. From the **Oracle Identity Federation** menu, select **Administration**, then **Service Provider Integration Modules**.

3. On the Custom SP Engines tab, click **Add** to create a new Authentication Engine, and then enter values for the following fields:

- **Name** – a name for the engine

- **Enabled** – selected

- **Web Context** – the root context where the engine is deployed

- **Authentication Relative Path** – the relative path to the engine

- **Logout Enabled** – select this check box if the engine needs to perform logout when a logout operation is performed.

- **Logout Relative Path** – the relative path of the engine logout service.

4. Click **Save**.

The Oracle Identity Federation server generates an Engine ID for the new engine. The Engine ID is the value of the `oracle.security.fed.sp.engineid` attribute that the custom engine needs to send to the Oracle Identity Federation server after authenticating the user.

6.5.3 Reconfiguring Oracle Single Sign-On Server After Upgrade to Work with Oracle Identity Federation 11*g*

If you are using Oracle Single Sign-On with Oracle Identity Federation 10*g*, then after you upgrade to Oracle Identity Federation 11*g*, you must reconfigure Oracle Single Sign-On.

This step is necessary because the values required for the `SASSOAuthnUrl` and `SASSOLogoutUrl` properfies have changed for Oracle Identity Federation 11*g*.

For more information, see "Configuring Single Sign-On" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

6.5.4 About Backwards Compatibility for ShareID Service URLs

Oracle Identity Federation 10*g*, as well as SHAREid/COREid Federation 2.x, provided service URLs for its SAML 1.x and WS-Federation protocol support, which were different from the SAML 2.0 and Liberty 1.x service URLs.

These URLs have been modified in the 11g Oracle Identity Federation server for consistency with the SAML 2.0 and Liberty 1.x service URLs. This means that customers upgrading to Oracle Identity Federation 11*g*, who use SAML 1.x or WS-Federation, will need to inform their partner providers of the new single sign-on service URLs.

To ease that transition, Oracle Identity Federation 11*g* provides a separate module that allows backwards compatibility with the SHAREid service URLs. This module is an installable J2EE application that is deployed alongside Oracle Identity Federation, which will handle requests for the ShareID/Oracle Identity Federation 10*g* service URLs and redirect or forward them to the corresponding Oracle Identity Federation 11*g* service URLs.

For information on how to set up this application, see "Setting up Backwards Compatibility for Oracle Identity Federation 10g and ShareID service URLs" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

6.5.5 Upgrading Oracle Identity Federation SSL Configuration

If you are using a shareId keystore for SSL support in Oracle Virtual Directory 10*g*, then the Upgrade Assistant automatically imports the keystore into Oracle Identity Federation 10*g*.

If the SSL identity and trust keystores you use in Oracle Virtual Directory 10*g* are stored in the following location, then there are no additional tasks to perform:

ORACLE_HOME/fed/shareid/oblix/config /keystore

However, if the keystores are stored in any other location, then you must perform the following tasks:

1. Copy the identify and trust keystores to a subdirectory inside the following directory:

    WLS_HOME/user_projects/domains/*domain_name*/servers/*server_name*/stage/OIF

2. Configure Oracle WebLogic Server to point to the new keystore location, as follows:

    a. Log in to the Oracle WebLogic Server Administration Console and select **Environment**, then **Servers**.

    b. Select the server for which you want to set up SSL.

    c. In the Keystores section, select **Custom Identity and Custom Trust**.

    d. In the Identity section, fill in the properties as follows:

    Custom Identity Keystore: *location_of_keystore_containing_SSL_private key_ and_certificate*

    Custom Identity Keystore type: jks

    Custom Identity Keystore Passphrase: *storepassword*

    e. In the Trust section, fill in properties as follows:

Custom Identity Keystore: *location_of_keystore_containing_the_trusted certificate_entries*

Custom Identity Keystore type: jks

Custom Identity Keystore Passphrase: *storepassword*

6.5.6 Setting Oracle Identity Federation System Properties After Upgrade

If you configured Oracle Identity Federation 10*g* by setting system properties, then you will have to manually configure those properties in the upgraded Oracle Identity Federation 11*g* instance. The Upgrade Assistant does not apply these settings to your 11*g* instance.

Table 6–4 lists the system properties that are not upgraded and explains how to set the equivalent properties in Oracle Identity Federation 11*g*. In many cases, the instructions refer to Oracle Enterprise Manager Fusion Middleware Control, the Oracle WebLogic Server Administration Console, or the WebLogic Scripting Tool (WLST), which are used to manage Oracle Fusion Middleware11*g* components.

For more information, see "Overview of Oracle Fusion Middleware Administration Tools" in the *Oracle Fusion Middleware Administrator's Guide*.

Note that these properties are documented in Section 9.3, "Managing Oracle Identity Federation Performance," in the *Oracle Identity Federation Administrator's Guide* for 10*g* (10.1.4.0.1). This document can be found in the Oracle Application Server 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN):

```
http://www.oracle.com/technology/documentation/
```

Table 6–4   Setting Oracle Identity Federation 10g System Properties in Oracle Identity Federation 11g

Oracle Identity Federation 10*g* System Property	How to Set the Property in Oracle Identity Federation 11*g*
-Dhttp.fed.host=*VALUE*	In Fusion Middleware Control, you can set this property as follows: 1. Navigate to the Oracle Identity Federation Home page. 2. From the **Oracle Identity Federation** menu, select **Administration**, then **Server Properties**. 3. Enter a value in the **Maximum SOAP Connection per Server** field.
-Dhttp.fed.max.conn=*VALUE*	In Fusion Middleware Control, you can set this property as follows: 1. Navigate to the Oracle Identity Federation Home page. 2. From the **Oracle Identity Federation** menu, select **Administration**, then **Server Properties**. 3. Enter a value in the **Maximum SOAP Connection** field.

Table 6–4   (Cont.) Setting Oracle Identity Federation 10g System Properties in Oracle Identity Federation

Oracle Identity Federation 10*g* System Property	How to Set the Property in Oracle Identity Federation 11*g*
-Dfed.ldap.ha=[true | false]	In Oracle Identity Federation 10*g*, you used this system property to set one flag for all datastores.
	In 11g you can set this flag seperately for the LDAP user datastore, LDAP federation datastore, and LDAP authentication engine.
	Enter the WLST script environment for the Oracle Identity Federation instance, and set the `ldaphaenabled`, `userldaphaenabled`, or `fedldaphaenabled` property to TRUE as follows:
	To enable this property for the LDAP authentication engine:
	`setConfigProperty('authnengines', 'ldaphaenabled',` `        'true', 'boolean')`
	To enable this for the LDAP user datastore:
	`setConfigProperty('datastore', 'userldaphaenabled',` `        'true', 'boolean')`
	For enabling this for LDAP federation datastore:
	`setConfigProperty('datastore', 'fedldaphaenabled',` `        'true', 'boolean')`
-Dfed.jdbc.min.conn=*VALUE* -Dfed.jdbc.max.conn=*VALUE* -Dfed.jdbc.max.usage=*VALUE*	Use the Oracle WebLogic Server Administration Console to set the appropriate values on the JDBC data source that you are using for your Oracle Identity Federation 11*g* datastores or authentication engines.

6.5.7 Additional Oracle Identity Federation Post-Upgrade Tasks

The following additional post-upgrade tasks should be performed after upgrading to Oracle Identity Federation 11*g*, in addition to those described in the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*:

- If you are have configured Oracle Identity Federation 10*g* to use the SAML 1.x/WS-FED protocol, then after you upgrade to Oracle Identity Federation 11*g*, you must set a default single sign-on identity provider.

    For more information, see "Configuring Service Providers" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

- Export the Identity Provider self-signed certificate to the service provider

    The procedure you use to perform this task varies, depending on whether your service provider is a 10*g* or 11*g* service provider:

    – If you are using a 10*g* service provider, then refer to "Exporting the IdP's self-signed certificate to the SP" in the *Oracle Identity Federation Administrator's Guide* in the Oracle Application Server 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN):

        `http://www.oracle.com/technology/documentation/`

    – If you are using an 11*g* service provider, then refer to "Set Up Single Sign-On for SAML 1.x and WS-Federation" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

- If you are using an 11*g* Identity Provider and a 10*g* service provider, and you are using the SAML 1.x/WS-FED protocol, then you configure the 10g service provider.

Specifically, for the 10*g* service provider, you must change the "Signing Certificate Subject DN" and "Signing Certificate Issuer DN" to 11g IdP format, which is of the form "CN=<host> Signing Certificate".

For more information, see "Configure This Domain as a Source/Identity Provider" in the *Oracle Identity Federation Administrator's Guide* in the Oracle Application Server 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN).

■ Enable "Send Signed Assertion" in Oracle Identity Federation 10*g*, or disable "Require Signed Assertions" in Oracle Identity Federation 11*g*.

This task is necessary because in 10g, signed assertions are disabled by default, and in 11*g*, signed assertions are enabled by default.

Depending whether you perform this task in 10*g* or 11*g*, refer to one the following:

– "Configuring Service Providers" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

– Section 6.5.5, "Add Assertion Profile" in the *Oracle Identity Federation Administrator's Guide* in the Oracle Application Server 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN).

6.6 Task 6: Verify that the Oracle Identity Federation Upgrade Was Successful

To verify that your Oracle Internet Directory and Oracle Directory Integration Platform upgrade was successful:

1. Run the Upgrade Assistant again and select **Verify Instance** on the Specify Operation page.

    Follow the instructions on the screen for information on how to verify that specific Oracle Fusion Middleware components are up and running.

2. Use the following URL to verify that Oracle Identity Federation 11*g* is up and running:

    ```
    http://<host>:<port>/fed/sp/metadata
    ```

    For example:

    ```
    http://host42.exmaple.com:7001/fed/sp/metadata
    ```

    Alternatively, you can use Fusion Middleware Control to verify that Oracle Identity Federation and any other Oracle Identity Management components are up and running in the Oracle Fusion Middleware environment.

    For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

Part III

Upgrading Oracle Identity Management High Availability Environments

Part II contains the following chapters:

7

Upgrading Oracle Internet Directory High Availability Environments

This chapter describe how to upgrade Oracle Internet Directory high availability environments that were supported in Oracle Application Server 10*g* Release 2 (10.1.2) and 10*g* (10.1.4).

This chapter contains the following sections:

- Summary of Oracle Internet Directory High Availability Upgrade Starting Points
- Before You Begin Upgrading Your Oracle Identity Management High Availability Environment
- Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a High Availability Environment
- Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a Colocated High Availability Environment
- Upgrading Oracle Internet Directory Only

7.1 Summary of Oracle Internet Directory High Availability Upgrade Starting Points

The following high availability topologies are supported for upgrade from Oracle Identity Management 10*g* Release 2 (10.1.2) and 10*g* (10.1.4):

- High Availability Topologies Based on a Distributed Identity Management Environment
- High Availability Topologies Based on a Colocated Identity Management Environment
- High Availability Environments Based on Standalone Oracle Internet Directory Instances

7.1.1 High Availability Topologies Based on a Distributed Identity Management Environment

This type of topology is based on the Oracle Internet Directory and Oracle Directory Integration Platform components when they are installed on a separate host from Oracle Single Sign-On and Oracle Delegated Administration Services.

This was the recommended topology for high availability environments in Oracle Application Server 10*g*. It is sometimes referred to as a distributed Oracle Identity Management environment or a non-colocated Identity Management environment.

Refer to Section 3.2.2, "Upgrading a Non-Colocated Identity Management Environment" for a description the single-node variant of a non-colocated Identify Management high availability environment.

7.1.2 High Availability Topologies Based on a Colocated Identity Management Environment

This type of topology is based on the Oracle Internet Directory and Oracle Directory Integration Platform components when they are installed and configured in the same Oracle home as Oracle Single Sign-On and Oracle Delegated Administration Services.

This type of environment is referred to as a colocated Identity Management environment. For more information, refer to Section 3.2.1, "Upgrading a Colocated Identity Management Environment" for a description of a single-node variant of a colocated Identity Management high availability environment.

Because Oracle Single Sign-On and Oracle Delegated Administration Services are not available in Oracle Fusion Middleware 11*g*, the upgrade of this topology requires some additional steps.

7.1.3 High Availability Environments Based on Standalone Oracle Internet Directory Instances

This type of topology is based on Oracle Internet Directory when it is upgraded without an associated Oracle Directory Integration Platform instance.

This Oracle Internet Directory topology can be upgraded and associated with a local Oracle WebLogic Server domain, an existing remote domain, or with no Oracle WebLogic Server domain.

For more information, see Section 4.3.2.1, "When is Oracle WebLogic Server Required?".

7.2 Before You Begin Upgrading Your Oracle Identity Management High Availability Environment

Before you begin using the procedures in this chapter, note the following:

- Conventions Used in This Chapter
- Prerequisites for Oracle Identity Management High Availability Upgrade
- Supported High Availability Environments for Upgrade
- Reducing Downtime During Upgrade With Directory Replication

7.2.1 Conventions Used in This Chapter

The procedures in this chapter typically involve two host computers. For the purposes of the examples in this chapter, the two hosts are referred to as IDMHOST1 and IDMHOST2.

Some of the examples in this chapter provide the commands required to perform particular tasks on a UNIX system. The commands for Windows are similar, but you would replace the environment variables with the Windows equivalent (for example, `%ORACLE_HOME%`).

7.2.2 Prerequisites for Oracle Identity Management High Availability Upgrade

Before you begin the upgrade procedures in this chapter, be sure the following prerequisites have been met.

Oracle Identity Management 10*g* Components Are Installed and Running on IDMHOST1

It is assumed that the Oracle Identity Management 10*g* components you are about to upgrade are installed and running on IDMHOST1. This is important because the Oracle Identity Management 11*g* components that you are upgrading must be installed on the same host as the Oracle Identity Management 10*g* components.

All Other Oracle Application Server 10*g* Instances That Use the Same Metadata Repository Are Stopped

Before you begin the upgrade, stop all the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* instances, except the instances that you are about to upgrade.

In addition, stop all the Oracle Application Server 10*g* instances that share the same OracleAS Metadata Repository as the Oracle Internet Directory instance you are about to upgrade. For example, if you have any Oracle Portal 10*g* or other Oracle Identity Management 10*g* instances running, be sure to stop those instances as well. This will ensure that no other Oracle Application Server components are accessing the repository during the upgrade.

All Instances of Oracle Enterprise Manager Are Stopped

Before you begin any of the high availability procedures documented in this chapter, be sure to stop all instances of Oracle Enterprise Manager that are managing the Oracle Internet Directory instances you are about to upgrade.

This step is important because Oracle Enterprise Manager Application Server Control sometimes accesses the Oracle Internet Directory schema (the ODS schema) when it monitors and configures the Oracle Internet Directory target. To avoid any possibility of conflict when you are upgrading the Oracle Internet Directory middle tier and schema, it is important to stop all instances of Oracle Enterprise Manager during the upgrade proces.

For information on stopping and starting Application Server Control, refer to the *Oracle Application Server Administrator's Guide* in the Oracle Application Server 10*g* documentation library.

Load Balancer Is Configured to Route Only to Primary Instance

Before you begin the upgrade, make sure the load balancer virtual servers are routing requests only to the primary instance of the OracleAS Cluster (Identity Management) node.

The primary instance of the OracleAS Cluster is the first node where you installed Oracle Internet Directory.

Any Modifications to ias.properties Have Been Removed

If you have modified the `ias.properties` file in the Oracle Identity Management Oracle home to redefine port values, then you must update the ias.properties file with the actual, physical port values for each OID instance before upgrade.

Some organizations modify the `ias.properties` file, for example, to reference specific load balancer ports. If you performed such a customization, be sure to restore

the `ias.properties` to its original state so it references the physical ports of the Oracle Internet Directory instances in your environment.

The Current Version of the Database is Supported by Oracle Fusion Middleware 11*g*

The procedures in this chapter assume you are storing the Oracle Internet Directory schema (the ODS schema) in a Real Application Clusters (RAC) database that has been upgraded to a database version supported by Oracle Fusion Middleware 11*g*.

For more information database requirements for upgrade, as well as additional upgrade information for Oracle Fusion Middleware 11*g*, see the *Oracle Fusion Middleware Upgrade Planning Guide*.

7.2.3 Supported High Availability Environments for Upgrade

This chapter describe how to upgrade Oracle Internet Directory high availability environments that were supported in Oracle Application Server 10*g* Release 2 (10.1.2) and 10*g* (10.1.4).

High Availabilty Configurations for Administration Tools

This chapter does not provide information on configuring the administration tools (such as Oracle WebLogic Server Administration Console, Oracle Enterprise Manager Fusion Middleware Control, or Oracle Directory Services Manager) for high availability.

Additional Resources

For information about the supported high availability topologies in Oracle Fusion Middleware 11*g*, see the *Oracle Fusion Middleware High Availability Guide*.

Before you begin these procedures, review the procedures and prerequisites available in Chapter 4, "Upgrading Your Oracle Internet Directory Environment".

7.2.4 Reducing Downtime During Upgrade With Directory Replication

The procedures in this chapter assume your organization can support a limited amount of Identity Management downtime.

If your organization has no tolerance for Identity Management downtime, consider the following approach to the upgrade process:

1. Configure your existing Oracle Identity Management 10*g* environment using Oracle Internet Directory Advanced Replication.

2. Use the upgrade procedures in Section 9.3.2, "Upgrading One Replica at a Time".

When you implement Oracle Internet Directory Advanced Replication, you can route client traffic to one replica while upgrading the other replica. The result is an upgrade procedure that requires little or no downtime while each replica is upgraded.

For more information about using Oracle Internet Directory replication, refer to the following sections in the Oracle Internet Directory Administrator's Guide in the 10*g* (10.1.4) documentation library on the Oracle Technology Network (OTN):

■ "Oracle Internet Directory Replication Concepts"

■ "Oracle Internet Directory Replication Installation and Configuration"

The Oracle Identity Management 10*g* (10.1.4) documentation library is available on OTN at the following URL:

```
http://www.oracle.com/technology/documenation/
```

7.3 Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a High Availability Environment

Perform the following tasks to upgrade an Oracle Internet Directory and Oracle Directory Integration Platform high availability environment when when both components are installed on a separate host from Oracle Single Sign-On and Oracle Delegated Administration Services:

- Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

- Task 2: On IDMHOST1, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform and Create the Oracle WebLogic Server Cluster

- Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11g

- Task 4: On IDMHOST1, Configure Oracle Directory Integration Platform to Use the Oracle Internet Directory Virtual Host

- Task 5: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

- Task 6: On IDMHOST2, Install Oracle WebLogic Server and Create the Middleware Home

- Task 7: On IDMHOST2, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform

- Task 8: Copy the Oracle Directory Integration Platform Directory from IDMHOST1 to IDMHOST2

- Task 9: On IDMHOST2, Set the Anonymous Bind Property to Allow

- Task 10: Start the Managed Server on IDMHOST2

- Task 11: Verify That the Components Are Up and Running on IDMHOST2

7.3.1 Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

7.3.2 Task 2: On IDMHOST1, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform and Create the Oracle WebLogic Server Cluster

For complete instructions for installing and configuring the Oracle Identity Management 11*g* components, including all the prerequisites and system requirements, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

The instructions provided here outline the key installation steps required when installing Oracle Internet Directory and Oracle Directory Integration Platform in preparation for an upgrade of your high availability environment.

To install and configure Oracle Internet Directory and Oracle Directory Integration Platform 11*g* on IDMHOST1:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network (OTN):

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the `setup.exe` file.

4. Refer to Table 7–1 for specific instructions about how to respond to each screen in the Oracle Identity Management installation and configuration tool.

   For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

Table 7–1   Summary of Screens for Installing and Configuring Oracle Internet Directory and Oracle Directory Integration Platform on IDMHOST1

Screen	Instructions
Welcome	Click **Next**.
Select Installation Type	Select **Install and Configure**. Click **Next**.
Prerequisite Checks	Click **Next**.
Select Domain	Select **Create New Domain** and enter the domain details. For the purposes of this exercise, enter IDMDomain in the **Domain Name** field. Click **Next**.

Table 7–1   (Cont.) Summary of Screens for Installing and Configuring Oracle Internet Directory and Oracle Directory Integration Platform on IDMHOST1

Screen	Instructions
Specify Installation Location	Specify the following values: ■ **Middleware Home Location:** Enter the complete path to the Middleware home you created in "Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home". ■ **Oracle Home Directory:** For the purposes of this example, enter `idm` as the name of the Oracle home directory. ■ **WebLogic Server Directory:** This is usually the `wlserver_10.3` inside the Middleware home. ■ **Oracle Instance Location:** Enter a path for the Oracle instance. This directory can be any acccessible directory location; unlike the Oracle home, it does not need to be inside the Middleware home. ■ **Oracle Instance Name:** For the purposes of this example, enter `idm_instance1.`
Specify Email for Security Updates	Specify the following values: ■ **Email Address:** Provide the email address for your My Oracle Support (formerly Oracle*MetaLink*) account. You can register for My Oracle Support at the following URL: `http://metalink.oracle.com/` ■ **Oracle Support Password:** Provide the password for your My Oracle Support account. ■ **I wish to receive security updates via My Oracle Support**: Select this check box.
Configure Components	Select the following components: ■ **Oracle Internet Directory** ■ **Oracle Directory Integration Platform** ■ **Oracle Directory Services Manager** Selected the **Clustered** check box.
Configure Ports	Select **Auto Port Configuration**. Click **Next**.
Specify Schema Database	Select **Use Existing Schema**. In the **Connect String** field, enter the connect string to each nodes in the Real Application Clusters (RAC) database. Separate each node with a carot symbol (^). For example: `INFRADBHOST1.MYCOMPANY.COM:1521:IDMDB1^INFRADBHOST2.MYCOMPANY.com:1521:IDMDB2@IDMEDG.MYCOMPANY.COM` Enter the ODS schema password in the **Password** field. Note that the ODS schema is used by Oracle Internet Directory. By default, the password for the ODS schema is the `ias_admin` password you provided when you installed Oracle Internet Directory 10*g*. However, the password might have been changed using the `oidpasswd` utility, which is documented in the Oracle Identity Management 10*g* User Reference. Click **Next**.
Upgrade Scenario Detected Warning dialog box	Click **Yes**.
OID Password	Enter the Administrator password for Oracle Internet Directory instance.

Table 7–1 (Cont.) Summary of Screens for Installing and Configuring Oracle Internet Directory and Oracle Directory Integration Platform on IDMHOST1

Screen	Instructions
Installation Summary	Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.
Installation Progress	On UNIX systems, a dialog appears, prompting you to run the `oracleRoot.sh` script.
	Open a window and run the script, following the prompts in the window.
	Click **OK**.
Configuration	Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the Installation Complete screen appears.
	Click **Finish**, and then confirm your choice to exit.

7.3.3 Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11*g*

Use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* instances on IDMHOST1 to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Click **Next** to display the Select Operation screen.

4. Select **Upgrade Identity Management Instance** on the Select Operation screen.

5. Refer to Table 7–2 for a description of the Upgrade Assistant screens that require input from you during an Oracle Internet Directory and Oracle Directory Integration Platform upgrade.

6. After the Target Database Details screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

> **See Also:** "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

- Displays the End of Upgrade screen, which confirms that the upgrade was complete.

7. Exit the Upgrade Assistant.

Table 7–2   Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* Release 2 (10.1.2) or 10*g* (10.1.4) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the 11*g* Oracle instance, or click **Browse** to locate the instance directory.
Specify WebLogic Server	Enter the host and Administration Server port for the Oracle WebLogic Server you configured in "Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home".
	Note this information is required if you are upgrading Oracle Directory Integration Platform. It is also required if you associated your Oracle Internet Directory 11*g* installation with Oracle WebLogic Server.
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.

Table 7–2   (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Upgrade Options	Select the upgrade options you want to apply to the Oracle Identity Management upgrade: ■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance. Note if you select this option, you will not be able to run both the 10*g* and 11*g* middle tiers at the same time; otherwise, port conflicts will occur. ■ **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade. Click **Help** to display more information about the upgrade options on this screen.
Specify OID Details	Use this screen to enter the details required to connect to the Oracle Internet Directory 10*g* instance, including the physical host and the password to the Oracle Internet Directory super user account (`cn=orcladmin`). For more information, click **Help**.
Specify Database Details	Use this screen to enter the details required to connect to the database where the Oracle Identity Management schemas reside, including the host, service name, port, and SYS password for the database. Note the following important information about this screen: ■ You must enter the password for the ODS schema password. The default ODS password is the same as the Oracle Application Server administrator password, but this password can be changed after installation, using the OID Database Password Utility. ■ The instructions for identifying a Real Application Clusters (RAC) database are different, depending upon whether you are identifying the RAC database that contains the Oracle Internet Directory (ODS) schema or a RAC database that is being used for Oracle Directory Integration Platform. For more information, see Section 4.4.3.2, "About Specifying Real Application Clusters (RAC) Database Details on the Specify Database Details Screen".
Root action required screen	This is only if you are using privileged port on a UNIX system. A configuration script needs to be run as root before upgrade can proceed. Leaving this window open, open another window, and run the `upgroot.sh` file as root: When the script has completed, return to the Upgrade Assistant and click **OK**.

7.3.4 Task 4: On IDMHOST1, Configure Oracle Directory Integration Platform to Use the Oracle Internet Directory Virtual Host

After you upgrade the Oracle Internet Directory and Oracle Directory Integration Platform instances to 11*g*, update the `dip-config.xml` file so it references the Oracle Internet Directory Virtual Host Name (for example, `oid.mycompany.com`), which is associated with the load balancer that is directing traffic to your Oracle Internet Directory instances.

If the load balancer/virtual host has a different port value than the Oracle Internet Directory physical port value, then you must also change the port.

This task is accomplished using the `manageDIPServerConfig` command, as described in the following procedure.

Use the following procedure perform this step on IDMHOST1:

1. Make a backup of the `dip-config.xml` file, which is located under the following directory:

   ```
   MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers
         /wls_ods1/applications/DIP_11.1.1.2.0/configuration/
   ```

2. Set the ORACLE_HOME environment variable to the directory where you installed the Identity Management binaries.

   For example:

   ```
   export ORACLE_HOME=/u01/app/oracle/product/11g/mw_home/idm
   ```

3. Set the WLS_HOME environment variable to the directory where you installed the WebLogic Server. For example:

   ```
   export WLS_HOME=/u01/app/oracle/product/11g/fmw_home/wlserver_10.3
   ```

4. Run the following command to update the value of the Oracle Internet Directory host and port:

   ```
   ORACLE_HOME/bin/manageDIPServerConfig set
        -h hostName
        -p port -D wlsuser
        -attr oidhostport
        -val OIDVIRTUALHOSTNAME:PORT
   ```

   For example, on IDMHOST1, the command and output are shown below:

   ```
   ORACLE_HOME/bin/manageDIPServerConfig set
        -h idmhost1.mycompany.com
        -p 7005
        -D weblogic
        -attr oidhostport
        val oid.mycompany.com:636

        [Weblogic user password]
        Connection parameters initialized.
        Connecting at idmhost1.mycompany.com:7005, with userid "weblogic"..
        Connected successfully

        The attribute oidhostport is successfully changed to value
        oid.mycompany.com:636
   ```

5. Using the WebLogic Server Administration Console, stop and start the `wls_ods1` managed server.

7.3.5 Task 5: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Step 1 Verify the Oracle Internet Directory is up and running
Use the following OPMN command to verify that Oracle Internet Directory is up and running:

```
ORACLE_INSTANCE/opmnctl status
```

The output of the command should be similar to the following example:

```
Processes in Instance: oid_instance1
-------------------------------+-------------------+---------+---------
ias-component                  | process-type      |     pid | status
-------------------------------+-------------------+---------+---------
oid1                           | oidldapd          |   31394 | Alive
oid1                           | oidldapd          |   31392 | Alive
oid1                           | oidmon            |   31384 | Alive
```

Use the `ldapbind` command-line tool to ensure that you can connect to each Oracle Internet Directory instance and the LDAP Virtual Server. The `ldapbind` tool enables you to determine whether you can authenticate a client to a server.

For non-SSL:

```
ldapbind -h idmhost1.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h idmhost2.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h oid.mycompany.com -p 389 -D "cn=orcladmin" -q
```

For SSL:

```
ldapbind -h idmhost1.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h idmhost2.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h oid.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

where:

- U = SSL authentication mode
- 1 = No authentication required
- 2 = One way authentication required. With this option, you must also supply a wallet location (`-W "file:/home/my_dir/my_wallet"`) and wallet password (`-P wallet_password`).
- 3 = Two way authentication required. With this option, you must also supply a wallet location (`-W "file:/home/my_dir/my_wallet"`) and wallet password (`-P wallet_password`).

Step 2 Verify the Oracle Directory Integration Platform is up and running
Validate the Oracle Directory Integration Platform installation by using the WLST dipStatus command. To run this command, follow these steps:

1. Set the ORACLE_HOME environment variable to the directory where you installed the Identity Management binaries. For example:

   ```
   export ORACLE_HOME=/u01/app/oracle/product/11g/fmw_home/ods
   ```

2. Set the WLS_HOME environment variable to the directory where you installed the WebLogic Server.

   For example:

```
export WLS_HOME=/u01/app/oracle/product/11g/fmw_home/wlserver_10.3
```

3. Run the following command:

```
$ORACLE_HOME/bin/dipStatus -h <hostName> -p <port> -D <wlsuser>
```

For example, on IDMHOST1, the command and successful output are shown below:

```
$ORACLE_HOME/bin/dipStatus
    -h idmhost1.mycompany.com
    -p 7005
    -D weblogic
    [Weblogic user password]
     Connection parameters initialized.
     Connecting at idmhost1.mycompany.com:7005, with userid "weblogic"..
     Connected successfully.
     ODIP Application is active at this host and port.
```

Step 3 Verify Oracle Directory Services Manager (ODSM)

Verify the Oracle Directory Services Manager installation by bringing up the ODSM Administration Console in a web browser.

The URL to access the ODSM Administration Console is:

```
http://hostname.mycompany.com:<port>/odsm/faces/odsm.jspx
```

For example, on IDMHOST1, enter this URL:

```
http://idmhost1.us.oracle.com:7005/odsm/faces/odsm.jspx
```

7.3.6 Task 6: On IDMHOST2, Install Oracle WebLogic Server and Create the Middleware Home

Before you can expand the Oracle WebLogic Server cluster you created on IDMHOST1 to include IDMHOST2, you must install the Oracle WebLogic Server binary files on IDMHOST2 and create Middleware home on IDMHOST2.

> **Note:**   When installing the Middleware home for the second (and any subsequent) Oracle Internet Directory installations, you must specify a path for the Middleware home that is identical to the first Oracle Internet Directory.
>
> For example, suppose you are using the Linux operating system and you installed the first Oracle Internet Directory in a Middleware home in the following directory on IDMHOST1:
>
> ```
> /dua1/Oracle/Middleware/
> ```
>
> When you are prompted for the Middleware home on IDMHOST2, you must enter the identical path specification.

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

7.3.7 Task 7: On IDMHOST2, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform

To install and configure Oracle Internet Directory and Oracle Directory Integration Platform 11*g* on IDMHOST1:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Prepare a `staticports.ini` file that will be used during the installation to configure the ports for the Oracle Internet Directory instance on IDMHOST2.

   This step will ensure that the two Oracle Internet Directory instances on IDMHOST1 and IDMHOST2 use the same ports:

   a. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a temporary directory.

   b. Edit the `staticports.ini` file you copied to the temporary directory to assign the following custom ports (uncomment the lines where you specify the port numbers for Oracle Internet Directory):

   ```
   # The non-SSL port for Oracle Internet Directory
   Oracle Internet Directory port = oid_port_on_IDMHOST1
   # The SSL port for Oracle Internet Directory
   Oracle Internet Directory (SSL) port = oid_ssl_port_on_IDMHOST1
   ```

   In this example, replace *oid_port_on_IDMHOST1* with the listening port of the Oracle Internet Directory instance you installed and upgraded on IDMHOST1.

   Replace *oid_ssl_port_on_IDMHOST1* with SSL port of the Oracle Internet Directory instance you installed and updated on IDMHOST1.

   c. Make a note of the path to this modified `staticports.ini` file; you will need to enter it on the Configure Ports page of the Oracle Identity Management installer.

4. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the `setup.exe` file.

5. Refer to Table 7–3 for specific instructions about how to respond to each screen in the Oracle Identity Management installation and configuration tool.

   For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

6. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

Table 7–3   Summary of Screens for Installing and Configuring Oracle Internet Directory and Oracle Directory Integration Platform on IDMHOST2

Screen	Instructions
Welcome	Click **Next**.
Select Installation Type	Select **Install and Configure**. Click **Next**.
Prerequisite Checks	Click **Next**.
Select Domain	Select **Expand Cluster** and enter the domain details. Enter the host, port, user name, and password for the administration server in the domain you created on IDMHOST1 in "Task 2: On IDMHOST1, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform and Create the Oracle WebLogic Server Cluster". Click **Next**.

Specify Installation Location	Specify the following values:
	■ **Middleware Home Location:** Enter a location for the Middleware home on IDMHOST2.
	   Important Note: This location must be identical to the Middleware home path on IDMHOST1.
	■ **Oracle Home Directory:** For the purposes of this example, enter `idm` as the name of the Oracle home directory.
	   Important Note: This directory name must be identical to the Oracle home directory name on IDMHOST1.
	■ **WebLogic Server Directory:** This is usually the `wlserver_10.3` inside the Middleware home.
	■ **Oracle Instance Location:** Enter a path for the Oracle instance. This directory can be any acccessible directory location; unlike the Oracle home, it does not need to be inside the Middleware home.
	■ **Oracle Instance Name:** For the purposes of this example, enter `idm_instance2`.
	   Important Note: The instance name must be unique and cannot be the same as any other instance name in the cluster.

Specify Email for Security Updates	Specify the following values: ■ **Email Address:** Provide the email address for your My Oracle Support (formerly Oracle*MetaLink*) account. You can register for My Oracle Support at the following URL: `http://metalink.oracle.com/` ■ **Oracle Support Password:** Provide the password for your My Oracle Support account. ■ **I wish to receive security updates via My Oracle Support**: Select this check box.
Configure Components	Select the following components: ■ **Oracle Internet Directory** ■ **Oracle Directory Integration Platform** ■ **Oracle Directory Services Manager** Selected the **Clustered** check box.
Configure Ports	Select **Specify Ports Using Configuration File** and enter the filename for the `staticports.ini` file that you copied to the temporary directory earlier in this procedure.

Table 7–3   (Cont.) Summary of Screens for Installing and Configuring Oracle Internet Directory and Oracle Directory Integration Platform on IDMHOST2

Screen	Instructions
Specify Schema Database	Select **Use Existing Schema**. In the **Connect String** field, enter the connect string to each nodes in the Real Application Clusters (RAC) database. Separate each node with a carot symbol (^). For example: `INFRADBHOST1.MYCOMPANY.COM:1521:IDMDB1^INFRADBHOST2.MYCOMPANY.com:1521:IDMDB2@IDMEDG.MYCOMPANY.COM` Enter the ODS schema password in the **Password** field. Note that the ODS schema is used by Oracle Internet Directory. By default, the password for the ODS schema is the `ias_admin` password you provided when you installed Oracle Internet Directory 10*g*. However, the password might have been changed using the `oidpasswd` utility, which is documented in the Oracle Identity Management 10*g* User Reference. Click **Next**.
ODS Schema In Use	This warning indicates that you are selecting an ODS schema that is already being used by an Oracle Internet Directory instance. In fact, in a high availability environment, you want the two Oracle Internet Directory instances to share the same schema. This prompt verifies that you have selected the correct schema. Click **Yes** to continue.
System Time warning dialog box	When you are using the same ODS schema for multiple Oracle Internet Directory instances, the installer displays this dialog box (Figure 7–1) to warn you that the system time on each system that is sharing the same schema must be synchronized. Various third-party tools are available to help you synchronize clocks across clustered systems, including the Network Time Protocol (NTP), which is a commonly-used tool for synchronizing system clocks. The following URL provides information on NTP and system time synchronization: `http://www.ntp.org/`
OID Password	Enter the Administrator password for Oracle Internet Directory instance.
Installation Summary	Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.
Installation Progress	On UNIX systems, a dialog appears, prompting you to run the `oracleRoot.sh` script. Open a window and run the script, following the prompts in the window. Click **OK**.
Configuration	Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the Installation Complete screen appears. Click **Finish**, and then confirm your choice to exit.

Figure 7–1   System Time Warning When Installing Second Oracle Internet Directory Instance Against the Same ODS Schema

7.3.8 Task 8: Copy the Oracle Directory Integration Platform Directory from IDMHOST1 to IDMHOST2

The Oracle Directory Integration Platform application is deployed on IDMHOST1 as an externally staged application. The application must be copied from IDMHOST1 to IDMHOST2; otherwise, the managed server on IDMHOST2 is listed in the Oracle WebLogic Server administration console as being in an "unknown" state:

1. Locate the `applications` directory in the Oracle WebLogic Server domain directory on IDMHOST1:

    ```
    MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers
            /wls_ods1/applications
    ```

2. Copy the `applications` directory on and its contents on IDMHOST1 to the same location in the domain directory on IDMHOST2.

    For example:

    ```
    scp -rp MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers
                /wls_ods1/applications
        user@IDMHOST2:MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig
                /servers/wls_ods2/applications
    ```

7.3.9 Task 9: On IDMHOST2, Set the Anonymous Bind Property to Allow

After you install and configure the second Oracle Internet Directory instance on IDMHOST2, you mustset the the "Anonymous Bind" server property to "allow," so it matches the first, upgraded Oracle Internet Directoryinstance on IDMHOST1.

This property allows the Oracle Single Sign-On 10*g* and Oracle Delegated Administration Services 10*g* (specifically, OC4J_Security) to correctly use the second

Oracle Internet Directory instance on IDMHOST2. Without this alteration to the second Oracle Internet Directory, the OC4J_Security instance on IDMHOST2 will not start.

To modify the anonymous bind property with Oracle Enterprise Manager Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

2. Navigate to the home page of the Oracle Internet Directory instance on IDMHOST2.

3. From the **Oracle Internet Directory** menu, select **Administration**, and then **Server Properties**.

4. Select **Allows** from the **Anonymous Bind** drop-down menu.

5. Click Apply

6. Start Oracle Single Sign-On as you normally would.

7.3.10 Task 10: Start the Managed Server on IDMHOST2

Follow these steps to start the wls_ods2 managed server in a cluster:

1. Open a browser and navigate to the WebLogic Administration Console at:

   ```
   http://idmhost1.mycompany.com:port/console
   ```

2. Login to the WebLogic Administration Console using the administrator credentials.

3. In the left pane of the WebLogic Administration Console, expand Environment and select Clusters.

4. Select the cluster (`cluster_ods`) containing the managed server (wls_ods2) you want to start.

5. Select **Control**.

6. Under Managed Server Instances in this Cluster, select the check box next to the managed server (`wls_ods2`) you want to start and click **Start**.

7. On the Server Life Cycle Assistant page, click **Yes** to confirm.

> **Note:** Node Manager starts the server on the target machine. When the Node Manager finishes its start sequence, the server's state is indicated in the **State** column in the Server Status table.

7.3.11 Task 11: Verify That the Components Are Up and Running on IDMHOST2

Use the procedure documented in "Task 5: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade" to verify the Oracle Internet Directory, Oracle Directory Integration Platform, and Oracle Directory Services Manager components on IDMHOST2.

7.4 Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a Colocated High Availability Environment

The procedure for upgrading an Oracle Internet Directory high availability enviroment based on colocated Oracle Identity Management components is similar to the

procedure described in Section 7.3, "Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a High Availability Environment".

However, there are additional steps required when upgrading this specific topology. Specifically, after you upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11*g*, you must then disable Oracle Internet Directory and Oracle Directory Integration Platform in the Oracle Application Server 10*g* Oracle home.

Perform the following tasks to upgrade an Oracle Internet Directory and Oracle Directory Integration Platform high availability environment when when both components are installed on a separate host from Oracle Single Sign-On and Oracle Delegated Administration Services:

- Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

- Task 2: On IDMHOST1, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform and Create the Oracle WebLogic Server Cluster

- Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11g

- Task 4: On IDMHOST1, Configure Oracle Directory Integration Platform to Use the Oracle Internet Directory Virtual Host

- Task 5: On IDMHOST1, Disable Oracle Internet Directory and Oracle Directory Integration Platform in the 10g Oracle Home

- Task 6: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

- Task 7: On IDMHOST2, Install Oracle WebLogic Server and Create the Middleware Home

- Task 8: On IDMHOST2, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform

- Task 9: Copy the Oracle Directory Integration Platform Directory from IDMHOST1 to IDMHOST2

- Task 10: On IDMHOST2, Set the Anonymous Bind Property to Allow

- Task 11: On IDMHOST2, Disable Oracle Internet Directory and Oracle Directory Integration Platform in the 10g Oracle Home

- Task 12: Start the Managed Server on IDMHOST2

- Task 13: Verify That the Components Are Up and Running on IDMHOST2

7.4.1 Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

7.4.2 Task 2: On IDMHOST1, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform and Create the Oracle WebLogic Server Cluster

To install and configure Oracle Internet Directory and Oracle Directory Integration Platform 11*g* on IDMHOST1:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the `setup.exe` file.

4. Refer to Table 7–1 for specific instructions about how to respond to each screen in the Oracle Identity Management installation and configuration tool.

   For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Internet Directory installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

7.4.3 Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11*g*

Use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* instances on IDMHOST1 to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Click **Next** to display the Select Operation screen.

4. Select **Upgrade Identity Management Instance** on the Select Operation screen.

5. Refer to Table 7–2 for a description of the Upgrade Assistant screens that require input from you during an Oracle Internet Directory and Oracle Directory Integration Platform upgrade.

6. After the Target Database Details screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

     See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

   - Displays the End of Upgrade screen, which confirms that the upgrade was complete.

7. Exit the Upgrade Assistant.

7.4.4 Task 4: On IDMHOST1, Configure Oracle Directory Integration Platform to Use the Oracle Internet Directory Virtual Host

After you upgrade the Oracle Internet Directory and Oracle Directory Integration Platform instances to 11*g*, update the `dip-config.xml` file so it references the Oracle Internet Directory Virtual Host Name (for example, `oid.mycompany.com`). This can be done using the `manageDIPServerConfig` command.

Refer to Section 7.3.4, "Task 4: On IDMHOST1, Configure Oracle Directory Integration Platform to Use the Oracle Internet Directory Virtual Host" for specific instructions for this task.

7.4.5 Task 5: On IDMHOST1, Disable Oracle Internet Directory and Oracle Directory Integration Platform in the 10*g* Oracle Home

After you upgrade the Oracle Internet Directory and Oracle Directory Integration Platform components on IDMHOST1, you cannot start Oracle Internet Directory or use the Oracle Single Sign-On 10*g* component until you disassociate Oracle Internet Directory from the Oracle Single Sign-On and Oracle Delegated Administration Services components in the 10*g* Oracle home.

For specific instructions for performing this task, see the following:

- Section 4.5.2, "Disabling the Oracle Internet Directory and Oracle Directory Integration Platform 10g Components"

- Section 4.5.6, "Removing Oracle Internet Directory and Oracle Directory Integration Platform 10g from Application Server Control"

7.4.6 Task 6: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Use the procedure documented in "Task 5: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade" to verify the Oracle Internet Directory, Oracle Directory Integration Platform, and Oracle Directory Services Manager components on IDMHOST2.

7.4.7 Task 7: On IDMHOST2, Install Oracle WebLogic Server and Create the Middleware Home

Before you can expand the Oracle WebLogic Server cluster you created on IDMHOST1 to include IDMHOST2, you must install the Oracle WebLogic Server binary files on IDMHOST2 and create Middleware home on IDMHOST2.

> **Note:** When installing the Middleware home for the second (and any subsequent) Oracle Internet Directory installations, you must specify a path for the Middleware home that is identical to the first Oracle Internet Directory.
>
> For example, suppose you are using the Linux operating system and you installed the first Oracle Internet Directory in a Middleware home in the following directory on IDMHOST1:
>
> `/dua1/Oracle/Middleware/`
>
> When you are prompted for the Middleware home on IDMHOST2, you must enter the identical path specification.

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

7.4.8 Task 8: On IDMHOST2, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform

To install and configure Oracle Internet Directory and Oracle Directory Integration Platform 11*g* on IDMHOST1:

1. Locate the Oracle Identity Management CD–ROM.

    Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

    `http://www.oracle.com/technology/`

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

    Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

On UNIX systems, enter the following command to install Repository Creation Utility:

```
./runInstaller
```

On Windows systems, double-click the `setup.exe` file.

4. Refer to Table 7–3 for specific instructions about how to respond to each screen in the Oracle Identity Management installation and configuration tool.

> **Note:** When specifying the installation details, the path to the Oracle home must be identical to the path used on IDMHOST1, but the name of the OID instance must be unique.

For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

7.4.9 Task 9: Copy the Oracle Directory Integration Platform Directory from IDMHOST1 to IDMHOST2

The Oracle Directory Integration Platform application is deployed on IDMHOST1 as an externally staged application. The application must be copied from IDMHOST1 to IDMHOST2; otherwise, the managed server on IDMHOST2 is listed in the Oracle WebLogic Server administration console as being in an "unknown" state:

1. Locate the `applications` directory in the Oracle WebLogic Server domain directory on IDMHOST1:

```
MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers
        /wls_ods1/applications
```

2. Copy the `applications` directory on and its contents on IDMHOST1 to the same location in the domain directory on IDMHOST2.

For example:

```
scp -rp MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers
               /wls_ods1/applications
      user@IDMHOST2:MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig
               /servers/wls_ods2/applications
```

7.4.10 Task 10: On IDMHOST2, Set the Anonymous Bind Property to Allow

After you install and configure the second Oracle Internet Directory instance on IDMHOST2, you mustset the the "Anonymous Bind" server property to "allow," so it matches the first, upgraded Oracle Internet Directoryinstance on IDMHOST1.

This property allows the Oracle Single Sign-On 10*g* and Oracle Delegated Administration Services 10*g* (specifically, OC4J_Security) to correctly use the second Oracle Internet Directory instance on IDMHOST2. Without this alteration to the second Oracle Internet Directory, the OC4J_Security instance on IDMHOST2 will not start.

To modify the anonymous bind property with Oracle Enterprise Manager Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

2. Navigate to the home page of the Oracle Internet Directory instance on IDMHOST2.

3. From the **Oracle Internet Directory** menu, select **Administration**, and then **Server Properties**.

4. Select **Allows** from the **Anonymous Bind** drop-down menu.

5. Click Apply

6. Start Oracle Single Sign-On as you normally would.

7.4.11 Task 11: On IDMHOST2, Disable Oracle Internet Directory and Oracle Directory Integration Platform in the 10*g* Oracle Home

After you upgrade the Oracle Internet Directory and Oracle Directory Integration Platform components on IDMHOST1, you cannot start Oracle Internet Directory or use the Oracle Single Sign-On 10*g* component until you disassociate Oracle Internet Directory from the Oracle Single Sign-On and Oracle Delegated Administration Services components in the 10*g* Oracle home.

For specific instructions for performing this task, see the following:

- Section 4.5.2, "Disabling the Oracle Internet Directory and Oracle Directory Integration Platform 10g Components"

- Section 4.5.6, "Removing Oracle Internet Directory and Oracle Directory Integration Platform 10g from Application Server Control"

7.4.12 Task 12: Start the Managed Server on IDMHOST2

Follow these steps to start the wls_ods2 managed server in a cluster:

1. Open a browser and navigate to the WebLogic Administration Console at:

   ```
   http://idmhost1.mycompany.com:port/console
   ```

2. Login to the WebLogic Administration Console using the administrator credentials.

3. In the left pane of the WebLogic Administration Console, expand Environment and select Clusters.

4. Select the cluster (`cluster_ods`) containing the managed server (wls_ods2) you want to start.

5. Select **Control**.

6. Under Managed Server Instances in this Cluster, select the check box next to the managed server (`wls_ods2`) you want to start and click **Start**.

7. On the Server Life Cycle Assistant page, click **Yes** to confirm.

> **Note:** Node Manager starts the server on the target machine. When the Node Manager finishes its start sequence, the server's state is indicated in the **State** column in the Server Status table.

7.4.13 Task 13: Verify That the Components Are Up and Running on IDMHOST2

Use the procedure documented in "Task 5: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade" to verify the Oracle Internet Directory, Oracle Directory Integration Platform, and Oracle Directory Services Manager components on IDMHOST2.

7.5 Upgrading Oracle Internet Directory Only

If you are using Oracle Internet Directory in a high availability environment without Oracle Directory Integration Platform or the other Oracle Identity Management 10*g* components, then the following procedure applies.

When you upgrade such an environment to Oracle Fusion Middleware 11*g*, note that you can choose to install Oracle Internet Directory in one of the following topologies:

- Upgrading Oracle Internet Directory With a Local Oracle WebLogic Server Domain

- Upgrading Oracle Internet Directory With a Remote Domain or No Domain

7.5.1 Upgrading Oracle Internet Directory With a Local Oracle WebLogic Server Domain

Perform the following tasks to upgrade an Oracle Internet Directory-only high availability environment to 11*g*:

- Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

- Task 2: On IDMHOST1, Install and Configure Oracle Internet Directory

- Task 3: On IDMHOST1, Upgrade Oracle Internet Directory to 11g

- Task 4: On IDMHOST1, Verify the Upgraded Oracle Internet Directory Instance

- Task 5: On IDMHOST2, Install and Configure Oracle Internet Directory

- Task 6: On IDMHOST2, Register the Oracle Internet Directory Instance with the Domain on IDMHOST1

- Task 7: On IDMHOST2, Verify the Oracle Internet Directory Instance

7.5.1.1 Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

7.5.1.2 Task 2: On IDMHOST1, Install and Configure Oracle Internet Directory

To install and configure Oracle Internet Directory 11*g* on IDMHOST1:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the `setup.exe` file.

4. With the following important exceptions, refer to Table 7–1 for instructions about how to respond to each screen in the installation and configuration tool:

   On the Configure Components screen:

   - Select only **Oracle Internet Directory**.

   - Do not select the **Clustered** check box.

   For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

7.5.1.3 Task 3: On IDMHOST1, Upgrade Oracle Internet Directory to 11*g*

Use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle Internet Directory 10*g* instance on IDMHOST1 to Oracle Internet Directory 11*g*.

Use the instructions in Section 7.3.3, "Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11g" to upgrade the Oracle Internet Directory instance.

7.5.1.4 Task 4: On IDMHOST1, Verify the Upgraded Oracle Internet Directory Instance

Use the following OPMN command to verify that Oracle Internet Directory is up and running:

```
ORACLE_INSTANCE/opmnctl status
```

The output of the command should be similar to the following example:

```
Processes in Instance: oid_instance1
--------------------------------+------------------+---------+---------
ias-component                   | process-type     |     pid | status
--------------------------------+------------------+---------+---------
oid1                            | oidldapd         |   31394 | Alive
oid1                            | oidldapd         |   31392 | Alive
oid1                            | oidmon           |   31384 | Alive
```

Use the `ldapbind` command-line tool to ensure that you can connect to each Oracle Internet Directory instance and the LDAP Virtual Server. The `ldapbind` tool enables you to determine whether you can authenticate a client to a server.

For non-SSL:

```
ldapbind -h idmhost1.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h idmhost2.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h oid.mycompany.com -p 389 -D "cn=orcladmin" -q
```

For SSL:

```
ldapbind -h idmhost1.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h idmhost2.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h oid.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

where:

- U = SSL authentication mode

- 1 = No authentication required

- 2 = One way authentication required. With this option, you must also supply a wallet location (`-W "file:/home/my_dir/my_wallet"`) and wallet password (`-P wallet_password`).

- 3 = Two way authentication required. With this option, you must also supply a wallet location (`-W "file:/home/my_dir/my_wallet"`) and wallet password (`-P wallet_password`).

7.5.1.5 Task 5: On IDMHOST2, Install and Configure Oracle Internet Directory

To install and configure Oracle Internet Directory 11*g* on IDMHOST1:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the `setup.exe` file.

4. With the following important exceptions, refer to Table 7–3 for instructions about how to respond to each screen in the installation and configuration tool:

   - On the Select Domain screen, select the **No Domain** option.

   - On the Specify Installation Screen, provide the Oracle Home Location, the Oracle Instance Location, and instance name.

     Note: When specifying the installation details, the path to the Oracle home must be identical to the path used on IDMHOST1, but the name of the OID instance must be unique.

- Select **Oracle Internet Directory** on the Configure Components Screen. Do not select the other components

- Note that the Specify Cluster Details screen does not appear in an Oracle Internet Directory only installation.

For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

7.5.1.6 Task 6: On IDMHOST2, Register the Oracle Internet Directory Instance with the Domain on IDMHOST1

Register the Oracle Internet Directory instance on IDMHOST2 with the Oracle WebLogic Server domain on IDMHOST1, using the following OPMN command.

```
ORACLE_INSTANCE/opmnctl registerinstance
    -adminHost adminHostName
    -adminPort adminServerPort
    -adminUsername DOMAIN_ADMINISTRATOR_USERNAME
    -oracleInstance ORACLE_INSTANCE_HOME
```

For example:

```
ORACLE_INSTANCE/opmnctl registerinstance
    -adminHost IDMHOST1 MYCOMPANY.COM
    -adminPort 7001
    -adminUsername weblogic
    -oracleInstance /u01/app/oracle/product/11g/instances/oid_inst2
```

7.5.1.7 Task 7: On IDMHOST2, Verify the Oracle Internet Directory Instance

Use the procedure in Section 7.5.1.4, "Task 4: On IDMHOST1, Verify the Upgraded Oracle Internet Directory Instance" to verify the Oracle Internet Directory instance on IDMHOST2.

7.5.2 Upgrading Oracle Internet Directory With a Remote Domain or No Domain

This section provides the upgrade procedure when you want to use a remote Oracle WebLogic Server domain to register the upgraded Oracle Internet Directory 11*g* instances.

These steps are also applicable if you do not plan to register the Oracle Internet Directory instances with an Oracle WebLogic Server domain:

- Task 1: On IDMHOST1, Install and Configure Oracle Internet Directory

- Task 2: On IDMHOST1, Upgrade Oracle Internet Directory to 11g

- Task 3: On IDMHOST1, Verify the Oracle Internet Directory Instance

- Task 4: On IDMHOST2, Install and Configure Oracle Internet Directory

- Task 5: Verify the Oracle Internet Directory Instances on IDMHOST1 and IDMHOST2

- Task 6: Optionally, Register the Oracle Internet Directory Instances on IDMHOST1 and OIDHOST2 with an Existing Remote Domain

7.5.2.1 Task 1: On IDMHOST1, Install and Configure Oracle Internet Directory

With the following important exceptions, refer to Table 7–1 for instructions about how to respond to each screen in the installation and configuration tool:

- On the Select Domain screen, select the **No Domain** option.

- On the Specify Installation Screen, provide the Oracle Home Location and the Oracle Instance Location.

- Select **Oracle Internet Directory** on the Configure Components Screen. Deselect all other components

- Note that the Specify Cluster Details screen does not appear in an Oracle Internet Directory only installation.

For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

7.5.2.2 Task 2: On IDMHOST1, Upgrade Oracle Internet Directory to 11*g*

Use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle Internet Directory 10*g* instance on IDMHOST1 to Oracle Internet Directory 11*g*.

Use the instructions in Section 7.3.3, "Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11g" to upgrade the Oracle Internet Directory instance.

7.5.2.3 Task 3: On IDMHOST1, Verify the Oracle Internet Directory Instance

Use the procedure in Section 7.5.1.4, "Task 4: On IDMHOST1, Verify the Upgraded Oracle Internet Directory Instance" to verify the Oracle Internet Directory instance on IDMHOST1.

7.5.2.4 Task 4: On IDMHOST2, Install and Configure Oracle Internet Directory

To install and configure Oracle Internet Directory 11*g* on IDMHOST1:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the `setup.exe` file.

4. With the following important exceptions, refer to Table 7–3 for instructions about how to respond to each screen in the installation and configuration tool:

- On the Select Domain screen, select the **No Domain** option.

- On the Specify Installation Screen, provide the Oracle Home Location and the Oracle Instance Location.

  > **Note:** When specifying the Oracle home page, enter a path identical to the path used for the Oracle home on IDMHOST1.

- Select **Oracle Internet Directory** on the Configure Components Screen. Do not select the other components

- Note that the Specify Cluster Details screen does not appear in an Oracle Internet Directory only installation.

  For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

7.5.2.5 Task 5: Verify the Oracle Internet Directory Instances on IDMHOST1 and IDMHOST2

Use the procedure in Section 7.5.1.4, "Task 4: On IDMHOST1, Verify the Upgraded Oracle Internet Directory Instance" to verify the Oracle Internet Directory instance on IDMHOST1.

7.5.2.6 Task 6: Optionally, Register the Oracle Internet Directory Instances on IDMHOST1 and OIDHOST2 with an Existing Remote Domain

Register both Oracle Internet Directory instances on IDMHOST1 and IDMHOST2 with the existing, remote Oracle WebLogic Server domain, using the following OPMN command.

```
ORACLE_INSTANCE/opmnctl registerinstance
    -adminHost adminHostName
    -adminPort adminServerPort
    -adminUsername DOMAIN_ADMINISTRATOR_USERNAME
    -oracleInstance ORACLE_INSTANCE_HOME
```

For example:

```
ORACLE_INSTANCE/opmnctl registerinstance
    -adminHost IDMHOST1 MYCOMPANY.COM
    -adminPort 7001
    -adminUsername weblogic
    -oracleInstance /u01/app/oracle/product/11g/instances/oid_inst2
```

8

Upgrading an Oracle Identity Management Cold Failover Cluster Environment

This chapter describes how to upgrade an Oracle Identity Management Cold Failover Cluster environment to Oracle Fusion Middleware 11*g*.

This upgrade procedure involves the following tasks:

- Task 1: Preparing for Upgrading Your Oracle Fusion Middleware Cold Failover Cluster Environment

- Task 2: Install Oracle WebLogic Server and Create the Middleware Home

- Task 3: Install Oracle Internet Directory and Oracle Directory Integration Platform

- Task 4: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Installation

- Task 5: Upgrade Oracle Internet Directory and Oracle Directory Integration Platform

- Task 6: Verify the Upgrade of Oracle Internet Directory and Oracle Directory Integration Platform

- Task 7: Configuring the Upgraded Components for Active-Passive Deployments

8.1 Task 1: Preparing for Upgrading Your Oracle Fusion Middleware Cold Failover Cluster Environment

The procedures in this chapter provide instructions for upgrading high availability environments supported in Oracle Application Server 10*g* Release 2 (10.1.2) and 10*g* (10.1.4.0.1).

Before you begin, review the following sections for important prerequisite for the upgrade process.

Oracle Identity Management 10*g* Components Must Be Installed and Running on IDMHOST1

It is assumed that your Oracle Identity Management 10*g* components are installed and runningon IDMHOST1. This is important because the Oracle Identity Management 11*g* components that you are upgrading must be installed on the same host as the Oracle Identity Management 10*g* components.

Only Oracle Internet Directory and Oracle Directory Integration Platform Components are Upgraded to 11*g*

As part of this procedure, only Oracle Internet Directory and Oracle Directory Integration Platform are upgraded to Oracle Fusion Middleware 11*g*. For more information about the differences between the components available in Oracle Application Server 10*g* and Oracle Fusion Middleware 11*g*, see Section 3.1, "Summary of the Oracle Identity Management 10g and 11g Components".

Understanding Oracle Fusion Middleware Cold Failover Cluster for 11*g*

Oracle Fusion Middleware provides an active-passive model for all its components using Oracle FMW Cold Failover Clusters. In an Oracle FMW Cold Failover Cluster configuration, two or more application server instances are configured to serve the same application workload but only one is active at any particular time.

For more information, see "Oracle Fusion Middleware Cold Failover Cluster Topology Concepts" in the *Oracle Fusion Middleware High Availability Guide*.

Database High Availability and Version Requirements

For information database requirements for upgrade, as well as additional upgrade information for Oracle Fusion Middleware 11*g*, see the *Oracle Fusion Middleware Upgrade Planning Guide*.

Additional Resources

For information about the supported high availability topologies in Oracle Fusion Middleware 11*g*, see the *Oracle Fusion Middleware High Availability Guide*.

Before you begin these procedures, review the procedures and prerequisites available in Chapter 4, "Upgrading Your Oracle Internet Directory Environment".

8.2 Task 2: Install Oracle WebLogic Server and Create the Middleware Home

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

8.3 Task 3: Install Oracle Internet Directory and Oracle Directory Integration Platform

To install and configure Oracle Internet Directory and Oracle Directory Integration Platform 11*g*:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   `./runInstaller`

   On Windows systems, double-click the `setup.exe` file.

4. Refer to Table 8–1 for specific instructions about how to respond to each screen in the Oracle Identity Management installation and configuration tool.

   For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

Table 8–1 Summary of Screens for Installing and Configuring Oracle Internet Directory and Oracle Directory Integration Platform on IDMHOST1

Screen	Instructions
Welcome	Click **Next**.
Select Installation Type	Select **Install and Configure**. Click **Next**.
Prerequisite Checks	Click **Next**.
Select Domain	Select **Create New Domain** and enter the domain details. For the purposes of this exercise, enter `IDMDomain` in the **Domain Name** field. Click **Next**.
Specify Installation Location	Specify the following values: ■ **Middleware Home Location:** Enter the complete path to the Middleware home you created in "Task 2: Install Oracle WebLogic Server and Create the Middleware Home". ■ **Oracle Home Directory:** For the purposes of this example, enter `idmcfc` as the name of the Oracle home directory. ■ **WebLogic Server Directory:** This is usually the `wlserver_10.3` inside the Middleware home. ■ **Oracle Instance Location:** Enter a path for the Oracle instance. This directory can be any acccessible directory location; unlike the Oracle home, it does not need to be inside the Middleware home. ■ **Oracle Instance Name:** For the purposes of this example, enter `cfcidm_instance`.

Table 8–1 (Cont.) Summary of Screens for Installing and Configuring Oracle Internet Directory and Oracle Directory Integration Platform on IDMHOST1

Screen	Instructions
Configure Components	Select the following components: ■ **Oracle Internet Directory** ■ **Oracle Directory Integration Platform** ■ **Oracle Directory Services Manager** Do not select the **Clustered** check box.
Configure Ports	Select **Auto Port Configuration**. Click **Next**.
Specify Schema Database	Select **Use Existing Schema**. In the **Connect String** field, enter the connect string to each nodes in the Real Application Clusters (RAC) database. Separate each node with a carot symbol (^). For example: `INFRADBHOST1.MYCOMPANY.COM:1521:IDMDB1^INFRADBHOST2.MYCOMPANY.com:1521:IDMDB2@IDMEDG.MYCOMPANY.COM` Enter the ODS schema password in the **Password** field. Note that the ODS schema is used by Oracle Internet Directory. By default, the password for the ODS schema is the `ias_admin` password you provided when you installed Oracle Internet Directory 10*g*. However, the password might have been changed using the `oidpasswd` utility, which is documented in the Oracle Identity Management 10*g* User Reference. Click **Next**.
Upgrade Scenario Detected Warning dialog box	This warning indicates that you have correctly selected the Oracle Internet Directory 10*g* schemas (ODS). You install Oracle Internet Directory 11*g* against the 10*g* schema and then later use the Upgrade Assistant to upgrade the schema to 11*g*. Click **Yes**.
OID Password	Enter the Administrator password for Oracle Internet Directory instance.
Installation Summary	Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.
Installation Progress	On UNIX systems, a dialog appears, prompting you to run the `oracleRoot.sh` script. Open a window and run the script, following the prompts in the window. Click **OK**.
Configuration	Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the Installation Complete screen appears. Click **Finish**, and then confirm your choice to exit.

8.4 Task 4: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Installation

Before you upgrade run the Upgrade Assistant, use the following procedure to ensure that Oracle Internet Directory and Oracle Directory Integration Platform 10*g* and 11*g* are up and running on the host.

Step 1 Verify the status of Oracle Internet Directory 10g instance

For example, you can use the `opmnctl` command:

```
ORACLE_HOME/opmm/bin/opmnctl status
Processes in Instance: cfc.mycompany.com
```

```
------------------+-------------------+---------+---------
ias-component     | process-type      |     pid | status
------------------+-------------------+---------+---------
DSA               | DSA               |     N/A | Down
LogLoader         | logloaderd        |     N/A | Down
dcm-daemon        | dcm-daemon        |     N/A | Down
HTTP_Server       | HTTP_Server       |   26117 | Alive
OID               | OID               |   26121 | Alive
```

Step 2 Verify the status of the Oracle Directory Integration Platform 10*g* instance

For example, on a UNIX system, you can use the `ps` command and the `grep` command to search for the `odisrv` process in the resulting output:

```
$ ps -ef | grep odisrv
oracle   15711 15552  0 21:17 pts/0    00:00:00 grep odisrv
oracle   21597     1  0 Feb18 ?        00:00:00 /bin/sh
/u01/app/oracle/product/10g/idm/odisrv instance=1 configset=0 port=636 sslauth=1
host=idmhost1.mycompany.com
```

Step 3 Verify the status of the Oracle Internet Directory 11*g* instance

Use the following OPMN command to verify that Oracle Internet Directory is up and running:

ORACLE_INSTANCE/opmnctl status

The output of the command should be similar to the following example:

```
Processes in Instance: oid_instance1
--------------------------------+-------------------+---------+---------
ias-component                   | process-type      |     pid | status
--------------------------------+-------------------+---------+---------
oid1                            | oidldapd          |   31394 | Alive
oid1                            | oidmon            |   31384 | Alive
```

Use the `ldapbind` command-line tool to ensure that you can connect to each Oracle Internet Directory instance and the LDAP Virtual Server. The `ldapbind` tool enables you to determine whether you can authenticate a client to a server.

For non-SSL:

```
ldapbind -h idmhost1.mycompany.com -p 389 -D "cn=orcladmin" -q
```

For SSL:

```
ldapbind -h idmhost1.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

where:

- U = SSL authentication mode

- 1 = No authentication required

- 2 = One way authentication required. With this option, you must also supply a wallet location (`-W "file:/home/my_dir/my_wallet"`) and wallet password (`-P wallet_password`).

- 3 = Two way authentication required. With this option, you must also supply a wallet location (`-W "file:/home/my_dir/my_wallet"`) and wallet password (`-P wallet_password`).

Step 4 Verify the status of the Oracle Directory Integration Platform 11*g* instance

Validate the Oracle Directory Integration Platform installation by using the WLST dipStatus command. To run this command, follow these steps:

1. Set the ORACLE_HOME environment variable to the directory where you installed the Identity Management binaries. For example:

   ```
   export ORACLE_HOME=/u01/app/oracle/product/11g/fmw_home/ods
   ```

2. Set the WLS_HOME environment variable to the directory where you installed the WebLogic Server.

   For example:

   ```
   export WLS_HOME=/u01/app/oracle/product/11g/fmw_home/wlserver_10.3
   ```

3. Run the following command:

   ```
   $ORACLE_HOME/bin/dipStatus -h <hostName> -p <port> -D <wlsuser>
   ```

   For example, on IDMHOST1, the command and successful output are shown below:

   ```
   $ORACLE_HOME/bin/dipStatus
       -h idmhost1.mycompany.com
       -p 7005
       -D weblogic
       [Weblogic user password]
        Connection parameters initialized.
        Connecting at idmhost1.mycompany.com:7005, with userid "weblogic"..
        Connected successfully.
        ODIP Application is active at this host and port.
   ```

Step 5 Verify Oracle Directory Services Manager (ODSM)

Verify the Oracle Directory Services Manager installation by bringing up the ODSM Administration Console in a web browser.

The URL to access the ODSM Administration Console is:

```
http://hostname.mycompany.com:<port>/odsm/faces/odsm.jspx
```

For example, on IDMHOST1, enter this URL:

```
http://idmhost1.us.oracle.com:7005/odsm/faces/odsm.jspx
```

8.5 Task 5: Upgrade Oracle Internet Directory and Oracle Directory Integration Platform

Use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* instances on IDMHOST1 to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

```
ua.bat
```

The Upgrade Assistant displays the Welcome screen.

3. Click **Next** to display the Select Operation screen.

4. Select **Upgrade Identity Management Instance** on the Select Operation screen.

5. Refer to Table 8–2 for a description of the Upgrade Assistant screens that require input from you during an Oracle Internet Directory and Oracle Directory Integration Platform upgrade.

6. After the Target Database Details screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

     See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

   - Displays the End of Upgrade screen, which confirms that the upgrade was complete.

7. Exit the Upgrade Assistant.

Table 8–2   Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* Release 2 (10.1.2) or 10*g* (10.1.4) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the 11*g* Oracle instance, or click **Browse** to locate the instance directory.
Specify WebLogic Server	Enter the host and Administration Server port for the Oracle WebLogic Server you configured in "Task 2: Install Oracle WebLogic Server and Create the Middleware Home".
	Note this information is required if you are upgrading Oracle Directory Integration Platform. It is also required if you associated your Oracle Internet Directory 11*g* installation with Oracle WebLogic Server.

Table 8–2 (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	Select the upgrade options you want to apply to the Oracle Identity Management upgrade:
	■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance. Note if you select this option, you will not be able to run both the 10*g* and 11*g* middle tiers at the same time; otherwise, port conflicts will occur.
	■ **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade.
	Click **Help** to display more information about the upgrade options on this screen.
Specify OID Details	Use this screen to enter the details required to connect to the Oracle Internet Directory 10*g* instance, including the password to the Oracle Internet Directory super user account (`cn=orcladmin`).
	For more information, click **Help**.
Specify Database Details	Use this screen to enter the details required to connect to the database where the Oracle Identity Management schemas reside, including the host, service name, port, and SYS password for the database.
	Note the following important information about this screen:
	■ You must enter the password for the ODS schema password. The default ODS password is the same as the Oracle Application Server administrator password, but this password can be changed after installation, using the OID Database Password Utility.
	■ The instructions for identifying a Real Application Clusters (RAC) database are different, depending upon whether you are identifying the RAC database that contains the Oracle Internet Directory (ODS) schema or a RAC database that is being used for Oracle Directory Integration Platform.
	For more information, see Section 4.4.3.2, "About Specifying Real Application Clusters (RAC) Database Details on the Specify Database Details Screen".

Table 8–2   (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Root action required screen	This is only if you are using privileged port on a UNIX system.
	A configuration script needs to be run as root before upgrade can proceed.
	Leaving this window open, open another window, and run the upgroot.sh file as root:
	When the script has completed, return to the Upgrade Assistant and click **OK**.

8.6 Task 6: Verify the Upgrade of Oracle Internet Directory and Oracle Directory Integration Platform

Use Steps 3 through 5 of Section 8.4, "Task 4: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Installation" to verify that the upgraded Oracle Identity Management components are up and running.

8.7 Task 7: Configuring the Upgraded Components for Active-Passive Deployments

Use the following steps to configure the upgraded components in an active-passive high availability environment.

Note that these steps reference specific sections in the *Oracle Fusion Middleware High Availability Guide*, which provides comprehensive instructions for configuring hight availability in Oracle Fusion Middleware 11*g*:

- Task 7a: Transform the Infrastructure Components for Cold Failover Clusters
- Task 7b: Transforming Oracle Internet Directory and Its Clients for Cold Failover Clusters

8.7.1 Task 7a: Transform the Infrastructure Components for Cold Failover Clusters

Transform the infrastucture components that support the Oracle Internet Directory environment. For each step in this process, refer to the corresponding procedure in the *Oracle Fusion Middleware High Availability Guide*:

Table 8–3   Steps to Transform the Infrastructure Components for Cold Failover Cluster

Step #	Description	Section in Oracle Fusion Middleware High Availability Guide
1	Transform the Oracle WebLogic Server administration server	"Transforming the Administration Server for Cold Failover Clusters"
2	Transform the wls_ods managed server	"Transforming Oracle WebLogic Managed Servers"
3	Transform the Oracle WebLogic Server node manager	"Transforming Node Manager"
4	Transform the Fusion Middleware Control	"Transforming Oracle Enterprise Manager"
5	Transform the Oracle Process Manager and Notification Server (OPMN)	"Transforming Oracle Process Management and Notification Server"
6	Transform the Oracle HTTP Server	"Transforming Oracle HTTP Server"

8.7.2 Task 7b: Transforming Oracle Internet Directory and Its Clients for Cold Failover Clusters

After you have transformed the infrastructure components for Cold Failover Cluster, you can do the same for the upgraded Oracle Internet Directory 11*g* instance.

Refer to "Transforming Oracle Internet Directory and Its Clients" in the *Oracle Fusion Middleware High Availability Guide*.

8.8 Task 8: Configure Fusion Middleware Control to Monitor the Upgraded Components

After the Cold Failover Cluster transformation, the Oracle Enterprise Manager Fusion Middleware Control cannot display the correct status for some of the upgraded components.

To fix this problem, you must modify specific Fusion Middleware Control configuration files so they reference to the virtual host name used for the Cold Failover transformation instead of the physical host name.

Follow the steps below to update the Fusion Middleware Control configuration files:

1. Stop the Oracle Enterprise Manager Fusion Middleware Control agent:

   `ORACLE_HOME`/bin/emctl stop agent

2. Modify the `emd.properties` file in the Oracle instance directory:

   a. Change directory to the following directory in the Oracle instance:

   `ORACLE_INSTANCE`/emagent/`em_agent_name`/sysman/config

   b. Make a backup copy of the `emd.properties` file:

   For example, on UNIX systems:

   `cp emd.properties emd.properties.bak`

   c. Edit the `emd.properties` file so it references the virtual host name, rather than the physical host name.

   For example, if the physical host name is `host1.mycompany.com` and the virtual host name is `cfcvip.mycompany.com`, then you must change the reference accordingly in the following attributes in the `emd.properties` file:

   `REPOSITORY_URL`

   `EmdWalletSrcUrl`

   `emd_url`

3. Modify the `targets.xml` file in the Oracle instance:

   a. Change directory to the `emd` directory of the Oracle instance:

   `INSTANCE_HOME`/emagent/`em_agent_name`/sysman/emd

   b. Make a backup copy of the `targets.xml` file:

   For example, on UNIX systems:

   `cp targets.xml targets.xml.bak`

   c. Modify `targets.xml`, as follows:

Modify the entries related to `host` and `oracle_emd` so they reference the virtual host name (for example, `cfcvip.mycompany.com`):

For example:

```
<Targets AGENT_TOKEN="ad4e5899e7341bfe8c36ac4459a4d569ddbf03bc">
    <Target TYPE="oracle_emd" NAME=cfcvip.mycompany.com:5157"/>
    <Target TYPE="host" NAME=cfcvip.mycompany.com
                      DISPLAY_NAME=cfcvip.mycompany.com/>
</Targets>
```

Remove all other `<Target>` entries in the file.

4. Modify the `targets.xml` file in the domain directory:

   a. Change directory to the following directory in the Oracle WebLogic Server domain directory inside the Middleware home:

   MW_HOME/user_projects/domains/*domain_name*/sysman/state

   b. Make a backup copy of the `targets.xml` file:

   For example, on UNIX systems:

   ```
   cp targets.xml targets.xml.bak
   ```

   c. Edit the `targets.xml` file and change all occurrences of the physical host name to the virtual host name.

   For example, change all occurrences of `host1.mycompany.com` to `cfcvip.mycompany.com`.

5. Modify the `topology.xml` file in the domain directory:

   a. Change directory to the following location in the domain directory inside the Middleware home:

   MW_HOME/user_projects/domains/*domainName*/opmn

   b. Make a backup copy of the `topology.xml` file:

   For example, on UNIX systems:

   ```
   cp topology.xml topology.xml.bak
   ```

   c. Edit the `topology.xml` file and change all occurrences of the physical host name to the virtual host name.

   For example, change all occurrences of `host1.mycompany.com` to `cfcvip.mycompany.com`.

6. Restart the administration server for the Oracle WebLogic Server domain.

7. Restart the Oracle Enterprise Manager Fusion Middleware Control agent:

   ```
   INSTANCE_HOME/emagent/em_agent_name/emctl start agent
   INSTANCE_HOME/emagent/em_agent_name/emctl status agent
   ```

8.9 Task 9: Verify the Upgraded High Availability Environment

This section provides the steps to verify the transformation of the infrastructure and Oracle Identity Management components to Cold Failover Cluster:

1. Use the Virtual Hostname instead of the physical hostname to display the Fusion Middleware Control and the Oracle WebLogic Server Administration Console in your Web browser. The URLs are listed below:

- Fusion Middleware Control: `http://VirtualHostname:port/em`

- Oracle WebLogic Server Console:
  `http://VirtualHostname:port/console`

For example use a web browser and access the following consoles:

- Fusion Middleware Control: `http://idmhost-vip.mycompany.com/em`

- Oracle WebLogic Server Console: `http://idmhost-vip.mycompany.com`

2. Verify that the Oracle Identity Management 11*g* components are up and running. Use steps 3 through 5 in Section 8.4, "Task 4: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Installation".

9

Performing an Oracle Identity Management Multimaster and Fan-Out Replication Upgrade

This appendix describes how to upgrade to Oracle Identity Management 11*g* Release 1 (11.1.1) in an Oracle Internet Directory replicated environment.

Refer to the following sections for more information:

- Task 1: Review the Terminology, Prerequisites, and Key Concepts For Upgrading a Replication Environment

- Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade

- Task 3: Perform the Oracle Internet Directory Replica Upgrade

- Task 4: Completing the Upgrade of Each Replica

9.1 Task 1: Review the Terminology, Prerequisites, and Key Concepts For Upgrading a Replication Environment

Review the following prerequisites and requirements before proceeding with the upgrade procedures in this chapter:

- Terminology Conventions for This Chapter

- Valid Starting Points When Upgrading a Replication Environment

- Oracle Recommendations When Upgrading a Replication Environment

9.1.1 Terminology Conventions for This Chapter

In this chapter, the **destination replica** is the newly installed and upgraded 11*g* Release 1 (11.1.1) replica; the **source replica** is the 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) replica you are upgrading.

9.1.2 Valid Starting Points When Upgrading a Replication Environment

The upgrade procedures in this chapter are designed for administrators who have installed and configured an Oracle Internet Directory 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) multimaster or fan-out replication environment.

This chapter assumes that the Oracle Identity Management components in the replication environment are distributed. In other words, you have installed the Oracle Internet Directory (and optionally Oracle Directory Integration Platform) components

in one or more Oracle homes, and you installed the Oracle Single Sign-On and Oracle Delegated Administration Services components in one or more additional Oracle homes.

Figure 9–1 shows a typical Oracle Identity Management 10g Release 2 (10.1.2) multimaster replication environment, which is described in detail in "Deploying Identity Management with Multimaster Replication," in the 10g Release 2 (10.1.2) *Oracle Fusion Middleware High Availability Guide*.

Figure 9–1   A Typical Oracle Identity Management 10g Release 2 (10.1.2) Multimaster Replication Environment
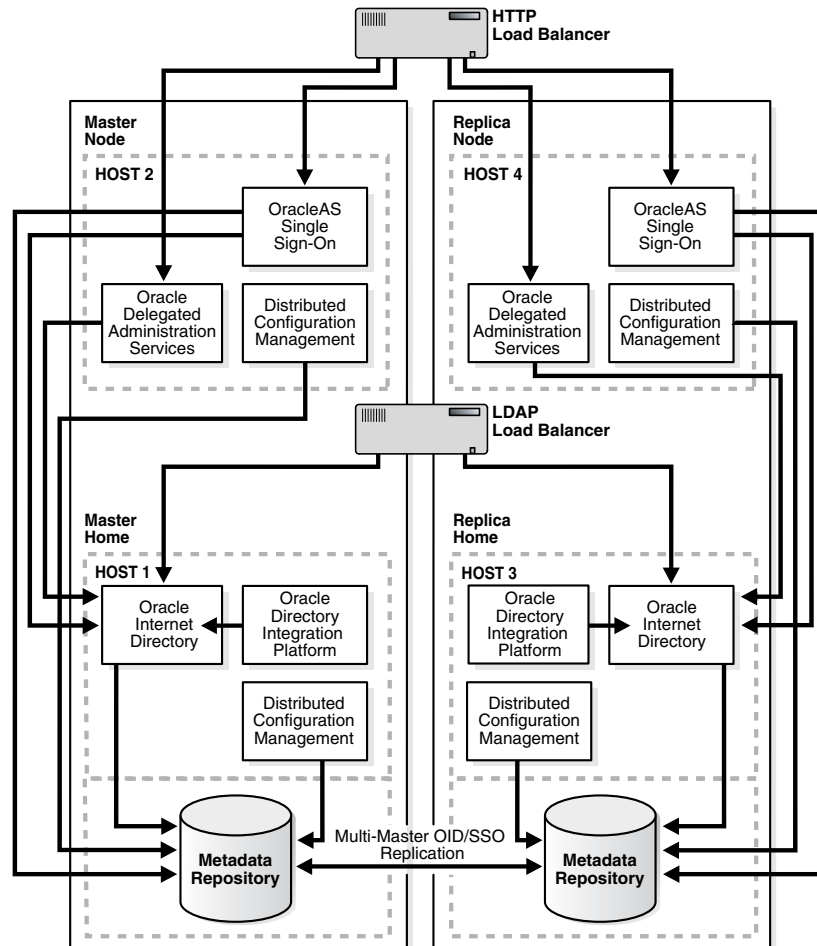
Information about deploying Oracle Identity Management with fan-out replication can be found in the Oracle Application Server 10*g* (10.1.4.0.1) *Oracle Identity Management Concepts and Deployment Planning Guide*, which is available in the Oracle Application Server 10g Release 2 (10.1.2) documentation library.

9.1.3 Oracle Recommendations When Upgrading a Replication Environment

Oracle Corporation recommends the following during the upgrade procedure:

- After you upgrade the destination replica, disable replication between the destination replica and the source replica. The destination replica can receive and process changes from source replica, but the source replica cannot process changes originated and received from destination replica.

■ The replication environment can be a Single Master (that is, only one replica is set to read and write, and all others are set to read only).

9.2 Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade

Before you begin upgrading Oracle Internet Directory in a replicated environment, you must perform the following steps for all replicas other than Master Definition Site (MDS) Replica or Primary supplier replica:

1. Locate the database registration entry of the database of replica to be upgraded.

   On Window systems:

   ```
   SOURCE_ORACLE_HOME\bin\ldapsearch
        -h hostname_of_replica_being_upgraded
        -p port
        -D cn=orcladmin
        -w superuser_password
        -b "cn=oraclecontext"
        -s one "(objectclass=orcldbserver)" dn
   ```

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/bin/ldapsearch
        -h hostname_of_replica_being_upgraded
        -p port
        -D cn=orcladmin
        -w superuser_password
        -b "cn=oraclecontext"
        -s one "(objectclass=orcldbserver)" dn
   ```

   This will return a list of Distinguished Names (DNs) corresponding to all the Databases registered in Oracle Internet Directory in the following form:

   ```
   cn=database_name,cn=oraclecontext
   ```

   From the returned list of entries, locate and make a note of the DN of the following entry, which corresponds to the replica upgraded:

   ```
   cn=dbname_of_replica_to_be_upgraded,cn=oraclecontext
   ```

2. Identify the replica ID of the replica to be upgraded by issuing following command:

   On Windows systems:

   ```
   SOURCE_ORACLE_HOME\bin\ldapsearch
        -h hostname_of_replica_being_upgraded
        -p port
        -D cn=orcladmin
        -w superuser_password
        -b "" -s base "(objectclass=*)" orclreplicaid
   ```

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/bin/ldapsearch
        -h hostname_of_replica_being_upgraded
        -p port
        -D cn=orcladmin
        -w superuser_password
        -b ""
   ```

```
-s base "(objectclass=*)" orclreplicaid
```

3. Modify the `seeAlso` attribute of the replica subentry so that it points to the database you are about to upgrade.

   The `seeAlso` attribute is a standard Oracle Internet Directory attribute. For more information, refer to "seeAlso" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management*.

   To modify the `seeAlso` attribute:

   a. Create a file, for example `mod.ldif`, with following contents:

   ```
   #File Name : mod.ldif
   dn: orclreplicaid=replicaid_from_step_2,cn=replication configuration
   changetype: modify
   replace: seeAlso
   #The DN used in seealso attribute is obtained in Step #1.
   seeAlso: cn=dbname_of_replica_being_upgraded,cn=oraclecontext
   ```

   b. Modify the replica subentry using ldapmodify command.

      On Windows systems:

   ```
   SOURCE_ORACLE_HOME\bin\ldapmodify
       -h hostname_of_replica_being_upgraded
       -p port
       -D superuser_DN
       -w superuser_password
       -v
       -f mod.ldif
   ```

      On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/bin/ldapmodify
       -h hostname_of_replica_being_upgraded
       -p port
       -D superuser_DN
       -w superuser_password
       -v
       -f mod.ldif
   ```

4. Navigate to the following directory and locate `ias.properties` file:

   On Windows systems:

   ```
   SOURCE_ORACLE_HOME\config
   ```

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/config
   ```

5. Open the `ias.properties` file and verify that the properties shown in Table 9–1 are correct and valid.

6. Make sure the Oracle Internet Directory server is up and running.

   To verify that Oracle Internet Directory is running, enter one of the following commands.

> **Note:** You may have to temporarily set the ORACLE_HOME environment variable to the Oracle Internet Directory Oracle home before running the `ldapbind` command.
>
> After you verify that the Oracle Internet Directory is running, you must then make sure the ORACLE_HOME environment variable is not defined before you start the 11*g* Release 1 (11.1.1) installer to begin the upgrade procedure.

If you are running Oracle Internet Directory on a non-secure port:

SOURCE_ORACLE_HOME/bin/ldapbind -p *Non-SSL_port*

If you are running Oracle Internet Directory on a secure port:

SOURCE_ORACLE_HOME/bin/ldapbind -p *SSL_port* -U 1

These commands should return a "bind successful" message.

7. Stop the second LDAP server as shown below.

   This example assumes that the instance number used for the second instance was 2.

   SOURCE_ORACLE_HOME/bin/oidctl connect=*connect_string_of_db* server=oidldapd instance=2 stop

Table 9–1   Properties to Verify in ias.properties Before Replication Upgrade

Property Name	Correct Value Before Replication Upgrade
OID.LaunchSuccess	True
OIDhost	*host name of replica*
OIDport	*port of replica*
OIDsslport	*SSL port for replica*

9.3 Task 3: Perform the Oracle Internet Directory Replica Upgrade

You can upgrade one replica at a time, or all of the replicas simultaneously. Refer to the following sections for more information:

- Selecting a Replica Upgrade Method
- Upgrading One Replica at a Time
- Upgrading Oracle Internet Directory on Multiple Replicas Simultaneously

9.3.1 Selecting a Replica Upgrade Method

Upgrading one computer at a time in a replicated environment ensures that Oracle Internet Directory is available during the upgrade for additions, modifications, and searching. When you use this method, only the replica you are upgrading is down. The other replicas continue to run and are available to your users.

Upgrading multiple replicas simultaneously ensures that the entire network is upgraded without a transient stage. The procedure is simpler than upgrading one replica at a time, but involves directory service downtime.

9.3.2 Upgrading One Replica at a Time

Follow these steps to upgrade one replica at a time:

1. Make sure you have completed the procedure in Section 9.2, "Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade".

2. Identify the replication server on the replica to be upgraded.

   The replica can be an LDAP-based partial or fan-out replica, or it can be an Oracle Advanced Replication (ASR) based multimaster replica.

   > **See Also:** "Directory Replication Concepts" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

3. Modify your load balancer to route traffic away from the replica you are about to upgrade; instead route all client traffic to the other replicas.

4. Make sure the replica is up-to-date with changes from the other replica.

   This check is required to make sure that all the changes from the first replicea are captured in the second replica before we turn off replication.

5. Stop the replication server on the replica to be upgraded.

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/oidctl
       connect=db_connect_string
       server=OIDREPLD
       instance=1
       flags="-p port_at_which_ldap_server_is_listening"
       stop
   ```

   On Windows systems:

   ```
   SOURCE_ORACLE_HOME\oidctl
       connect=db_connect_string
       server=OIDREPLD
       instance=1
       flags="-p port_at_which_ldap_server_is_listening"
       stop
   ```

   > **See Also:** "Oracle Identity Management Server Administration Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for more information about the `oidctl` administration tool

6. Make sure that the Oracle Internet Directory server, the Oracle Internet Directory database, and the database listener are up and running.

7. If you are upgrading an ASR-based replica, then delete all ASR jobs on other replicas by issuing the oidrdjob.sql script.

   For example:

   ```
   export TWO_TASK=db_name_of_replica_being_upgraded
   ORACLE_HOME/bin/sqlplus repadmin/password@connect_string_of_db
           @ORACLE_HOME/ldap/admin/oidrdjob.sql
   ```

   All ASR jobs on other master sites that transfer changes to this replica are deleted. This has the effect of taking the replica currently being upgraded out of the

replication environment, so that no changes come to it, while other replicas continue to operate and replicate changes.

8. Depending on the configuration of the replica, refer to the following documentation resources to perform the upgrade of the replica:

   - If the replica you are upgrading is configured for Oracle Identity Management high availability, then use the instructions in Section 7.3, "Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a High Availability Environment".

   - If the replica you are upgrading is not configured for high availability, then use the instructions in Chapter 4, "Upgrading Your Oracle Internet Directory Environment" to upgrade the replica to Oracle Internet Directory 11*g*.

   Note that upgrading the replica involves the following steps:

   - Installing Oracle WebLogic Server and creating the Middleware home

   - Installing and configuring Oracle Internet Directory.

   - Running the Upgrade Assistant to upgrade the configuration from the Oracle Internet Directory 10*g* instance to 11*g*

   - Performing any post-upgrade tasks for your environment.

9. After you upgrade the replica, verify that the database in the upgraded replica Oracle home is up and running.

10. Test the connectivity to the other replicas.

    The Net Services Upgrade assistant might have modified `listener.ora` and `tnsnames.ora`, breaking connectivity. If connectivity is broken, identify the entries that were modified in the files, and restore the entries from the corresponding files in the source Oracle home.

    For example, copy the original entries from the following files in the source Oracle home to the corresponding files in the destination Oracle home:

    ```
    SOURCE_ORACLE_HOME/network/admin/listener.ora
    SOURCE_ORACLE_HOME/network/admin/sqlnet.ora
    SOURCE_ORACLE_HOME/network/admin/tnsnames.ora
    ```

11. If you are upgrading an Oracle Advanced Replication (ASR) based Replica, recreate the jobs on each replica, after it is upgraded, by issuing the following command:

    ```
    export LD_LIBRARY_PATH=DESTINATION_ORACLE_HOME/lib
    DESTINATION_ORACLE_HOME/ldap/bin/remtool -asrrectify
    ```

    The jobs that were deleted in previously are re-created. They will begin transferring the existing changes and new changes from other replicas to the upgraded replicas.

12. Perform the procedures described in Section 9.4, "Task 4: Completing the Upgrade of Each Replica" for the newly upgraded replica.

13. Stop the 10*g* replication servers.

    This is to avoid replicating the upgraded replica with those that have not been upgraded yet.

    Run the following command:

    ```
    export TWO_TASK=db_name_of_second_replica
    ```

```
sqlplus repadmin/welcome1@db_connect_string
        @$ORACLE_HOME/ldap/admin/oidrdjob.sql
```

14. Redefine the following environment variables:

    For example:

```
export INSTANCE_NAME=asinst_1
export COMPONENT_NAME=oid1
export ORACLE_HOME=11g_ORACLE_HOME_PATH
export ORACLE_INSTANCE=11g_ORACLE_INSTANCE_PATH
```

15. Start the replication server on the newly upgrade replica, if it is not already running:

```
DESTINATION_ORACLE_HOME/oidctl
    connect=db_connect_string
    server=OIDREPLD
    instance=1
    flags="-p port_at_which_ldap_server_is_listening"
    start
```

> **See Also:** "Oracle Identity Management Server Administration Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for more information about the `oidctl` administration tool

16. Modify the load balancer to route client traffic back to the newly upgraded replica.

17. Upgrade the remaining replicas using the same procedures you used to upgrade the first replica.

9.3.3 Upgrading Oracle Internet Directory on Multiple Replicas Simultaneously

Use the following procedure to upgrade all the replicas simultaneously:

1. In all replicas other than MDS replica or primary supplier replica, make sure you have completed the pre-upgrade steps provided in Section 9.2, "Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade".

2. Stop the replication server on all replicas in the Directory Replication Group (DRG):

```
SOURCE_ORACLE_HOME/oidctl
    connect=db_connect_string
    server=OIDREPLD
    instance=1
    flags="-p port_at_which_ldap_server_is_listening"
    stop
```

> **See Also:** "Oracle Identity Management Server Administration Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for more information about the `oidctl` administration tool

3. Use the instructions in Chapter 4, "Upgrading Your Oracle Internet Directory Environment" to upgrade the replica to Oracle Internet Directory 11*g*.

    Note that upgrading the replica involves the following steps, which are documented in Chapter 4:

- Installing Oracle WebLogic Server and creating the Middleware home

- Installing and configuring Oracle Internet Directory.

- Running the Upgrade Assistant to upgrade the configuration from the Oracle Internet Directory 10*g* instance to 11*g*

- Performing any post-upgrade tasks for your environment.

4. After you upgrade the replica, verify that the database on each upgraded replica is up and running.

5. Test the connectivity to the other replicas.

   The Net Services Upgrade assistant might have modified `listener.ora` and `tnsnames.ora`, breaking connectivity. If connectivity is broken, identify the entries that were modified in the files, and restore the entries from the corresponding files in the source Oracle home.

   For example, copy the original entries from the following files in the source Oracle home to the corresponding files in the destination Oracle home:

   ```
   SOURCE_ORACLE_HOME/network/admin/listener.ora
   SOURCE_ORACLE_HOME/network/admin/sqlnet.ora
   SOURCE_ORACLE_HOME/network/admin/tnsnames.ora
   ```

6. For each upgraded replica, perform the steps in Section 9.4, "Task 4: Completing the Upgrade of Each Replica".

7. Start the replication server on each of the upgraded replicas:

   ```
   DESTINATION_ORACLE_HOME/oidctl
      connect=db_connect_string
      server=OIDREPLD
      instance=1
      flags="-p port_at_which_ldap_server_is_listening"
      start
   ```

   > **See Also:** "Oracle Identity Management Server Administration Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for more information about the `oidctl` administration tool

9.4 Task 4: Completing the Upgrade of Each Replica

The following sections describe tasks you must perform after you have completed the upgrade of a replica:

- Changing the Replication DN Password in the Oracle Internet Directory Wallet for Each Replica

- Setting the orclreplicationid Attribute in the Upgraded 11g Directory

9.4.1 Changing the Replication DN Password in the Oracle Internet Directory Wallet for Each Replica

After you upgrade a replica, change the password for the replication distinguished name (DN). After you change or reset the password, you can then start `oidmon`, LDAP server, and replication server.

Refer to the following sections for more information:

- Changing the Replication DN Password

- [Resetting the Replication DN Password](#)

9.4.1.1 Changing the Replication DN Password

After you upgrade each replica, you must change the replication distinguished name (DN) password, using the Replication Environment Management Tool (remtool), as follows:

```
DESTINATION_ORACLE_HOME/ldap/bin/remtool
    -pchgwalpwd -v -bind host:port/repl_dn_pwd
```

Note that you must provide the existing password on the remtool command line. If you do not know the replication DN password, see Section 9.4.1.2, "Resetting the Replication DN Password".

> **See Also:** "remtool" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for details about the arguments you can use with the remtool command, including the -pchgwalpwd and -presetpwd arguments

9.4.1.2 Resetting the Replication DN Password

If you do not know replication DN password, reset the replication DN password using the following command:

```
DESTINATION_ORACLE_HOME/ldap/bin/remtool -presetpwd -v -bind host:port
```

If you are upgrading a fan-out replica, you must also reset the password of the replication DN at its supplier. To reset the password of replication DN at its supplier:

1. Identify the replica ID of the replica to be upgraded by issuing following command:

   On Windows systems:

   ```
   SOURCE_ORACLE_HOME\bin\ldapsearch
       -h hostname_of_replica_being_upgraded
       -p port
       -D cn=orcladmin
       -w superuser_password
       -b "" -s base "(objectclass=*)" orclreplicaid
   ```

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/bin/ldapsearch
       -h hostname_of_replica_being_upgraded
       -p port
       -D cn=orcladmin
       -w superuser_password
       -b ""
       -s base "(objectclass=*)" orclreplicaid
   ```

2. Create an LDIF file (for example, modpwd.ldif), with following contents:

   ```
   dn: cn=replication dn,orclreplicad=consumer_replicaid,cn=replication
   configuration
   changetype: modify
   replace: userpassword
   userpassword: new_password
   ```

3. Apply the change at supplier using ldapmodify tool as shown below:

   ```
   ldapmodify  -h supplier_hostname
   ```

```
-p supplier_port_number>
-D cn=orcladmin
-w super_user_password_of_supplier
-f modpwd.ldif
```

9.4.2 Setting the orclreplicationid Attribute in the Upgraded 11*g* Directory

If you are upgrading a 10*g* Release 2 (10.1.2) replica in an environment with fan-out replication, you must set the orclreplicationid in the Oracle Internet Directory attribute to a valid value.

This procedure is not necessary if you are upgrading from 10*g* (10.1.4.0.1), because this is a new attribute that was introduced in Oracle Identity Management 10*g* (10.1.4.0.1).

Oracle recommends that you set the value of this attribute so it matches the value of the existing orclagreementID attribute. To perform this task:

1. Identify the replica ID of the replica to be upgraded by issuing following command:

    On Windows systems:

    ```
    SOURCE_ORACLE_HOME\bin\ldapsearch
         -h hostname_of_replica_being_upgraded
         -p port
         -D cn=orcladmin
         -w superuser_password
         -b "" -s base "(objectclass=*)" orclreplicaid
    ```

    On UNIX systems:

    ```
    SOURCE_ORACLE_HOME/bin/ldapsearch
         -h hostname_of_replica_being_upgraded
         -p port
         -D cn=orcladmin
         -w superuser_password
         -b ""
         -s base "(objectclass=*)" orclreplicaid
    ```

2. Create an LDIF file called id.ldif with the following content:

    ```
    dn: orclagreementid=000002,orclreplicaid=replicaid,cn=replication configuration
    changetype: modify
    replace: orclreplicationid
    orclreplicationid: 2
    ```

    Note that in the above example, the first two lines should appear all in one line in the LDIF file.

3. Apply the LDIF file by using the following ldapmodify command:

    ```
    ldapmodify -p port
               -h host
               -D DN
               -w password
               -f id.ldif
    ```

    In this example, replace *port*, *host*, *DN*, and *password* with the appropriate values for your environment.

> **See Also:** "The Replication Agreement Entry" in the chapter, "Oracle Internet Directory Replication Concepts" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for information about the `orclreplicationid` attribute
>
> "Oracle Internet Directory Data Management Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for more information about using the `ldapmodify` command

10

Upgrading an Oracle Virtual Directory High Availability Environment

This chapter describes how to upgrade Oracle Virtual Directory in a high availability environment.

The upgrade steps vary slightly depending on whether you are registering with a domain and the location of the domain. Refer to the following for more information:

- Upgrading Oracle Virtual Directory When Using a Local Oracle WebLogic Server Domain
- Upgrading Oracle Virtual Directory When Using a Remote Oracle WebLogic Server Domain or No Domain

10.1 Understanding the Oracle Virtual Directory High Availability Upgrade

Before you begin using the procedures in this chapter, note the following.

Assumptions About the Active-Active Oracle Virtual Directory Upgrade

This chapter describes how to upgrade Oracle Virtual Directory in an active-active high-availability environment.

In this type of high availability environment, you upgrade Oracle Virtual Directory on two independent hosts. In this example, the two hosts are identfied as IDMHOST1 and IDMHOST2.

The procedures included here assume that Oracle Virtual Directory is the only component being upgraded in the Oracle Application Server 10*g* topology and that the Oracle Virtual Directory 10*g* intance and the Oracle Virtual Directory 11*g* instance are on the same host.

Upgrading Oracle Virtual Directory With and Without an Oracle WebLogic Server Domain

In Oracle Fusion Middleware 11*g*, you can optionally register Oracle Virtual Directory with an Oracle WebLogic Server domain. However, if you want to manage Oracle Virtual Directory with Oracle Enterprise Manager Fusion Middleware Control, then you must register the Oracle Virtual Directory instance with a domain.

Further, you can register Oracle Virtual Directory with a local or remote Oracle WebLogic Server domain. The registration can be completed during the upgrade or as a post-upgrade step.

10.2 Upgrading Oracle Virtual Directory When Using a Local Oracle WebLogic Server Domain

The following procedure describes how to upgrade Oracle Virtual Directory in a high availability environment when you are planning to create a new, local Oracle WebLogic Server domain as part of the Oracle Virtual Directory installation and upgrade process.

In this scenario, you create an Oracle WebLogic Server domain on IDMHOST1 along with the first Oracle Virtual Directory instance. Then, you install and configure the second Oracle Virtual Directory instance on IDMHOST2 and register the second Oracle Virtual Directory instance with the domain on IDMHOST1.

To upgrade Oracle Virtual Directory in this scenarios, refer to the following tasks:

- Task 1: On IDMHOST1, Optionally Install Oracle WebLogic Server and Create the Middleware Home

- Task 2: On IDMHOST1, Install and Configure Oracle Virtual Directory 11g

- Task 3: On IDMHOST1, Upgrade the Oracle Virtual Directory Instance to 11g

- Task 4: On IDMHOST2, Install and Configure the Second Oracle Virtual Directory Instance

- Task 5: On IDMHOST2, Upgrade the Second Oracle Virtual Directory Instance

- Task 6: On IDMHOST2, Register the Second Oracle Virtual Directory Instance with the Domain on IDMHOST1

10.2.1 Task 1: On IDMHOST1, Optionally Install Oracle WebLogic Server and Create the Middleware Home

If you want to associate the upgraded Oracle Virtual Directory instances with Oracle WebLogic Server, you must first install Oracle WebLogic Server and create the Middlewareware home.

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

10.2.2 Task 2: On IDMHOST1, Install and Configure Oracle Virtual Directory 11*g*

To install and configure Oracle Virtual Directory, in preparation for upgrade:

1. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

2. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

On UNIX systems, enter the following command to install Repository Creation Utility:

```
./runInstaller
```

On Windows systems, double-click the `setup.exe` file.

4. Refer to Table 10–1 for specific instructions about how to respond to each screen in the Oracle Identity Management installation and configuration tool.

For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

Table 10–1   Summary of Installation and Configuration Screens for Installing and Configuring Oracle Virtual Directory on IDMHOST1

Screen	Instructions
Welcome	Click Next.
Select Installation Type	Select **Install and Configure**. Click **Next**.
Prerequisite Checks	Click **Next**.
Select Domain	Select **Create New Domain** and enter the domain details.
Specify Installation Location	Specify the following values: ■ **Middleware Home Location:** Enter the complete path to the Middleware home you created in "Task 1: On IDMHOST1, Optionally Install Oracle WebLogic Server and Create the Middleware Home". ■ **Oracle Home Directory:** For the purposes of this example, enter `idm` as the name of the Oracle home directory. ■ **WebLogic Server Directory:** This is usually the `wlserver_10.3` inside the Middleware home. ■ **Oracle Instance Location:** Enter a path for the Oracle instance. This directory can be any acccessible directory location; unlike the Oracle home, it does not need to be inside the Middleware home. ■ **Oracle Instance Name:** For the purposes of this example, enter `idm_instance1`.
Specify Email for Security Updates	Choose how you want to be notified about security issues: ■ If you want to be notified about security issues through email, enter your email address in the Email field. ■ If you want to be notified about security issues through My Oracle Support, select the My Oracle Support option and enter your My Oracle Support Password. ■ If you do not want to be notified about security issues, leave all fields empty. Click **Next**.

Table 10–1   (Cont.) Summary of Installation and Configuration Screens for Installing and Configuring Oracle Virtual Directory on IDMHOST1

Screen	Instructions
Configure Components	Select **Oracle Virtual Directory**.
	When you select Oracle Virtual Directory, the Oracle Directory Services Manager and Fusion Middleware Control components are automatically selected for configuration.
Configure Ports	Select Auto Port Configuration.
Specify Oracle Virtual Directory Information	Select the following Client Listeners
	■ **LDAP v3 Namespace:** Enter the name space for Oracle Virtual Directory. The default value is dc=us,dc=oracle,dc=com.
	■ **HTTP Web Gateway:** Select this option to enable the Oracle Virtual Directory HTTP Web Gateway.
	■ **Secure**: Select this option if you enabled the HTTP Web Gateway and you want to secure it using SSL.
	Enter `cn=orcladmin` as the OVD Administrator and provide and confirm the password for the account.
	Select **Configure Admin Server in Secure Mode**.
	Click **Next**.
Installation Summary	Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.
Installation Progress	On UNIX systems, a dialog appears, prompting you to run the `oracleRoot.sh` script.
	Open a window and run the script, following the prompts in the window.
	Click **OK**.
Configuration	Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the Installation Complete screen appears.
	Click **Finish**, and then confirm your choice to exit

10.2.3 Task 3: On IDMHOST1, Upgrade the Oracle Virtual Directory Instance to 11*g*

Use the following procedure to upgrade the Oracle Virtual Directory instance to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Refer to Table 10–2 for instructions on how to respond to each Upgrade Assistant screen.

Table 10–2   Summary of Upgrade Screens When Upgrading Oracle Virtual Directory for High Availability

Screen	Instructions
Welcome	Click **Next**.
Select Operation	Select Upgrade Identity Management Instance. Click **Next**.
Specify Source Home	Select the 10*g* Release 2 (10.1.2) or 10*g* (10.1.4) source Oracle home. If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the 11*g* Oracle instance, or click **Browse** to locate the instance directory.
Specify WebLogic Server	This screen appears only if you chose to associate the Oracle Virtual Directory 11*g* instance with Oracle WebLogic Server during the Oracle Virtual Directory installation. If you selected to install Oracle Virtual Directory without an Oracle WebLogic Server domain, then this screen does not appear. Enter the host and Administration Server port for the Oracle WebLogic Server you configured in Section 10.2.1, "Task 1: On IDMHOST1, Optionally Install Oracle WebLogic Server and Create the Middleware Home".
Specify Upgrade Options	Select **Use source Oracle Home ports in destination**. Select **Start destination components after upgrade**. Click **Next**.
Examining Components	Click **Next**.
Summary	Click **Upgrade** to proceed with the upgrade process.
Upgrade Progress	Monitor the upgrade progress until the Upgrade Complete screen appears.
Upgrade Complete	Click **Close**.

4. Verify the upgraded Oracle Virtual Directory instance using the following OPMN command:

```
ORACLE_INSTANCE/bin/opmnctl status
```

You should see output similar to the following:

```
Processes in Instance: asinst_1
------------------------+-------------------+---------+---------
ias-component           | process-type      |     pid | status
------------------------+-------------------+---------+---------
ovd1                    | OVD               |   22091 | Alive
EMAGENT                 | EMAGENT           |       0 | NONE
```

10.2.4 Task 4: On IDMHOST2, Install and Configure the Second Oracle Virtual Directory Instance

Use the following instructions to install and configure the second Oracle Virtual Directory instance. For this instance, you install, configure, and upgrade the instance without a domain. Then, afte the upgrade, you register the upgraded instance with the domain you created on IDMHOST1:

1. Start Oracle Universal Installer:

On UNIX systems, enter the following command to install Repository Creation Utility:

```
./runInstaller
```

On Windows systems, double-click the setup.exe file.

2. Refer to Table 10–3 for specific instructions about how to respond to each screen in the Oracle Identity Management installation and configuration tool.

   For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

3. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

Table 10–3   Summary of Installation and Configuration Screens for Installing and Configuring Oracle Virtual Directory on IDMHOST2

Screen	Instructions
Welcome	Click Next.
Select Installation Type	Select **Install and Configure**. Click **Next**.
Prerequisite Checks	Click **Next**.
Select Domain	Select **Configure without a Domain** and enter the domain details.
Specify Installation Location	Specify the following values: ■ **Oracle Home Location:** /u01/app/oracle/product/11g/fmw_home ■ **Oracle Instance Location:** /u01/app/oracle/product/11g/instances/idm_instance1 ■ **Oracle Instance Name:** idm_instance1 Click **Next**.
Specify Email for Security Updates	Choose how you want to be notified about security issues: ■ If you want to be notified about security issues through email, enter your email address in the Email field. ■ If you want to be notified about security issues through My Oracle Support, select the My Oracle Support option and enter your My Oracle Support Password. ■ If you do not want to be notified about security issues, leave all fields empty. Click **Next**.
Configure Components	Select **Oracle Virtual Directory**.
Configure Ports	Select Auto Port Configuration.

Table 10–3 (Cont.) Summary of Installation and Configuration Screens for Installing and Configuring Oracle Virtual Directory on IDMHOST2

Screen	Instructions
Specify Oracle Virtual Directory Information	Client Listeners ■ **LDAP v3 Namespace:** ■ **HTTP Web Gateway:** ■ **Secure** OVD Administrator ■ **Username:** cn=orcladmin ■ **Password:** ******** ■ **Confirm Password**: ******** ■ **Configure Admin Server in Secure Mode** Click **Next**.
Installation Summary	Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click Install.
Installation Progress	On UNIX systems, a dialog appears, prompting you to run the `oracleRoot.sh` script. Open a window and run the script, following the prompts in the window. Click Ok.
Configuration	Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the Installation Complete screen appears. Click **Finish**, and then confirm your choice to exit

10.2.5 Task 5: On IDMHOST2, Upgrade the Second Oracle Virtual Directory Instance

Use the following procedure to upgrade the Oracle Virtual Directory instance to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Refer to Table 10–2 for instructions on how to respond to each Upgrade Assistant screen.

4. Verify the upgraded Oracle Virtual Directory instance using the following OPMN command:

   ```
   ORACLE_INSTANCE/bin/opmnctl status
   ```

   You should see output similar to the following:

   ```
   Processes in Instance: asinst_1
   -------------------------+--------------------+---------+---------
   ias-component            | process-type       |    pid  | status
   -------------------------+--------------------+---------+---------
   ```

```
ovd1                          | OVD                    |  22091 | Alive
EMAGENT                       | EMAGENT                |      0 | NONE
```

10.2.6 Task 6: On IDMHOST2, Register the Second Oracle Virtual Directory Instance with the Domain on IDMHOST1

Register the upgraded Oracle Virtual Directory instance with the Oracle WebLogic Server domain you created and configured on IDMHOST1:

Use the following OPMN command:

```
ORACLE_INSTANCE/opmnctl registerinstance
        -adminHost adminHostName
        -adminPort adminServerPort
        -adminUsername DOMAIN_ADMINISTRATOR_USERNAME
        -oracleInstance ORACLE_INSTANCE
```

10.3 Upgrading Oracle Virtual Directory When Using a Remote Oracle WebLogic Server Domain or No Domain

The following procedure describes how to upgrade Oracle Virtual Directory in a high availability environment in either of the following scenarios:

■   When you are planning to register the Oracle Virtual Directory environment with an existing remote Oracle WebLogic Server domain (on the host other than the hosts where Oracle Virtual Directory is installed).

■   When you are planning to install and configure the Oracle Virtual Directory environment in standalone mode (with no Oracle WebLogic Server domain).

This procedure assumes you either have a remote Oracle WebLogic Server domain already installed and configured on a remote host, or you have no plans to register Oracle Virtual Directory with Oracle WebLogic Server.

To upgrade Oracle Virtual Directory in these scenarios, refer to the following tasks:

■   Task 1: On IDMHOST1, Install and Configure Oracle Virtual Directory 11g

■   Task 2: On IDMHOST1, Upgrade the Oracle Virtual Directory Instance to 11g

■   Task 3: On IDMHOST2, Install and Configure the Second Oracle Virtual Directory Instance

■   Task 4: On IDMHOST2, Upgrade the Second Oracle Virtual Directory Instance

■   Task 5: On IDMHOST2, Optionally Register the Second Oracle Virtual Directory Instance with the Domain on WLSHOST1

10.3.1 Task 1: On IDMHOST1, Install and Configure Oracle Virtual Directory 11*g*

To install and configure Oracle Virtual Directory, in preparation for upgrade:

1.   Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

2.   If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

3. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the `setup.exe` file.

4. Refer to Table 10–3 for specific instructions about how to respond to each screen in the Oracle Identity Management installation and configuration tool.

   For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

5. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

10.3.2 Task 2: On IDMHOST1, Upgrade the Oracle Virtual Directory Instance to 11*g*

Use the following procedure to upgrade the Oracle Virtual Directory instance to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Refer to Table 10–2 for instructions on how to respond to each Upgrade Assistant screen.

4. Verify the upgraded Oracle Virtual Directory instance using the following OPMN command:

   ```
   ORACLE_INSTANCE/bin/opmnctl status
   ```

   You should see output similar to the following:

   ```
   Processes in Instance: asinst_1
   ------------------------+-------------------+---------+---------
   ias-component           | process-type      |     pid | status
   ------------------------+-------------------+---------+---------
   ovd1                    | OVD               |   22091 | Alive
   EMAGENT                 | EMAGENT           |       0 | NONE
   ```

10.3.3 Task 3: On IDMHOST2, Install and Configure the Second Oracle Virtual Directory Instance

Use the following instructions to install and configure the second Oracle Virtual Directory instance. For this instance, you install, configure, and upgrade the instance without a domain. Then, afte the upgrade, you register the upgraded instance with the domain you created on IDMHOST1:

1. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the `setup.exe` file.

2. Refer to Table 10–3 for specific instructions about how to respond to each screen in the Oracle Identity Management installation and configuration tool.

   For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and prompts required during an Oracle Virtual Directory installation.

3. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

10.3.4 Task 4: On IDMHOST2, Upgrade the Second Oracle Virtual Directory Instance

Use the following procedure to upgrade the Oracle Virtual Directory instance to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Refer to Table 10–2 for instructions on how to respond to each Upgrade Assistant screen.

4. Verify the upgraded Oracle Virtual Directory instance using the following OPMN command:

   ```
   ORACLE_INSTANCE/bin/opmnctl status
   ```

   You should see output similar to the following:

   ```
   Processes in Instance: asinst_1
   ------------------------+--------------------+---------+---------
   ias-component           | process-type       |     pid | status
   ------------------------+--------------------+---------+---------
   ovd1                    | OVD                |   22091 | Alive
   EMAGENT                 | EMAGENT            |       0 | NONE
   ```

10.3.5 Task 5: On IDMHOST2, Optionally Register the Second Oracle Virtual Directory Instance with the Domain on WLSHOST1

Register the upgraded Oracle Virtual Directory instance with an existing Oracle WebLogic Server domain you created and configured on WLSHOST1:

Use the following OPMN command:

```
ORACLE_INSTANCE/opmnctl registerinstance
        -adminHost adminHostName
        -adminPort adminServerPort
        -adminUsername DOMAIN_ADMINISTRATOR_USERNAME
        -oracleInstance ORACLE_INSTANCE
```

11

Upgrading an Oracle Identity Federation High Availability Environment

This chapter describes how to upgrade Oracle Identity Federation in a high availability environment.

This chapter contains the following sections:

- Task 1: Understand the Oracle Identity Federation High Availability Upgrade
- Task 2: Install the Oracle Identity Federation Schema in the Database
- Task 3: Install Oracle WebLogic Server and Create the Middleware Home
- Task 4: Configure the Oracle WebLogic Server Domain with Only Oracle Enterprise Manager Fusion Middleware Control
- Task 5: Extend the Domain and Create the First Oracle Identity Federation 11g Oracle Instance
- Task 6: Use the Upgrade Assistant to Upgrade the First Oracle Identity Federation Oracle Instance
- Task 7: Install Oracle WebLogic Server and Create the Middleware Home on IDMHOST2
- Task 8: Deinstall the Oracle Identity Federation 10g Instance on IDMHOST2
- Task 9: Install and Configure the Second Oracle Identity Federation Instance on IDMHOST2
- Task 10: Copy the Oracle Identity Federation Application from IDMHOST1 to IDMHOST2
- Task 11: Start the Managed Server on IDMHOST2
- Task 12: Complete Post-Upgrade Procedures
- Task 13: Verify the Oracle Identity Federation High Availbility Upgrade

11.1 Task 1: Understand the Oracle Identity Federation High Availability Upgrade

Refer to the following sections to prepare for the Oracle Identity Federation high availbility upgrade:

- Prerequisites for Oracle Identity Federation High Availability Upgrade
- Conventions Used in This Chapter

11.1.1 Prerequisites for Oracle Identity Federation High Availability Upgrade

Before you begin this upgrade procedure, it is assumed that:

- The 10g source topology is equivalent to the 11g destination topology.

  In other words, the Oracle Identity Federation topology that you are planning to install should be similar in its design to the 10*g* environment. For example, it is assumed that you will be running the same number hosts and the same number Oracle Identity Federation instances in the 11*g* environment.

- For each Oracle Identity Federation instance you are upgrading, the target Oracle Identity Federation 11*g* Oracle Home must be on the same host as the source Oracle Identity Federation 10*g* Oracle home.

- The database that will be used to host the Oracle Identity Federation schema has been upgraded to a version supported by Oracle Fusion Middleware 11*g*.

  For more information, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

- If you are also upgrading the associated Oracle HTTP Server, stop all processes for any additional Oracle Identity Federation 10*g* installations on other hosts, prior to beginning the upgrade process.

  For more information about upgrading the Oracle HTTP Server associated with your Oracle Identity Federation 10*g* installations, see Section 11.5.2, "About Selecting and Configuring Oracle HTTP Server with Oracle Identity Federation".

11.1.2 Conventions Used in This Chapter

The examples in this chapter assume you are upgrading two Oracle Identity Federation instances running on two separate host computers. These are referre to as IDMHOST1 and IDMHOST2.

In addition, the examples assume you have two database servers, also running two separate hosts, DBHOST1 and DBHOST2.

11.2 Task 2: Install the Oracle Identity Federation Schema in the Database

Before you can install Oracle Identity Federation 11*g* in preparation for upgrade, you must install the Oracle Identity Federation 11*g* schema in a supported database.

You use the Repository Creation Utility to create the schema and select the Oracle Identity Federation component on the Select Components screen of the Repository Creation Utility.

For more information, refer to Section 6.2, "Task 2: Use the Repository Creation Utility to Install the Oracle Identity Federation Schema in the Database".

11.3 Task 3: Install Oracle WebLogic Server and Create the Middleware Home

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

11.4 Task 4: Configure the Oracle WebLogic Server Domain with Only Oracle Enterprise Manager Fusion Middleware Control

Use the following procedure to install and configure Oracle Internet Directory in preparation for an Oracle Identity Federation high availability upgrade:

1. Review the first four chapters of the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

   These chapters include important pre-installation information, such as system requirements and prerequisite tasks.

2. Make sure that the port numbers `7001` and `5556` are not in use by any service on the computer.

   For example, on UNIX systems, enter the following commands. If a port is not in use, no output is returned from the command:

   ```
   netstat -an | grep "7001"
   netstat -an | grep "5556"
   ```

   On the Windows operating system:

   ```
   netstat -an | findstr "LISTEN" | findstr "7001"
   netstat -an | findstr "LISTEN" | findstr "5556"
   ```

   If the ports are in use (if the command returns output identifying the port), you must free them.

   For example, on UNIX systems, if the port is in use by one or more services, remove the entries for ports `7001` and `5556` in the `/etc/services` file and restart the services, or restart the computer.

3. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

4. Copy the `staticports.ini` file from the following directory on the CD–ROM, or from the directory where you downloaded and unpacked the software download, to a temporary directory:

   ```
   Disk1/stage/Response
   ```

5. Edit the `staticports.ini` file that you copied to the temporary directory and assign the following custom ports:

   ```
   Domain Port No: 7001
   Node Manager Port No: 5556
   ```

   You will need to reference the location of this file later in the installation procedure.

6. If you are installing from the CD–ROM, then navigate to the root directory of the CD–ROM.

   Or, if you downloaded and unpacked the software from the Oracle Technology Network, then change directory to the `Disk1` directory in the location where you unpacked the software.

7. Start Oracle Universal Installer:

On UNIX systems, enter the following command to install Repository Creation Utility:

```
./runInstaller
```

On Windows systems, double-click the `setup.exe` file.

8. Follow the instructions in the installer to install Oracle Identity Federation.

   Refer to the following resources during the installation and configuration:

   Table 11–1, which provides information on specific instructions required when installing and configuring the software for an Oracle Identity Federation high availability upgrade.

   Oracle Fusion Middleware Installation Guide for Oracle Identity Management or click **Help** for general information about the prerequisites and other prompts required during an Oracle Identity Federation installation.

9. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

Table 11–1 Summary of the Installation Screens When Installing and Configuring Oracle Identity Federation High Availability in Preparation for Upgrade

Screen	Description and Actions to Take
Specify Inventory Directory	If you are installing on a UNIX system, and if this is the first time any Oracle product is being installed on your system with the Oracle Universal Installer, provide the location of an inventory directory.
	This is where the installer will set up subdirectories and maintain inventory data for each Oracle product that is installed on this system.
	If this screen appears, then enter the following:
	■ **Specify the Inventory Directory:** *path*/oraInventory
	For example: /u01/app/oraInventory
	■ **Operating System Group Name:** oinstall
Inventory Location Confirmation dialog	If the Specify Inventory Directory screen appears, then it is followed by this dialog box. Follow the instructions in the dialog box and log in as root and run the following script:
	orainventory_directory/createCentralInventory.sh
	For example:
	/u01/app/oraInventory/createCentralInventory.sh
Welcome	Click **Next** to begin the installation.
Select Installation Type	Select **Install and Configure**.
Prerequisite Checks	This screen verifies that your host computer meets all the system requirements for the Oracle Identity Management components.
Select Domain	Select **Create New Domain**, and provide a password for the `weblogic` administrator user.
	Enter an easy to recognize domain name, such as `ODMDomain`.

Table 11–1   (Cont.) Summary of the Installation Screens When Installing and Configuring Oracle Identity Federation High Availability in Preparation for Upgrade

Screen	Description and Actions to Take
Specify Installation Locations	■ Specify the location of the Middleware home and Oracle WebLogic Server directory you created in "Task 3: Install Oracle WebLogic Server and Create the Middleware Home". ■ Specify a name for the Oracle home that will be created inside the Middleware home during this installation. For this example, use the Oracle home name `oif`. ■ Specify a name and location for the Oracle instance that will be created during this installation. For this example, enter `admin_inst`. For this high availability environment, this will identify the Oracle instance where Fusion Middleware Control and the Oracle WebLogic Server Administration Console are running. For more information, click **Help** or refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.
Specify Email for Security Updates	Choose how you want to be notified about security issues: ■ If you want to be notified about security issues through email, enter your email address in the **Email** field. ■ If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the **My Oracle Support** option and enter your My Oracle Support Password. ■ If you do not want to be notified about security issues, leave all fields empty.
Configure Components	This screen identifies the components that will be configured during this installation and configuration session. For the purposes of this procedure, select only **Enterprise Manager**. Do not select any other components on this screen. You will configure the Oracle Identity Federation component later.
Configure Ports	Select **Specify Ports using Configuration file** and enter the full path to `staticports.ini` file that you edited and saved in the temporary directory.
Installation Summary	Review the review the choices you made. If you need to make any changes click **Back**. If you made the correct selections, click **Install**.
Installation Progress	Monitor the progress of the installation of the files onto disk.
oracleRoot.sh script dialog box	During installation on UNIX platforms, this dialog box prompts you to log in as the root user and run the `oracleRoot.sh` script. You must log in as the root user because the script creates files, edits files, and changes the permissions of certain Oracle executable files in the `/usr/local/bin/` directory.
Configuration progress	Monitor the progress of the software configuration.
Installation Complete	Click **Finish** to finish the installation and quit the installer.

11.5 Task 5: Extend the Domain and Create the First Oracle Identity Federation 11*g* Oracle Instance

Now that you have configured an Oracle WebLogic Server domain, you can extend the domain and create the first Oracle Identity Federation component Oracle instance. Refer to the following sections for more information:

■ Extending the Domain and Configuring Oracle Identity Federation

■ About Selecting and Configuring Oracle HTTP Server with Oracle Identity Federation

11.5.1 Extending the Domain and Configuring Oracle Identity Federation

To extend the domain and configure Oracle Identity Federation:

1. Review the first four chapters of the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

   These chapters include important pre-installation information, such as system requirements and prerequisite tasks.

2. Make sure that the port number 7499 is not in use by any service on the computer.

   On the UNIX operating system:

   ```
   netstat -an | grep "7499"
   ```

   On the Windows operating system:

   ```
   netstat -an | findstr "LISTEN" | findstr "7499"
   ```

   If the ports are in use (if the command returns output identifying the port), you must free them.

   For example, on UNIX systems, if the port is in use by a service, remove the entry for port 7499 in the /etc/services file and restart the service, or restart the computer.

3. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

4. Copy the staticports.ini file from the following directory on the CD–ROM, or from the directory where you downloaded and unpacked the software download, to a temporary directory:

   ```
   Disk1/stage/Response
   ```

5. Edit the staticports.ini file that you copied to the temporary directory and assign the following custom ports:

   ```
   [OIF]
   # The OIF Server Port
   OIF Server Port = 7499
   ```

   You will need to reference the location of this file later in the installation procedure of the first Oracle Identity Federation instance.

6. Start Oracle Identity Management configuration tool by running the following command:

   ```
   OIF_ORACLE_HOME/bin/config.sh
   ```

   For example:

   ```
   /u01/app/oracle/product/fmw/idm/bin/config.sh
   ```

7. Follow the instructions in the configuration wizard to extend the existing domain.

   Refer to the following resources during the installation and configuration:

- Table 11–2, which provides information on specific instructions required when installing and configuring the software for an Oracle Identity Federation high availability upgrade.

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and other prompts required during an Oracle Identity Federation installation.

8. When the installation and configuration is complete, exit from the configuration tool.

Table 11–2   Summary of the Configuration Screens When Configuring the First Oracle Identity Federation Oracle Instance

Screen	Description and Actions to Take
Welcome	Click **Next** to start configuring the Oracle Identity Federation
Select Domain	- Select **Extend Existing Domain**. - Enter the host, port, and administration credentials for the domain you created in "Task 4: Configure the Oracle WebLogic Server Domain with Only Oracle Enterprise Manager Fusion Middleware Control".
Specify Installation Locations	- The first two fields on this page are read-only. - In the **WebLogic Server Directory** field, enter the name and path of the `wlserver_10.3` directory inside the existing Middleware home. - In the **Oracle Instance Location** field, Enter the path to the location where you want to create the Oracle Instance directory. Do not enter a path to an existing directory that contains files—if you enter a path to an existing directory, that directory must be empty. - In the **Instance Name** field, enter `oif_inst1` to identify this as the first Oracle Identity Federation instance in the high availability topology. For more information, click **Help** or refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.
Specify Email for Security Updates	Choose how you want to be notified about security issues: - If you want to be notified about security issues through email, enter your email address in the **Email** field. - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the **My Oracle Support** option and enter your My Oracle Support Password. - If you do not want to be notified about security issues, leave all fields empty.
Configure Components	This screen identifies the components to configure during this installation and configuration session. For the purposes of this procedure: - Select only **Oracle Identity Federation**. Do not select any other components on this screen. Oracle Identity Federation can be configured with Oracle HTTP Server. For more information, see Section 11.5.2, "About Selecting and Configuring Oracle HTTP Server with Oracle Identity Federation" - Select the **Clustered** check box.
Configure Ports	Select **Specify Ports using Configuration file** and enter the full path to `staticports.ini` file that you edited and saved in the temporary directory.

Table 11–2   (Cont.) Summary of the Configuration Screens When Configuring the First Oracle Identity Federation Oracle Instance

Screen	Description and Actions to Take
Specify OIF Details	For this example, enter the following in the fields on this screen: ■ **PKCS12 Password:** Enter a security password. ■ **Confirm Password:** Enter the password again to confirm you typed it correctly. ■ **Server Id:** For this example, enter `oif_OIFDomain`.
OIF Advanced Flow Attributes	Enter the following for each field on this screen: **Authentication Type:** JAAS **User Store:** NONE **Federation Store:** NONE **User Session Store:** RDBMS (default selection, which cannot be changed for a cluster) **Message Store:** RDBMS (default selection, which cannot be changed for a cluster. **Configuration Store:** RDBMS (default selection, which cannot be changed for a cluster.

Transient Store Database Details	Enter the following information on this screen:
	■ **Connect String:** Provide the connect string to your database. If it is a RAC database, then enter each node, separated with the carot character (^). For example:
	`oifdbhost1-vip.mycompany.com:1521:oifdb1^`
	`oifdbhost2-vip.mycompany.com:1521:oifdb2@ oifdb.mycompany.com`
	■ **User Name:** Enter the name (including the prefix) for the Oracle Identity Federation schema that you created in Section 11.2, "Task 2: Install the Oracle Identity Federation Schema in the Database"
	■ **Password:** The password you entered when you created the Oracle Identity Federation schema.

Installation Summary	Review the review the choices you made. If you need to make any changes click **Back**. If you made the correct selections, click **Install**.
Installation Progress	Monitor the progress of the installation of the files onto disk.
oracleRoot.sh script dialog box	During installation on UNIX platforms, this dialog box prompts you to log in as the root user and run the `oracleRoot.sh` script. You must log in as the root user because the script creates files, edits files, and changes the permissions of certain Oracle executable files in the `/usr/local/bin/` directory.
Configuration progress	Monitor the progress of the software configuration.
Installation Complete	Click **Finish** to finish the installation and quit the installer.

11.5.2 About Selecting and Configuring Oracle HTTP Server with Oracle Identity Federation

Oracle Identity Federation requires an Oracle HTTP Server instance. However, you can choose to install and configure the Oracle HTTP Server instance on the same host as Oracle Identity Federation, or you can install it on a separate host as part of a Web tier installation.

Note the following when deciding whether or not to install Oracle HTTP Server on the same host or not:

■ If you install Oracle HTTP Server on the same host as Oracle Identity Federation, you can use the Oracle Fusion Middleware Upgrade Assistant to upgrade the

Oracle HTTP Server instance at the same time you are upgrading Oracle Identity Federation.

This means that the Upgrade Assistant can then migrate all your SSL certificates, OSSO integration configuration from the source Oracle Identity Federation 10*g* source topology to the Oracle Identity Federation 11*g* destination topology.

■ If you install Oracle HTTP Server on a separate host, the Upgrade Assistant will not migrate the SSL certificates and OSSO integration configuration. These artifacts will have to be migrated manually post upgrade.

11.6 Task 6: Use the Upgrade Assistant to Upgrade the First Oracle Identity Federation Oracle Instance

The Oracle Fusion Middleware Upgrade Assistant automates the upgrade of many aspects of your Oracle Application Server 10*g* environment.

The Upgrade Assistant is installed automatically into the `bin` directory of your Oracle Fusion Middleware Oracle home.

The following sections provide more information:

■ Task 6a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade

■ Task 6b: Upgrade Oracle Identity Federation

11.6.1 Task 6a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade

To start the Upgrade Assistant using the graphical user interface:

Note: You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

---

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

On UNIX system:

```
./ua
```

On Windows systems:

```
ua.bat
```

The Upgrade Assistant displays the Welcome screen as shown in Figure 11–1

Figure 11–1   Upgrade Assistant Welcome Screen
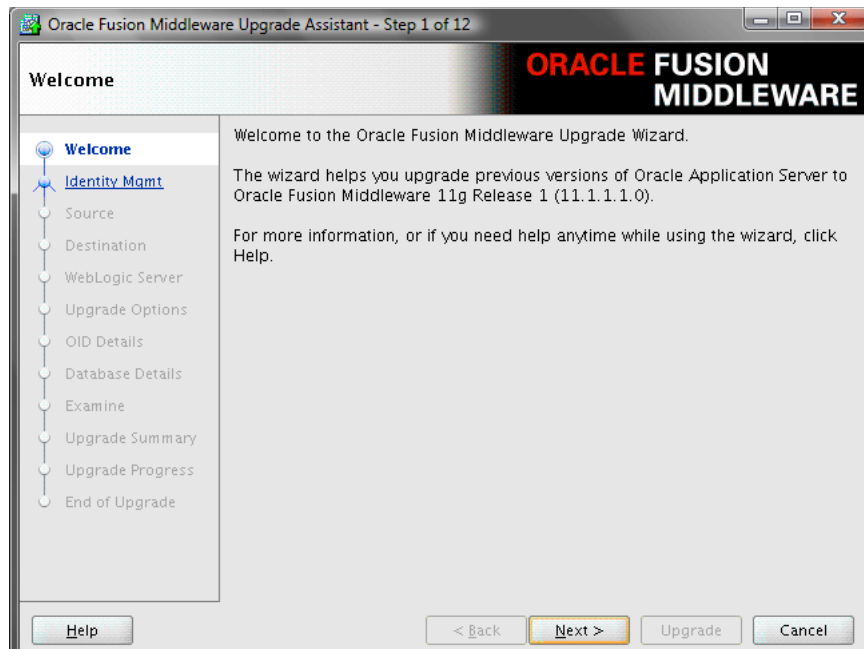
3. Click **Next** to display the Select Operation screen (Figure 11–2).

The options available in the Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Identity Management Oracle home, the options shown on the Select Operation screen are the valid options for an Oracle Identity Management Oracle home.

Figure 11–2   Upgrade Assistant Select Operation Screen for an Oracle Identity Federation Upgrade
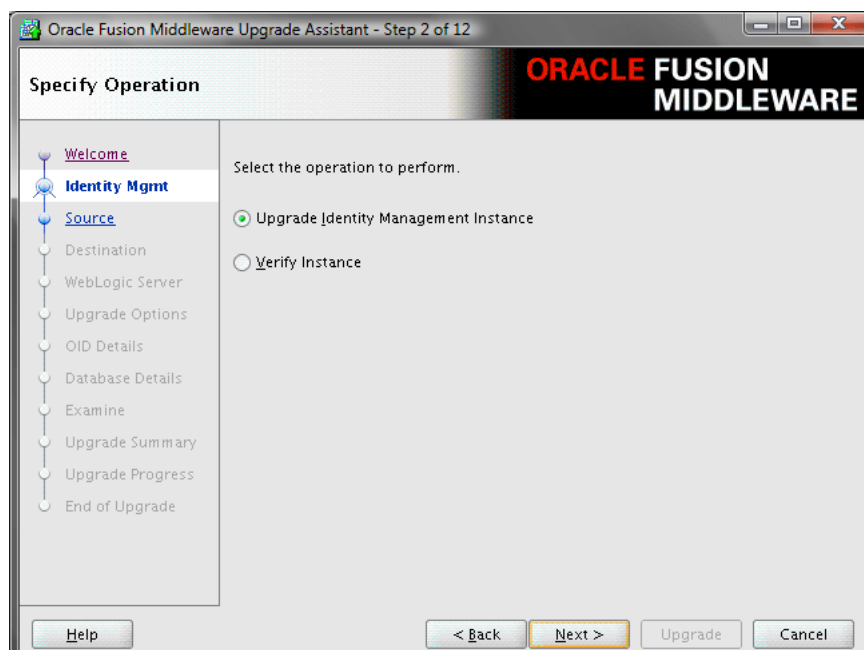
11.6.2 Task 6b: Upgrade Oracle Identity Federation

When you upgrade Oracle Identity Federation, the Upgrade Assistant upgrades the configuration files in the Oracle Identity Federation middle tier.

To upgrade Oracle Identity Federation when they reside in the same Oracle instance:

1. Start the Upgrade Assistant as described in Task 6a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade.

2. Select **Upgrade Identity Management Instance** on the Select Operation screen (Figure 11–2).

3. Refer to Table 11–3 for a description of the Upgrade Assistant screens that require input from you during an Oracle Identity Federation upgrade.

4. After the Specify Upgrade Options screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

    ■   Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

    ■   Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

    ■   Provides a progress screen so you can see the status of the upgrade as it proceeds.

    ■   Alerts you of any errors or problems that occur during the upgrade.

        See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

    ■   Displays the End of Upgrade screen, which confirms that the upgrade was complete.

5. Exit the Upgrade Assistant.

Table 11–3   Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* (10.1.4.0.1) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the destination 11*g* Oracle home that you installed inside the middleware home. This is the Oracle home that contains the Oracle Identity Federation software.
	Alternatively, click **Browse** to select the directory.
Specify WebLogic Server	Enter the host, Administration Server port, and administration user credentials for the Oracle WebLogic Server domain you configured in Section 11.4, "Task 4: Configure the Oracle WebLogic Server Domain with Only Oracle Enterprise Manager Fusion Middleware Control".

Table 11–3   (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	This screen offers these upgrade options:
	■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance.
	Note that Oracle recommends that you always select this option when upgrading Oracle Identity Federation.
	■ **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade.
	For the purposes of this example, select both of these upgrade options.

11.7 Task 7: Install Oracle WebLogic Server and Create the Middleware Home on IDMHOST2

Before you can expand the Oracle WebLogic Server cluster you created on IDMHOST1 to include IDMHOST2, you must install the Oracle WebLogic Server binary files on IDMHOST2 and create Middleware home on IDMHOST2.

To install Oracle WebLogic Server and create the middleware home, refer to "Installing Oracle WebLogic Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

11.8 Task 8: Deinstall the Oracle Identity Federation 10*g* Instance on IDMHOST2

Before you install Oracle Identity Federation 11*g* on the second host in your Oracle Identity Federation high availability environment, Oracle recommends that you remove (deinstall) the Oracle Identity Federation 10*g* instance that is currently running on the second host.

This step is necessary to avoid port conflicts between the existing Oracle Identity Federation 10*g* instance and the new Oracle Identity Federation 11*g* instance.

For more information, see the following topics:

- Procedure for Deinstalling the Oracle Identity Federation 10g Instance
- Alternative Procedure to Avoid Port Conflicts

11.8.1 Procedure for Deinstalling the Oracle Identity Federation 10*g* Instance

For instructions on deinstalling Oracle Identity Federation 10*g*, refer to Section 5.4, "Un-installing Oracle Identity Federation" in the *Oracle Identity Federation Administrator's Guide*, which is available in the Oracle Application Server 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN):

```
http://www.oracle.com/technology/documentation/oim1014.html
```

11.8.2 Alternative Procedure to Avoid Port Conflicts

If deinstalling Oracle Identity Federation 10*g* is not an option for your organization, you can consider the following alternative solution, which involves modifying Oracle HTTP Server 10*g* configuration files.

To modify the Oracle HTTP Server 10*g* instance to avoid port conflicts during the Oracle Identity Federation 11*g* installation:

1. Change directory to the Oracle HTTP Server configuration directory:

   `10g_ORACLE_HOME\Apache\Apache\conf\`

2. Create a backup copy of the files following files in this directory:

   ```
   httpd.conf
   ssl.conf
   ```

3. Edit the file `httpd.conf`, and search for any occurrence of the HTTP Non-SSL Port that you need to reuse during the Oracle Identity Federation 11*g* installation.

4. For each each occurrence, edit or remove the value from the `httpd.conf` file.

   For example, if the HTTP Non-SSL port is `7786`, remove the value, or change the value from `7786` to `77861`.

5. In a similar manner, edit the file `ssl.conf` file and search for any occurrence of the HTTP SSL Port that you need to reuse.

6. For each occurrence, edit or remove the value from the `ssl.conf` file.

11.9 Task 9: Install and Configure the Second Oracle Identity Federation Instance on IDMHOST2

To install and configure the domain and configure Oracle Identity Federation:

1. Review the first four chapters of the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

   These chapters include important pre-installation information, such as system requirements and prerequisite tasks.

2. Make sure that the port number `7499` is not in use by any service on the computer.

   On the UNIX operating system:

   `netstat -an | grep "7499"`

   On the Windows operating system:

```
netstat -an | findstr "LISTEN" | findstr "7499"
```

If the ports are in use (if the command returns output identifying the port), you must free them.

For example, on UNIX systems, if the port is in use by a service, remove the entry for port 7499 in the /etc/services file and restart the service, or restart the computer.

3. Locate the Oracle Identity Management CD–ROM.

   Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

   ```
   http://www.oracle.com/technology/
   ```

4. Copy the staticports.ini file from the following directory on the CD–ROM, or from the directory where you downloaded and unpacked the software download, to a temporary directory:

   ```
   Disk1/stage/Response
   ```

5. Edit the staticports.ini file that you copied to the temporary directory and assign the following custom port:

   ```
   [OHS]
   #The Listen Port For OHS
   Oracle Http Server Administrator Port No = 10g Non-SSL Value

   #The SSL Port For OHS
   Oracle Http Server SSL Port No = 10g SSL Value

   [OIF]
   # The OIF Server Port
   OIF Server Port = 7499
   ```

   You will need to reference the location of this file later in the installation procedure.

6. Start Oracle Universal Installer:

   On UNIX systems, enter the following command to install Repository Creation Utility:

   ```
   ./runInstaller
   ```

   On Windows systems, double-click the setup.exe file.

7. Follow the instructions in the installer to install Oracle Identity Federation.

   Refer to the following resources during the installation and configuration:

   Table 11–2, which provides information on specific instructions required when installing and configuring the software for an Oracle Identity Federation high availability upgrade.

   Oracle Fusion Middleware Installation Guide for Oracle Identity Management or click **Help** for general information about the prerequisites and other prompts required during an Oracle Identity Federation installation.

8. When the installation and configuration is complete, exit from the Oracle Identity Management installation and configuration tool.

Table 11–4   Summary of the Installation Screens When Configuring the Second Oracle Identity Federation Oracle Instance

Screen	Description and Actions to Take
Specify Inventory Directory	If you are installing on a UNIX system, and if this is the first time any Oracle product is being installed on your system with the Oracle Universal Installer, provide the location of an inventory directory. This is where the installer will set up subdirectories and maintain inventory data for each Oracle product that is installed on this system. If this screen appears, then enter the following: ■ **Specify the Inventory Directory:** `path`/oraInventory For example: `/u01/app/oraInventory` ■ **Operating System Group Name:** `oinstall`
Inventory Location Confirmation dialog	If the Specify Inventory Directory screen appears, then it is followed by this dialog box. Follow the instructions in the dialog box and log in as root and run the following script: `orainventory_directory`/createCentralInventory.sh For example: `/u01/app/oraInventory/createCentralInventory.sh`
Welcome	Click **Next** to begin the installation.
Select Installation Type	Select **Install and Configure**.
Prerequisite Checks	This screen verifies that your host computer meets all the system requirements for the Oracle Identity Management components.
Select Domain	Select **Expand Cluster** and enter the domain details. Enter the host, port, user name, and password for the administration server in the domain you created on IDMHOST1 in "Task 4: Configure the Oracle WebLogic Server Domain with Only Oracle Enterprise Manager Fusion Middleware Control". For more information, click **Help** or refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
Specify Installation Locations	■ Specify the location of the Middleware home and Oracle WebLogic Server directory you created in "Task 7: Install Oracle WebLogic Server and Create the Middleware Home on IDMHOST2". ■ Specify a name for the Oracle home that will be created inside the Middleware home during this installation. For this example, enter `oif` to identify this as the Oracle home that contains the program files for the first Oracle Identity Federation intance. ■ Specify a name and location for the Oracle instance that will be created during this installation. Enter `oif_inst2` to identify this as the second Oracle Identity Federation instance in the high availability topology. For more information, click **Help** or refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.
Specify Email for Security Updates	Choose how you want to be notified about security issues: ■ If you want to be notified about security issues through email, enter your email address in the **Email** field. ■ If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the **My Oracle Support** option and enter your My Oracle Support Password. ■ If you do not want to be notified about security issues, leave all fields empty.

Table 11–4   (Cont.) Summary of the Installation Screens When Configuring the Second Oracle Identity Federation Oracle Instance

Screen	Description and Actions to Take
Configure Components	This screen identifies the components to configure during this installation and configuration session. Select only **Oracle Identity Federation**. Do not select any other components on this screen. Oracle Identity Federation can be configured with Oracle HTTP Server. For more information, see Section 11.5.2, "About Selecting and Configuring Oracle HTTP Server with Oracle Identity Federation"
Installation Summary	Review the review the choices you made. If you need to make any changes click **Back**. If you made the correct selections, click **Install**.
Installation Progress	Monitor the progress of the installation of the files onto disk.
oracleRoot.sh script dialog box	During installation on UNIX platforms, this dialog box prompts you to log in as the root user and run the `oracleRoot.sh` script. You must log in as the root user because the script creates files, edits files, and changes the permissions of certain Oracle executable files in the `/usr/local/bin/` directory.
Configuration progress	Monitor the progress of the software configuration.
Installation Complete	Click **Finish** to finish the installation and quit the installer.

11.10 Task 10: Copy the Oracle Identity Federation Application from IDMHOST1 to IDMHOST2

The Oracle Directory Integration Platform application is deployed on IDMHOST1 as an externally staged application. The application must be copied from IDMHOST1 to OIFHOST2; otherwise the managed server on IDMHOST2 is listed in the Oracle WebLogic Server administration console as being in an "unknown" state:

1. Locate the `applications` directory in the Oracle WebLogic Server domain directory on IDMHOST1:

   ```
   MW_HOME/user_projects/domains/OIFDomain/config/fmwconfig/servers
           /wls_oif1/applications
   ```

2. Copy the `applications` directory on and its contents on IDMHOST1 to the same location in the domain directory on IDMHOST2.

   For example:

   ```
   scp -rp MW_HOME/user_projects/domains/OIFDomain/config/fmwconfig/servers
                  /wls_oif1/applications
           user@IDMHOST2:MW_HOME/user_projects/domains/OIFDomain/config/fmwconfig
                       /servers/wls_oif2/applications
   ```

11.11 Task 11: Start the Managed Server on IDMHOST2

Follow these steps to start the wls_ods2 managed server in a cluster:

1. Open a browser and navigate to the WebLogic Administration Console at:

   ```
   http://idmhost1.mycompany.com:port/console
   ```

2. Log in to the WebLogic Administration Console using the administrator credentials.

3. In the left pane of the WebLogic Administration Console, expand **Environment** and select **Clusters**.

4. Select the cluster (`cluster_oif`) containing the managed server (`wls_oif2`) you want to start.

5. Select **Control**.

6. Under Managed Server Instances in this Cluster, select the check box next to the managed server (`wls_ods2`) you want to start and click **Start**.

7. On the Server Life Cycle Assistant page, click **Yes** to confirm.

> **Note:** Node Manager starts the server on the target machine. When the Node Manager finishes its start sequence, the server's state is indicated in the **State** column in the Server Status table.

11.12 Task 12: Complete Post-Upgrade Procedures

Refer to the following sections for information about important post-upgrade Oracle Identity Federation high availability procedures:

- Configuring Routing Between Oracle Identity Federation and Oracle HTTP Server
- Configuring the Load Balancer
- Set Oracle Identity Federation Configuration Properties

11.12.1 Configuring Routing Between Oracle Identity Federation and Oracle HTTP Server

Follow the steps shown below to create a new Oracle HTTP Server instance and to enable communication between the Oracle HTTP Server instance and the Oracle Identity Federation server instance on IDMHOST1 and IDMHOST2.

When you install and configure Oracle Identity Federation, the Oracle HTTP Server software is installed in the Oracle home, but an Oracle HTTP Server instance is not configured by default:

1. Create an Oracle HTTP Server instance to configure with Oracle Identity Federation:

```
INSTANCE_HOME/bin/opmnctl createcomponent
        -componentType OHS
        -componentName ohs1
```

2. On IDMHOST2, edit the following configuration file:

```
INSTANCE_HOME/config/OHS/ohs_name/moduleconf/oif.conf
```

In this example, *ohs_name* is the name of the Oracle HTTP Server component; for example: `ohs1`

3. Uncomment and set the `WebLogicCluster` variable to reference the managed servers running the Oracle Identity Federation Server instances.

For example, if the host and port of each managed server is as follows:

```
idmhost1.mycompany.com:7499
idmhost2.mycompany.com:7499
```

Then update the file to contain the following entry:

```
<Location /fed>
    WebLogicCluster idmhost1.mycompany.com:7499,idmhost2.mycompany.com:7499
    SetHandler weblogic-handler
</Location>
```

4. Save the `oif.conf` file.

5. Start the Oracle HTTP Server as shown below:

   INSTANCE_HOME /bin/opmnctl startproc process-type=OHS

11.12.2 Configuring the Load Balancer

Oracle Identity Federation topologies deployed in high availability configurations are front-ended by an external load balancer, which provides load balancing of the HTTP requests between the various OIF instances.

After upgrading the Oracle Identity Federation high availability environment, configure your load balancer to listen to the Oracle HTTP Server instances on IDMHOST1 and IDMHOST2.

Refer to the documentation provided by the load balancer vendor to accomplish this task.

11.12.3 Set Oracle Identity Federation Configuration Properties

Follow the steps below to enable the Oracle Identity Federation instances on IDMHOST1 and IDMHOST2 to recognize the Load Balancer Virtual Hostname.

Use Oracle Enterprise Manager Fusion Middleware Control to complete this task.

1. Log in to Fusion Middleware Control and locate the Oracle Identity Federation instance home page.

2. Modify the server properties as follows:

   a. From the **Oracle Identity Federation** menu, select **Administration**, and then **Server Properties**.

   b. Change the **Host** field to reflect the virtual host name of the load balancer.

   c. Change the **Port** and **SSL Enabled**, as well as the **SOAP Port** and **SSL Enabled** options to reflect the ports used by the load balancer.

   d. Save the changes.

3. Modify the Identity Provider properties as follows:

   a. From the **Administration** menu, select **Identity Provider**.

   b. In the Provider ID field, enter the URL for the load balancer virtual host name and port.

      For example:

      http://*load_balancer_host*:*port*

4. Modify the Service Provider properties as follows:

   a. From the **Administration** menu, select **Service Provider**.

   b. In the **Provider ID** field, enter the URL for the load balancer virtual host name and port.

      For example:

```
http://load_balancer_host:port
```

5. Repeat Steps 2 through 4 for the subsequent Oracle Identity Federation instances in the high availability environment.

6. Because the Oracle Identity Federation metadata will have changed, redistribute the metadata to any remote partners to notify them of the configuration changes you just made.

11.12.4 Additional High Availability Tasks Associated

In addition to this tasks listed in this section, be sure to review any additional tasks required to configure the Oracle Identity Federation 11*g* high availability environment.

In particular, refer to these sections of the *Oracle Fusion Middleware High Availability Guide*:

- "Configuring Oracle HTTP Server for Oracle Directory Services Manager High Availability"

- "Configure Oracle HTTP Server"

- "Oracle Identity Federation Configuration"

11.13 Task 13: Verify the Oracle Identity Federation High Availbility Upgrade

Follow the steps below to validate the upgraded Oracle Identity Federation high availability upgrade:

1. Use a web browser to access the URL's shown below:

```
http://<LoadBalancerHost>:<LoadBalancerPort>/fed/sp/metadata
http://<LoadBalancerHost>:<LoadBalancerPort>/fed/idp/metadata
```

2. Follow the instructions in the following sections of the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation* to import metadata from the SP into the IdP and the IDP metadata into the SP:

- "Obtain Server Metadata"

- "Add Trusted Providers"

3. Go to the following URL and do a Single Sign-On operation:

```
http://Loadbalancer_SP_Host:Loadbalancer SP_port/fed/user/testspsso
```

4. During the upgrade, the single sign-on configurations from your 10*g* environment should have been migrated to the upgraded instances. As a result, you should be able to access those URLs, if the upgrade process completed successfully.

Index

W

Welcome screen
   in the Upgrade Assistant,   4-9, 5-4, 6-5