Oracle® Application Server

Enterprise Deployment Guide

10*g* (10.1.4.0.1)

B28184-02

February 2007

ORACLE®

Oracle Application Server Enterprise Deployment Guide, 10*g* (10.1.4.0.1)

B28184-02

Primary Author: Julia Pond

Contributing Authors: Janga Aliminati, Dheeraj Goswami, Peter LaQuerre, Peter Lubbers, Greg Sowa, Tim Willard

Contributors: Senthil Arunagirinathan, Rachel Chan, Somendu Chakraborty, Orlando Cordero, Eileen He, Pavana Jain, Pushkar Kapasi, Rajiv Maheshwari, Mark Nelson, Lei Oh, Ted Regan, Theresa Bandy, Malai Stalin, Yaqing Wang

Contents

3 Installing and Configuring the myJ2EECompany Application Infrastructure

4 Installing and Configuring JAZN-SSO/DAS

5 Installing and Configuring Oracle Access Manager

Index

Preface

This preface describes the audience, contents and conventions used in the *Oracle Application Server Enterprise Deployment Guide*.

Intended Audience

This guide is intended for system administrators who are responsible for installing and configuring Oracle Application Server.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

The following manuals in the Oracle Application Server documentation library provide additional information on the process of installing and configuring the Enterprise Deployment architectures:

- *Oracle Application Server Concepts*
- *Oracle Application Server Installation Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle Application Server Single Sign-On Administrator's Guide*
- *Oracle Application Server 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.
/	A forward slash is used as a directory separator in paths, regardless of platform.

1

What is an Enterprise Deployment?

1.1 Description

An enterprise deployment an Oracle Application Server configuration that is designed to support large-scale, mission-critical business software applications. The hardware and software in an Enterprise Deployment configuration delivers:

High quality service

- The system workload is managed and balanced effectively
- Applications continue to operate when resources are added or removed
- System maintenance and unexpected failures cause zero downtime

Built-in Security

- All incoming network traffic is received by the Load Balancing Router on a single, secure port and directed to internal IP addresses within the firewall; inside the firewall, functional components are grouped within DMZs
- User accounts are provisioned and managed centrally
- Security systems are integrated
- Administrative access is isolated

Efficient software provisioning and management

- Application distribution is simple
- Systems are managed and monitored as one logical unit in a central console
- Death detection and restart mechanisms ensure availability

1.2 Benefits

The Oracle Application Server configurations discussed in this guide are designed to ensure security of all transactions, maximize hardware resources, and provide a reliable, standards-compliant system for enterprise computing with a variety of applications. The security and high availability benefits of the Oracle Application Server configurations are realized through isolation in firewall zones and replication of software components.

1.2.1 Built-in Security

The Enterprise Deployment architectures are secure because every functional group of software components is isolated in its own DMZ, and all traffic is restricted by protocol and port. The following characteristics ensure security at all needed levels, as well as a high level of compliance with standards:

- All external communication received on port 80 is redirected to port 443.
- Communication from external clients does not go beyond the Load Balancing Router level.
- No direct communication from the Load Balancing Router to the Data tier DMZ is allowed.
- Components are separated between DMZs on the Web Tier, Application Tier, and the Data Tier.
- Direct communication between two firewalls at any one time is prohibited.
- If a communication begins in one firewall zone, it must end in the next firewall zone.
- Oracle Internet Directory is isolated in the Data tier DMZ.
- Identity Management components are in the DMZ.
- All communication between components across DMZs is restricted by port and protocol, according to firewall rules.

1.2.2 High Availability

The Enterprise Deployment architectures are highly available, because each component or functional group of software components is replicated on a different computer, and configured for component-level high availability.

1.3 Enterprise Deployments In This Guide

This guide provides configuration instructions for two Enterprise Deployments:

Figure 1–1 shows the enterprise deployment architecture for J2EE applications that use JAZN/SSO-DAS for user authentication.

Figure 1–2 shows the enterprise deployment architecture for J2EE applications that use Oracle Access Manager or JAZN LDAP for user authentication.

Note: The Load Balancing Router is not used in front of the Oracle Internet Directory servers; JAZN LDAP could be configured to individual Oracle Internet Directory servers, or a Load Balancing Router can be placed in front of the servers for high availability.

The servers in the myJ2EECompany system are grouped into tiers as follows:

- **Web Tier** — WEBHOST1 and WEBHOST2, with Oracle HTTP Server installed.

  Note: The WebPass component is not available on Windows at the time of publication. Therefore, WEBHOST1 and WEBHOST2 in the myJ2EEOracle Access Manager configuration must be servers with operating systems other than Windows.

- **Application Tier** — APPHOST1 and APPHOST2, with Oracle Containers for J2EE installed, and multiple OC4J instances with applications deployed. In myJ2EE with Oracle Access Manager, this tier also includes WebGate, WebPass, and Oracle Access Manager Identity Server, Access Server, Access Manager, and ADMINHOST, for administrator use.

  Note: The Access Manager component is not available on Windows at the time of publication. Therefore, ADMINHOST in the myJ2EEOracle Access Manager configuration must be a server with an operating system other than Windows.

- **Data Tier** — OIDHOST1 and OIDHOST2, with 10*g* (10.1.4.0.1) Oracle Internet Directory installed, and INFRADBHOST1 and INFRADBHOST2, the two-node Real Application Clusters database.

Figure 1–1 Enterprise Deployment Architecture for myJ2EEcompany.com with JAZN-SSO/DAS

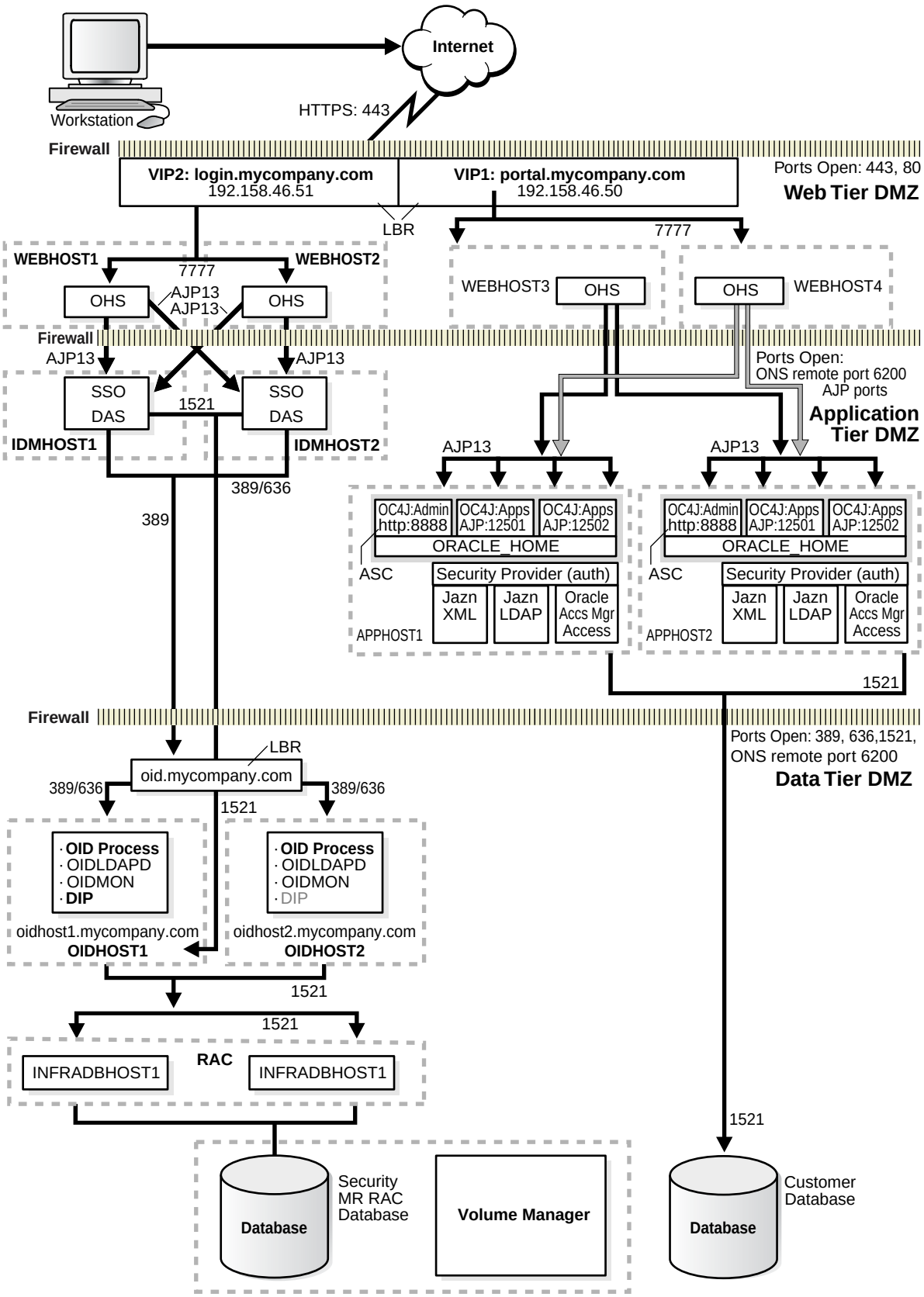
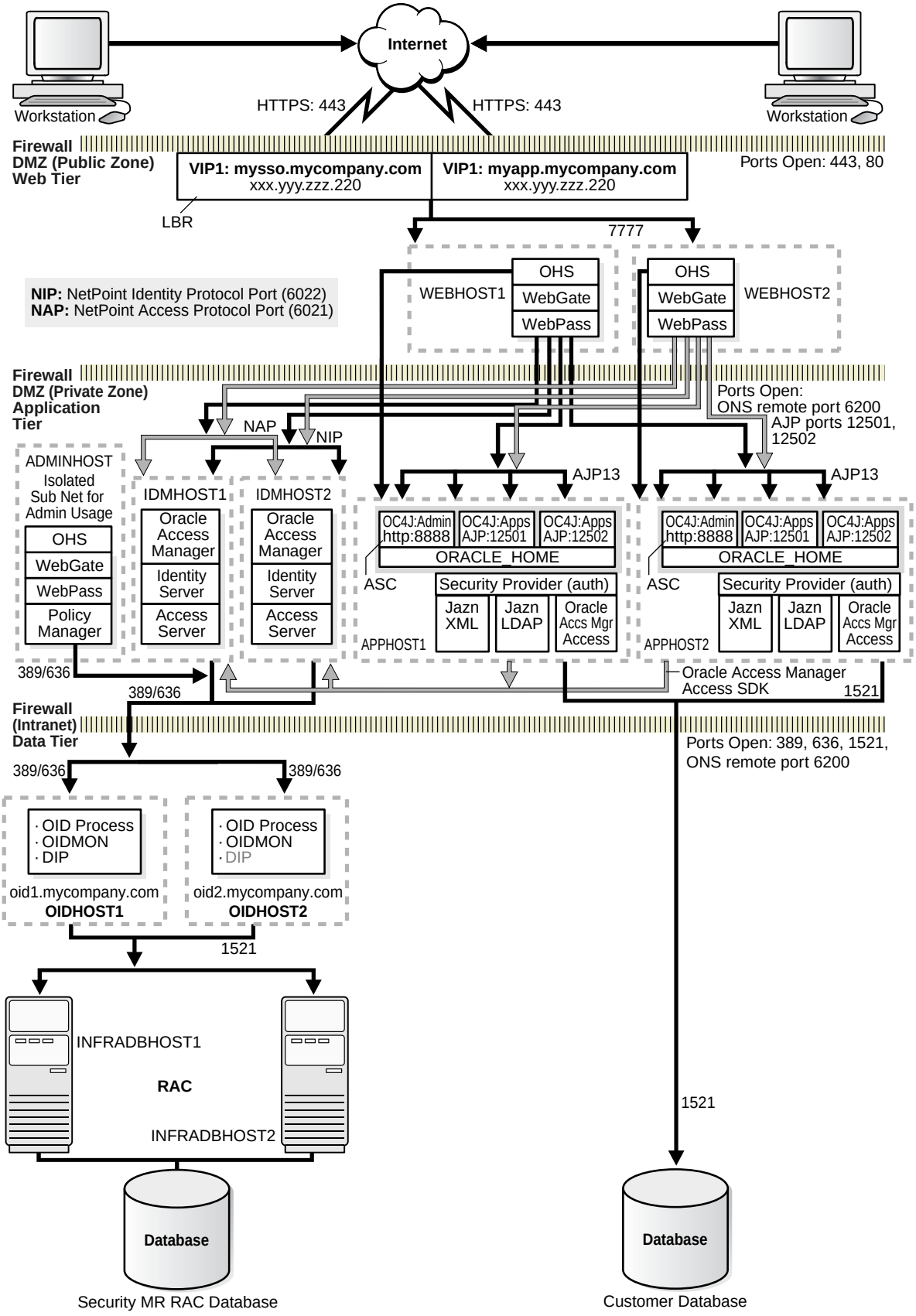


Figure 1–2 Enterprise Deployment Architecture for myJ2EEcompany.com with Oracle Access Manager



1.4 Hardware Requirements

Table 1–1, Table 1–2 and Table 1–3 list minimum hardware requirements for the Enterprise Deployments on Windows, Linux and Solaris operating systems, respectively. The memory figures represent the memory required to install and run Oracle Application Server; however, for most production sites, you should configure at least 1 GB of physical memory.

For detailed requirements, or for requirements for a platform other than these, see the *Oracle Application Server Installation Guide* for the platform in use.

Table 1–1 myJ2EECompany Hardware Requirements (Windows)

Server	Processor	Disk	Memory	TMP Directory	Swap
WEBHOST and APPHOST	300 MHz or higher Intel Pentium processor recommended	400 MB	512 MB	55 MB to run the installer; 256 MB needed for some installation types	512 MB
OIDHOST and INFRADBHOST	300 MHz or higher Intel Pentium processor recommended	2.5 GB	1 GB	55 MB to run the installer; 256 MB needed for some installation types	1 GB
ADMINHOST	300 MHz or higher Intel Pentium processor recommended	400 MB	512 MB	n/a	512 MB

Table 1–2 myJ2EECompany Hardware Requirements (Linux)

Server	Processor	Disk	Memory	TMP Directory	Swap
WEBHOST and APPHOST	Pentium (32-bit), 450 MHz or greater	520 MB	512 MB	400 MB	1.5 GB
OIDHOST and INFRADBHOST	Pentium (32-bit), 450 MHz or greater	2.5 GB	1 GB	400 MB	1.5 GB
ADMINHOST	Pentium (32-bit), 450 MHz or greater	520 MB	512 MB	400 MB	1.5 GB

Table 1–3 myJ2EECompany Hardware Requirements (Solaris)

Server	Processor	Disk	Memory	TMP Directory	Swap
WEBHOST and APPHOST	450 MHz or greater; Oracle recommends a multiple CPU computer	750 MB	512 MB	250 MB	1.5 GB
OIDHOST	450 MHz or greater; Oracle recommends a multiple CPU computer	1.54 GB	1 GB	250 MB	1.5 GB
INFRADBHOST	450 MHz or greater; Oracle recommends a multiple CPU computer	3.93 GB	1 GB	250 MB	1.5 GB
ADMINHOST	450 MHz or greater; Oracle recommends a multiple CPU computer	750 MB	512 MB	250 MB	1.5 GB

Production requirements vary depending on applications and the number of users. All Enterprise Deployment configurations described in this guide use two servers for each tier to provide failover capability; however, this does not presume adequate computing resources for any application or user population. If the system workload increases such that performance is degraded, you can add servers to the configuration by repeating the instructions for the installation and configuration of the second server on the tier (WEBHOST2, APPHOST2, INFRADBHOST2) to add a third server where it is needed.

To determine hardware needs with a greater degree of precision, you might consider the options presented in Table 1–4.

Table 1–4 Hardware Sizing Options

Option	Benefit	Disadvantage
Create a prototype of the deployment architecture and stress test it	■ Accurate estimate; provides ability to extrapolate ■ Accomodates custom scenarios and complex implementations ■ Incorporates third-party components (firewalls, load balancing router); exposes performance and network-specific issues	■ Time and effort required to configure ■ Additional software for load simulation required
Use the iSizer tool	■ Fast and easy to use ■ Works best in common implementations with one component for each server	■ Inexact results for systems with third-party components, many custom implementation details ■ Results difficult to extrapolate in multiple-component architectures

1.5 Variants

The variants described in this section enable you to achieve deployment goals using fewer servers, different software, or alternative configurations.

1.5.1 Multimaster Replication with Oracle Internet Directory

Multimaster replication is an Oracle Internet Directory software solution that ensures read and write access to Oracle Internet Directory at all times, if at least one of the directory servers in the system remains available. When an Oracle Directory server resumes functioning after being unavailable, replication from the surviving directory server resumes automatically and synchronizes the contents between the directory servers forming the directory replication group. In addition, any changes made on one directory server instance are reflected on the second directory server instance.

To implement multimaster replication in Oracle Internet Directory, follow the instructions in the *Oracle Internet Directory Administrator's Guide*, Oracle Internet Directory Replication Administration chapter, section titled "Installing and Configuring Multimaster Replication".

1.5.2 OracleAS Cold Failover Cluster (Identity Management)

The OracleAS Cold Failover Cluster (Identity Management) solution is a hardware cluster comprising two computers. The computer that is actively executing an Infrastructure installation at any given time is called the primary (hot) node. If this node fails, the hardware cluster automatically diverts Infrastructure operations to the secondary (cold) node.

Each hardware cluster node is a standalone server that runs its own set of processes, but accesses a shared storage subsystem. The cluster can access the same storage, usually disks, from both nodes, but only the primary node has active access to the

storage at any given time. If the primary node fails, the hardware cluster's software grants the secondary node access to the storage.

> **Note:** For a detailed discussion of the OracleAS Cold Failover Cluster (Identity Management) solution, see the *Oracle Application Server High Availability Guide*.

The OracleAS Cold Failover Cluster (Identity Management) solution differs from the standard configuration in the following ways:

- The Oracle Internet Directory server and the database are on the same computer, whereas in the standard configuration the first Oracle Internet Directory instance and a database instance occupy OIDHOST1 and INFRADBHOST1, while the second Oracle Internet Directory instance and a database instance occupy OIDHOST2 and INFRADBHOST2. Thus, the OracleAS Cold Failover Cluster (Identity Management) solution operates two fewer servers than the RAC configuration.
- In the event of node failure, clients will experience a brief interruption of service while the workload is diverted to the cold node.

To implement the OracleAS Cold Failover Cluster (Identity Management) solution:

1. Obtain and configure a hardware cluster.
2. Install and configure the Oracle Application Server instances on the cluster computers to use the OracleAS Cold Failover Cluster (Identity Management) solution. Follow the instructions in the *Oracle Application Server Installation Guide*, "Installing an OracleAS Cold Failover Cluster (Identity Management) Configuration".
3. Manage the OracleAS Cold Failover Cluster (Identity Management) solution, following the instructions from the *Oracle Application Server High Availability Guide*, "Managing Oracle Application Server Cold Failover Cluster (Identity Management)".

1.5.3 Forward and Reverse Proxies for Oracle HTTP Server

Proxies change the way the Oracle HTTP Server processes client requests.

A forward proxy is an intermediary server between a client and the origin server containing the content. Forward proxies are usually used to provide Internet access to internal clients that are otherwise restricted by a firewall. To get content from the origin server, the client sends a request to the proxy, naming the origin server as the target. The proxy requests the content from the origin server and returns it to the client. The client must be configured to use the forward proxy to access other sites.

A reverse proxy is a server that appears to outside clients to be the content server. It relays requests from outside the firewall to servers behind the firewall, and delivers retrieved content back to the client. A firewall rule allows access only to the proxy server, so that the content servers are protected. The proxy server changes URLs listed in the headers of any messages generated by the content servers, so that external clients are given no information about the servers behind the firewall. No configuration of clients is necessary with a reverse proxy (the client makes requests for content in the name-space of the reverse proxy). The reverse proxy decides where to send the requests, and returns the content as if it was the origin server.

1.5.4 Variants for J2EE Applications

For certain types of J2EE applications, such as JMS-based or EJB-based applications, there may be other variants to these architectures. Refer to the *Oracle Containers for J2EE Configuration and Administration Guide*, *the Oracle Containers for J2EE Developer's Guide* and the *Oracle Containers for J2EE Developer's Guide* for more information on these variants.

1.6 How to Use This Guide

Table 1–5 summarizes the process by which you install and configure myJ2EECompany with each of the user authentication methods. Follow the procedures indicated in the column for the configuration of your choice.

Table 1–5 Enterprise Deployment Configuration Procedures

Perform the steps in this section...	To configure myJ2EECompany with OracleAS Single Sign-On	To configure myJ2EECompany with Oracle Access Manager	To configure myJ2EECompany with JAZN LDAP
Section 2.1, "Installing the Oracle Application Server Metadata Repository for the Security Infrastructure"	*x*	*x*	*x*
Section 2.2, "Installing the Oracle Internet Directory Instances in the Data Tier"	*x*	*x*	*x*
Section 2.3, "Configuring the Virtual Server to Use the Load Balancing Router"	*x*	*x*	*x*
Section 2.4, "Testing the Data Tier Components"	*x*	*x*	*x*
Section 3.2, "Installing and Configuring the Application and Web Tiers"	*x*	*x*	*x*
Section 3.4, "Configuring the Oracle HTTP Server with the Load Balancing Router"	*x*	*x*	*x*
Section 3.5, "Configuring OC4J Routing"	*x*	*x*	*x*
Section 3.6, "Managing Oracle Application Server Component Connections"	*x*	*x*	*x*
Section 3.7, "Configuring Application Authentication and Authorization"		*x*	*x*
Section 4.1, "Setting up the Load Balancing Router"	*x*		
Section 4.2, "Installing and Configuring Oracle Application Server Single Sign-On"	*x*		
Section 4.3, "Reconfiguring Oracle Application Server Single Sign-On and Oracle Delegated Administration Services with the Oracle HTTP Servers"	*x*		
Section 4.5, "Configuring Session State Replication for the OC4J_SECURITY Instance"	*x*		
Section 4.6, "Disabling the Oracle HTTP Server on the Identity Management Tier"	*x*		
Section 5.3, "Preparing to Install Oracle Access Manager Components"		*x*	
Section 5.5, "Installing WebPass on WEBHOST1"		*x*	
Section 5.6, "Configuring the First Identity Server"		*x*	
Section 5.7, "Installing the Second Identity Server on IDMHOST2"		*x*	
Section 5.8, "Installing WebPass on WEBHOST2"		*x*	
Section 5.9, "Configuring the Second Identity Server"		*x*	
Section 5.10, "Installing the Access System"		*x*	

Table 1–5 (Cont.) Enterprise Deployment Configuration Procedures

Perform the steps in this section...	To configure myJ2EECompany with OracleAS Single Sign-On	To configure myJ2EECompany with Oracle Access Manager	To configure myJ2EECompany with JAZN LDAP
Section 5.11, "Configuring the Access Server with the Load Balancing Router"		*x*	
Section 5.12, "Installing the Access Server SDK"		*x*	
Section 5.13, "Configuring Oracle Access Manager Single Sign-On for OC4J Applications"		*x*	
Section 5.14, "Configuring the Second Identity Server as a Failover Server"		*x*	
Section 5.15, "Configuring the Second Access Server as a Failover Server"		*x*	
Section 5.16, "Mitigating Identity Server Product Installation Failures on Linux"		*x*	
Section 5.17, "Configuring Directory Server Failover"		*x*	
Section 5.18, "Configuring Access Server Directory Failover for Oracle and Policy Data"		*x*	
Section 5.19, "Configuring Policy Manager Failover"		*x*	
Section 5.20, "Creating Failover LDAP Directory Server Profiles for the Identity and Access Servers"		*x*	
Section 5.21, "Verifying the Status of the Identity Servers"		*x*	

2

Installing and Configuring the Security Infrastructure

2.1 Installing the Oracle Application Server Metadata Repository for the Security Infrastructure

You must install the 10*g* (10.1.4.0.1) OracleAS Metadata Repository before you install components into the Security DMZ. Oracle Application Server provides a tool, the Oracle Application Server Repository Creation Assistant, to create the OracleAS Metadata Repository in an existing database.

The 10*g* (10.1.4.0.1) OracleAS RepCA is available on the OracleAS RepCA CD-ROM or the Oracle Application Server DVD-ROM. You install the OracleAS RepCA in its own, separate Oracle home.

To install the OracleAS Metadata Repository, you must perform these steps:

1. Install the OracleAS RepCA, following the steps in Section 2.1.1.
2. Ensure that the database meets the requirements specified in the "Database Requirements" section of the *Oracle Application Server Metadata Repository Creation Assistant User's Guide*. You can find this guide in the Oracle Application Server platform documentation library for the platform and version you are using. In addition, ensure that:
   - The database computer has at least 512 MB of swap space available for execution of the OracleAS RepCA
   - There are no dependencies of any kind related to the `ultrasearch` directory in the database's Oracle home. The OracleAS RepCA replaces this directory with a new version, renaming the existing version of the directory to `ultrasearch_`*timestamp*.
3. Execute the OracleAS RepCA, following the steps in Section 2.1.2 or Section 2.1.3.
   - To install into a database using raw devices, follow the steps in Section 2.1.2, "Installing the Metadata Repository in a Database Using Raw Devices" on page 2-3.

- To install into a database using Oracle Cluster File System, follow the steps in Section 2.1.3, "Installing the Metadata Repository in an Oracle Cluster File System (OCFS)" on page 2-4.

4. Perform the post-installation step described in Section 2.1.4.

2.1.1 Installing the OracleAS RepCA

Follow these steps to install the OracleAS RepCA into its own Oracle home:

1. Insert the OracleAS RepCA CD-ROM or the Oracle Application Server DVD-ROM.

   Note: If your computer does not mount CD-ROMs or DVD-ROMs automatically, you must set the mount point manually.

2. Start the installer, using the method corresponding to the installation media:

   (CD-ROM)

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   (DVD-ROM) Navigate to the `repca_utilities` directory and do one of the following:

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   The **Welcome** screen appears.

3. Click **Next**.

   The **Specify File Locations** screen appears.

4. In the **Name** field, specify a name for the OracleAS RepCA Oracle home. The Oracle home name must contain only alphanumeric characters and the underscore character, and be 128 characters or fewer.

   In the **Destination** field, enter the full path to a new Oracle home in which to install the OracleAS RepCA, and click **Next**.

5. The **Launch Repository Creation Assistant** screen appears.

6. Select **No** and click **Next**.

   The **Summary** screen appears.

7. Click **Install**.

   The Configuration Assistants screen appears, executing the OracleAS RepCA, and indicating "In Progress".

8. When the OracleAS RepCA is no longer running, exit the OracleAS RepCA.

   The **End of Installation** screen appears.

9. Click **Exit**, and then confirm your choice to exit.

2.1.2 Installing the Metadata Repository in a Database Using Raw Devices

Follow these steps to install the Metadata Repository into an existing two-node Real Application Clusters (RAC) database using raw devices:

1. Create raw devices for the OracleAS Metadata Repository.

   Tip: The command to create tablespaces is specific to the volume manager used. For example, the command to create a tablespace in VERITAS Volume Manager is `vxassist`.

2. Create a file to map the tablespaces to the raw devices. Each line in the file has the format:

   ```
   tablespace name=raw device file path
   ```

   Note: Creating the sample file is not mandatory; you can enter the tablespace values into the Specify Tablespace Information screen during execution of the OracleAS RepCA.

3. Populate the `DBCA_RAW_CONFIG` environment variable with the full path and filename of the tablespace mapping file.
4. Ensure that the database and listener are running.
5. Ensure that the NLS_LANG environment variable is not set to a non-English locale, or is set to `american_america.us7ascii`, with one of the following commands:

   UNIX:

   - **`unsetenv NLS_LANG`**
   - **`setenv NLS_LANG american_america.us7ascii`**

   Windows:

   - **`set NLS_LANG=`**
   - **`set NLS_LANG=american_america.us7ascii`**

   Note: If you need to, you can set NLS_LANG to its original value after executing the OracleAS RepCA.

6. Start the OracleAS RepCA from the OracleAS RepCA Oracle home with this command:

   `runRepca`

   The **Welcome** screen appears.

7. Click **Next**.

   The **Specify Oracle Home** screen appears.

8. In the **Oracle Home** field, specify the full path of the database Oracle home.

   In the **Log File Directory** field, specify the full path of the directory on the current computer in which you want the OracleAS RepCA to write its log files. Ensure correct input for the **Log File Directory** on this screen, as you will not be able to change it after you have proceeded beyond this screen.

9. Click **Next**.

   The **Select Operation** screen appears.

10. Select **Load** and click **Next**.

    The **Specify Database Connection** screen appears.

11. Enter the SYS user name and password and the host and port information. For example:

    ```
    infradbhost1.mycompany.com:1521,infradbhost2.mycompany.com:1521
    ```

12. Click **Next**.

    The **Specify Storage Options** screen appears.

13. Select **Regular or Cluster File System**.

    The **Specify Tablespace Information** screen appears, displaying the values from the file specified by the DBCA_RAW_CONFIG environment variable.

14. Correct the values, if necessary, and click **Next**.

    The **Warning: Check Disk Space** dialog appears if your SYSTEM and UNDO tablespaces are set to autoextend.

15. Check the disk space as specified in the dialog and click **OK**.

    The **Loading Repository** screen appears. The tablespaces and schemas are created and populated.

    The **Success** screen appears.

16. Click **OK**.

    The OracleAS RepCA exits.

If the installation was unsuccessful, or you need more information, see the *Oracle Application Server Metadata Repository Creation Assistant User's Guide*.

2.1.3 Installing the Metadata Repository in an Oracle Cluster File System (OCFS)

Follow these steps to install the Metadata Repository into an existing two-node Real Application Clusters (RAC) database using an OCFS file system:

1. Ensure that the database and listener are running.
2. Start the OracleAS RepCA from the OracleAS RepCA Oracle home with this command:

   ```
   runRepca
   ```

   The **Welcome** screen appears.

3. Click **Next**.

   The **Specify Oracle Home** screen appears.

4. In the **Oracle Home** field, specify the full path of the database Oracle home.

   In the **Log File Directory** field, specify the full path of the directory on the current computer in which you want the OracleAS RepCA to write its log files. Ensure correct input for the **Log File Directory** on this screen, as you will not be able to change it after you have proceeded beyond this screen.

5. Click **Next**.

   The **Select Operation** screen appears.

6. Select **Load** and click **Next**.

   The **Specify Database Connection** screen appears.

7. Enter the SYS user password, select the **Real Application Clusters Database** option, and enter the host and port information. For example:

   ```
   infradbhost1.mycompany.com:1521,infradbhost2.mycompany.com:1521
   ```

   Enter the service name.

8. Click **Next**.

   The **Specify Storage Options** screen appears.

9. Select **Regular or Cluster File System**.

   The **Specify Tablespace Information** screen appears.

10. Select a directory option (**Use Same Directory for All Tablespaces** or **Use Individual Directories for Each Tablespace**) and complete the remaining fields. When specifying a directory, ensure that it is an existing, writable directory with sufficient free space. Click **Next**.

    The **Warning: Check Disk Space** dialog appears if your SYSTEM and UNDO tablespaces are set to autoextend.

11. Check the disk space as specified in the dialog and click **OK**.

    The **Loading Repository** screen appears. The tablespaces and schemas are created and populated.

    The **Success** screen appears.

12. Click **OK**.

    The OracleAS RepCA exits.

If the installation was unsuccessful, or you need more information, see the *Oracle Application Server Metadata Repository Creation Assistant User's Guide*.

2.1.4 Configuring the Time out Value in the sqlnet.ora File

You must configure the `SQLNET.EXPIRE_TIME` parameter in the `sqlnet.ora` file on the application infrastructure database.

1. Open the file *`ORACLE_HOME`*`/network/admin/sqlnet.ora` file (UNIX) or the *`ORACLE_BASE`*`/` *`ORACLE_HOME`*`/network/admin/sqlnet.ora` file (Windows).
2. Set the `SQLNET.EXPIRE_TIME` parameter to a value lower than the TCP session time out value for the Load Balancing Router and firewall.
3. Restart the listener by issuing these commands in *`ORACLE_HOME`*`/bin`:

```
lsnrctl stop
lsnrctl start
```

2.2 Installing the Oracle Internet Directory Instances in the Data Tier

Follow these steps to install the Oracle Internet Directory components (OIDHOST1 and OIDHOST2) on the Data Tier with the Metadata Repository. The procedures for the installations are very similar, but the selections in the configuration options screen differ.

> **Note:** Ensure that the clocks are synchronized between the two computers on which you intend to install the Oracle Internet Directory instances. Errors will occur if this is not done.

2.2.1 Installing the First Oracle Internet Directory

The OracleAS Metadata Repository must be running before you perform this task. Follow these steps to install the 10*g* (10.1.4.0.1)Oracle Internet Directory on OIDHOST1:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Application Server Quick Installation Guide* in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Ensure that ports 389 and 636 are not in use by any service on the computer by issuing these commands for the operating system you are using. (If the port is not in use, no output is returned from the command.)

   On UNIX:

```
netstat -an | grep "389"
netstat -an | grep "636"
```

   On Windows:

```
netstat -an | findstr :389
netstat -an | findstr :636
```

If the port is in use (if the command returns output identifying the port), you must free the port.

In UNIX:

Remove the entries for ports 389 and 636 in the `/etc/services` file and restart the services, or restart the computer.

In Windows:

Stop the component that is using the port.

3. Copy the `staticport.ini` file from the `Disk1/stage/Response` directory to the Oracle home directory.
4. Edit the `staticport.ini` file to assign the following custom ports:

```
Oracle Internet Directory port = 389
Oracle Internet Directory (SSL) port = 636
```

5. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   The **Welcome** screen appears.
6. Click **Next**.

   On UNIX systems, the **Specify Inventory Directory and Credentials** screen appears.
7. Specify the directory you want to be the `oraInventory` directory and the operating system group that has permission to write to it.
8. Click **Next**.

   On UNIX systems, a dialog appears, prompting you to run the `oraInstRoot.sh` script.
9. Open a window and run the script, following the prompts in the window.
10. Return to the Oracle Universal Installer screen and click **Next**.

    The **Specify File Locations** screen appears with default locations for:

    - The product files for the installation (Source)
    - The name and path to an Oracle home (Destination)

    Note: Ensure that the Oracle home directory path for OIDHOST1 is the same as the path to the Oracle home location of OIDHOST2. For example, if the path to the Oracle home on OIDHOST1 is:

    `/u01/app/oracle/product/AS10gOID`

    then the path to the Oracle home on OIDHOST2 must be:

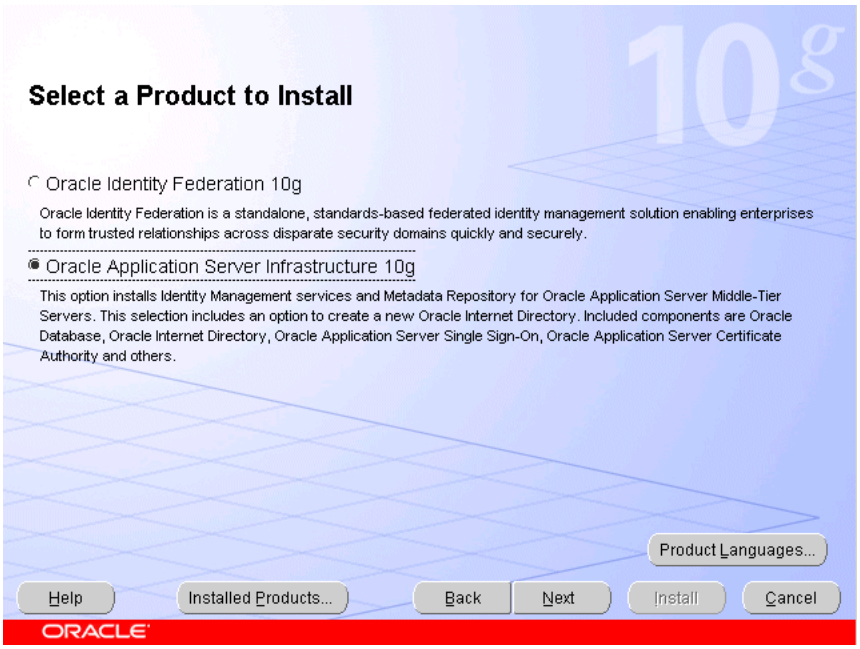
    `/u01/app/oracle/product/AS10gOID`

    ---

11. Specify the **Destination Name** and **Path**, if different from the default, and click **Next**.

    The **Select a Product to Install** screen appears.

Figure 2–1 Oracle Universal Installer Select a Product to Install Screen

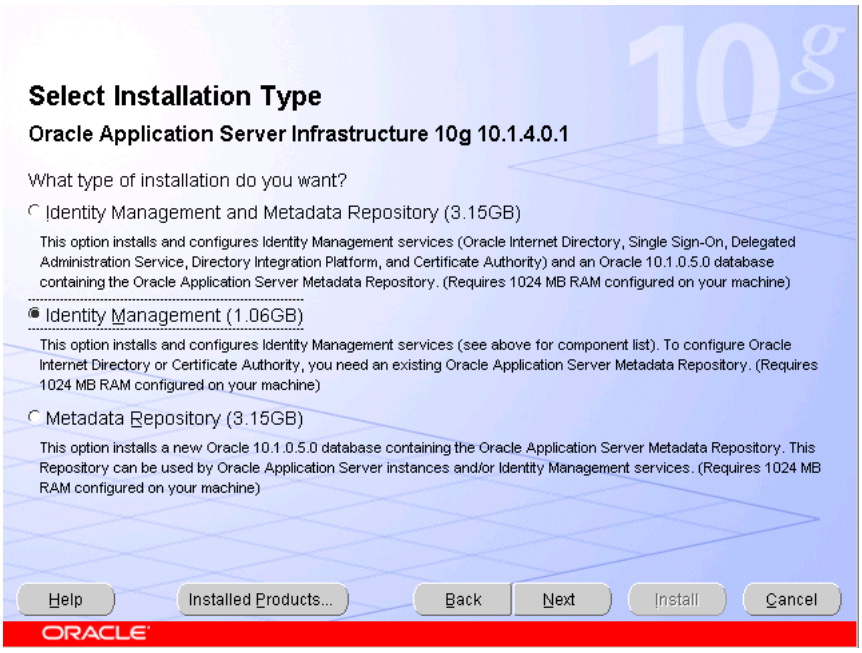


12. Select OracleAS Infrastructure 10*g*, as shown in Figure 2–1, and click **Next**.

    The **Select Installation Type** screen appears.

13. Select **Identity Management**, as shown in Figure 2–2, and click **Next**.

Figure 2–2 Oracle Universal Installer Select Installation Type Screen



    The **Product-Specific Prerequisite Checks** screen appears.

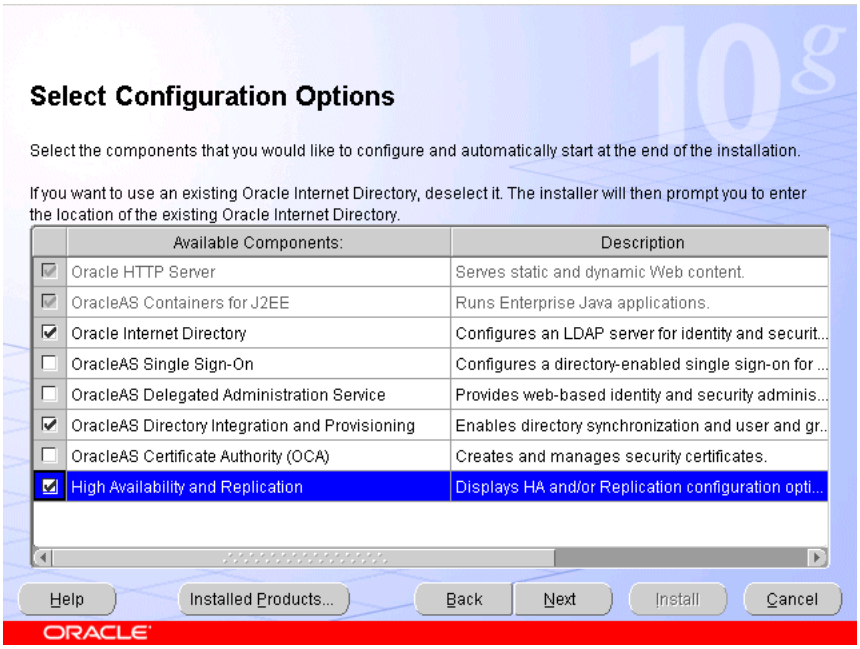
14. Click **Next**.

    The **Confirm Pre-Installation Requirements** screen appears.

15. Ensure that the requirements are met, check the box for each, and click **Next**.

    The **Select Configuration Options** screen appears.

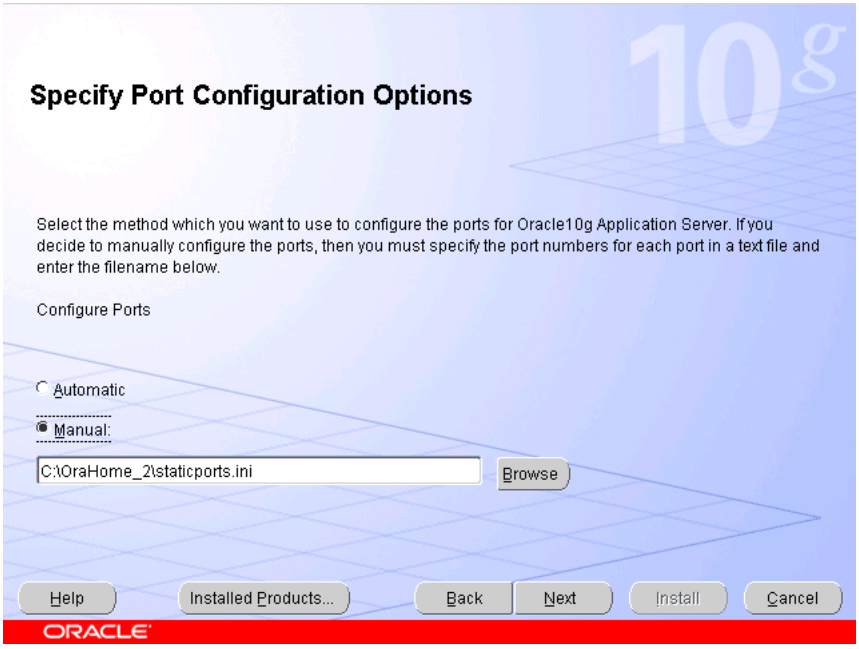
Figure 2–3 Oracle Universal Installer Select Configuration Options Screen



16. Select **Oracle Internet Directory**, **OracleAS Directory Integration and Provisioning**, and **High Availability and Replication**, as shown in Figure 2–3, and click **Next**.

    The **Specify Port Configuration Options** screen appears.

Figure 2–4 Oracle Universal Installer Specify Port Configuration Options Screen

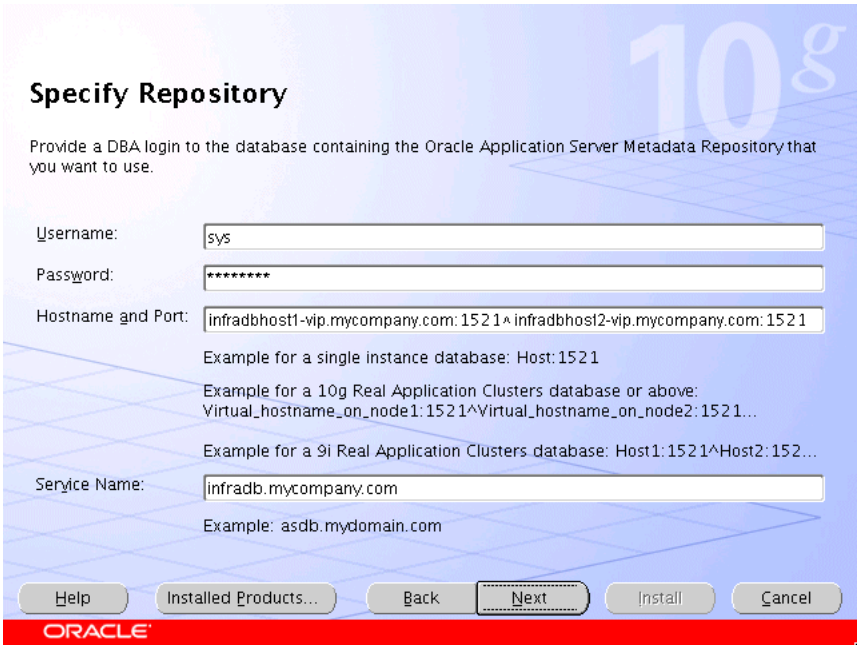


17. Select **Manual**, as shown in Figure 2–4, and click **Next**.

    The **Specify Repository** screen appears.

18. Provide the DBA login and computer information as shown in Figure 2–5 and click **Next**.

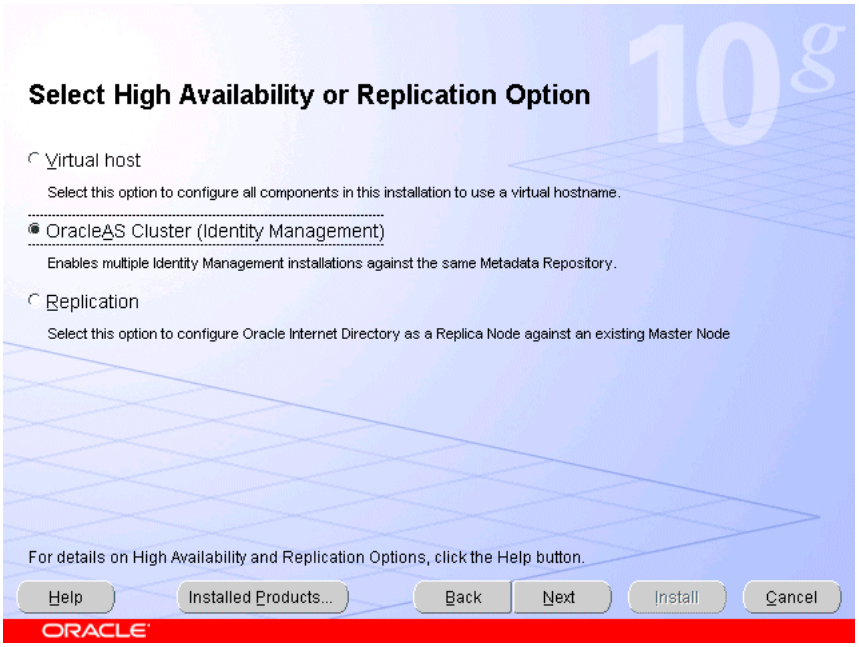
Figure 2–5 Oracle Universal Installer Specify Repository Screen



    The **Select High Availability or Replication Option** screen appears.

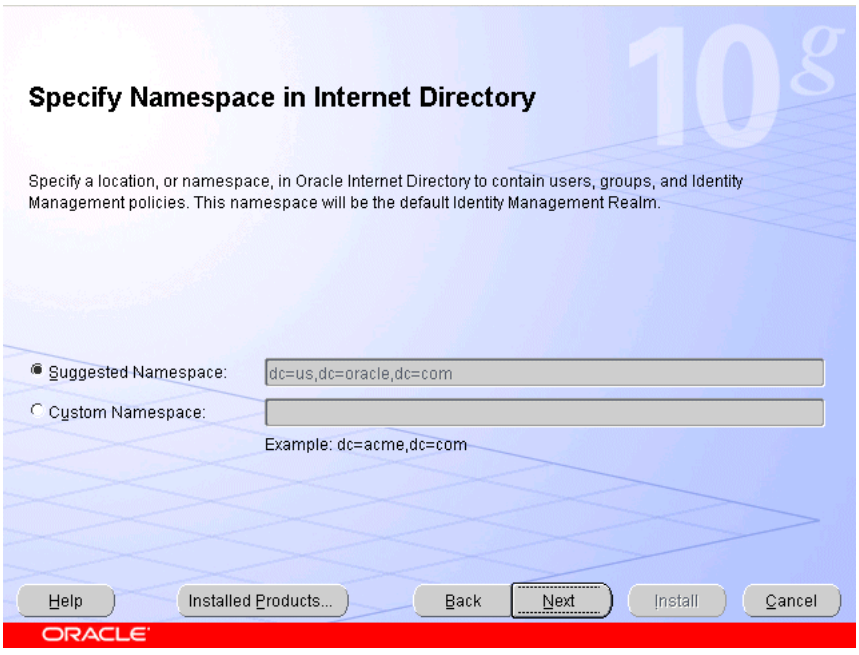
19. Select **OracleAS Cluster (Identity Management)**, as shown in Figure 2–6, and click **Next**.

Figure 2–6 Oracle Universal Installer Select High Availability or Replication Option Screen



The **Specify Namespace in Internet Directory** screen appears.

Figure 2–7 Oracle Universal Installer Specify Namespace in Internet Directory



20. Click **Next** to specify the default **Suggested Namespace** shown in Figure 2–7, or enter values for the **Custom Namespace** and click **Next**.

    The **Specify Instance Name and ias_admin Password** screen appears.

21. Specify the instance name and password and click **Next**.

    The **Summary** screen appears.

22. Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.

    The **Install** screen appears with a progress bar. On UNIX systems, a dialog opens prompting you to run the `root.sh` script.

23. Open a window and run the script.

    The **Configuration Assistants** screen appears. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the **End of Installation** screen appears.

24. Click **Exit**, and then confirm your choice to exit.

2.2.2 Installing the Second Oracle Internet Directory

The OracleAS Metadata Repository and the first Oracle Internet Directory must be running before you perform this task. Follow these steps to install the 10*g* (10.1.4.0.1) Oracle Internet Directory on OIDHOST2:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Application Server Quick Installation Guide* in the Oracle Application Server platform documentation library for the platform and version you are using.

2. Ensure that ports 389 and 636 are not in use by any service on the computer by issuing these commands for the operating system you are using. (If the port is not in use, no output is returned from the command.)

   On UNIX:

   ```
   netstat -an | grep "389"
   ```

   ```
   netstat -an | grep "636"
   ```

   On Windows:

   ```
   netstat -an | findstr :389
   ```

   ```
   netstat -an | findstr :636
   ```

   If the port is in use (if the command returns output identifying the port), you must free the port.

   In UNIX:

   Remove the entries for ports 389 and 636 in the `/etc/services` file and restart the services, or restart the computer.

   In Windows:

   Stop the component that is using the port.

3. Copy the `staticport.ini` file from the `Disk1/stage/Response` directory to the Oracle home directory.

4. Edit the `staticport.ini` file and uncomment, and update these entries:

   ```
   Oracle Internet Directory port = 389
   Oracle Internet Directory (SSL) port = 636
   ```

5. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

The **Welcome** screen appears.

6. Click **Next**.

   On UNIX systems, the **Specify Inventory Directory and Credentials** screen appears.

7. Specify the directory you want to be the `oraInventory` directory and the operating system group that has permission to write to it.

8. Click **Next**.

   On UNIX systems, a dialog appears, prompting you to run the `oraInstRoot.sh` script.

9. Open a window and run the script, following the prompts in the window.

10. Return to the Oracle Universal Installer screen and click **Next**.

    The **Specify File Locations** screen appears with default locations for:

    - The product files for the installation (Source)
    - The name and path to an Oracle home (Destination)

    Note: Ensure that the Oracle home directory path for OIDHOST1 is the same as the path to the Oracle home location of OIDHOST2. For example, if the path to the Oracle home on OIDHOST1 is:

    `/u01/app/oracle/product/AS10gOID`

    then the path to the Oracle home on OIDHOST2 must be:

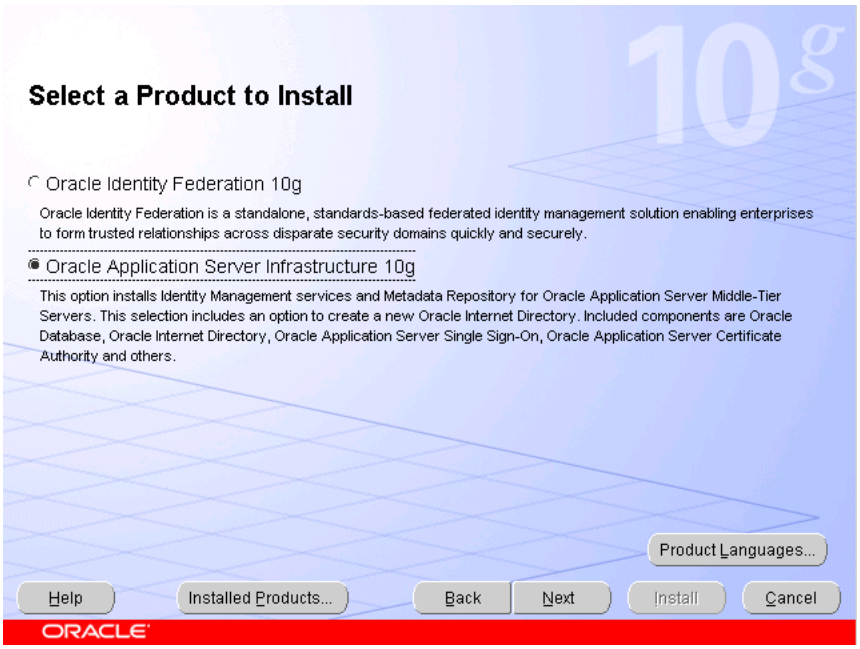
    `/u01/app/oracle/product/AS10gOID`

    ---

11. Specify the **Destination Name** and **Path**, if different from the default, and click **Next**.

    The **Select a Product to Install** screen appears.

Figure 2–8 Oracle Universal Installer Select a Product to Install Screen

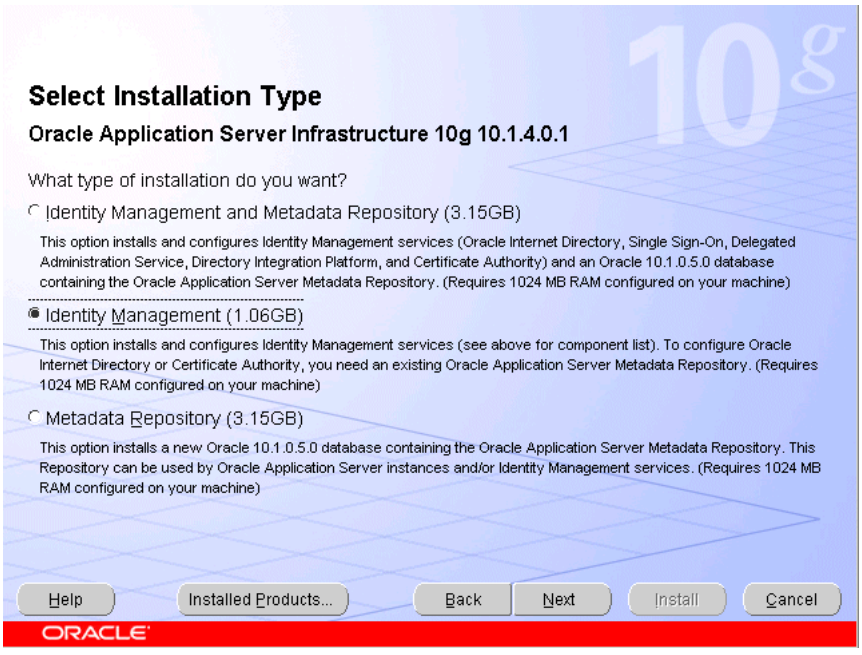


12. Select OracleAS Infrastructure 10*g*, as shown in Figure 2–8, and click **Next**.

    The **Select Installation Type** screen appears.

13. Select **Identity Management**, as shown in Figure 2–9, and click **Next**.

Figure 2–9 Oracle Universal Installer Select Installation Type Screen



    The **Product-specific Prerequisite Checks** screen appears.

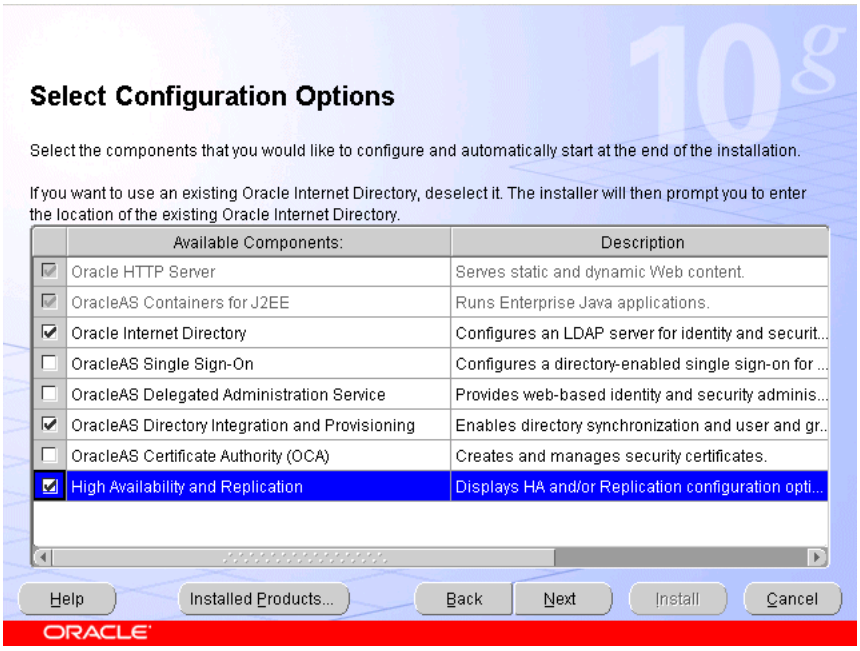
14. Click **Next**.

    The **Confirm Pre-Installation Requirements** screen appears.

15. Ensure that the requirements are met, check the box for each, and click **Next**.

    The **Select Configuration Options** screen appears.

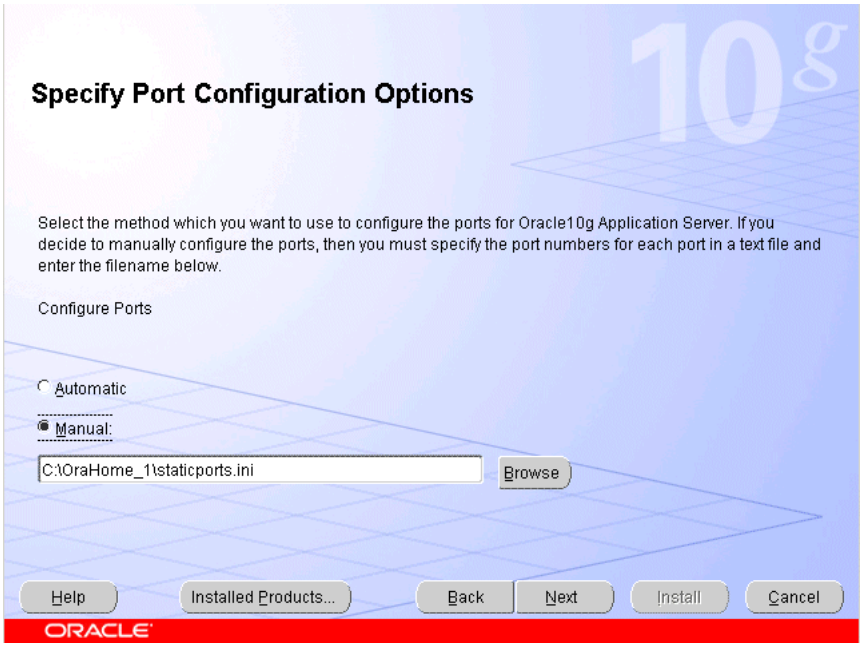
Figure 2–10 Oracle Universal Installer Select Configuration Options Screen



16. Select **Oracle Internet Directory**, **OracleAS Directory Integration and Provisioning**, and **High Availability and Replication**, as shown in Figure 2–10, and click **Next**.

    The **Specify Port Configuration Options** screen appears.

Figure 2–11 Oracle Universal Installer Specify Port Configuration Options Screen

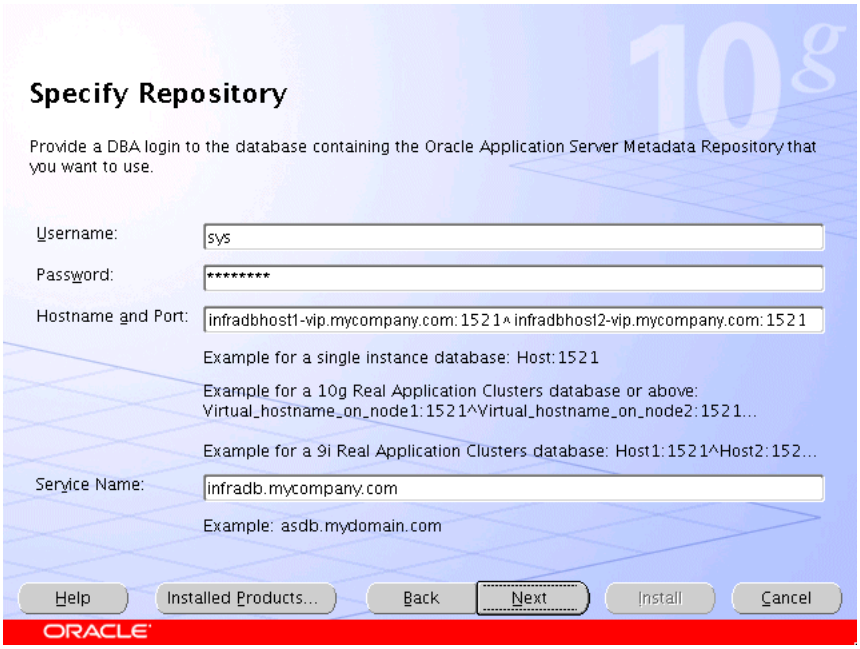


17. Select **Manual**, as shown in Figure 2–11, and click **Next**.

    The **Specify Repository** screen appears.

18. Provide the DBA login and computer information as shown in Figure 2–12 and click **Next**.

Figure 2–12 Oracle Universal Installer Specify Repository Screen



    A dialog opens, prompting you to synchronize the system time of the primary Oracle Internet Directory computer and the system time on the computer on which you are installing.

19. Synchronize the system time on the computers and click **OK**.

    The **Specify ODS Password** screen appears.

20. Specify the ODS password (by default, the ias_admin password), as shown in Figure 2–13, and click **Next**.

Figure 2–13 Oracle Universal Installer Specify ODS Password Screen

The **Specify OID Login** screen appears.

21. Specify the user name and password, as shown in Figure 2–14, and click **Next**.

Figure 2–14 Oracle Universal Installer Specify OID Login Screen

The **Specify Instance Name and ias_admin Password** screen appears.

22. Specify the instance name and password and click **Next**.

The **Summary** screen appears.

23. Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.

    The **Install** screen appears with a progress bar. On UNIX systems, a dialog opens prompting you to run the `root.sh` script.

24. Open a window and run the script.

    The **Configuration Assistants** screen appears. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the **End of Installation** screen appears.

25. Click **Exit**, and then confirm your choice to exit.

2.3 Configuring the Virtual Server to Use the Load Balancing Router

If you plan to use the Enterprise Deployment Architecture for myJ2EEcompany.com with JAZN-SSO/DAS (shown in Figure 2–1), you must configure the Load Balancing Router to perform these functions:

- Listen on oid.mycompany.com.
- Balance the requests received on ports 389 and 636 to oidhost1.mycompany.com and oidhost2.mycompany.com on ports 389 and 636.
- Monitor the heartbeat of the Oracle Internet Directory processes on both computers. If an Oracle Internet Directory process stops on one of the computers, the Load Balancing Router must route the LDAP traffic to the surviving computer.

Note: Some tuning of the Load Balancing Router's monitoring interval and time out values may be required to ensure system availability. If the interval or time out value is too long, the Load Balancing Router will not detect service failures in time; if it is too short, the Load Balancing Router may erroneously detect that a server is down.

For example, suppose the Load Balancing Router maps the virtual IP address oid.mycompany.com to the two Oracle Internet Directory servers for round robin load balancing, and the monitoring scheme attempts an ldapbind at 10-second intervals.

If the Oracle Internet Directory on OIDHOST1 is down, then the Load Balancing Router directs all traffic to the Oracle Internet Directory on OIDHOST2 only.

However, there is a10-second interval during which the Load Balancing Router is unaware that the Oracle Internet Directory on OIDHOST1 is down. There is also a 30-second time out period. During this period, the Load Balancing Router continues to direct traffic to both Oracle Internet Directory servers in round robin mode, and ldapbind failures will occur when it attempts connections to the Oracle Internet Directory on OIDHOST1.

2.4 Testing the Data Tier Components

Perform these steps to test the Data Tier components:

1. Ensure that you can connect to each Oracle Internet Directory instance and the Load Balancing Router, using this command:

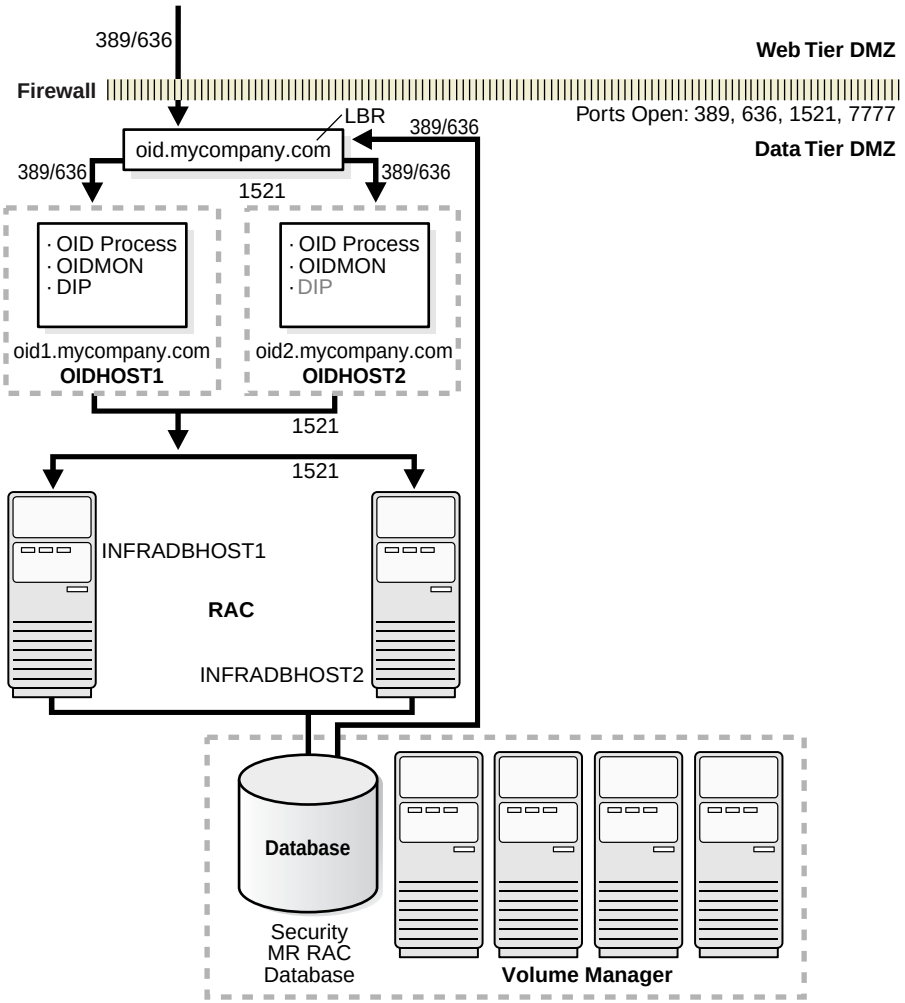
   ```
   ldapbind -p 389 -h OIDHOST1
   ldapbind -p 389 -h OIDHOST2
   ldapbind -p 389 -h oid.mycompany.com
   ```

2. Start the oidadmin tool on each Oracle Internet Directory instance in *ORACLE_HOME*/bin with this command:

   ```
   oidadmin
   ```

The Data Tier configuration is now as shown in Figure 2–15.

Figure 2–15 Data Tier Configuration



3

Installing and Configuring the myJ2EECompany Application Infrastructure

3.1 Installing and Configuring the Security Infrastructure

The security infrastructure for myJ2EECompany contains the components depicted in Figure 2–15, "Data Tier Configuration". The Oracle Internet Directory administration utility `oiddas` is required for Oracle Internet Directory administration. `oiddas` is installed in the application server environment with the Oracle Internet Directory server.

To install and configure this security infrastructure:

1. Follow all instructions in Section 2.1, "Installing the Oracle Application Server Metadata Repository for the Security Infrastructure" on page 2-1.
2. Follow all instructions in Section 2.2, "Installing the Oracle Internet Directory Instances in the Data Tier" on page 2-6.
3. Follow all instructions in Section 2.3, "Configuring the Virtual Server to Use the Load Balancing Router" on page 2-18.
4. Follow all instructions in Section 2.4, "Testing the Data Tier Components" on page 2-19.

3.2 Installing and Configuring the Application and Web Tiers

The Application Tier consists of multiple computers hosting middle tier Oracle Application Server Release 3 (10.1.3) instances. Each instance can contain multiple Oracle Containers for J2EE instances on which you deploy applications. In the complete configuration, requests are balanced among the OC4J instances on the application tier computers to create a performant and fault tolerant application environment.

The Web Tier(WEBHOST1 and WEBHOST2) consists of Oracle HTTP Servers from the Release 2 (10.1.2.0.0) Companion CD. Figure 2–1, "Enterprise Deployment Architecture for myJ2EEcompany.com with JAZN-SSO/DAS" on page 2-4 and Figure 2–2, "Enterprise Deployment Architecture for myJ2EEcompany.com with Oracle Access Manager" on page 2-5, show the Application Tier (APPHOST1 and APPHOST2) and Web tiers.

3.2.1 Installing the Application Tier Application Server Instances on APPHOST1 and APPHOST2

You can install an Oracle Application Server instance consisting only of one OC4J instance, using the Advanced installation option of the Oracle Universal Installer. Follow these steps to install and create the instances on APPHOST1 and APPHOST2:

1. Ensure that the system, patch, kernel and other requirements are met as specified in the *Oracle Application Server Installation Guide*. You can find this guide in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Start the Oracle Universal Installer as follows:

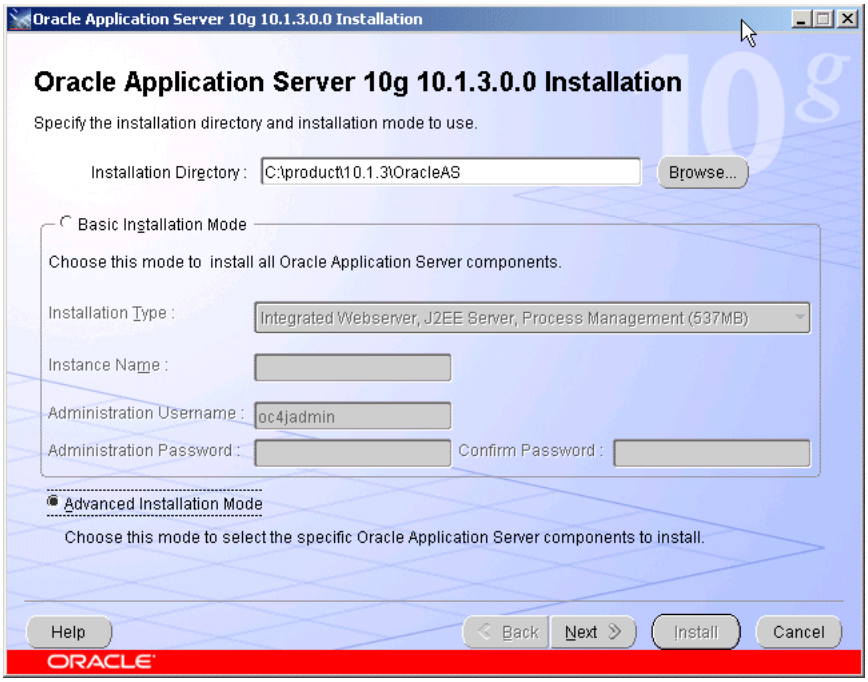
   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   The **Oracle Application Server 10.1.3.0.0 Installation** screen appears with the Basic Installation Mode and the Integrated Web Server, J2EE Web Server and Process Management installation type selected.
3. Specify an installation directory for the instance, or leave the default.
4. Select the **Advanced Installation Mode** and click **Next**.

   A confirmation dialog appears.

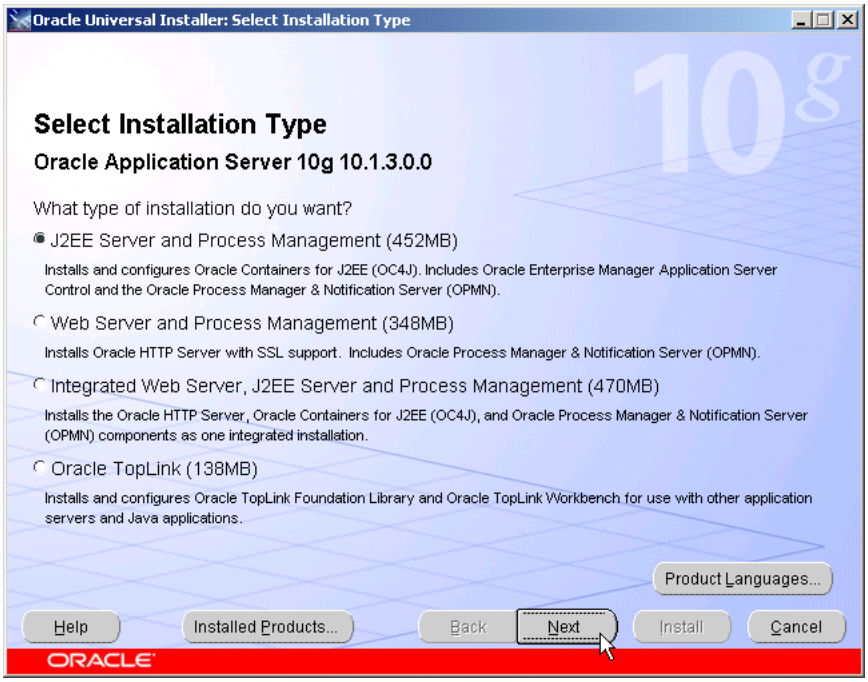
Figure 3–1 Oracle Universal Installer Oracle Application Server 10.1.3.0.0 Installation Screen with Advanced Installation Mode Selected



5. Click **Yes**.

   A progress dialog appears, then the **Select Installation Type** screen appears.

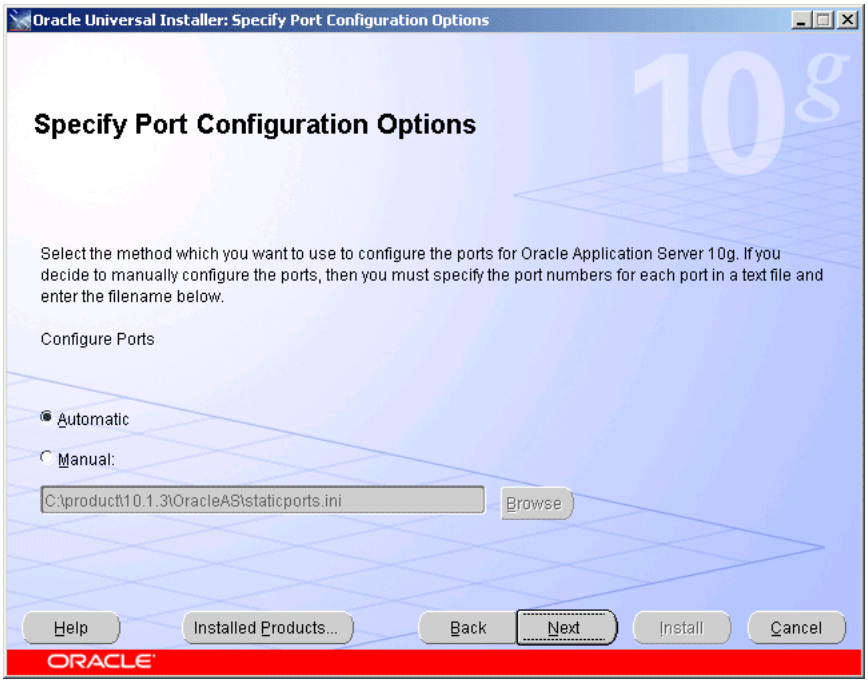
Figure 3–2 Oracle Universal Installer Select Installation Type Screen



6. Select the **J2EE Server and Process Management** option and click **Next**.

   The Specify **Port Configuration Options** screen appears.

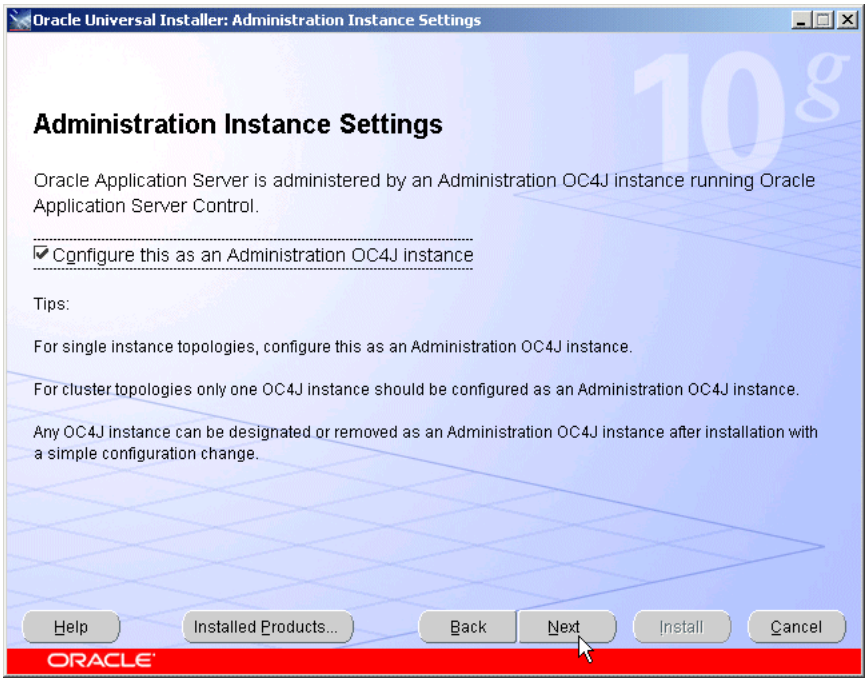
Figure 3–3 Oracle Universal Installer Specify Port Configuration Options Screen



7. Select **Automatic** and click **Next**.

   The **Administration Instance Settings** screen appears.

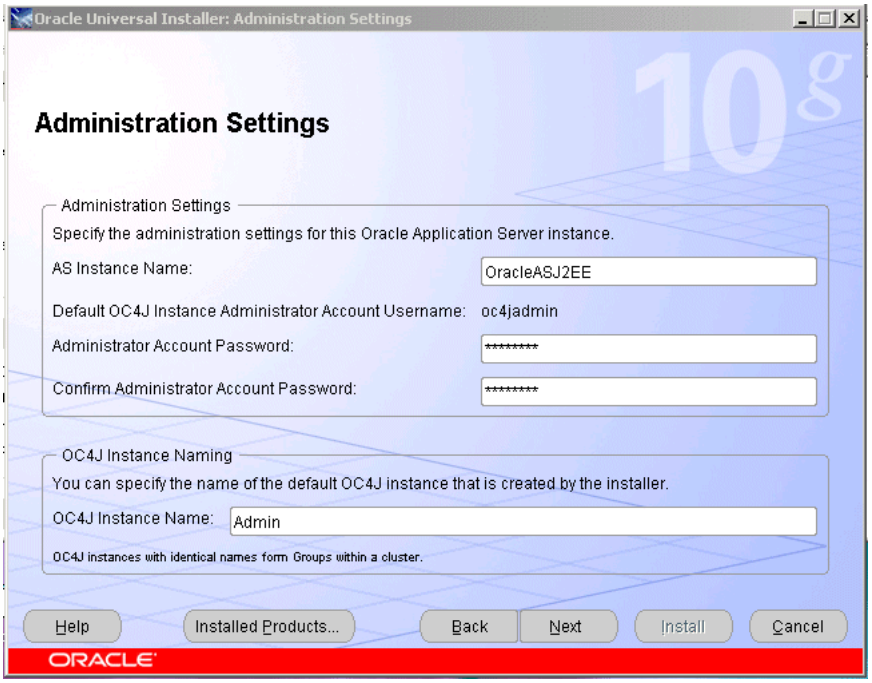
Figure 3–4 Oracle Universal Installer Administration Instance Settings Screen



8. Check the box to designate the instance installed on APPHOST1 as an administration OC4J instance.
9. Click **Next**.

   The **Administration Settings** screen appears.

Figure 3–5 Oracle Universal Installer Administration Settings Screen



10. Specify an instance name for the application server instance.

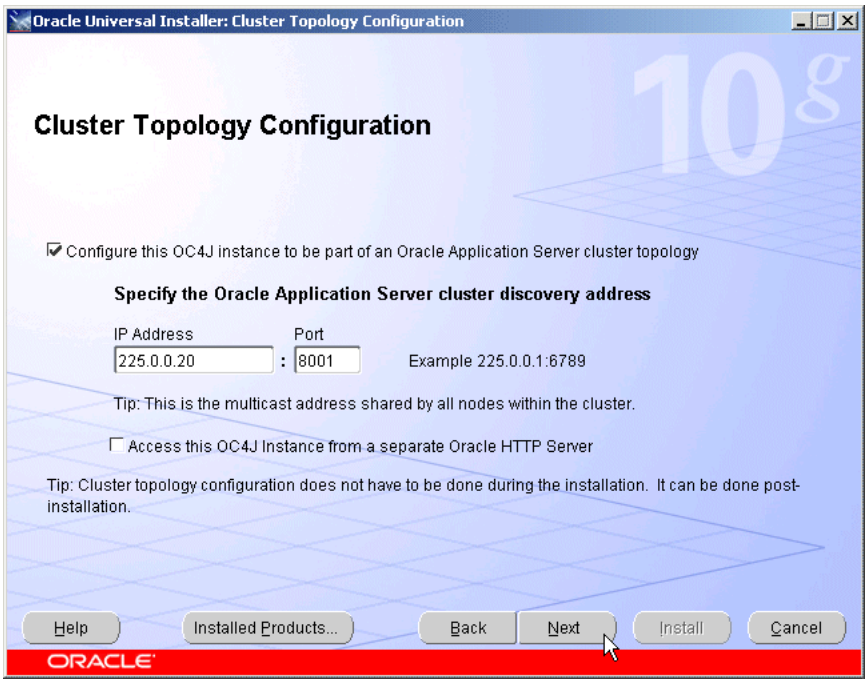
> **Note:** The instance name you specify will be prepended to the host name. For example, if you specify `J2EE` as the instance name and the host name is `server1.mycompany.com`, the instance name will be `J2EE.server1.mycompany.com`.

11. Specify and confirm the administrator password for the default OC4J instance.
12. Specify a name for the default OC4J instance created by the installer (the default is `home`), such as `Admin`, or a similar name that designates it as the instance dedicated to Application Server Control, and click **Next**.

> **Note:** You will not deploy applications to this instance; it will not be clustered with the user-created OC4J instances on which applications are deployed.

The **Cluster Topology Configuration** screen appears.

Figure 3–6 Oracle Universal Installer Cluster Topology Configuration Screen



13. Specify the multicast address and port.
14. Leave the checkbox blank for the option **Access this OC4J instance from a separate Oracle HTTP Server** for the OC4J Admin instance installed on APPHOST1.
15. Click **Next**.

    The **Summary** screen appears.
16. Click **Install**.

    The **Preparing to Install** dialog appears, then the **Install** screen appears.
17. The **Configuration Assistants** screen appears. When the configuration process completes, the **End of Installation** screen appears.
18. Click **Exit**, and then confirm your choice to exit.
19. Use the `netstat` command to identify an unoccupied HTTP port:

    ```
    netstat -an
    ```
20. Create one or more OC4J instances for application deployment by performing these steps:

    a. Issue this command in *APPHOST1_ORACLE_HOME*`/BIN`:

    ```
    createinstance -instancename Apps -port HTTP port
    ```

    In the preceding command, *Apps* is the instance name and *HTTP port* is an unoccupied http port. Use the same instance name for all of the instances, so that the OC4J instances will be members of the same group.

The following message appears:

```
Creating OC4J instance "Apps"...

Set OC4J administrator's password for "Apps" (password
text will not be displayed as it is entered:
```

b. Provide and confirm a password.

Note: The instances in a group of OC4J instances must have the same password, so that the user specified in a deployment command can deploy to the entire group.

The following message appears:

```
The password for OC4J administrator "oc4jadmin" has been
set.

New OC4J instance "Apps" is created.
```

Note: An OC4J instance that you create does not have its own OC4J binary libraries; it uses the libraries installed in the instance created by the installer.

---

21. Start the newly created instance by issuing this command in *APPHOST1_ORACLE_HOME*/OPMN/BIN:

```
opmnctl startproc process-type=Apps
```

In the preceding command, *Apps* is the name you gave the OC4J instance when creating it.

22. Ensure that the AJP ports in the series 12501, 12502... are not in use by issuing the `netstat` command:

```
netstat -an
```

23. Specify the AJP port by issuing this command in *APPHOST1_ORACLE_HOME*/OPMN/BIN:

```
opmnctl config port update ias-component=OC4J
process-type=Apps portid=default-web-site protocol=ajp
range=12501
```

In the preceding command, *Apps* is the name you gave the OC4J instance when creating it.

24. Restart OPMN by issuing this command in *APPHOST1_ORACLE_HOME*/OPMN/BIN:

```
opmnctl reload
```

25. Verify that the installation was successful by viewing the instance in Oracle Enterprise Manager 10*g*. Start a browser and access the OC4J Admin instance at:

```
http://APPHOST1:8888/em
```

Note: The *ORACLE_HOME*/install/readme.txt file contains the URLs for the installation and a command to verify the status of processes.

---

26. Repeat Steps 1 through 24 to install the second Oracle Application Server instance on APPHOST2 and create OC4J instances, specifying the APPHOST2 host name.
27. Verify that the installation was successful by viewing the instance in Oracle Enterprise Manager 10*g*. Start a browser and access the OC4J Admin instance at:

    `http://APPHOST2:8888/em`

    Note: The *`ORACLE_HOME`*`/install/readme.txt` file contains the URLs for the installation and a command to verify the status of processes.

3.2.2 Installing the Oracle HTTP Servers on WEBHOST1 and WEBHOST2

Obtain the standalone Oracle HTTP Server from the Oracle Application Server Companion CD, included in the Oracle Application Server CD Pack.

Follow these steps to install an Oracle HTTP Server on WEBHOST1 and WEBHOST2:

1. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   The **Welcome** screen appears.
2. Click **Next**.

   On UNIX systems, the **Specify Inventory Directory and Credentials** screen appears.
3. Specify the directory you want to be the `oraInventory` directory and the operating system group that has write permission to it.
4. Click **Next**.

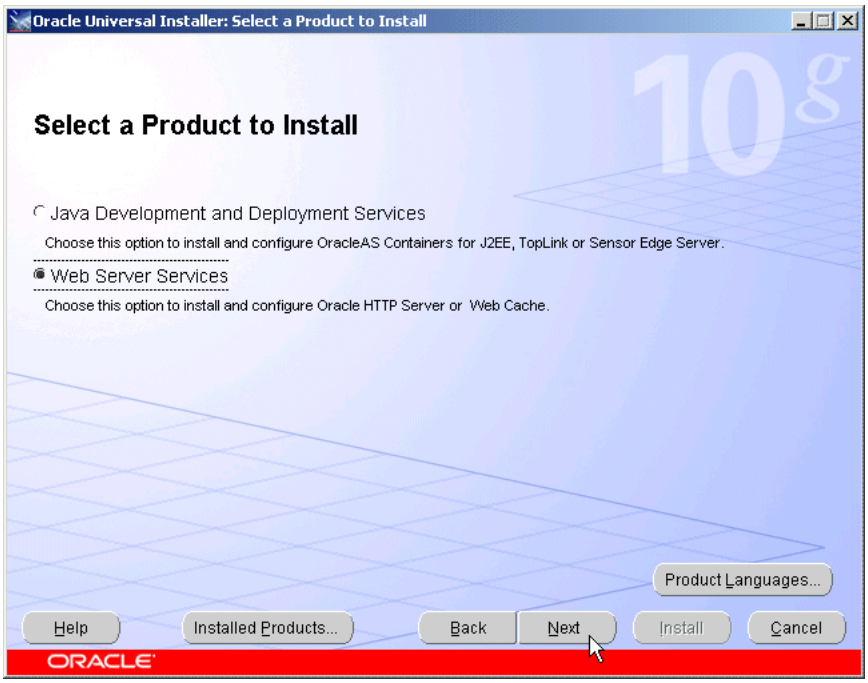
   On UNIX systems, a dialog appears, prompting you to run the `orainstRoot.sh` script.
5. Open a window and run the script, following the prompts in the window.
6. Return to the Oracle Universal Installer screen and click **Next**.

   The **Specify File Locations** screen appears with default locations for:

   - The product files for installation (Source)
   - The name and path to the Oracle home (Destination)
7. Click **Next**.

   The **Select a Product to Install** screen appears.

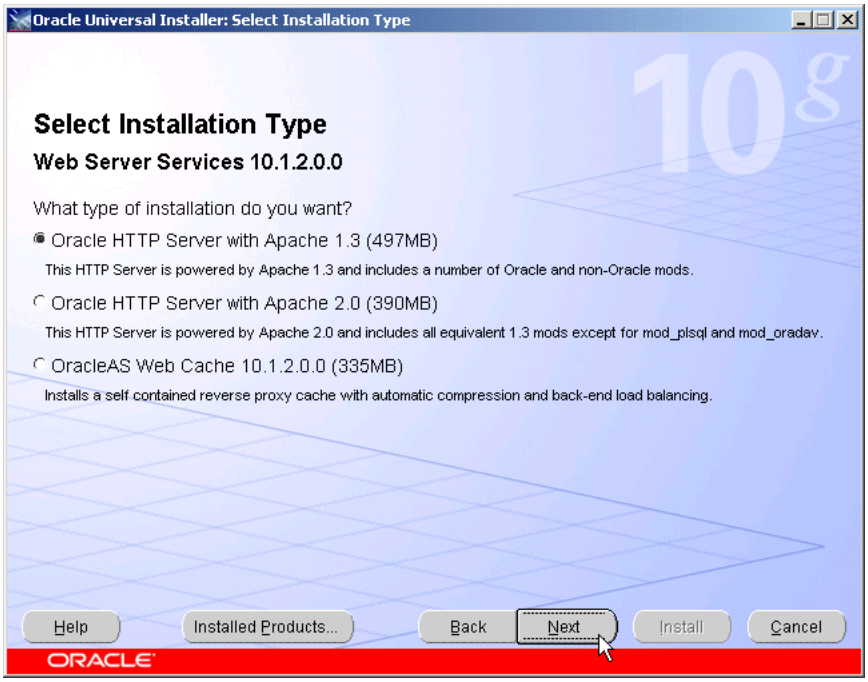
Figure 3–7 Oracle Universal Installer Select a Product to Install Screen



8. Select **Web Server Services**, as shown in Figure 3–7, and click **Next**.

   The **Select Installation Type** screen appears.

Figure 3–8 Oracle Universal Installer Select Installation Type Screen



9. Select **Oracle HTTP Server with Apache 1.3** and click **Next**.

> **Note:** If you wish to use the Oracle HTTP Server based on Apache 2.0 for the OracleAS Single Sign-On/Oracle Delegated Administration Services configuration, select Oracle HTTP Server with Apache 2.0 and perform the steps in Section 3.3, "Configuring the Oracle HTTP Server with Apache 2.0 for Use With Oracle Application Server Single Sign-On/Oracle Delegated Administration Services".

The **Summary** screen appears.

10. Click **Install**.

    The **Install** screen appears. When processing completes, the **Next** button activates.

11. Click **Next**.

    The **Configuration Assistants** screen appears. When the configuration completes, the **End of Installation** screen appears.

12. Click **Exit**, and then confirm your choice to exit.

13. Verify that the installation was successful by viewing the Oracle HTTP Server server home page. Start a browser and access **`http://hostname:7777`**.

3.3 Configuring the Oracle HTTP Server with Apache 2.0 for Use With Oracle Application Server Single Sign-On/Oracle Delegated Administration Services

If you chose Oracle HTTP Server with Apache 2.0 as the installation option and are configuring myJ2EE with SSO/DAS, you must perform the following configuration steps after installation:

1. Stop the Oracle HTTP Server.
2. Apply Patch No. 5070025 (available on MetaLink).
3. Comment out or remove these LoadModule directives in *ORACLE_HOME*/ohs/conf/httpd.conf:

```
LoadModule auth_module modules/mod_auth.so
LoadModule auth_anon_module modules/mod_auth_anon.so
LoadModule auth_dbm_module modules/mod_auth_dbm.so
```

4. Start the Oracle HTTP Server.

3.4 Configuring the Oracle HTTP Server with the Load Balancing Router

The Load Balancing Router (myapp.mycompany.com (shown in Figure 2–1, "Enterprise Deployment Architecture for myJ2EEcompany.com with JAZN-SSO/DAS" must be configured to receive client requests and balance them to the two Oracle HTTP Server instances on the Web tier. See the load balancing router documentation for instructions on configuring the load balancer, and follow the instructions in this section configure the Oracle HTTP Server.

Incoming requests must be associated with the Load Balancing Router hostname and port in the myJ2EECompany configuration. To configure this, perform these steps on WEBHOST1 and WEBHOST2:

1. Open the Oracle HTTP Server configuration file:

   ORACLE_HOME/Apache/Apache/conf/httpd.conf

2. Perform the following steps:

   a. Add the `LoadModule certheaders_module` directive for the appropriate platform.

      UNIX:

      ```
      LoadModule certheaders_module libexec/mod_certheaders.so
      ```

      Windows:

      ```
      LoadModule certheaders_module modules/ApacheModuleCertHeaders.dll
      ```

b. Add the following lines to create a `NameVirtualHost` directive and a `VirtualHost` container for myapp.mycompany.com and port 443.

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName myapp.mycompany.com
  Port 443
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
  SimulateHttps On
</VirtualHost>
```

Notes: The `LoadModule` directives (in particular, the `LoadModule rewrite_module` directive) must appear in the `httpd.conf` file at a location preceding the `VirtualHost` directives. The server must load all modules before it can execute the directives in the `VirtualHost` container.

It is a good idea to create the `VirtualHost` directives at the end of the `httpd.conf` file.

---

3. Save the `httpd.conf` file.
4. Restart the components using these commands in *ORACLE_HOME*`/opmn/bin`:

```
opmnctl stopall
opmnctl startall
```

3.5 Configuring OC4J Routing

mod_oc4j, an Oracle HTTP Server module, performs the request routing to the OC4J instances over the AJP13 protocol. The routing configuration is specified in the `mod_oc4j.conf` file. (The `mod_oc4j.conf` file is referenced by the main server configuration file for Oracle HTTP Server, `httpd.conf`, with an `Include` directive.) The path to the `mod_oc4j.conf` file is:

ORACLE_HOME`/Apache/Apache/conf/mod_oc4j.conf`

For complete descriptions of all directives and their uses, see the *Oracle HTTP Server Administrator's Guide.*

The default file at installation resembles Example 3–1:

Example 3–1 mod_oc4j.conf File

```
LoadModule oc4j_module modules/ApacheModuleOc4j.dll
<IfModule mod_oc4j.c>
    <Location /oc4j-service>
        SetHandler oc4j-service-handler
        Order deny,allow
        Deny from all
        Allow from localhost my-pc.mycompany.com my-pc
    </Location>
</IfModule>
```

Before you configure `mod_oc4j.conf` on WEBHOST1 and WEBHOST2, copy the `mod_oc4j.conf` file from APPHOST1 to WEBHOST1.

Follow these steps on WEBHOST1:

1. Open the *ORACLE_HOME*/Apache/Apache/conf/mod_oc4j.conf file.
2. Add an Oc4JConnTimeout directive to specify a time out value smaller than the time out value used by the firewall between the Web tier and the Application Tier. For example:

   ```
   Oc4jConnTimeout 10
   ```

3. Modify the Oc4JMount directives to specify the destinations to which requests should be load balanced.

   The syntax for the Oc4JMount directive is:

   ```
   Oc4jMount path [destination]
   ```

   path is the context root of the application and *destination* is an ajp13 destination, a cluster, or an instance. cluster is the default destination type.

Example 3–2 OC4JMount Directive to Route to FAQApp Using the AJP13 Protocol

```
Oc4jMount /FAQApp/* ajp13://myHost:8888
```

Example 3–3 OC4JMount Directive to Load Balance Requests to FAQApp on Multiple Instances

```
Oc4jMount /FAQApp/* instance://myOracleASInstance:myOC4Jinstance,
anotherOracleASInstance:anotherOC4Jinstance...
```

4. Save and close the file.
5. Copy the file from WEBHOST1 to WEBHOST2.
6. Restart the Oracle HTTP Server on WEBHOST1 and WEBHOST2.

3.6 Managing Oracle Application Server Component Connections

In order to ensure consistent availability of all services, ensure that the connection time out values for all Oracle Application Server components are set to a lower time out value than that on the firewall and Load Balancing Router. If the firewall or Load Balancing Router drops a connection without sending a TCP close notification message, then Oracle Application Server components will continue to try to use the connection when it is no longer available.

3.7 Configuring Application Authentication and Authorization

The Oracle Application Server Java Authentication and Authorization Service (JAAS) Provider (also referred to as JAZN) LDAP-based provider is used for authentication and authorization to the OC4J applications.

In the myJ2EECompany configuration, this provider is used without Oracle Application Server Single Sign-On. This section explains how to configure the Oracle Application Server instances on the application tier to use the JAZN LDAP provider. For instructions on how to use Oracle Enterprise Manager 10*g* to manage the data in this provider, see Chapter 8 in the *Oracle Containers for J2EE Security Guide.*

3.7.1 Using the Oracle Application Server Java Authentication and Authorization Service (JAAS) Provider

You will need to follow the steps in this section on both Oracle Application Server instances (APPHOST1 and APPHOST2) that will use the JAZN LDAP provider. Ensure that you specify the same Oracle Internet Directory computer for APPHOST1 and APPHOST2—that is, the load balancing router for OIDHOST1 and OIDHOST2.

Before you begin the steps in this section, ensure that the middle tier instance is stopped and the Oracle Internet Directory instance is running. Start the Oracle Enterprise Manager 10*g* Application Server Control Console, if necessary, and perform these steps:

1. On the **OC4J:home** page, click the **Administration** link.

   The **Administration Tasks** list appears.

2. In the **Security** section, click the **Go To Task** icon for **Identity Management**.

   The **Identity Management:** page appears.

3. Click **Configure** if no host is configured, or click **Change** if you want to change the configured host.

   The **Configure Identity Management: Connect Information** screen appears.

4. In the **Oracle Internet Directory Host** field, enter the host name of the Load Balancing Router (for example, **`oid.mycompany.com`**, in Figure 2–1).

5. In the **Oracle Internet Directory User DN** field, enter the Distinguished Name of the user that can log in to Oracle Internet Directory (the user must be in the IASAdmins group).

6. In the Password field, enter the Oracle Internet Directory user's password.

7. Select the checkbox to use the non-SSL connection to Oracle Internet Directory. In the **Port** field, enter `389`.

8. Click **Next**.

   The **Configure Identity Management: Application Server Control** page appears.

9. Select **Use Oracle Identity Management Security Provider**.

10. Click **Next**.

    The **Configure Identity Management: Deployed Applications** page appears.

11. Select the applications deployed to the OC4J instance that you want to use the Oracle Identity Management Security Provider.

12. Click **Configure**.

    A message appears notifying you that the configuration was successful, and notifies you that you must restart the OC4J instance.

13. Click **Restart**.

    The instance is restarted, and the configuration is complete.

3.7.2 Adding Administrative Users and Groups to Oracle Internet Directory for the OracleAS JAAS Provider

To use the OracleAS JAAS Provider, you must populate Oracle Internet Directory with certain user entries. In 10*g* (10.1.4.0.1), the accounts and groups are managed by Mbeans. You may still need to map or create an anonymous user account. See "Summary of OC4J Accounts" in the *Oracle Containers for J2EE Security Guide*.

4

Installing and Configuring JAZN-SSO/DAS

4.1 Setting up the Load Balancing Router

Before installing the Identity Management components, you must set up the Load Balancing Router to listen for requests to login.mycompany.com on port 443 (https), and balance the requests to the Oracle HTTP Servers' listening port 7777 (http). The Load Balancing Router should perform the protocol conversion, and must be configured for persistent HTTP sessions.

4.2 Installing and Configuring Oracle Application Server Single Sign-On

After the Data Tier is complete, follow these steps to install the Identity Management components (IDMHOST1 and IDMHOST2). configure OracleAS Single Sign-On on IDMHOST1 and IDMHOST2.

4.2.1 Installing the First Identity Management Configuration

Follow these steps to install Identity Management on IDMHOST1:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Application Server Quick Installation Guide* in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Copy the `staticport.ini` file from the `Disk1/stage/Response` directory to the Oracle home directory.
3. Edit the `staticport.ini` file and uncomment these entries:

```
Oracle HTTP Server port = 7777
Oracle HTTP Server Listen port = 7777
Application Server Control port = 1810
```

> **Note:** See Section A.3, "Using the Static Ports Feature with Oracle Universal Installer" on page A-2 for more information.

4. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   The **Welcome** screen appears.

5. Click **Next**.

   On UNIX systems, the **Specify Inventory Directory and Credentials** screen appears.

6. Specify the directory you want to be the `oraInventory` directory and the operating system group that has permission to write to it.

7. Click **Next**.

   On UNIX systems, a dialog appears, prompting you to run the `oraInstRoot.sh` script.

8. Open a window and run the script, following the prompts in the window.

9. Return to the Oracle Universal Installer screen and click **Next**.

   The **Specify File Locations** screen appears with default locations for:

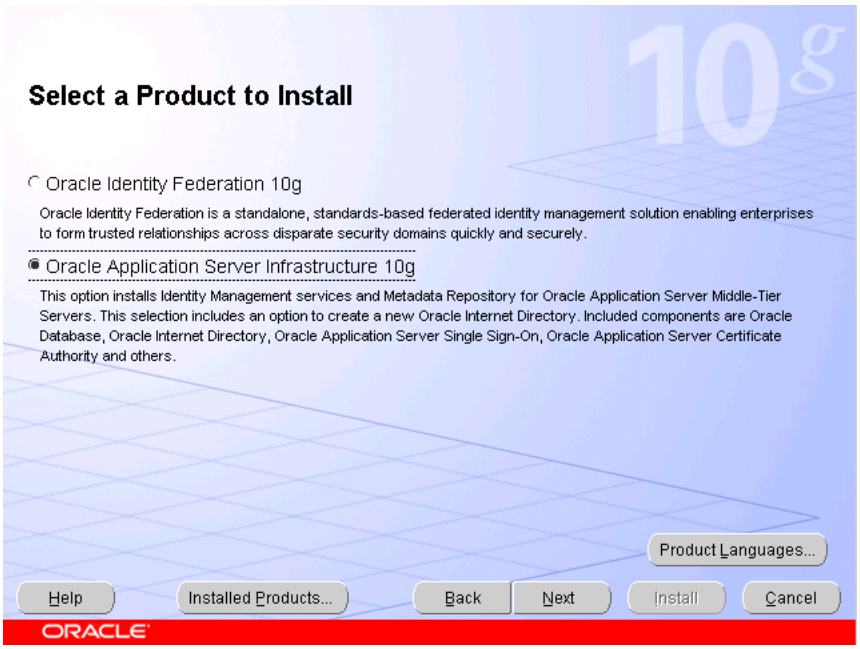
   - The product files for the installation (Source)
   - The name and path to an Oracle home (Destination)

   > **Note:** Ensure that the Oracle home directory path for IDMHOST1 is the same as the path to the Oracle home location of IDMHOST2. For example, if the path to the Oracle home on IDMHOST1 is:
   >
   > `/u01/app/oracle/product/AS10gSSO`
   >
   > then the path to the Oracle home on IDMHOST2 must be:
   >
   > `/u01/app/oracle/product/AS10gSSO`

10. Specify the **Destination Name** and **Path**, if different from the default, and click **Next**.

    The **Select a Product to Install** screen appears.

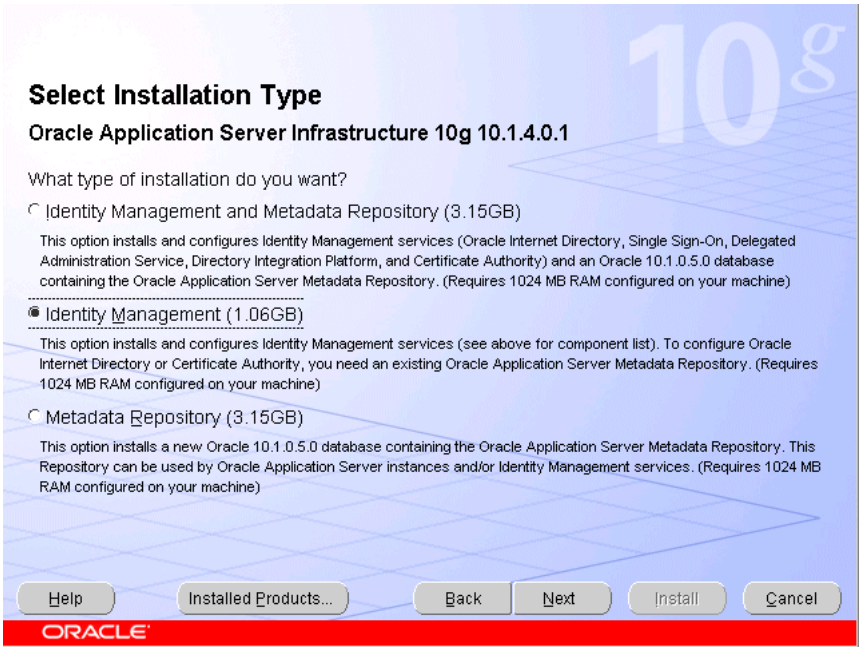
Figure 4–1 Oracle Universal Installer Select a Product to Install Screen



11. Select OracleAS Infrastructure 10g, as shown in Figure 4–1, and click **Next**.

The **Select Installation Type** screen appears.

Figure 4–2 Oracle Universal Installer Select Installation Type Screen



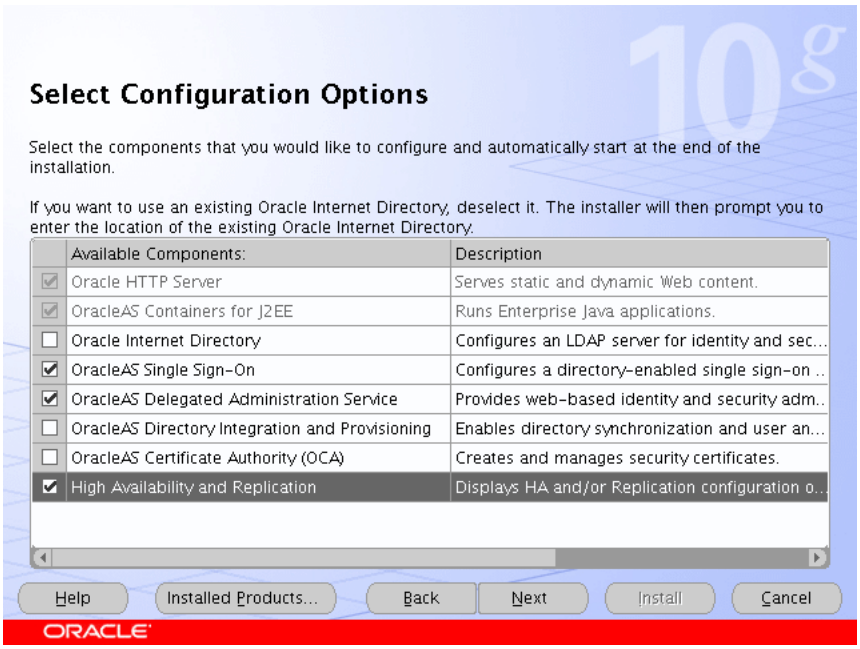
12. Select **Identity Management**, as shown in Figure 4–2, and click **Next**.

The **Confirm Pre-Installation Requirements** screen appears.

13. Ensure that the requirements are met and click **Next**.

The **Select Configuration Options** screen appears.

Figure 4–3 Oracle Universal Installer Select Configuration Options Screen



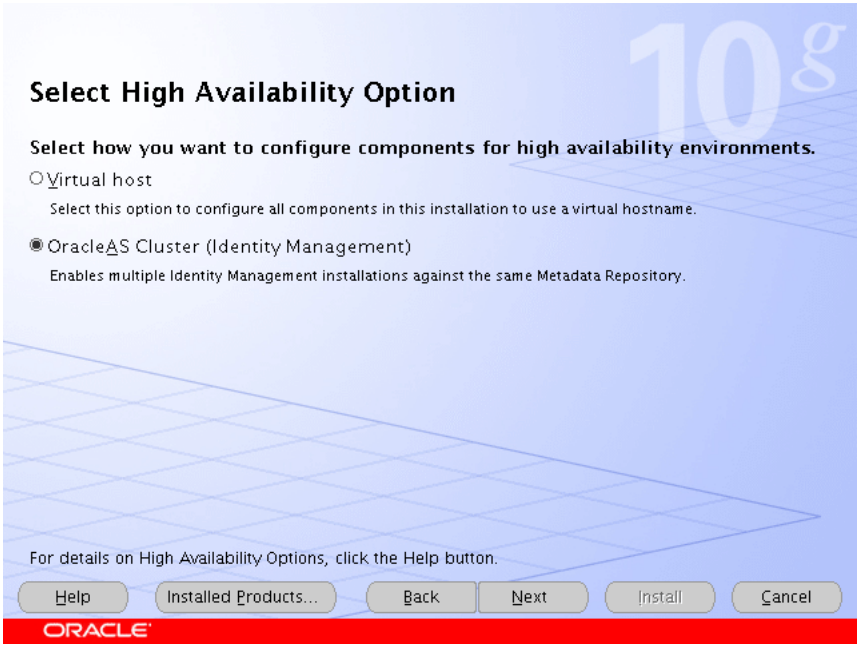
14. Select **OracleAS Single Sign-On, Oracle Delegated Administration Services**, and **High Availability and Replication**, as shown in Figure 4–3.

    The **Specify Port Configuration Options** screen appears.

15. Select **Manual**, specify the location of the `staticports.ini` file, and click **Next**.

    The **Select High Availability Option** screen appears.

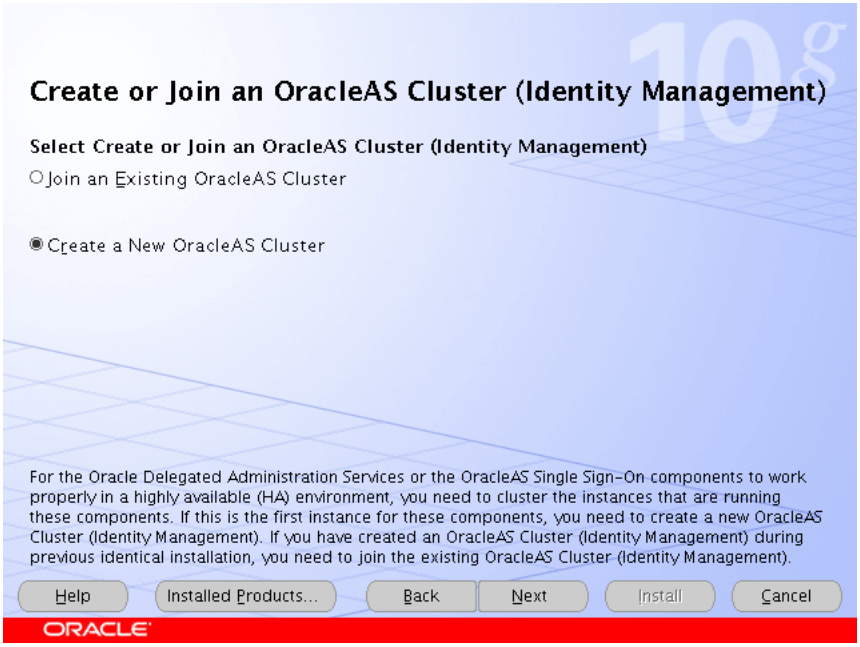
Figure 4–4 Oracle Universal Installer Select High Availability Option Screen



16. Select **OracleAS Cluster (Identity Management)**, as shown in Figure 4–4, and click **Next**.

The **Create or Join an OracleAS Cluster (Identity Management)** screen appears.

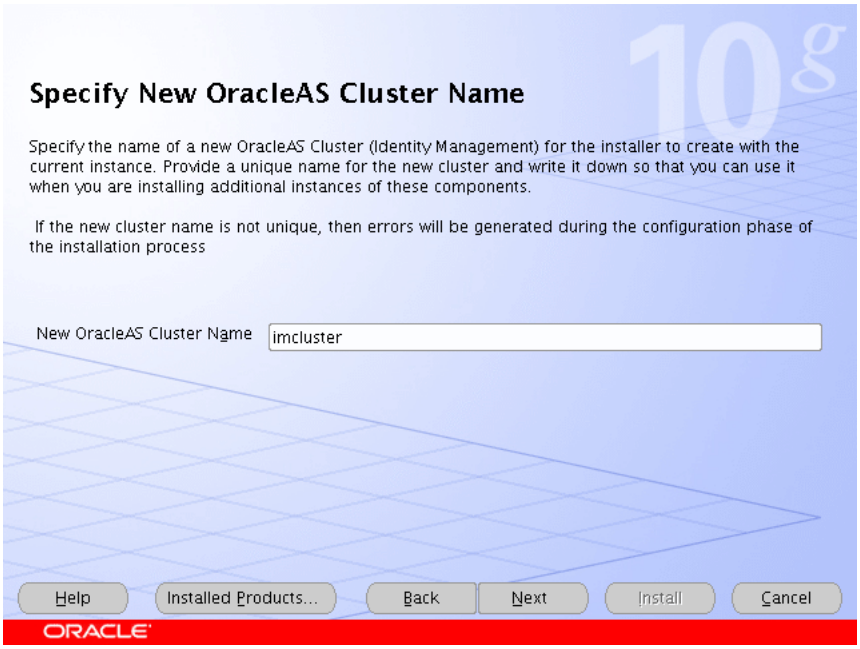
Figure 4–5 Oracle Universal Installer Create or Join an OracleAS Cluster (Identity Management) Screen



17. Select **Create a New OracleAS Cluster**, as shown in Figure 4–5, and click **Next**.

The **Specify New OracleAS Cluster Name** screen appears.

Figure 4–6 Oracle Universal Installer Specify New OracleAS Cluster Name Screen

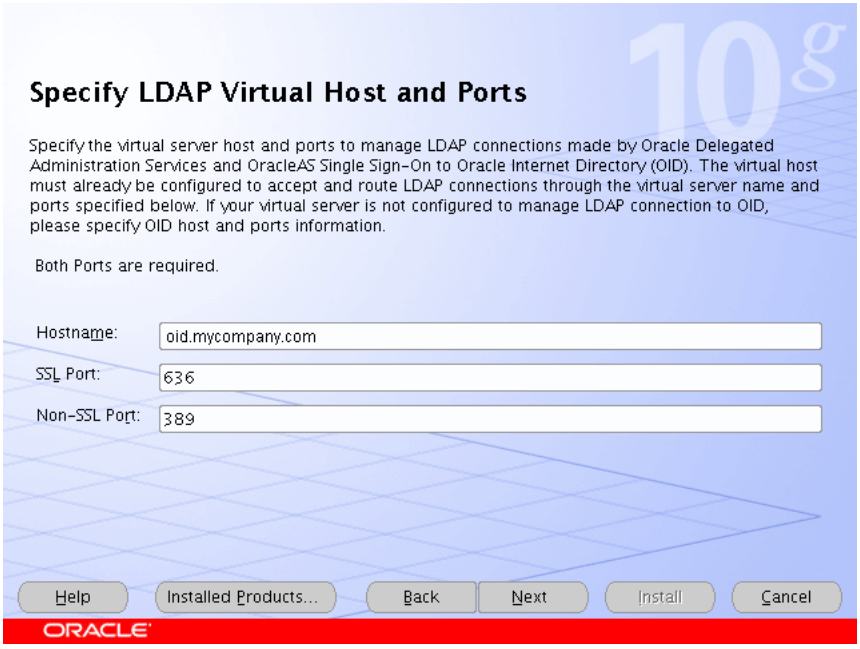


18. Complete the **New OracleAS Cluster Name** field with a name for the cluster, as shown in Figure 4–6, and click **Next**.

Note: Write down the cluster name. You will need to provide it in subsequent installations of instances that will join the cluster.

The **Specify LDAP Virtual Host and Ports** screen appears.

Figure 4–7 Oracle Universal Installer Specify LDAP Virtual Host and Ports Screen

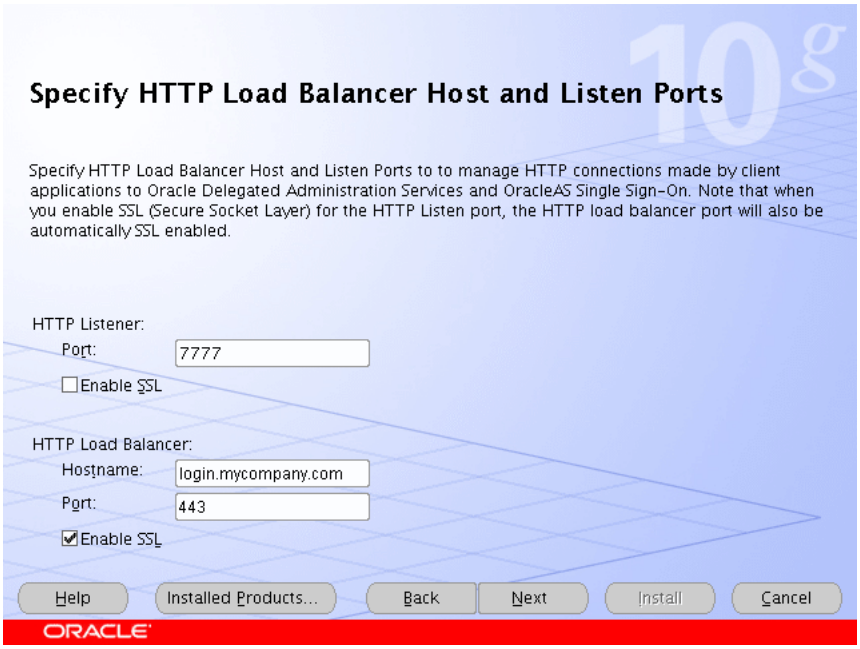


19. Enter the name of the Load Balancing Router, the SSL port, and the non-SSL port, as shown in Figure 4–7.
20. Click **Next**.

    The **Specify OID Login** screen appears.
21. Complete the fields and click **Next**.

    The **Specify HTTP Load Balancer and Listen Ports** screen appears.

Figure 4–8 Oracle Universal Installer Specify HTTP Load Balancer Host and Listen Ports Screen



22. Enter the listen port of the HTTP Server and the host name and port of the HTTP Load Balancer, enabling the SSL option for the load balancer, as shown in Figure 4–8.
23. Click **Next**.

    The **Specify Instance Name and ias_admin Password** screen appears.
24. Specify the instance name and password and click **Next**.

    The **Summary** screen appears.
25. Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.

    The **Install** screen appears with a progress bar. On UNIX systems, a dialog opens prompting you to run the `root.sh` script.
26. Open a window and run the script.

    The **Configuration Assistants** screen appears. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the **End of Installation** screen appears.
27. Click **Exit**, and then confirm your choice to exit.

4.2.2 Testing the Identity Management Components With Oracle Internet Directory

Follow these steps to test the first Identity Management installation with the Oracle Internet Directory:

1. Stop all components on OIDHOST1, using this command:

   ***ORACLE_HOME*/opmn/bin/opmnctl stopall**

2. Ensure that all components on OIDHOST2 are running:

   ***ORACLE_HOME*/opmn/bin/opmnctl status**

3. Access the following URL:

   https://IDMHOST1.mycompany.com/pls/orasso

4.2.3 Installing the Second Identity Management Configuration

Follow these steps to install Identity Management on IDMHOST2:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Application Server Quick Installation Guide* in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Copy the `staticport.ini` file from the `Disk1/stage/Response` directory to the Oracle home directory.
3. Edit the `staticport.ini` file and uncomment these entries:

   ```
   Oracle HTTP Server port = 7777
   Oracle HTTP Server Listen port = 7777
   Application Server Control port = 1810
   ```

   > **Note:** See Section A.3, "Using the Static Ports Feature with Oracle Universal Installer" on page A-2 for more information.

4. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **runInstaller**

   On Windows, double-click **setup.exe**

   The **Welcome** screen appears.

5. Click **Next**.

   On UNIX systems, the **Specify Inventory Directory and Credentials** screen appears.

6. Specify the directory you want to be the `oraInventory` directory and the operating system group that has permission to write to it.
7. Click **Next**.

   On UNIX systems, a dialog appears, prompting you to run the `oraInstRoot.sh` script.

8. Open a window and run the script, following the prompts in the window.

9. Return to the Oracle Universal Installer screen and click **Next**.

   The **Specify File Locations** screen appears with default locations for:

   - The product files for the installation (Source)
   - The name and path to an Oracle home (Destination)

   Note: Ensure that the Oracle home directory path for IDMHOST1 is the same as the path to the Oracle home location of IDMHOST2. For example, if the path to the Oracle home on IDMHOST1 is:

   `/u01/app/oracle/product/AS10gSSO`

   then the path to the Oracle home on IDMHOST2 must be:

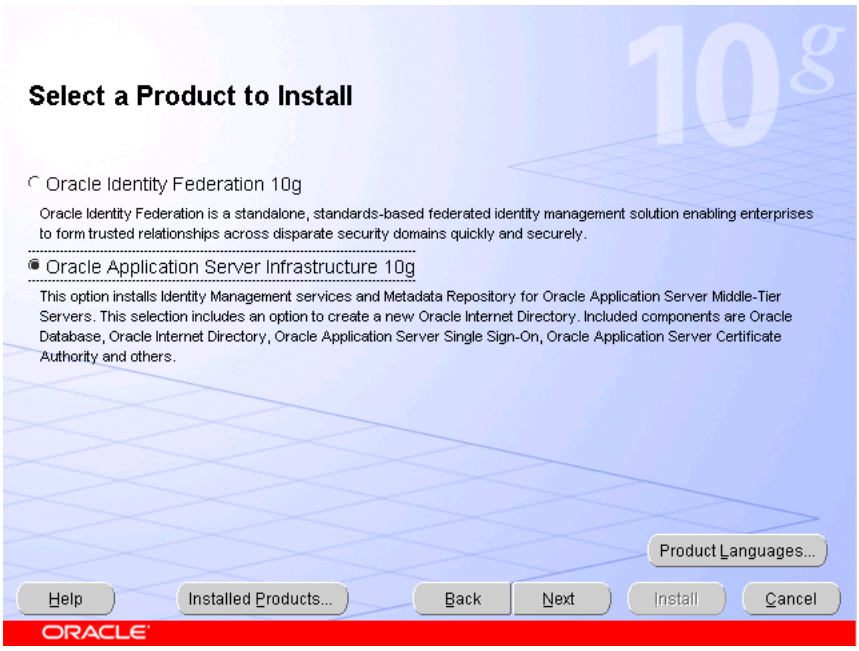
   `/u01/app/oracle/product/AS10gSSO`

   ---

10. Specify the **Destination Name** and **Path**, if different from the default, and click **Next**.

    The **Select a Product to Install** screen appears.

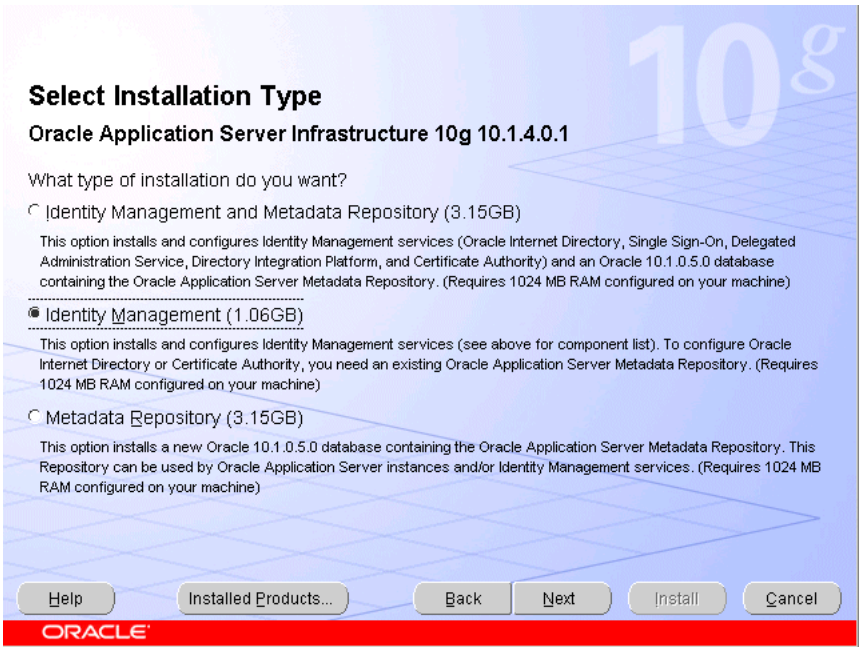
Figure 4–9 Oracle Universal Installer Select a Product to Install Screen



11. Select OracleAS Infrastructure 10g, as shown in Figure 4–9, and click **Next**.

    The **Select Installation Type** screen appears.

Figure 4–10 Oracle Universal Installer Select Installation Type Screen



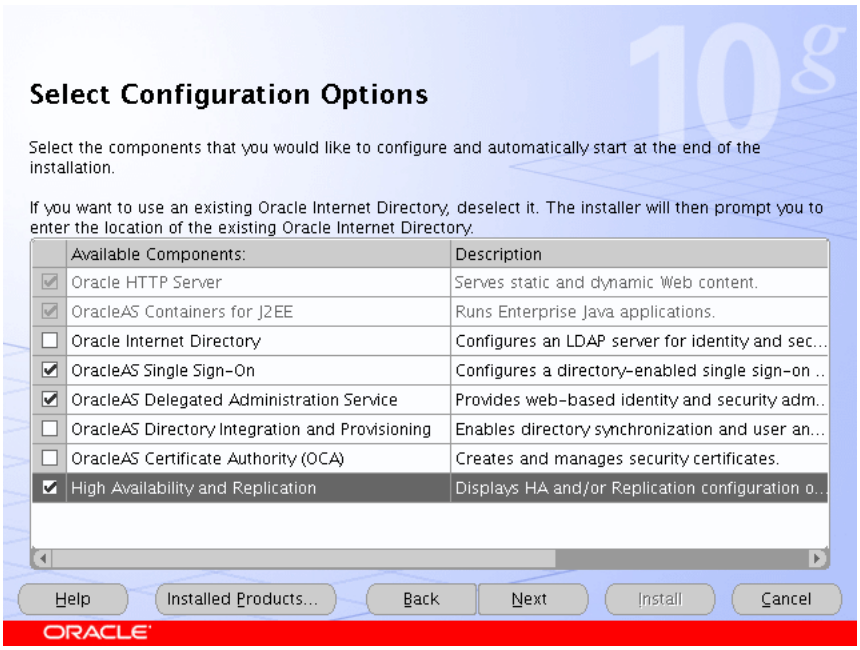
12. Select **Identity Management** as shown in Figure 4–10, and click **Next**.

    The **Confirm Pre-Installation Requirements** screen appears.

13. Ensure that the requirements are met and click **Next**.

    The **Select Configuration Options** screen appears.

Figure 4–11 Oracle Universal Installer Select Configuration Options Screen

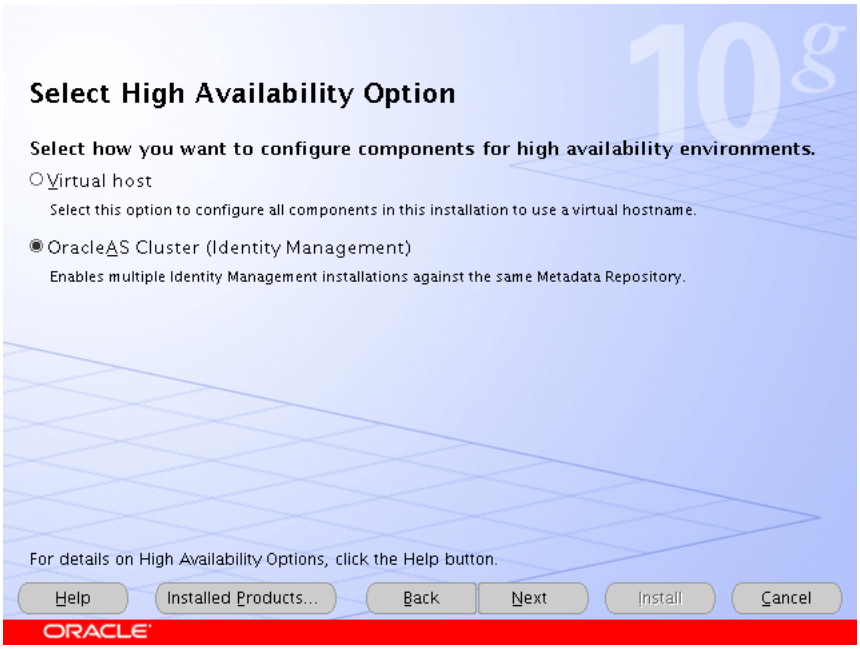


14. Select **OracleAS Single Sign-On, Oracle Delegated Administration Services**, and **High Availability and Replication**, as shown in Figure 4–11.

15. Click **Next**.

    The **Select High Availability Option** screen appears.

Figure 4–12 Oracle Universal Installer Select High Availability Option Screen



16. Select **OracleAS Cluster (Identity Management)**, as shown in Figure 4–12, and click **Next**.

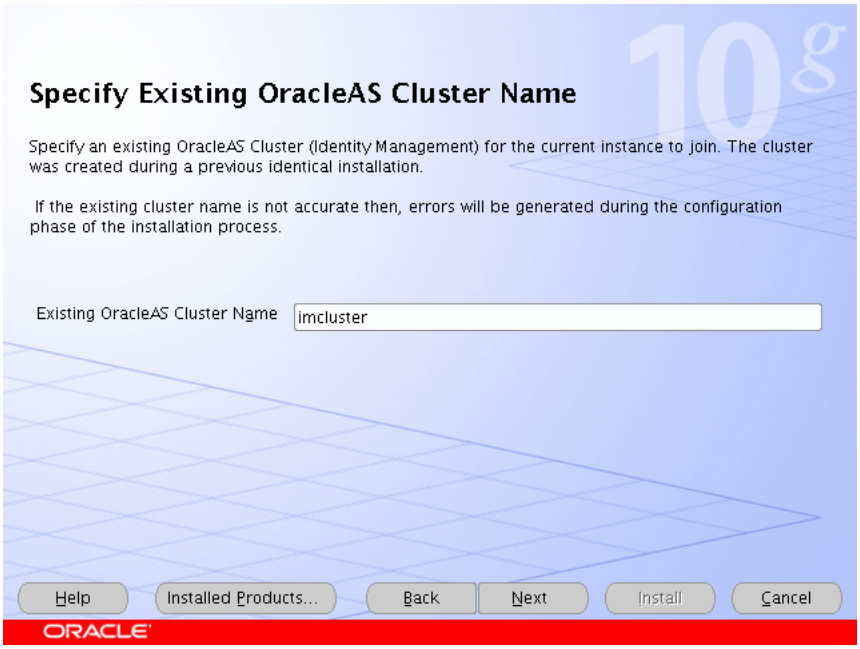
    The **Create or Join an OracleAS Cluster (Identity Management)** screen appears.

Figure 4–13 Oracle Universal Installer Create or Join an OracleAS Cluster (Identity Management) Screen

17. Select **Join an Existing OracleAS Cluster**, as shown in Figure 4–5, and click **Next**.

    The **Specify Existing OracleAS Cluster Name** screen appears.

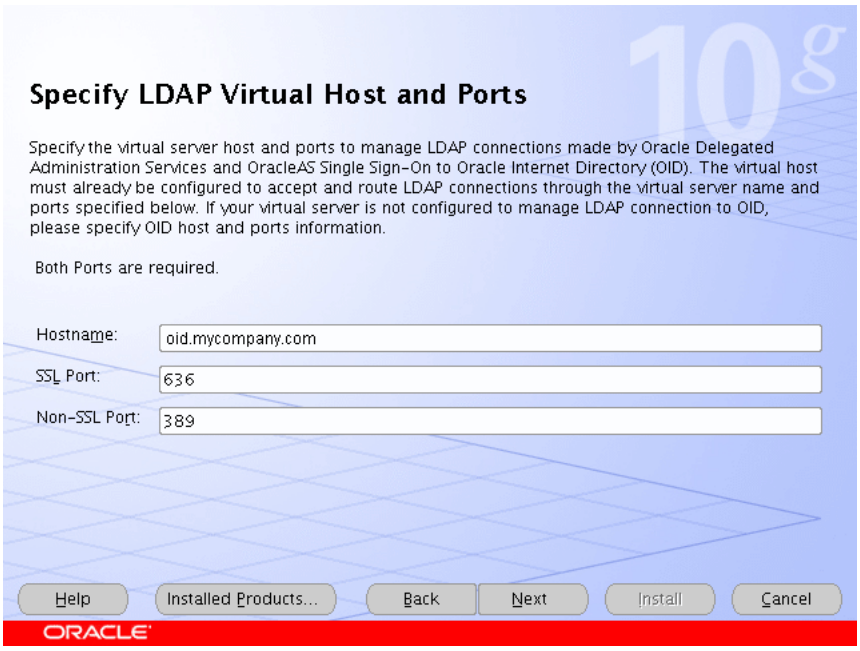
Figure 4–14 Oracle Universal Installer Specify Existing OracleAS Cluster Name Screen



18. Complete the **Existing OracleAS Cluster Name** field with the name you provided for the cluster when installing the first instance, as shown in Figure 4–6, and click **Next**.

    The **Specify LDAP Virtual Host and Ports** screen appears.

Figure 4–15 Oracle Universal Installer Specify LDAP Virtual Host and Ports Screen

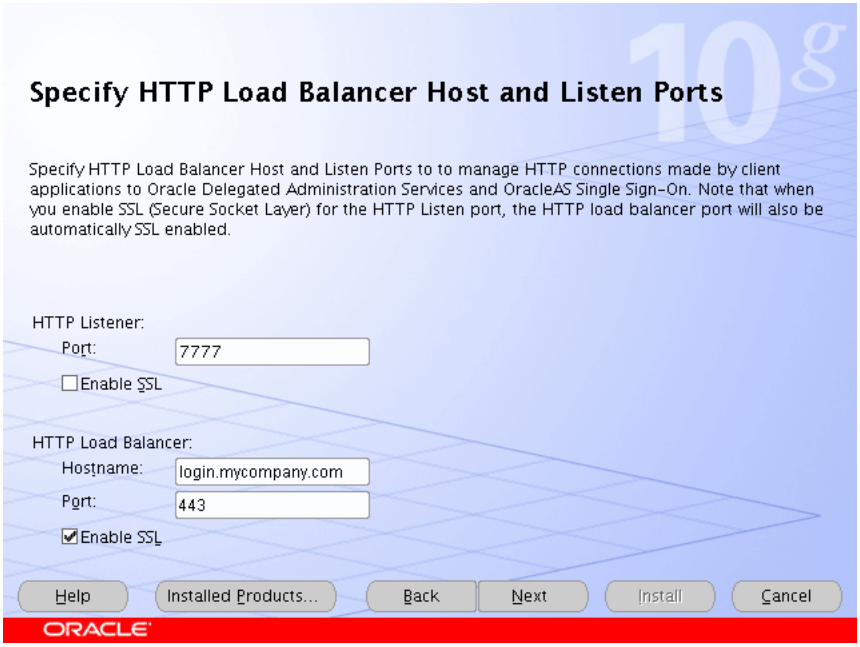


19. Enter the name of the Load Balancing Router, the SSL port, and the non-SSL port, as shown in Figure 4–7.
20. Click **Next**.

    The **Specify OID Login** screen appears.
21. Complete the fields and click **Next**.

    The **Specify HTTP Load Balancer and Listen Ports** screen appears.

Figure 4–16 Oracle Universal Installer Specify HTTP Load Balancer Host and Listen Ports Screen



22. Enter the listen port of the HTTP Server and the host name and port of the HTTP Load Balancer, enabling the SSL option for the load balancer, as shown in Figure 4–16.
23. Click **Next**.

    The **Specify Instance Name and ias_admin Password** screen appears.
24. Specify the instance name and password and click **Next**.

    The **Summary** screen appears.
25. Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.

    The **Install** screen appears with a progress bar. On UNIX systems, a dialog opens prompting you to run the `root.sh` script.
26. Open a window and run the script.

    The **Configuration Assistants** screen appears. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the **End of Installation** screen appears.
27. Click **Exit**, and then confirm your choice to exit.

4.3 Reconfiguring Oracle Application Server Single Sign-On and Oracle Delegated Administration Services with the Oracle HTTP Servers

Follow the steps in this section to reconfigure OracleAS Single Sign-On and Oracle Delegated Administration Services.

1. Ensure that:
   - The Oracle Identity Management instance is started (status is Up).
   - You have the Oracle Internet Directory host and port numbers.
   - You have the password for cn=orcladmin, or another user who is a member of the iASAdmins group
2. Issue the command **`ssocfg.sh`** (UNIX) or (Windows) in *`IDMHOST1_ORACLE_HOME`*`/sso/bin` and *`IDMHOST2_ORACLE_HOME`*`/sso/bin`:

   `ssocfg.sh https `*`login.mycompany.com`*` 443`

   In the preceding command, *login.mycompany.com* is the VIP hostname for the Load Balancing Router.
3. On IDMHOST1 and IDMHOST2, set the environment variables `ORACLE_HOME` and `ORACLE_SID`.
4. Issue the command **`ssoreg.sh`** (UNIX), or **`ssoreg.bat`** (Windows) in *`IDMHOST1_ORACLE_HOME`*`/sso/bin`:

   `ssoreg.sh -oracle_home_path $ORACLE_HOME`

   `-config_mod_osso TRUE`

   `-site_name `*`login.mycompany.com`*`:443`

   `-remote_midtier`

   `-config_file $ORACLE_HOME/Apache/Apache/conf/osso/`*`myosso.conf`*

   `-mod_osso_url https://`*`myapp.mycompany.com`*`:443`

   In the example, *myossof.conf* is the name of the resulting obfuscated osso configuration file created.
5. Copy the *myosso.conf* file to *`WEBHOST1_ORACLE_HOME`*`/Apache/Apache/conf/osso` and *`WEBHOST2_ORACLE_HOME`*`/Apache/Apache/conf/osso`.
6. Configure mod_osso by following the instructions for the Oracle HTTP Server version in use:

   Release 3 (10.1.3):

   a. Issue this command on WEBHOST1 and WEBHOST2:

      (UNIX) ***`ORACLE_HOME`*`/Apache/Apache/bin/osso1013 config_file`**

      (Windows) **`perl `*`ORACLE_HOME`*`/Apache/Apache/bin/osso1013 config_file`**

   Release 3 (10.1.2):

   a. Copy the obfuscated osso configuration file created in Step 4 to the ***`ORACLE_HOME`*`/Apache/Apache/conf/osso`** directory in WEBHOST1 and WEBHOST2:

   b. Modify the *`ORACLE_HOME`*`/Apache/Apache/conf/httpd.conf` file by uncommenting the `Include mod_osso.conf` directive.

c. Modify the *ORACLE_HOME*/Apache/Apache/conf/mod_osso.conf file to add this directive:

```
OssoConfigFile $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf
```

7. Copy the *IDMHOST1_ORACLE_HOME*/sso/conf/sso_apache.conf file to WEBHOST1.

8. Modify the *WEBHOST1_ORACLE_HOME*/Apache/Apache/conf/httpd.conf file to add this directive:

```
Include sso_apache.conf
```

9. Modify the sso_apache.conf file on WEBHOST1 to enable the SSL section and comment out the rewrite section (only the section shown in the example is enabled).

```
<IfDefine SSL>
   Oc4jExtractSSL on
   <Location /sso>
       SSLOptions +ExportCertData +StdEnvVars
   </Location>
</IfDefine>
```

10. Copy the sso_apache.conf file from WEBHOST1 to WEBHOST2.

11. Modify the *WEBHOST2_ORACLE_HOME*/Apache/Apache/conf/httpd.conf file to add this directive:

```
Include sso_apache.conf
```

12. Use these commands to identify the AJP port on IDMHOST1 and IDMHOST2:

```
IDMHOST1_ORACLE_HOME/opmn/bin/opmnctl status -l
```

```
IDMHOST2_ORACLE_HOME/opmn/bin/opmnctl status -l
```

13. Modify the *WEBHOST1_ORACLE_HOME*/Apache/Apache/conf/mod_oc4j.conf and *WEBHOST2_ORACLE_HOME*/Apache/Apache/conf/mod_oc4j.conf files by substituting the port values obtained in Step 21 for *AJP port 1* and *AJP port 2* in the Oc4jMount directives). This configuration directs OracleAS Single Sign-On and Oracle Delegated Administration Services requests to the identity management server using the AJP protocol.

```
<IfModule mod_oc4j.c>
...
Oc4jMount /oiddas ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /oiddas/* ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /sso ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /sso/* ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /ssohelp ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /ssohelp/* ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
 Oc4jMount /pls ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /pls/* ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
...
</IfModule>
```

14. Configure Oracle Delegated Administration Services by adding the following to *WEBHOST1_ORACLE_HOME*/Apache/Apache/conf/mod_osso.conf:

```
<IfModule mod_osso.c>
# for oiddas protected region
  <Location /oiddas/ui/oracle/ldap/das>
   require valid-user
   AuthType Basic
  </Location>
</IfModule>
<IfModule mod_alias.c>
# Define the alias which maps the "/uixi/" URI to
# the current version of the UIX installables
  Alias /uixi/ "ORACLE_HOME/uix/cabo/"
# Turn on browser caching for the UIX installables
  <Location /uixi>
# Use mod_headers to set the cache-control header
   Header set cache-control "Public"
# Use mod_expires to set the expires header to some
# date in the distant future
    ExpiresActive on
    ExpiresDefault "access plus 364 days"
  </Location>
</IfModule>
```

15. Copy *WEBHOST1_ORACLE_HOME*/Apache/Apache/conf/mod_osso.conf to *WEBHOST2_ORACLE_HOME*/Apache/Apache/conf/, changing the *ORACLE_HOME* value in `Alias /uixi/ "ORACLE_HOME/uix/cabo/"` to specify *WEBHOST2_ORACLE_HOME*.

16. Configure the Oracle HTTP Server with the Load Balancing Router by adding the following to *WEBHOST1_ORACLE_HOME*/Apache/Apache/conf/httpd.conf:

    a. Add the `LoadModule certheaders_module` directive for the appropriate platform.

    b. UNIX Apache 1.3:

    ```
    LoadModule certheaders_module libexec/mod_certheaders.so
    ```

    UNIX Apache 2.0; use this directive if you plan to use Apache 2.0 on UNIX:

    ```
    LoadModule certheaders_module modules/mod_certheaders.so
    ```

    Windows:

    ```
    LoadModule certheaders_module modules/ApacheModuleCertHeaders.dll
    ```

c. Add the following lines to create a `NameVirtualHost` directive and a `VirtualHost` container for **myapp.mycompany.com** and port **443**.

Apache 1.3:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName myapp.mycompany.com
  Port 443
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
  SimulateHttps On
</VirtualHost>
```

Apache 2.0:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName myapp.mycompany.com:443
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
  SimulateHttps On
</VirtualHost>
```

Notes: The `LoadModule` directives (in particular, the `LoadModule rewrite_module` directive) must appear in the `httpd.conf` file at a location preceding the `VirtualHost` directives. The server must load all modules before it can execute the directives in the `VirtualHost` container.

It is a good idea to create the VirtualHost directives at the end of the `httpd.conf` file.

---

17. Copy *WEBHOST1_ORACLE_HOME*`/Apache/Apache/conf/httpd.conf` to *WEBHOST2_ORACLE_HOME*`/Apache/Apache/conf/`.

18. Restart the Oracle HTTP Server.

4.4 Testing the Identity Management Tier Components

After both Identity Management configurations are complete, test the configurations as follows:

1. Stop all components on APPHOST1, using this command:

   ***ORACLE_HOME*/opmn/bin/opmnctl stopall**

2. Ensure that all components on APPHOST2 are running, using this command:

   ***ORACLE_HOME*/opmn/bin/opmnctl status**

3. Access the following URLs from two browsers:

   https://login.mycompany.com/pls/orasso

   https://login.mycompany.com/oiddas

4. Start all components from APPHOST1, using this command:

   ***ORACLE_HOME*/opmn/bin/opmnctl startall**

5. Stop all components on APPHOST2, using this command:

   ***ORACLE_HOME*/opmn/bin/opmnctl stopall**

6. Ensure that the login session is still valid for the `orasso` and `oiddas` logins.

4.5 Configuring Session State Replication for the OC4J_SECURITY Instance

1. Access the Application Server Control Console at:

   http://*s*.us.oracle.com:8888/em

   A login dialog opens.

2. Provide the user name and password that was set during installation and click **Login**.

   The **Farm** page appears.

3. Select the application server instance.

   A login dialog opens.

4. Provide the user name and password that was set during installation and click OK.

5. Select the OC4J_SECURITY OC4J instance.

   The OC4J_SECURITY page appears.

6. Click **Administration**.

7. Click **Replication Properties**.

8. Check the **Replicate session state** box and enter values for Multicast Host and Multicast Port.

9. Click **Apply**.

10. Restart the OC4J_SECURITY instance.

4.6 Disabling the Oracle HTTP Server on the Identity Management Tier

Follow these instructions on IDMHOST1 and IDMHOST2 to disable the Oracle HTTP Server on the Identity Management tier.

1. Edit the *ORACLE_HOME*/opmn/bin/opmn.xml file to change the Oracle HTTP Server status to disabled, as shown in bold.

```
<ias-component id="HTTP_Server" status="disabled" >
     <process-type id="HTTP_Server" module-id="OHS">
         <module-data>
...
</ias-component>
```

2. Issue this command in *ORACLE_HOME*/opmn/bin:

```
opmnctl stopall
```

3. Issue this command in *ORACLE_HOME*/opmn/bin:

```
opmnctl startall
```

5

Installing and Configuring Oracle Access Manager

5.1 Understanding Oracle Access Manager Components

The Oracle Access Manager authentication and authorization services are provided by the components described in this section. The components are shown in Figure 2–2.

Note: The WebPass and AccessManager components are not available on Windows at the time of publication. Therefore, WEBHOST1, WEBHOST2 and ADMINHOST in the myJ2EEOracle Access Manager configuration must be servers with operating systems other than Windows.

WebGate and WebPass on the Web tier with Oracle HTTP Server

WebGate is a web server plug-in access client that intercepts HTTP requests and forwards them to the Access Server for authentication and authorization.

WebPass is a web server plug-in that passes information between a web server and a Oracle Access Manager server. Every web server instance that communicates with a Oracle Access Manager server must be configured with WebPass. WebPass is also required on each computer hosting an Access Manager.

Oracle Access Manager, Identity Server and Access Server on the Application Tier

The Access Manager is a software component that writes policy data to Oracle Internet Directory, and updates the Access Server with policy modifications. It includes an Access System Console that enables administrators to manage policies and the system configuration.

The Oracle Access Manager Identity Server is a software component that processes all user identity, group, organization, and credentials management requests.

The Access Server is a software component that receives requests, responds to the access client, and manages the login session. The Access Server receives requests from WebGate and queries the authentication, authorization, and auditing rules in Oracle Internet Directory to:

- Determine whether and how a requested resource is protected
- Whether a user is already authenticated
- Challenge unauthenticated users for credentials
- Determine validity of credentials
- Determine whether, and under what conditions, the user is authorized for the requested resource (and communicates the authentication scheme to WebGate, authorizing the user)

The Access Server also manages the login session by helping WebGate to terminate sessions, setting user session time-outs, re-authenticating when time-outs occur, and tracking session activity.

Isolated Subnet for Administration

An isolated subnet on ADMINHOST hosts the Oracle HTTP Server, WebGate, WebPass, and the Access Manager for administrator use.

Access SDK

The Access SDK provides API libraries that protect non-HTTP resources (the AJP protocol is used for communication to OC4J instances) and implement single sign-on for the OC4J applications.

5.2 The myJ2EECompany Oracle Access Manager Authentication and Authorization Process

This section describes the sequence for authentication and authorization for J2EE applications using Oracle Access Manager single sign-on:

1. The user requests an application URL.
2. A login page is presented.

3. The user provides a user name and password.
4. WebGate captures the name and password and communicates with Access Server.
5. The Access Server communicates with Oracle Internet Directory.
6. The Access Server authenticates the user and returns the `ObSSOCookie` to WebGate.
7. WebGate transmits the cookie and other HTTP headers to mod_oc4j, which routes the request to the appropriate OC4J instance.
8. OC4J validates the cookie, and/or fetches extra roles from the Access Server.

5.3 Preparing to Install Oracle Access Manager Components

Before you install the Oracle Access Manager software:

- Synchronize the clocks on WEBHOST1, WEBHOST2, IDMHOST1 and IDMHOST2 within 60 seconds. In addition, ensure that:

  WEBHOST1 and WEBHOST2 (WebGate, WebPass) are not running ahead of IDMHOST1 and IDMHOST2 (Access and Oracle Access Manager Servers).

  The clocks must be synchronized in this manner so that an incoming request is not stamped with a time that has not yet occurred on the receiving server. See `http://www.ntp.org` for information about time synchronization.
- Obtain the DNS host names of all the servers on which you will install Oracle Access Manager components.
- Define the Master Identity Administrator user account (this user has access to all Oracle Access Manager functionality).
- Have a user account with administrator privileges on all computers.
- On Windows, ensure that the user account used to install the Oracle Access Manager server and Access Server has the privilege to log on as a service. The Oracle Access Manager Administrator must have the "Log on as a service" privilege. (Select Control Panel, Administrative Tools, Local Security Policy, Local Policies, User Rights Assignments, Log on as a service.)
- Ensure that the directory server you plan to use is installed and configured. If you use Oracle Internet Directory, follow the instructions in Chapter 2, "Installing and Configuring the Security Infrastructure".

5.4 Installing the First Identity Server on IDMHOST1

1. Log in to IDMHOST1 as an administrator.
2. Issue one of the commands below to start the installation (according to platform and installation option):

   Windows console installation:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_Identity_Server.exe
   -console
   ```

   Windows GUI installation:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_Identity_Server.exe
   ```

   Solaris console installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_sparc-s2_Identity_Server
   ```

Solaris GUI installation:

```
./Oracle_Access_Manager10_1_4_0_1_sparc-s2_Identity_Server
-gui
```

Linux console installation:

```
./Oracle_Access_Manager10_1_4_0_1_linux_Identity_Server
```

Linux GUI installation:

```
./Oracle_Access_Manager10_1_4_0_1_linux_Identity_Server -gui
```

Note: If a password error occurs with the `-gui` installation option, use the console option instead. You may safely ignore any warnings about fonts or scroll bars that occur when using the (default) GUI installation on Solaris.

The Welcome screen appears.

3. Click **Next**.

   The license agreement appears.

4. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.

5. Specify credentials as appropriate to the platform:

   Windows:

   Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   UNIX:

   Specify the user name and group that the Oracle Access Manager server will use and click **Next**.

   You are prompted for the installation directory.

6. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 5.16.

   On Linux systems, you are prompted to install and provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with GCC 3.3.2.

   On non-Linux platforms, you are prompted to select the locale (language).

7. Do one of the following:

   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.

8. Click **Next**.

A progress message appears, then you are prompted for the transport security mode.

9. Specify **Simple** and click **Next**.

   You are prompted for the Identity Server configuration details.

10. Specify the server name. This name must:

    - Be unique among all server names in the Oracle Access Manager System Console
    - Be unique among all server names accessing the same Oracle Internet Directory
    - Not contain any spaces

11. Specify the host name on which the Identity Server will reside.

12. Specify the port on which the Identity server will communicate with WebPass.

    You are asked if this is the first Identity server to be installed for the directory server.

13. Select **Yes**.

    You are prompted for communication details.

14. Select the **Simple** option.

    You are prompted to update the directory server with the Oracle Access Manager schema. (This includes Oracle Access Manager-specific workflow definitions, attribute policies, tab and panel configurations, configuration attributes, etc.

15. Select **Yes**.

16. Select the option that indicates where data is stored.

17. Select the schema update option and click **Next**.

18. Select the directory server type and click **Next**.

    You are prompted for directory server configuration details.

19. Specify the Oracle Internet Directory host name, port, bind DN and password and click **Next**.

    Note: The distinguished name you enter for the bind DN must have full permissions for the user and Oracle Access Manager branches of the directory information tree (DIT). Oracle Access Manager will access the directory server as this account.

    Documentation references and contact information appears.

20. Click **Next**.

    An installation summary appears.

21. Note any details about the installation and click **Finish**.

22. Start the Identity server by doing one of the following:

    Windows:

    Select **Start**, **All Programs, Administrative Tools**, **Services** and start the Identity server service.

Solaris:

Issue this command in *Oracle Access Manager installation directory*/identity/oblix/apps/common/bin:

```
start_ois_server
```

5.5 Installing WebPass on WEBHOST1

1. Log in to the computer as an administrator.
2. Issue one of the commands below to start the installation (according to platform and installation option):

   Solaris console installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_sparc-s2_OHS_WebPass
   ```
   [1]

   Solaris GUI installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_sparc-s2_OHS_WebPass -gui
   ```

   Linux console installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_linux_OHS_WebPass
   ```

   or

   ```
   ./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_WebPass
   ```
   [2]

   Linux GUI installation:

   ```
   ./Oracle_Access_Manager10_1_4_linux_OHS2_WebPass -gui
   ```

   The Welcome screen appears.
3. Click **Next**.

   The license agreement appears.
4. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.
5. Specify credentials as appropriate to the platform:

   Windows:

   Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   UNIX:

   Specify the user name and group that the WebPass web server will use and click **Next**.

   You are prompted for the installation directory.
6. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice (other than the Identity server directory), and click **Next**.

[1] OHS is the Oracle HTTP Server based on the Apache HTTP Server version 1.3

[2] OHS2 is the Oracle HTTP Server based on the Apache HTTP Server version 2.0

Note: (Linux only) If the installation stops after you specify the directory, see Section 5.16.

On Linux systems, you are prompted to install and provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with GCC 3.3.2.

On non-Linux platforms, you are prompted to select the locale (language).

7. Do one of the following:
   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.
8. Click **Next**.

   A progress message appears, then you are prompted for the transport security mode.
9. Specify `Simple` and click **Next**.

   You are prompted for WebPass configuration details.
10. Specify the WebPass name. This name must:
    - Be unique among all server names in the Oracle Access Manager System Console
    - Be unique among all server names accessing the same Oracle Internet Directory
    - Not contain any spaces
11. Specify the host name of IDMHOST1, on which the Identity server resides.
12. Specify the port number of the Identity server with which the WebPass will communicate, and click **Next**.

    A progress message appears, then you are prompted to update the WebPass web server configuration.
13. Click **Yes**, then click **Next**.
14. Specify the full path of the directory containing the `httpd.conf` file (*`ORACLE_HOME`*`/ohs/conf/httpd.conf`.
15. Click **Yes** to automatically update the web server.
16. Stop the WebPass web server instance.
17. If you are using Linux RedHat Advanced Server 3.0:

    Update the *`ORACLE_HOME`*`/opmn/conf/opmn.xml` file to set the environment variable LD_ASSUME_KERNEL for the HTTP_Server component, as shown in this example:

```
...
<ias-component id="HTTP_Server">
        <process-type id="HTTP_Server" module-id="OHS2">
          <environment>
            <variable id="LD_ASSUME_KERNEL" value="2.4.19"/>
          </environment>
          <module-data>
```

...

18. Stop the Identity server service by issuing the following command in the *Oracle Access Manager installation directory*/oblix/apps/common/bin directory:

    stop_ois_server

19. Start the Identity server service by issuing the following command in the *Oracle Access Manager installation directory*/oblix/apps/common/bin directory:

    start_ois_server

20. Start the WebPass web server instance.

21. Click **Next**.

    The Read Me file appears.

22. Review the file and click **Next**.

23. Confirm that the WebPass is installed correctly by performing the following steps:

    a. Ensure that the Identity server and the WebPass web server are running.

    b. Access the Oracle Access Manager system console at this URL:

       http://*WEBHOST1*:*port*/identity/oblix

       The Oracle Access Manager system main page appears.

5.6 Configuring the First Identity Server

After the Identity server and the WebPass instance are installed, you must specify the associations between them to make the system functional. Follow these steps to configure the first Identity server:

1. Access the Oracle Access Manager system console at this URL:

   http://*WEBHOST1*:*port*/identity/oblix

2. Click the Identity System Console link.

   The System Console setup page appears.

3. Click **Setup**.

   The Product Setup page appears.

4. Select **Directory Server Type** and click **Next**.

   The **Schema Change** page appears.

5. Click **Next**.

6. Specify the following server details:

   In the **Host** field, specify the DNS host name of the user data directory server.

   In the **Port Number** field, specify the port of the user data directory server.

   In the **Root DN** field, specify the bind distinguished name of the user data directory server.

   In the **Root Password** field, specify the password for the bind distinguished name.

   In the **Directory Server Security Mode** field, specify **Simple**.

In the **Is Oracle data stored in this directory also?** field, specify **Yes**.

7. Click **Next**.

   A page containing fields for location of user and configuration data appears.

   > **Note:** For detailed information on completing these fields, see "Specifying Object Class Details" on page 140 of the *Oracle Access Manager Access and Identity Installation Guide*.

8. Provide the **Searchbase** and **Configuration DN** and click **Next**.

   For example, the bind distinguished name and location and location of user and configuration data would be an entry resembling the following:
   `dc=us,dc=oracle,dc=com`

9. Provide the Person object class and click the **Auto configure objectclass** text box, and click **Next**.

   For example, the Person object class would be an entry resembling the following:
   `inetorgPerson`

   The Group object class screen appears.

10. Provide the Group object class and click **Next**.

    For example, the Group object class would be an entry resembling the following:
    `groupOfUniqueNames`

    A message appears instructing you to restart the Oracle Access Manager system.

11. Stop the Web Pass web server instance.

12. Stop, then start the Identity server service.

13. Start the WebPass web server instance.

14. Return to the Oracle Access Manager system setup window and click **Next**.

    A screen appears summarizing the object class changes that were made automatically.

15. Click **Yes** to accept the changes.

16. Review the Group object class attributes, then click **Yes**.

    The Configure Administrators page appears.

17. Click **Select User**.

    The Selector page appears.

18. Complete the fields with the search criteria for the user you want to select as an administrator and click **Go**.

    Search results matching the specified criteria appear.

19. Click **Add** next to the person you want to select as an administrator.

    The name of the person appears under the Selected column on the right.

20. Add other names as needed.

21. Click **Done**.

    The Configure Administrators page appears with the selected users listed as administrators.

22. Click **Next**.

    The Securing Data Directories page appears.

23. Verify the configuration by performing these steps:

    a. Access the Oracle Access Manager system console at this URL:

       http://*WEBHOST1*:*port*/identity/oblix

    b. Click User Manager, Group Manager, or Org. Manager and log in with the newly created administrator user's credentials.

5.7 Installing the Second Identity Server on IDMHOST2

1. Log in to IDMHOST2 as an administrator.
2. Issue one of the commands below to start the installation (according to platform and installation option):

   Windows console installation:

   Oracle_Access_Manager10_1_4_0_1_Win32_Identity_Server.exe -console

   Windows GUI installation:

   Oracle_Access_Manager10_1_4_0_1_Win32_Identity_Server.exe

   Solaris console installation:

   ./Oracle_Access_Manager10_1_4_0_1_sparc-s2_Identity_Server

   Solaris GUI installation:

   ./Oracle_Access_Manager10_1_4_0_1_sparc-s2_Identity_Server -gui

   Linux console installation:

   ./Oracle_Access_Manager10_1_4_0_1_linux_Identity_Server

   Linux GUI installation:

   ./Oracle_Access_Manager10_1_4_0_1_linux_Identity_Server -gui

   > **Note:** If a password error occurs with the `-gui` installation option, use the console option instead. You may safely ignore any warnings about fonts or scroll bars that occur when using the (default) GUI installation on Solaris.

   The Welcome screen appears.

3. Click **Next**.

   The license agreement appears.

4. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.

5. Specify credentials as appropriate to the platform:

   Windows:

   Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   UNIX:

   Specify the user name and group that the Identity Server will use and click **Next**.

   You are prompted for the installation directory.

6. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 5.16.

   On Linux systems, you are prompted to install and provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with GCC 3.3.2.

   On non-Linux platforms, you are prompted to select the locale (language).

7. Do one of the following:

   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.

8. Click **Next**.

   A progress message appears, then you are prompted for the transport security mode.

9. Specify Simple and click **Next**.

   You are prompted for Identity Server configuration details.

10. Specify the Identity Server name. This name must:

    - Be unique among all server names in the System Console
    - Be unique among all server names accessing the same Oracle Internet Directory
    - Not contain any spaces

11. Specify the host name on which the Identity Server will reside.

12. Specify the port on which the Identity Server will communicate with WebPass.

    You are asked if this is the first Identity Server to be installed for the directory server.

13. Select **No**.

    You are prompted for communication details.

14. Select the **Simple** option.

You are prompted to update the directory server with the Identity Server schema. (This includes Identity Server-specific workflow definitions, attribute policies, tab and panel configurations, configuration attributes, etc.

15. Select **Yes**.
16. Select the option that indicates where data is stored.
17. Select the schema update option and click **Next**.
18. Select the directory server type and click **Next**.

    You are prompted for directory server configuration details.
19. Specify the second instance's Oracle Internet Directory host name, port, bind DN and password and click **Next**.

    Note: The distinguished name you enter for the bind DN must have full permissions for the user and Identity Server branches of the directory information tree (DIT). Oracle Access Manager will access the directory server as this account.

    Documentation references and contact information appears.
20. Click **Next**.

    An installation summary appears.
21. Note any details about the installation and click **Finish**.
22. Start the Identity Server by doing one of the following:

    Windows:

    Select **Start**, **All Programs, Administrative Tools**, **Services** and start the Identity Server service.

    Solaris:

    Issue this command in *`Identity Server installation directory`*`/identity/oblix/apps/common/bin`:

    `start_ois_server`

5.8 Installing WebPass on WEBHOST2

Follow the steps in Section 5.5, "Installing WebPass on WEBHOST1" on page 5-6 to install WebPass on WEBHOST2. After the installation is complete, confirm that the WebPass is installed correctly by performing the following steps:

1. Ensure that the Identity Server and the WebPass web server are running.
2. Access the Identity Server system console at this URL:

   `http://`*`WEBHOST2`*`:`*`port`*`/identity/oblix`

   The Identity Server system main page appears.

5.9 Configuring the Second Identity Server

1. Access the Identity Server system console at this URL:

   `http://WEBHOST2:port/identity/oblix`

   The Identity Server System screen appears.

2. Click **Identity Server System Console**.

   A dialog appears with the message "Application is not set up."

3. Click **Setup**.

4. The **Directory Server Type containing User Data** screen appears.

5. Select **Oracle Internet Directory** from the drop-down list and click **Next**.

   The **Location of Directory Server with User Data** screen appears.

6. Complete the fields and selections as follows:

   Host - Type the OIDHOST2 host name.

   Port Number - `389`

   Root DN - `cn=orcladmin`

   Root Password - Type the root password.

   Directory Server Security Mode - `Open`

   Is the Configuration Data stored in this directory also? - `Yes`

7. Click **Next**.

   The **Location of Configuration Data and the Identity Server Searchbase** screen appears.

8. Complete the fields as follows:

   Configuration DN - `dc=us,dc=oracle,dc=com`

   Searchbase - `dc=us,dc=oracle,dc=com`

9. Click **Next**.

   The **Securing Data Directories** screen appears.

10. Click **Done**.

11. Restart the identity server and the web server.

12. Access this URL:

    `http://WEBHOST2:port/identity/oblix`

13. Click any of the links (User Manager, Group Manager, Org. Manager or Identity Server System Console) and log as the administrator user specified in Section 5.6.

14. Access this URL:

    `http://WEBHOST2:port/identity/oblix`

15. Click **Identity Server System Console**.

    A login dialog appears.

16. Provide the orcladmin user name and password and click **Login**.

    The **System Configuration** screen appears.

17. Scroll down, and then click **Identity System Console**. Click **System Configuration**, then click **WebPass**.

    The two WebPass instances are listed.

18. Click the WebPass instance for WEBHOST1.

    The **Details for WebPass** screen appears.

19. Select the WebPass that is installed on WEBHOST1 and click **List Identity Servers**.

    The Identity Servers associated with the WebPass are listed.

20. Click **Add**.

    The **Add a new Identity Server to the WebPass:** screen appears.

21. Select the identity server installed on APPHOST2, select **Primary Server** and specify 2 connections, then click **Add**.

22. Repeat Steps 18 through 21 for the WEBHOST2 WebPass instance.

5.10 Installing the Access System

The Access System consists of three components: The Policy Manager, the Access Server, and the WebGate. The Access System must also have a web server instance installed.

Policy Manager

The Policy Manager is the login interface for the Access System. Administrators use the Access Manager to define the resources to be protected, and to group resources into policy domains.

Access Server

The Access Server is a software component that provides dynamic policy evaluation services for resources and applications. The Access Server receives a request from the web server, queries the LDAP directory to authenticate users, and manages user sessions.

WebGate

The WebGate is a web server plug-in access client that intercepts HTTP requests for Web resources and forwards them to the Access Server for authentication and authorization.

The primary function of the Access System is to provide an access system console for administrators. It is installed on an isolated subnet to provide secure system administrator access to the Identity Server system.

In myJ2EECompany with Oracle Access Manager, these components are installed on the following servers:

- Policy Manager on ADMINHOST
- Access Server on IDMHOST1 and IDMHOST2
- WebGate on ADMINHOST and WEBHOST1 and WEBHOST2
- WebPass on ADMINHOST and WEBHOST1 and WEBHOST2

5.10.1 Installing the Web Server for the Policy Manager

A web server instance is needed to host the Policy Manager components. Follow the steps in Section 3.2.2, "Installing the Oracle HTTP Servers on WEBHOST1 and WEBHOST2" on page 3-8 to install a Web Server on ADMINHOST for use with the Policy Manager.

5.10.2 Installing WebPass for the Policy Manager

A WebPass instance must be installed on ADMINHOST, at the same directory level on which the Policy Manager will be installed. Follow the steps in Section 5.5, "Installing WebPass on WEBHOST1" on page 5-6 to install WebPass for the Policy Manager.

During the installation:

- You will be prompted to configure the WebPass against the Identity Server on IDMHOST1:6022; follow the prompts to configure the WebPass.
- Note the installation path for the WebPass, since this is the path you will specify in the Policy Manager installation.

After the installation, access the system console at **`http://ADMINHOST:port/identity/oblix`** and add a second Identity Server instance, IDMHOST2 on port 6022, for the WebPass.

5.10.3 Installing the Policy Manager on ADMINHOST

The Policy Manager must be installed in the same directory as the WebPass on ADMINHOST. Follow these steps to install the Policy Manager:

1. Log in to ADMINHOST as an administrator.
2. Issue one of the commands below to start the installation (according to platform and installation option):

   `Oracle_Access_Manager10_1_4_0_1_Win32_NSAPI_Policy_Manager.exe`

   Solaris console installation:

   `./Oracle_Access_Manager10_1_4_0_1_sparc-s2_OHS_Policy_Manager`[3]

   Solaris GUI installation:

   `./Oracle_Access_Manager10_1_4_0_1_sparc-s2_OHS_Policy_Manager -gui`[4]

   or

   Linux console installation:

   `./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_Policy_Manager`

   Linux GUI installation:

   `./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_Policy_Manager -gui`

   The Welcome screen appears.

[3] OHS is the Oracle HTTP Server based on the Apache HTTP Server version 1.3

[4] OHS is the Oracle HTTP Server based on the Apache HTTP Server version 1.3

3. Click **Next**.

   The license agreement appears.

4. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.

5. Specify credentials as appropriate to the platform:

   Windows: Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   UNIX: Specify the user name and group that the web server will use and click **Next**.

   You are prompted for the installation directory.

6. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 5.16.

   On Linux systems, you are prompted to install and provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with GCC 3.3.2.

   On non-Linux platforms, you are prompted to select the locale (language).

7. Do one of the following:

   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.

8. Click **Next**.

   A progress message appears, then you are prompted for the location of policy data.

9. Select **No**.

   You are prompted for the communication method for Oracle Internet Directory.

10. Select the **Open** option.

    A progress message appears, then you are prompted to update the WebPass web server configuration.

11. Click **Yes**, then click **Next**.

12. Specify the full path of the directory containing the `httpd.conf` file (*`ORACLE_HOME`*`/Apache/Apache/conf`).

13. Click **Next**.

    A message informs you that the web server configuration has been updated.

14. Stop the Policy Manager web server instance.

15. Stop and then start the Identity Server instance.

16. Start the Policy Manager web server instance.

17. Click **Next**.

    Read Me information appears.

18. Review the information and click **Next**.

    A message appears informing you that the installation was successful.

19. Click **Finish**.

5.10.4 Configuring the Policy Manager

The Policy Manager must be configured to communicate with Oracle Internet Directory. Follow these steps to configure the communication:

1. Ensure that the web server is running.
2. Access the Access System Console at the URL for the WebPass instance that connects to the Policy Manager:

   `http://`*`ADMINHOST`*`:`*`port`*`/access/oblix`

   The Access System main page appears.
3. Click the Access System Console link.

   A message informs you that the application is not yet set up.
4. Click **Setup**.

   You are prompted for the directory server type.
5. Select the user data directory server type.
6. Specify the following server details:

   In the **Machine** field, specify the DNS host name of the user data directory server.

   In the **Port Number** field, specify the port of the user data directory server.

   In the **Root DN** field, specify the bind distinguished name of the user data directory server.

   In the **Root Password** field, specify the password for the bind distinguished name.

   You are prompted for the type of directory server containing Oracle configuration data.
7. Select the configuration data directory server type and click **Next**.

   A message informs you that you can store user data and Oracle data in the same or different directories.
8. Select **Store Oracle data in the User Directory Server**.

   You are prompted for the location of policy data.
9. Select **Store Policy and Oracle data in the same directory server**.
10. Specify the following:

    Searchbase `dc=us,dc=oracle,dc=com` (the same searchbase specified during Identity Server installation)

    Configuration DN `dc=us,dc=oracle,dc=com` (the same configuration distinguished name specified during Identity Server installation)

    Policy Base `dc=us,dc=oracle,dc=com`

    You are prompted to specify the Person object class.

11. Specify the Person object class that was specified during Identity Server system configuration, and click **Next**.

    You are prompted to restart the web server.

12. Stop and then start the WebPass and Access Manager web server instance and the related Identity Server instance.

13. Click **Next**.

    You are prompted for the root directory for policy domains.

14. Accept the default root directory for policy domains, or specify a root directory, then click **Next**.

    You are prompted for information about configuring authentication schemes.

15. Select **Yes** to start the automatic configuration.

16. Select **Basic Over LDAP** and **Client Certificate** and click **Next**.

    The Define a new authentication scheme screen appears with the Basic over LDAP parameters.

17. Change the parameters, if needed, and click **Next**.

    The Define a new authentication scheme screen appears with the Client Certificate parameters.

18. Change the parameters, if needed, and click **Next**.

    You are prompted to configure policies to protect NetPoint URLs.

19. Select **Yes** and click **Next**.

    Instructions for completing the Policy Manager setup appear.

20. Read the information.

21. Stop the WebPass/Access Manager web server instance.

22. In the *ACCESS_MANAGER_HOME*/Apache/Apache/conf/httpd.conf file, comment out this directive:

    ```
    LoadModule php4_module modules/mod_php4.so
    ```

23. Stop and then start the Identity Server service for the WebPass.

24. Restart the WebPass/Policy Manager web server instance.

25. After the Web server reastarts, click **Done**.

    The Policy Manager home page appears.

26. Confirm that the Policy Manager is installed correctly by performing the following steps:

    a. Access the Access System Console at this URL:

       http://*ADMINHOST*:*port*/access/oblix

    b. Click the Access System Console link.

    c. Log in as an administrator.

    d. Click the Access System Configuration tab.

    e. Click Authentication Management.

       A list of the authentication schemes configured appears.

5.10.5 Installing the Access Server on IDMHOST1 and IDMHOST2

Before you begin installing the Access Server:

- On Windows, ensure that the user account used to install the Access Server has the privilege to log on as a service. The Access Server Administrator must have the "Log on as a service" privilege. (Select Control Panel, Administrative Tools, Local Security Policy, Local Policies, User Rights Assignments, Log on as a service.)
- Note that the Access Server cannot be installed in the same directory as the Access Manager.

Follow these instructions to install the Access Server:

1. Create an instance for the Access Server in the Access System Console:
   a. Access the Access System Console at this URL:

      `http://ADMINHOST:port/access/oblix`

   b. Click the Access System Console link.
   c. Log in as an administrator.
   d. Click the Access System Configuration tab.
   e. Click Access Server Configuration.
   f. Click **Add**.

      The Add Access Server page appears.

   g. In the **Name** field, provide a name for the Access Server that is different from all others already specified for this directory server.

      In the **Hostname** field, specify IDMHOST1.

      In the **Port** field, specify the port on which the Access Server will listen.

      In the **Transport Security** field, specify Simple (the transport security mode must be the same between all Access Servers and WebGates).

   h. Click **Save**.

      The List All Access Servers page appears with a link to the newly created instance.

   i. Click the link for the instance, print the Details page for reference, and then click **Back**.
   j. Click **Logout** and close the browser window.
2. Issue one of the commands below to start the installation (according to platform and installation option):

   Windows console installation:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_Access_Server.exe
   -console
   ```

   Windows GUI installation:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_Access_Server.exe
   ```

   Solaris console installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_sparc-s2_Access_Server
   ```

   Solaris GUI installation:

```
./Oracle_Access_Manager10_1_4_0_1_sparc-s2_Access_Server -gui
```

Linux GUI installation:

```
./Oracle_Access_Manager10_1_4_0_1_linux_Access_Server
```

The Welcome screen appears.

3. Click **Next**.

   The license agreement appears.

4. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.

5. Specify credentials as appropriate to the platform:

   Windows:

   Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   UNIX:

   Specify the user name and group that the web server will use and click **Next**.

   You are prompted for the installation directory.

6. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 5.16.

   On Linux systems, you are prompted to install and provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with GCC 3.3.2.

   On non-Linux platforms, you are prompted to select the locale (language).

7. Do one of the following:

   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.

8. Click **Next**.

   A progress message appears, then you are prompted for the transport security mode.

9. Specify `Simple` for the transport security mode.

   You are prompted for mode in which the Directory Server containing Oracle configuration data is running.

10. Specify `Open`.

    You are prompted for directory server details.

11. Specify the following server details:

In the **Host** field, specify the DNS host name of the Oracle configuration data directory server.

In the **Port Number** field, specify the port of the Oracle configuration data directory server.

In the **Root DN** field, specify the bind distinguished name of the Oracle configuration data directory server.

In the **Root Password** field, specify the password for the bind distinguished name.

In the **Oblix Directory** field, specify the type of directory server for the Oracle configuration data.

12. Choose `Oracle Directory` to specify the location of the policy data.

    You are prompted for the Access Server instance ID specified in the Access System Console, and the configuration DN and policy base.

13. Specify the following:

    Access Server ID the name specified when installing the Access Server (step 1.g. in Section 5.10.5, "Installing the Access Server on IDMHOST1 and IDMHOST2").

    Configuration DN `dc=us,dc=oracle,dc=com` (the same configuration distinguished name specified during Identity Server installation)

    Policy Base `dc=us,dc=oracle,dc=com`

14. Click **Next**.

    Read Me information appears.

15. Review the information and click **Next**.

    A message appears informing you that the installation was successful.

16. Click **Finish**.

17. Start the Access Server by doing one of the following:

    Windows: Locate and start the Windows service for this Access Server. The service name will be the Access Server ID you specified in the Access System Console prepended with `NetPoint AAA Server`.

    Solaris: In the *`Access Server installation directory`*`/access/oblix/apps/common/bin` directory, issue this command:

    `start_access_server`

    Note: If you used a password file, you must start the Access Server locally.

18. Repeat the preceding steps on IDMHOST2, substituting the hostname where appropriate.

5.10.6 Installing the WebGate

Before you begin installing the WebGate:

- Ensure that the user account used to install the WebGate has administration privileges.
- Note that the WebGate may be installed in the same directory as the Access Manager and WebPass. Separate `_jvmWebGate` and `_uninstWebGate` subdirectories are included and WebGate information is added to the `/oracle` directory. If you install WebGate into the same directory as the Access Manager and WebPass, a prompt will appear asking you if you want to replace files. Select **No to All**.
- The WebGate may be installed at the root level or the site level. However, if you have multiple virtual sites, you still only have one instance of WebGate.
- You must install WebGate on a computer that hosts a web server. You can configure the WebGate at the machine level or the virtual web server level. However, do not install at both the machine level and the virtual server level.

Follow these instructions to install the WebGate:

1. Create an instance for the WebGate in the Access System Console:
   a. Access the Access System Console at one of these URLs (depending on where you are installing):

      `http://ADMINHOST:port/access/oblix`

   b. Click the Access System Console link.
   c. Log in as an administrator.
   d. Click the Access System Configuration tab.
   e. Click **Add New Access Gate**.
   f. In the **AccessGate Name** field, provide a name for the WebGate that is different from all others already specified for this directory server.

      In the **Description** field (optional), supply additional descriptive information about the WebGate.

      In the **Hostname** field, specify IDMHOST1 or IDMHOST2 or ADMINHOST.

      (Optional) In the **Port** field, specify the port on which the web server will listen.

      In the **AccessGate Password** and **Re-type AccessGate Password** fields, provide and confirm a unique password for the instance.

      In the **Transport Security** field, specify `Simple` (the transport security mode must be the same between all Access Servers and WebGates).

      In the **Preferred HTTP Host** field, you may enter the WebGate host name, or you may leave the field blank.

      The **Primary HTTP Cookie Domain** is used to designate a single-sign on domain between WebGates on different hosts. You may leave this field blank.

   g. Click **Save**.

      Details for the WebGate instance appear, and you are prompted to associate an Access Server or Access Server cluster with the WebGate.

   h. Print the page for reference, and then click **Back**.

2. Assign an Access Server to the WebGate by performing the following steps:

   a. Navigate to the Details for NetPoint AccessGate page, if necessary. (From the Access System Console, select Access System Configuration, then AccessGate Configuration, then the link for the WebGate.)

      The Details for NetPoint AccessGate page appears.

   b. Click **List Access Servers**.

      A page appears with a message that there are no primary or secondary Access Servers currently configured for this WebGate.

   c. Click **Add**.

      The Add a new Access Server page appears.

   d. Select an Access Server from the Select Server list, specify primary server, and define 2 Access Servers (connections) for the WebGate.

   e. Click **Add**.

      A page appears, showing the association of the Access Server with the WebGate.

   f. Repeat Steps c through e to add the second Access Server.

3. Issue one of the commands below to start the installation (according to platform and installation option):

   Windows console installation:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_Domino_WebGate.exe
   -console
   ```

   Windows GUI installation:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_Domino_WebGate.exe
   ```

   Solaris console installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_sparc-s2_OHS_WebGate
   ```
   [5]

   Solaris GUI installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_sparc-s2_OHS_WebGate -gui
   ```
   [6]

   Linux GUI installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_linux_OHS_WebGate
   ```

   or

   ```
   ./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_WebGate
   ```

4. The Welcome screen appears.

5. Click **Next**.

   The license agreement appears.

6. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.

7. Specify credentials as appropriate to the platform:

[5] OHS is the Oracle HTTP Server based on the Apache HTTP Server version 1.3

[6] OHS is the Oracle HTTP Server based on the Apache HTTP Server version 1.3

Windows: Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

UNIX: Specify the user name and group that the web server will use and click **Next**.

You are prompted for the installation directory.

8. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 5.16.

   On Linux systems, this prompt appears:

```
To proceed with installation of Oracle Access Manager 7.0.4 WebGate and for
successfully  running the product, you must install additional GCC runtime
libraries, namely  libgcc_s.so.1 and libstdc++.so.5. Note that these libraries
should be  compatible with GCC 3.3.2. The libraries are available for download
from  either of the following locations - http://metalink.oracle.com (requires
login), or http://www.oracle.com/technology/products/ias/index.html. Once
these libraries are locally available, please specify the directory containing
the files and proceed with the installation.

    Location of GCC runtime libraries []:
```

   On non-Linux platforms, you are prompted to select the locale (language).

9. Do one of the following:

   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.

10. Click **Next**.

    A progress message appears, then you are prompted for the transport security mode.

11. Specify Cert for the transport security mode for the WebGate.

    You are prompted for directory server details.

12. Specify the following WebGate details:

    In the **WebGate ID** field, specify the unique ID that identifies the WebGate in the Access System Console.

    In the **WebGate password** field, specify the password defined in the Access System Console. If no password was specified, leave this field blank.

    In the **Access Server ID** field, specify the Access Server associated with the WebGate.

    In the **DNS Hostname** field, specify the DNS host name of the Access Server.

    In the **Port Number** field, specify the port on which the Access Server listens for the WebGate.

Specify the password phrase.

13. Click **Next**.
14. Click **Yes** to automatically update the web server, then click **Next**.
15. Specify the full path of the directory containing the `httpd.conf` file (*`ORACLE_HOME`*`/Apache/Apache/conf`).

    A message informs you that the web server configuration has been updated.
16. Stop, and then start, the web server.
17. Click **Next**.

    Read Me information appears.
18. Review the information and click **Next**.

    A message appears informing you that the installation was successful.
19. Click **Finish**.
20. Restart the computer.
21. Verify the installation by performing the following steps:
    a. Ensure that the Identity Server, WebPass, and Access Server are running.
    b. Access this URL:

       `https://WEBHOST1:7777/access/oblix/apps/webgate/bin/webgate.cgi?progid=1`

       The WebGate page appears as shown in Figure 5–1.

Figure 5–1 Web Gate Page

Access Server	Connection State	Created	Installation Directory	Num Of Threads	Directory Information								
					Directory	Host:Port	State	Priority	Mode	Size limit	Time limit	Login Distinguished Name	Created
idmhost1.pdx.com:6021, 1	Up	June 1 2006 11:29 pm	/home/oracleqa/edg/M7/access	200	User	oidhost1.pdx.com:389	Up	0	OPEN,REFERRAL,PRIMARY	0	0	cn=orcladmin	June 2 2006 02:55 pm

Note: If the WebGate page does not appear, the installation was not successful. In this case you must uninstall, and then reinstall, the WebGate.

5.11 Configuring the Access Server with the Load Balancing Router

If the Load Balancing Router is configured for SSL acceleration, and Oracle HTTP Server is listening on a non-SSL port, you must perform the following steps to make the Access Server function properly:

1. Access the Access System Console at this URL:

   `http://ADMINHOST:port/access/oblix`
2. Click the Access System Console link.
3. Log in as an administrator.
4. Click the Access System Configuration tab.

5. Navigate to the WebGate entries section.
6. Add the user-defined parameter ProxySSLHeaderVar, providing a header variable name, for example:

   Name: ProxySSLHeaderVarVal: IS_SSL
7. Modify the Load Balancing Router (reverse proxy web server) settings to insert an HTTP header string that sets the `IS_SSL` value to `ssl`. For example, in the F5 load balancer, in Advanced Proxy Settings, you add the HTTP header string `IS_SSL:ssl`.

5.12 Installing the Access Server SDK

The Access Server SDK contains Access Server API libraries that are needed to perform authentication and authorization services on the Access Server for OC4J applications, specifically to:

- Protect non-HTTP resources (the AJP protocol is used for communication to OC4J instances)
- Implement single sign-on for the OC4J applications

The Access Server SDK is not included with the Access Server installation package. The SDK is provided in a separate setup package, `Oracle_Access_Manager10_1_4_`*`platform`*`_AccessServerSDK[.ext]`. You can obtain the Access SDK at:

(URL for Access SDK)

For a comprehensive discussion of the Access SDK, see Chapter 5 of the *Oracle Identity Management Application Developer's Guide*.

5.12.1 Installing the Access SDK on APPHOST1 and APPHOST2 (Windows)

Follow these steps to install the Access SDK on the computers on which you plan to install J2EE applications:

1. Log on to the computer as an administrator.
2. Navigate to the Access Server SDK installation package directory.
3. Launch the installer by double-clicking `Oracle_Access_Manager_Win32_AccessServerSDK.exe`

   The Welcome screen appears.
4. Click **Next**.
5. Click **Next**.

   The license agreement appears.
6. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.
7. Specify credentials as appropriate to the platform:

   Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   You are prompted for the installation directory.

8. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   You are prompted to select the locale (language).

9. Select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.

10. Make a note of the directory (you will be prompted to provide it later).

11. Click **Next**.

12. Respond to the successive prompts.

    A screen appears with a message that the installation was successful.

5.12.2 Installing the Access SDK on APPHOST1 and APPHOST2 (Solaris and Linux)

1. Log on to the computer as the owner of the application that the AccessGate will protect.

2. Navigate to the Access Server SDK installation package directory.

3. Launch the installer by issuing one of these commands (substituting the platform for the installation):

   Solaris GUI:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_sparc-s2_AccessServerSDK
   ```

   Solaris command line:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_sparc-s2_AccessServerSDK
   ```

   Linux:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_linux_AccessServerSDK
   ```

   The Welcome screen appears.

4. Click **Next**.

   The license agreement appears.

5. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.

6. Specify the user name and group of the owner of the application that the AccessGate will protect and click **Next**.

   You are prompted for the installation directory.

7. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 5.16.

   You are prompted to select the locale (language).

8. Select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.

9. Make a note of the directory (you will be prompted to provide it later).

10. Click **Next**.

    On Linux systems, this prompt appears:

    ```
    To proceed with installation of Oracle Access Manager 7.0.4 Access Server SDK
    and for successfully  running the product, you must install additional GCC
    runtime libraries, namely  libgcc_s.so.1 and libstdc++.so.5. Note that these
    libraries should be  compatible with GCC 3.3.2. The libraries are available for
    download from  either of the following locations - http://metalink.oracle.com
    (requires login), or http://www.oracle.com/technology/products/ias/index.html.
    Once these libraries are locally available, please specify the directory
    containing the files and proceed with the installation.

        Location of GCC runtime libraries []:
    ```

11. Respond to the prompts.

    A screen appears with a message that the installation was successful.

5.12.3 Configuring the AccessGate on APPHOST1 and APPHOST2

1. Create an instance for the AccessGate in the Access System Console:
   a. Access the Access System Console at this URL:

      `http://`*`ADMINHOST`*`:`*`port`*`/access/oblix`

   b. Click the Access System Console link.
   c. Log in as an administrator.
   d. Click the Access System Configuration tab.
   e. Click **Add New AccessGate**.
   f. In the **AccessGate Name** field, provide a name for the AccessGate that is different from all others already specified for this directory server.

      In the **Description** field (optional), supply additional descriptive information about the AccessGate.

      In the **Hostname** field, specify IDMHOST1 or IDMHOST2 or ADMINHOST.

      (Optional) In the **Port** field, specify the port on which the web server will listen.

      In the **AccessGate Password** and **Re-type AccessGate Password** fields, provide and confirm a unique password for the instance.

      In the **Transport Security** field, specify `Simple` (the transport security mode must be the same between all Access Servers and WebGates).

   g. Click **Save**.

      Details for the AccessGate instance appear, and you are prompted to associate an Access Server or Access Server cluster with the AccessGate.

   h. Print the page for reference, and then click **Back**.
2. Navigate to:

   ***`AccessServerSDK path`*`/oblix/tools/configureAccessGate`**
3. Issue this command:

   `./configureAccessGate -i` AccessServerSDK path **`-t AccessGate`**

The following prompt appears:

```
Please enter the Mode in which you want the AccessGate to
run: 1(Open) 2(Simple) 3(Cert):
```

4. Enter **2**.

   The following prompt appears:

   ```
   Please enter the AccessGate ID:
   ```

5. Enter **access_gate_*APPHOST1*_sdk1**

   The following prompt appears:

   ```
   Please enter the Password for this AccessGate:
   ```

6. Enter a password.

   The following prompt appears:

   ```
   Please enter the Access Server ID:
   ```

7. Enter **access_server_*IDMHOST1***.

   The following prompt appears:

   ```
   Please enter the Access Server Host Machine Name:
   ```

8. Enter ***IDMHOST1*.mycompany.com**.

   The following prompt appears:

   ```
   Please enter the Access Server Port:
   ```

9. Enter **6021**.

   The following prompts appear:

   ```
   Preparing to connect to Access Server. Please wait.

   AccessGate installed Successfully.

   Press enter key to continue...
   ```

10. Press **Enter**.

11. Repeat the steps above on APPHOST2, substituting the host name where appropriate.

12. Update the `opmn.xml` file in all OC4J instances to include the AccessSDK shared library path:

```
<process-type id="app1" module-id="OC4J" status="enabled">
                <module-data>
                    <category id="start-parameters">
                       <data id="java-options" value="-server
-Djava.library.path=AccessServerSDK path/oblix/lib
-Djava.security.policy=$ORACLE_HOME/j2ee/app1/config/java2.policy
-Djava.awt.headless=true -Dhttp.webdir.enable=false"/>
```

13. Restart OPMN by issuing this command in *APPHOST2_ORACLE_HOME*`/OPMN/BIN`:

    `opmnctl reload`

14. Restart the OC4J instances in which the applications using Oracle Access Manager are deployed.

5.13 Configuring Oracle Access Manager Single Sign-On for OC4J Applications

See the *Oracle Containers for J2EE Security Guide*, Chapter 10, "Oracle Access Manager as Security Provider" for instructions on how to implement single sign-on for OC4J applications on APPHOST1 and APPHOST2.

5.14 Configuring the Second Identity Server as a Failover Server

The Identity Server on IDMHOST2 must be configured to service requests routed to the Identity Server on IDMHOST1 if IDMHOST1 becomes unavailable. Before you can configure the Identity Server on IDMHOST2 as a failover server, it must:

- Communicate with the existing Oracle Internet Directory
- Be associated with the existing WebPass as a secondary server

There are two failover paths to configure:

- Identity Server and WebPass communications
- Access Server and WebGate communications

5.14.1 Configuring Failover Between the Secondary Identity Server on IDMHOST2 and the WebPass

1. Access the Identity Server system console at this URL:

   `http://ADMINHOST:port/identity/oblix`

   The Identity Server system main page appears.

2. Select System Admin, System Configuration, Configure WebPass, *WebPass name*, Modify.

3. Complete the fields as follows:

   Failover Threshold — The number of live connections from the web component to its primary NetPoint server.

   Identity Server Timeout Threshold — The number of seconds the web component waits for a non-responsive NetPoint server before it considers it unreachable and attempts to contact another.

   Sleep For (seconds) — The number of seconds after which the WebGate verifies that the number of valid connections equals the maximum number of connections configured.

4. Save the changes.

5. Click **List Identity Servers**.

6. Click **Add**.

7. Select the Identity Server from the drop-down list.

8. Set the **Priority** to **Primary Server**.

9. Set **Number of Connections** to 2 or more.

10. Click **Add**.

    Both Identity servers are listed. Ensure that the number of connections for each is 2 or more.

11. Select System Admin, System Configuration, Configure Directory Options.

    The Configure Profiles page appears with the directory server information.

12. Select the name of the Identity Server profile from under the Configure LDAP Directory Server Profiles heading.

    The Modify Directory Server Profile page appears.

13. Locate the Used by field and select All Identity Servers.

5.15 Configuring the Second Access Server as a Failover Server

The Access Server on IDMHOST2 must be configured to service requests routed to the Access Server on IDMHOST1 if IDMHOST1 becomes unavailable. Before you can configure the Access server on IDMHOST2 as a failover server, it must:

- Communicate with the existing Oracle Internet Directory
- Be associated with the existing WebPass as a secondary server

5.15.1 Configuring Failover Between the Access Server and WebGate

1. Access the Access System Console at the URL for the WebPass instance that connects to the Access Manager:

   `http://ADMINHOST:port/access/oblix`

   The Access system console page appears.

2. Select Access System Configuration, AccessGate Configuration, All, Go, *Name*.

   The AccessGate page appears.

3. Complete the fields as follows:

   Failover Threshold — The number of live connections from the web component to its primary NetPoint server.

   Access Server Timeout Threshold — The number of seconds the web component waits for a non-responsive NetPoint server before it considers it unreachable and attempts to contact another.

   Sleep For (seconds) — The number of seconds after which the WebGate verifies that the number of valid connections equals the maximum number of connections configured.

4. Save the changes.

5. Select System Configuration, View Server Settings.

   The View Server Settings page appears with the directory server information.

6. Select the name of the Access Server profile from under the Configure LDAP Directory Server Profiles heading.

   The Modify Directory Server Profile page appears.

7. Locate the Used by field and select All Access Servers.

8. Save the changes.

5.16 Mitigating Identity Server Product Installation Failures on Linux

At the time of publication, an unresolved defect in a third-party product, InstallShield, caused some Identity Server product installations to stop after the installation directory was specified. This occurred intermittently, and only in the Linux version.

If an installation stopped after the installation directory was specified, repeat the installation as follows:

1. Open a shell window and paste these lines into it:

```
cd /tmp
mkdir bin.$$
cd bin.$$
cat > mount <<EOF
#! /bin/sh
exec /bin/true
EOF
chmod 755 mount
export PATH=`pwd`:$PATH
```

2. Perform the installation steps for the product you want to install.
3. Issue this command to empty the temporary directory:

```
rm -r /tmp/bin.$$
```

5.17 Configuring Directory Server Failover

The instructions for configuring failover from Identity Server components to directory servers vary, depending on the component (Identity Server, Access Server, or Access Manager), and whether you are configuring failover for user data or Oracle data. Table 5–1 lists the components, data stores, and configuration methods.

Table 5–1 Supported Failover Configurations for Directory Servers

Component	Data Store	Operation	Configuration Method
Identity Server	User	Read/Write	Directory Profile See Section 5.17.1, "Configuring Directory Failover for User Data"
Identity Server	Oracle	Read/Write	Directory Profile and XML Configuration Files See Section 5.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Server	User	Read/Write[1]	Directory Profile See Section 5.17.1, "Configuring Directory Failover for User Data"
Access Server	Oracle	Read/Write[2]	`ConfigureAAAServer` command line tool Section 5.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Server	Policy	Read/Write[3]	`ConfigureAAAServer` command line tool Section 5.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Manager	User	Read	Directory Profile XML Configuration Files

Table 5–1 (Cont.) Supported Failover Configurations for Directory Servers

Component	Data Store	Operation	Configuration Method
Access Manager	Oracle	Read/Write[4]	Section 5.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Manager	Policy	Read/Write[5]	XML configuration files Section 5.17.2, "Configuring Directory Failover for Oracle and Policy Data"

[1] Only applicable when password policy is enabled

[2] Only applicable when the Access Management Service is On. Unless there is only one back-end RAC database, load balancing is not recommended due to cache synchronization problems.

[3] Only applicable when the Access Management Service is On. Unless there is only one back-end RAC database, load balancing is not recommended due to cache synchronization problems.

[4] Load balancing for the Access Manager Write profile is not supported unless there only one back-end RAC database, due to cache synchronization problems.

[5] Load balancing for the Access Manager Write profile is not supported unless there only one back-end RAC database, due to cache synchronization problems.

Note: Load balancing will work with Oracle Internet Directory, since the directory server instances refer to the same data. However, using load balancing with the directory server in replication mode (for example, IPlanet load balancing) is not recommended, because replication delays can occur, with resulting cache synchronization problems across access servers.

5.17.1 Configuring Directory Failover for User Data

This section explains how to configure failover of Identity Server requests to directory servers that contain user data. The failover sequence consists of the LDAP SDK detecting a failure, returning a connection or "server down" error, and directing the request to a secondary directory server.

Each installed component has a directory profile. Follow these steps to configure user data directory failover using the Identity Server System or Access System Directory Profile page:

1. Access the Directory Profile page for the server on which you are configuring failover:
   - From the Identity Server System Console, log in as the administrator, then navigate to System Configuration, Directory Profiles.
   - From the Access System Console, select System Configuration, Server Settings.
2. Under **Configure LDAP Directory Server Profiles**, select the directory profile that contains connection information for the component and data for which you want failover capability.
3. Complete the **Failover Threshold** field.

   Failover Threshold — The number of live primary directory servers required. If the number of primary directory servers drops below the failover threshold, Identity Server attempts to establish a connection to a primary server, if available, and if not, the first secondary server listed, and then the next secondary server listed, and so on.

4. Complete the **Sleep For** field with the number of seconds before the watcher thread wakes up and attempts to re-establish or create new connections when connections fail.
5. Navigate to **Database Instances**, select **Add**, and indicate the instances' status as secondary servers.

Note: To load balance requests between the two Directory Servers, specify both as primary servers here (which represents an active-active failover solution).

To configure one server as active and the other as standby (representing an active-passive solution), designate the directory server you added as the secondary server. The secondary server will not operate unless the primary server is not available.

In either case, failover is achieved; however, in this guide the active-active solution is emphasized. You may have special considerations that indicate use of an active-passive solution.

5.17.2 Configuring Directory Failover for Oracle and Policy Data

This section explains how to configure failover in the Identity Server for Oracle and Policy data.

5.17.2.1 Configuring Identity Server Failover for Oracle Data

Most of the configuration data is managed in XML configuration files. Multi-language and referential integrity data is managed on the Directory Profile page.

If there is a failure of the primary configuration data directory server, then the Identity Server cannot read any configuration entries. The `failover.xml` file provides bootstrap secondary directory server information. See Example 5–1 for an example of the `failover.xml` file.

The procedure for configuring Identity Server failover for Oracle data is:

1. Creating the failover.xml File
2. Configuring Identity Server directory Failover for Oracle Data
3. Creating the Encrypted Password for the Bind DN

5.17.2.1.1 Creating the failover.xml File Follow these steps to create the file for each Identity Server that needs failover capability:

1. Copy and paste the existing `sample_failover.xml` file template into the *`Oracle_Access_Manager_INSTALLATION_DIRECTORY`*`/identity/oblix/config/ldap` directory.
2. Use a text editor to add failover information for secondary servers, using Example 5–1 as a guide (server information and encrypted password shown in bold).

Note: Instructions for obtaining the encrypted password are provided in Section 5.17.2.1.3, "Creating the Encrypted Password for the Bind DN" on page 5-36.

---

3. Save the `sample_failover.xml` file as `failover.xml`.

Example 5–1 failover.xml File

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<CompoundList xmlns="http://www.oblix.com"
ListName="failover.xml">
<!-- # Max number of connections allowed to all the active ldap servers -- note
this is the same as Max Active Servers>
<SimpleList>
<NameValPair ParamName="maxConnections" Value="1">
</NameValPair>
</SimpleList>
<!-- # Number of seconds after which we switch to a secondary or
reconnect to a restarted primary ldap server -->
<SimpleList>
<NameValPair ParamName="sleepFor" Value="60">
</NameValPair>
</SimpleList>
<!-- # Max amount of time after which a connection to the ldap
server will expire -->
<SimpleList>
<NameValPair ParamName="maxSessionTime" Value="0"></
NameValPair>
</SimpleList>
<!-- # Minimun number of active primary ldap servers after which
failover to a secondary server will occur -->
<SimpleList>
NameValPair ParamName="failoverThreshold" Value="1">
</NameValPair>
</SimpleList>
<!-- # Specify the list of all secondary ldap servers here -->
<ValList xmlns="http://www.oblix.com"
ListName="secondary_server_list">
<ValListMember Value="sec_ldap_server">
</ValListMember>
</ValList>
<!-- # Specify the details of each secondary ldap server here -->
<ValNameList xmlns="http://www.oracle.com"
ListName="sec_ldap_server">
<NameValPair ParamName="ldapSecurityMode" Value="Open">
</NameValPair>
<NameValPair ParamName="ldapServerName" Value="oidhost.mycompany.com">
</NameValPair>
<NameValPair ParamName="ldapServerPort" Value="389">
</NameValPair>
<NameValPair ParamName="ldapRootDN" Value="cn=orcladmin">
</NameValPair>
<NameValPair ParamName="ldapRootPasswd"
Value="000A0259585F5C564C">
</NameValPair>
<NameValPair ParamName="ldapSizeLimit" Value="0"></
NameValPair>
<NameValPair ParamName="ldapTimeLimit" Value="0"></
NameValPair>
</ValNameList>
</CompoundList>
```

5.17.2.1.2 Configuring Identity Server directory Failover for Oracle Data To configure directory failover, access the Directory Profile page for the directory profile that

contains the Oracle branch of the tree, as described in Section 5.17.1, "Configuring Directory Failover for User Data".

5.17.2.1.3 Creating the Encrypted Password for the Bind DN Follow these steps to create the encrypted password:

1. Locate the `obencrypt` tool in the *`AccessServer_install_directory`*`/access/oblix/tools/ldap_tools` directory.
2. Issue this command:

   `obencrypt` *`password`*

   In the preceding command, *password* is the password to encrypt.
3. Copy and paste the encrypted password into the `ldapRootPasswd` parameter value.

5.18 Configuring Access Server Directory Failover for Oracle and Policy Data

This section explains how to configure directory failover in the Access Server for Oracle and Policy data.

5.18.1 Adding a Failover Directory Server Using the ConfigureAAAServer Tool

1. Navigate to the directory containing the configureAAAServer tool:

   `AccessServer installation directory``/access/oblix/tools/configureAAAServer`
2. Issue this command:

   `configureAAAServer reconfig` *`AccessServer installation directory`*

   In the preceding command, *AccessServer installation directory* is the directory in which the Access Server is located.
3. Type 2 to specify the Simple security mode for the Access Servers that will connect to the directory servers.

   You are asked if you want to specify failover information for Oracle or policy data.
4. Select `Y` (Yes).

   You are prompted to specify the location of the data.
5. Type the number that corresponds to the location of the data (`1` for **Oracle tree**, `2` for **Policy tree**).

   You are prompted for the action to take.
6. Type `1` (**Add a failover server**).
7. Complete the following fields:

   Directory server name

   Directory server port

> **Note:** For LDAP in an Active Directory forest environment, use port 3269 for SSL mode. These are the global catalog ports.

Directory server login DN

Directory server password

8. Select `2 (Open)` for **Security Mode** and `2 (Secondary)` for **Priority**.
9. Type `5` and press Enter to quit.

   You are prompted to commit the changes.
10. Select `1 (Y)` and press **Enter** to commit the changes.

    The `ConfigureAAAServer` tool automatically creates the following `.xml` files in the *`Access Server installation directory`*`/access/oblix/config/ldap` directory:

    - `AppDBfailover.xml`
    - `ConfigDBfailover.xml`
    - `WebResrcDBfailover.xml`

5.19 Configuring Policy Manager Failover

1. Copy the `WebResrcDBfailover.xml` file from the Access Server configuration directory to the Policy Manager install directory.
2. Copy the `AppDBfailover.xml` file from the Access Server configuration directory to the Policy Manager install directory.
3. Copy the `ConfigDBfailover.xml` file from the Access Server configuration directory to the Policy Manager install directory.

5.20 Creating Failover LDAP Directory Server Profiles for the Identity and Access Servers

Each Identity and Access Server must have a failover directory server profile for user data. A directory server profile is created for each Identity and Access Server at installation time. Each Identity and Access Server must also have a second profile that gives connection information to another directory server, so that if the default directory server is unavailable, the Identity or Access server can connect to another directory server.

5.20.1 Creating a Directory Server Profile for the Identity Servers

1. Access the Identity Server system console at this URL:

   `http://`*`ADMINHOST`*`:`*`port`*`/identity/oblix`

   The **Identity Administration** page appears.
2. Select **Identity System Console**.

   A login dialog appears.
3. Provide the user ID and password and click **Login**.

   The **System Configuration** page appears.
4. Click **System Configuration**, then **Directory Profiles**.

   The **Configure Profiles** screen appears as shown in Figure 5–2.

Figure 5–2 Oracle Access Administration Configure Profiles Screen

5. Click the link for the first Identity Server directory server profile in the **Configure LDAP Directory Server Profiles** section.

   The **Modify Directory Server Profile** screen appears.

6. In the **Database Instances** section, click **Add**.

   The **Create Database Instance** screen appears.

7. Specify *oidhost2.mycompany.com*, and select **Secondary** from the Server Type drop-down list.

8. Click **Save**.

   The **Modify Directory Server Profile** screen appears.

9. Click the link for the second Identity Server directory profile in the **Configure LDAP Directory Server Profiles** section.

10. In the **Database Instances** section, click **Add**.

    The **Create Database Instance** screen appears.

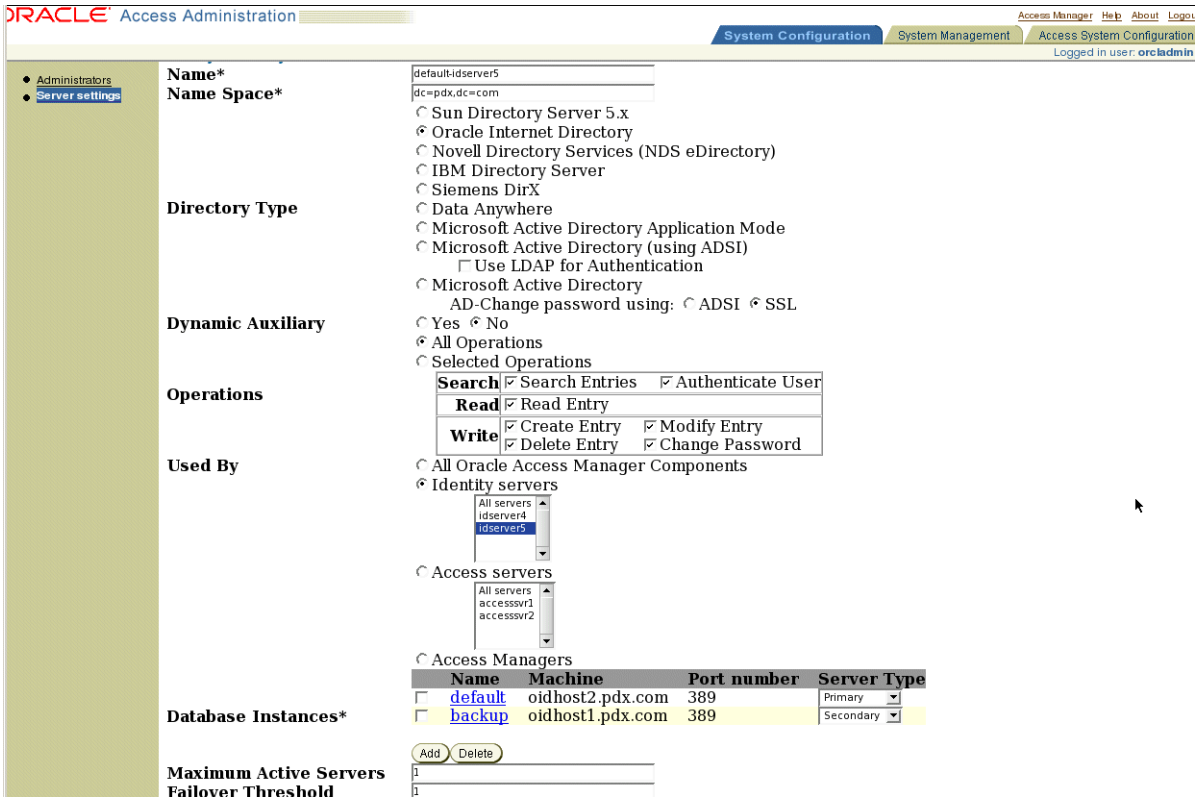
11. Specify *oidhost1.mycompany.com*, and select **Secondary** from the Server Type drop-down list.

12. Click **Save**.

    The **Modify Directory Server Profile** screen appears.

13. Restart both Identity Servers.

Figure 5–3 Oracle Access Administration Create Directory Server Profile Screen



5.20.2 Creating a Directory Server Profile for the Access Servers

1. Access the Identity System console at this URL:

   `http://ADMINHOST:port/access/oblix`

   The **Identity Administration** page appears.

2. Select **Identity System Console**.

   A login dialog appears.

3. Provide the user ID and password and click **Login**.

   The **System Configuration** page appears.

4. Click **System Configuration**, then **Directory Profiles**.

   The **Configure Profiles** screen appears as shown in Figure 5–2.

5. Click the link for the first Access Server directory server profile in the **Configure LDAP Directory Server Profiles** section.

   The **Modify Directory Server Profile** screen appears.

6. Record all entries and selections for the first Access Server's directory server profile (print the screen or write the entries and selections).

7. In the **Used By** section, select the **Access Servers** radio button and select Access Server 1 from the drop-down list.

8. In the **Database Instances** section, click **Add**.

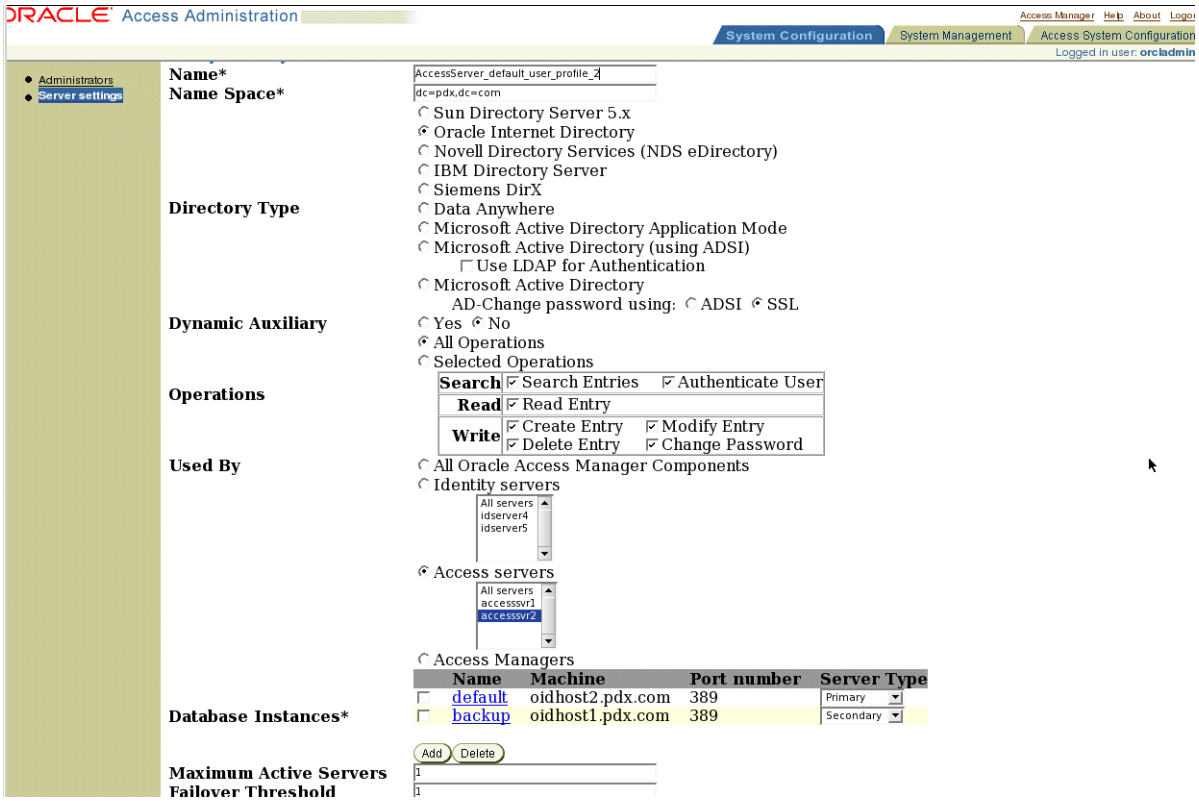
   The **Create Database Instance** screen appears.

9. Specify *oidhost2.mycompany.com*, and select **Secondary** from the Server Type drop-down list.
10. Click **Save**.

    The **Modify Directory Server Profile** screen appears.
11. Click **Add** in the **Configure LDAP Directory Server Profiles** section.

    The Create Directory Server Profile screen appears.

Figure 5–4 Oracle Access Administration Create Directory Server Profile Screen



12. Complete the **Name** field with a descriptive name for the directory server profile for the second Access Server on IDMHOST2.
13. Specify these entries and selections:

    Directory Type: Oracle Internet Directory

    Dynamic Auxiliary: No

    Operations: All Operations

    Used By: Access Servers (select Access Server 2 from the drop-down list)

    Database Instances: *oidhost1.mycompany.com* (select Secondary from the drop-down list), *oidhost2.mycompany.com* (select Primary from the drop-down list)
14. Click **Save**.

    A confirmation dialog appears.
15. Click **OK**.

    IDMHOST2 now has a default and a failover profile.

5.21 Verifying the Status of the Identity Servers

You can stop and start servers, perform operations, and then view the status to verify that failover is working.

1. Access the Identity System console at this URL:

   `http://IDMHOST1:port/identity/oblix`

   The Identity Administration page appears.

2. Select **Identity System Console**.

   A login dialog appears.

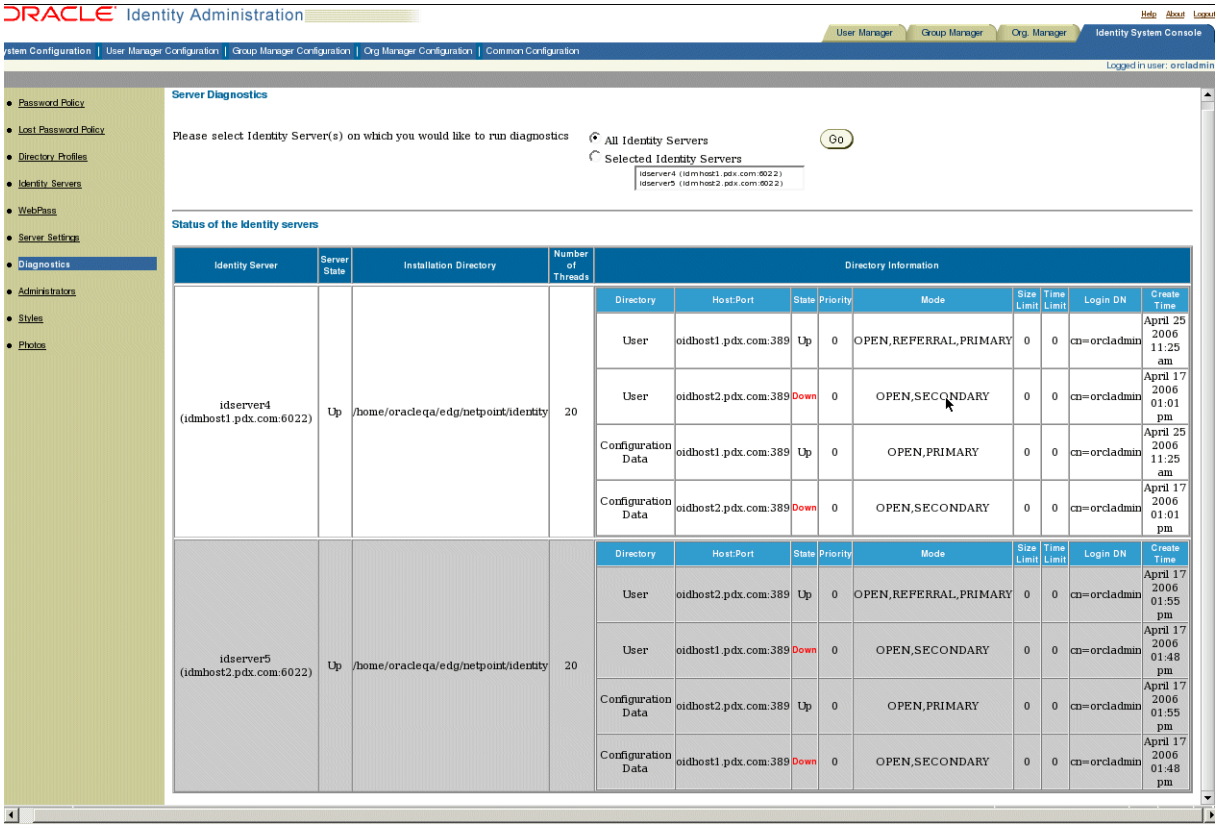
3. Provide the user ID and password and click **Login**.

   The **System Configuration** page appears.

4. Click **System Configuration**, then **Diagnostics**.

   The **Server Diagnostics** screen appears as shown in Figure 5–2.

Figure 5–5 Oracle Identity Administration Server Diagnostics Screen



Index

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W