Oracle® Application Server

Enterprise Deployment Guide

10*g* Release 3 (10.1.3.2.0)

B32125-02

April 2007

Oracle Application Server Enterprise Deployment Guide, 10*g* Release 3 (10.1.3.2.0)

B32125-02

Primary Author: Julia Pond

Contributing Authors: Janga Aliminati, Fermin Castro, Dheeraj Goswami, Mark Kennedy, Peter LaQuerre, Peter Lubbers, Greg Sowa, Tim Willard, Brian Wright

Contributors: Senthil Arunagirinathan, Theresa Bandy, Rachel Chan, Somendu Chakraborty, Orlando Cordero, Jeni Ferns, Eileen He, Barry Hiern, Pavana Jain, Pushkar Kapasi, Rajiv Maheshwari, Rahul Menezes, Mark Nelson, Lei Oh, Ted Regan, Dhaval Shah, Malai Stalin, Yaqing Wang

Contents

5 Installing and Configuring OracleAS Single Sign-On and Oracle Delegated Administration Services

6 Maintaining the WebCenter Suite

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*
- *Oracle WebCenter Framework Developer'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 of Oracle WebCenter Suite is a reference configuration that is designed to support large-scale, mission-critical business software applications using the Oracle WebCenter Framework (the runtime development framework for portlets, content integration and security) and Oracle WebCenter Services (of which Oracle Content DB is a part). 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 minimal 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 standards compliance:

- 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 In This Guide

Enterprise Deployments with the Oracle WebCenter Suite provide highly available, scalable and secure deployments of WebCenter Framework components.

This guide provides configuration instructions for these Enterprise Deployments of Oracle WebCenter Suite, with different security options:

- myWebCenter with JSSO and Oracle Internet Directory (shown in Figure 1–1)
- myWebCenter with Oracle COREid Access and Identity (shown in Figure 1–2)
- myWebCenter with Oracle Application Server Single Sign-On (shown in Figure 1–3).

Table 1–1 lists the security configurations and the identity and policy stores used with them.

The policy store is the repository for OracleAS JAAS Provider authorization permissions and grants. Oracle Internet Directory and XML (the `ORACLE_HOME/j2ee/home/system-jazn-data.xml` file) are supported as policy store repositories.

User accounts and roles are always seeded in an enterprise identity store (typically an LDAP server), and are not replicated in the policy store. The policy store only has grants and references to groups and roles in the enterprise identity store. The same repository (Oracle Internet Directory or an XML file) can be used as both the identity and policy store.

Table 1–1 Supported Security Configurations

Deployment Configuration	Policy Store	Identity Store
myWebCenter[1] with Java SSO	OracleAS JAAS Provider and Oracle Internet Directory	OracleAS JAAS Provider and Oracle Internet Directory
myWebCenter[1] with Oracle Application Server Single Sign-On	OracleAS JAAS Provider and Oracle Internet Directory	OracleAS JAAS Provider-Oracle Internet Directory
myWebCenter[1] with Oracle COREid Access and Identity[2]	OracleAS JAAS Provider and XML	OracleAS JAAS Provider and Oracle Internet Directory[3]

[1] Oracle Content DB and WebCenter Suite must use jazn.xml or Oracle Internet Directory. Any authentication mechanism that WebCenter Suite supports (JAZN-XML, Java SSO or OracleAS Single Sign-On), the adapter will also support. The Oracle Content DB server has a different support model (it doesn’t support Java SSO, for example).

[2] See Chapter 11 of the *Oracle Containers for J2EE Security Guide* for information on adding permissions in Oracle COREid Access and Identity environments.

[3] When Oracle COREid Access and Identity is used with OracleAS JAAS Provider and XML as the policy store and Oracle Internet Directory as the identity store, you must ensure that all user accounts and roles are in the identity store (Oracle Internet Directory), and that the policy grants are in the policy store (the `system-jazn-data.xml` file). Grants in this file must refer to users in the identity store (Oracle Internet Directory) See Section 4.22, "Configuring Oracle WebCenter Services User Roles for Oracle COREid Access and Identity" for instructions.

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

- **Web Tier** — WEBHOST1 and WEBHOST2, with Oracle HTTP Server installed.
- **Application Tier** — APPHOST1 and APPHOST2, with Oracle Containers for J2EE installed, and multiple OC4J instances with applications deployed.

  In myWebCenter with Oracle COREid Access and Identity, this tier also includes WebGate, WebPass, and Oracle COREid Access and Identity Identity Server, Access Server, Access Manager, and ADMINHOST, for administrator use.

  In myWebCenter with Oracle Application Server Single Sign-On, this tier includes IDMHOST1 and IDMHOST2, with Oracle Application Server Single Sign-On and Oracle Delegated Administration Services.
- **Data Tier** — OIDHOST1 and OIDHOST2, with 10*g* Release 3 (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 myWebCenter.com with JSSO and Oracle Internet Directory

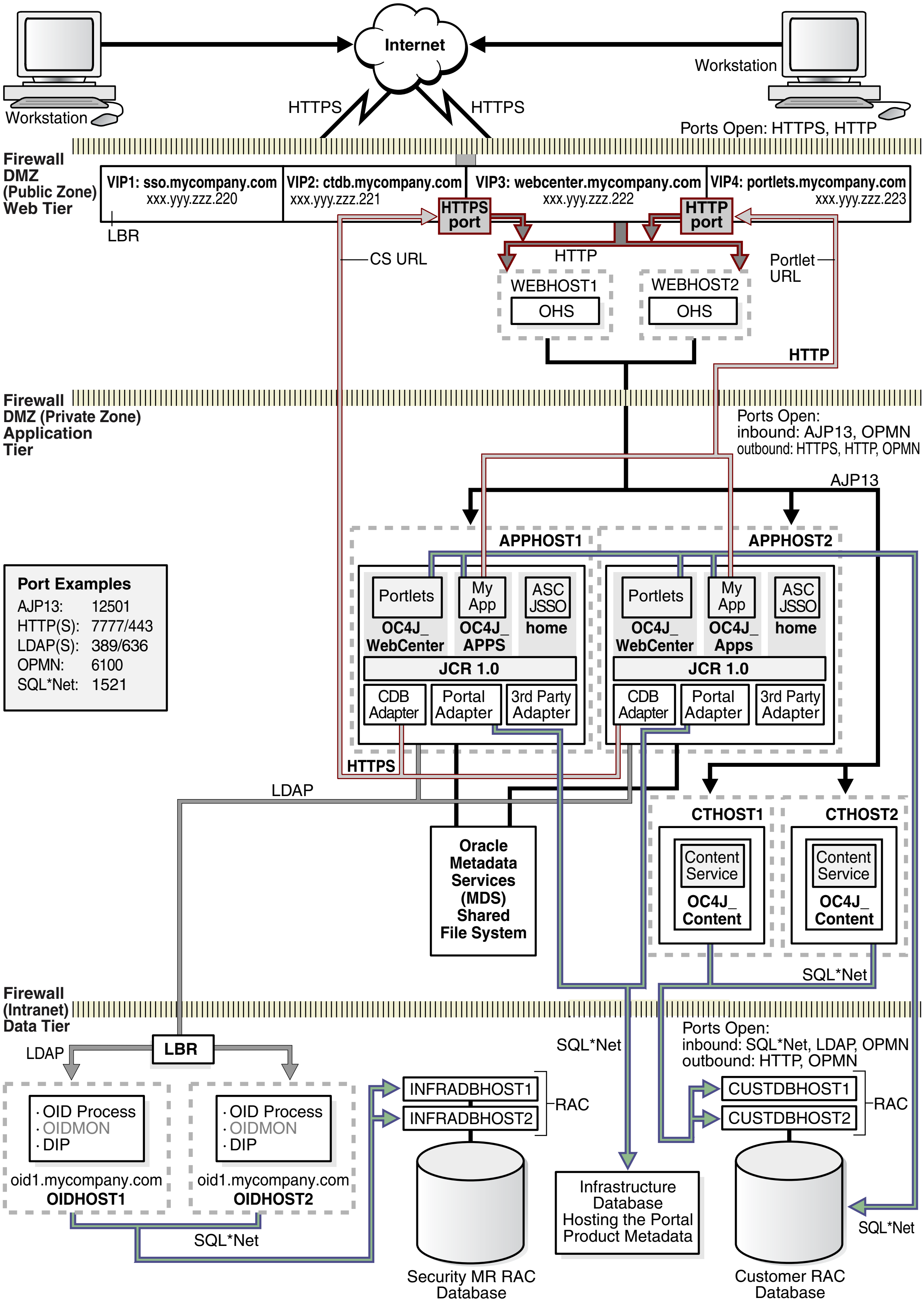


Figure 1–2 Enterprise Deployment Architecture for myWebCenter.com with Oracle COREid Access and Identity

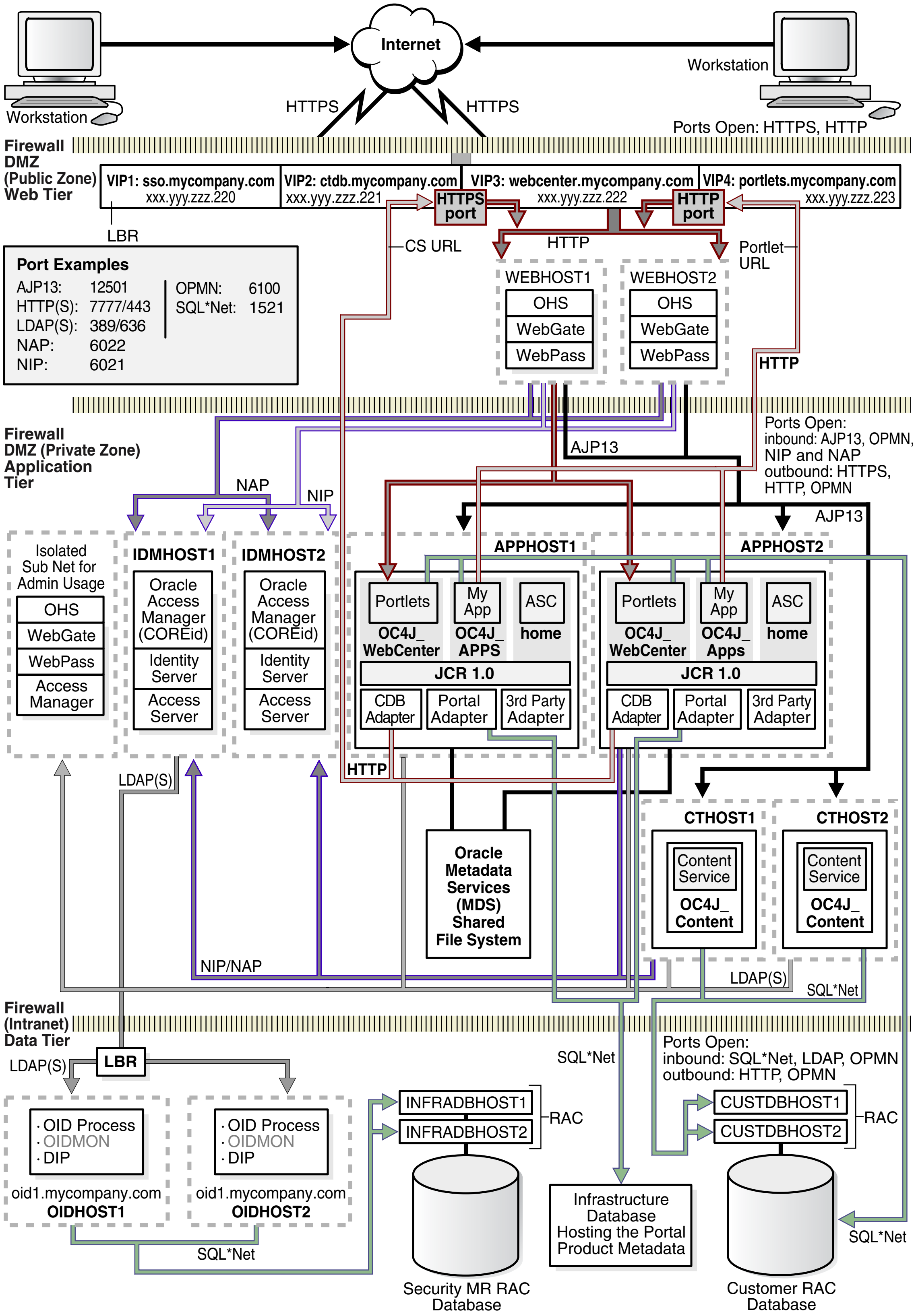
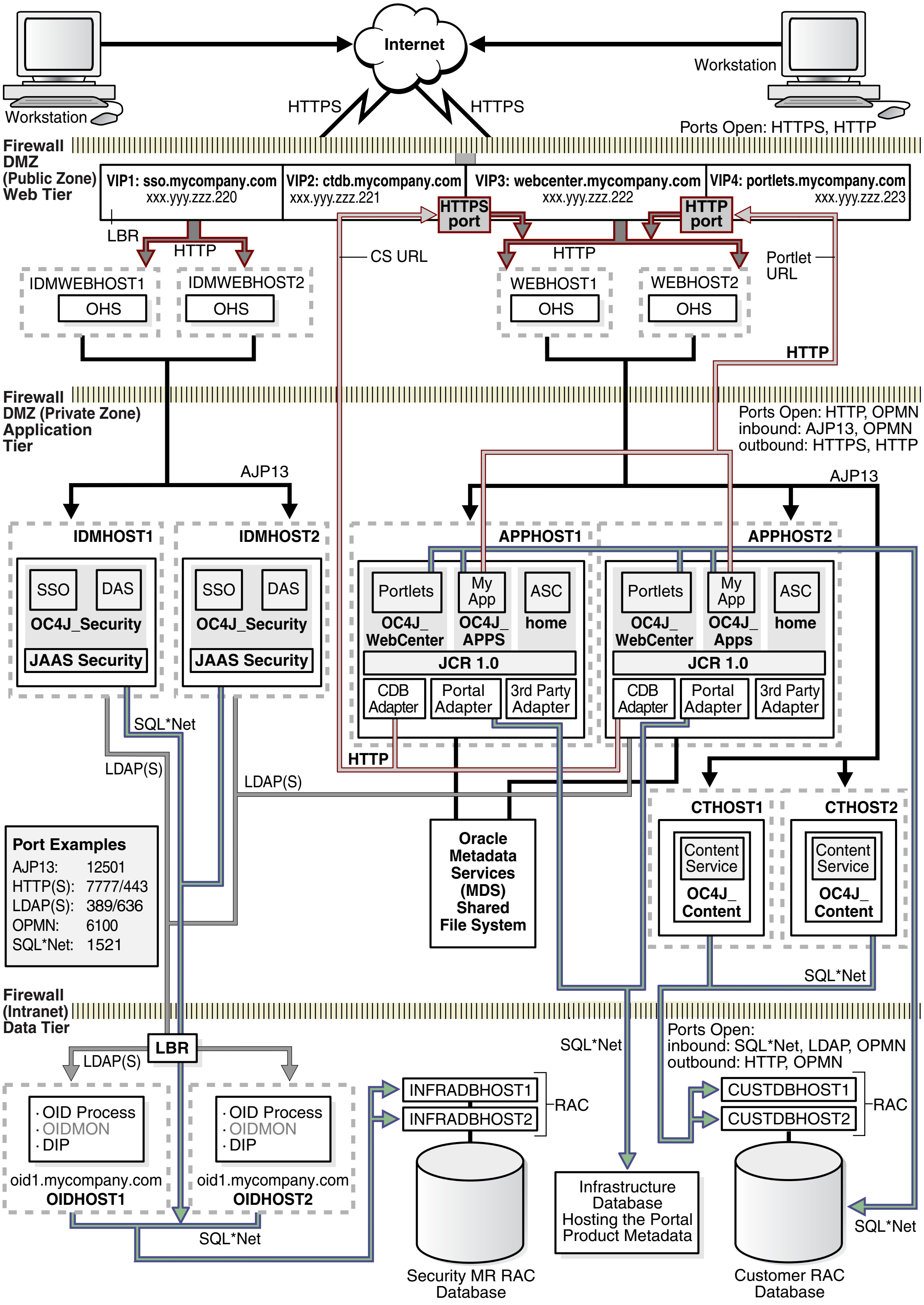


Figure 1–3 Enterprise Deployment Architecture for myWebCenter.com with Oracle Application Server Single Sign-On



1.4 How to Use This Guide

Table 1–2 summarizes the process for configuring myWebCenter with each of the user authentication methods. Follow the procedures indicated in the first column, in the order shown, for the chosen configuration.

Table 1–2 Enterprise Deployment Configuration Procedures

Perform the steps in...	To configure myWebCenter with JSSO and Oracle Internet Directory	To configure myWebCenter with Oracle Access Manager	To configure myWebCenter with Oracle Application Server Single Sign-On
Chapter 2, "Configuring the Data Tier"	Yes	Yes	Yes
Section 3.1, "Installing and Configuring the Web and Application Tiers"	Yes	Yes	Yes
Section 3.2, "Configuring Session State Replication for the OC4J_Apps and OC4J_WebCenter Instance"	Yes	Yes	Yes
Section 3.3, "Configuring APPHOST1 and APPHOST2 for the RAC Database"	Yes	Yes	Yes
Section 3.4, "Configuring Network Communication"	Yes	Yes	Yes
Section 3.5, "Configuring Application Authentication and Authorization"	Yes	**No**	Yes
Chapter 4, "Installing and Configuring Oracle COREid Access and Identity"	**No**	Yes	**No**
Chapter 5, "Installing and Configuring OracleAS Single Sign-On and Oracle Delegated Administration Services"	**No**	**No**	Yes

1.5 Hardware Requirements

Table 1–3 and Table 1–4 list minimum hardware requirements for the Enterprise Deployment on Windows and Linux 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 1–3 myWebCenter Hardware Requirements (Windows)

Server	Processor	Disk	Memory	TMP Directory	Swap
WEBHOST	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
APPHOST	300 MHz or higher Intel Pentium processor recommended	2 GB	1 GB	400	1 GB
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 1–4 myWebCenter Hardware Requirements (Linux)

Server	Processor	Disk	Memory	TMP Directory	Swap
WEBHOST	Pentium (32-bit), 450 MHz or greater	520 MB	512 MB	400 MB	1.5 GB
APPHOST	Pentium (32-bit), 450 MHz or greater	2 GB	1 GB	400	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

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.

1.6 Variants

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

1.6.1 Multi master Replication with Oracle Internet Directory

Multi master 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 multi master 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 Multi master Replication".

1.6.2 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)".

1.6.3 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.

2

Configuring the Data Tier

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 into the Real Application Clusters database 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 and execute the OracleAS Metadata Repository, you must perform these steps:

1. Install the OracleAS RepCA into the Real Application Clusters database, following the steps in the *Oracle Application Server Metadata Repository Creation Assistant User's Guide for Microsoft Windows* for the platform you are using. You can find this guide in the Oracle Application Server documentation library (Getting Started tab).

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 for Microsoft Windows*. In addition, ensure that the database computer has at least 512 MB of swap space available for execution of the OracleAS RepCA

3. Execute the OracleAS RepCA.

   The RepCA creates the schemas listed in the *Oracle Application Server Metadata Repository Creation Assistant User's Guide for Microsoft Windows.*

4. Perform the post-installation step described in Section 2.1.1.

2.1.1 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 Instance

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:** It is a good idea to make the Oracle home directory path for OIDHOST1 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 should 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.
12. Select OracleAS Infrastructure 10*g* and click **Next**.

    The **Select Installation Type** screen appears.
13. Select **Identity Management** and click **Next**.

    The **Upgrade Existing Oracle Application Server (10.1.2) Infrastructure** screen appears.

14. Select **Install New Oracle Application Server Infrastructure 10*g* (10.1.4.0.1)** and click **Next**.

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

15. Click **Next**.

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

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

    The **Select Configuration Options** screen appears.

17. Select **Oracle Internet Directory**, **OracleAS Directory Integration and Provisioning**, and **High Availability and Replication** and click **Next**.

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

18. Select **Manual** and click **Next**.

    The **Specify Repository** screen appears.

19. Provide the DBA login and computer information and click **Next**.

    > **Note:** The syntax for the hostname and port field for a RAC database is:
    >
    > `infradbhost1.mycompany.com:1521^infradbhost2.mycompany.com:1521^`

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

20. Select **OracleAS Cluster (Identity Management)** and click **Next**.

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

21. Click **Next** to specify the default **Suggested Namespace**, or enter values for the **Custom Namespace** and click **Next**.

    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.

2.2.2 Installing the Second Oracle Internet Directory Instance

The OracleAS Metadata Repository and the first Oracle Internet Directory instance must be running before you perform this task. Follow these steps to install the 10*g* Release 2 (10.1.2) 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: It is a good idea to make the Oracle home directory path for OIDHOST1 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 should 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.

12. Select OracleAS Infrastructure 10*g* and click **Next**.

    The **Select Installation Type** screen appears.

13. Select **Identity Management** and click **Next**.

    The **Upgrade Existing Oracle Application Server (10.1.2) Infrastructure** screen appears.

14. Select **Install New Oracle Application Server Infrastructure 10*g* (10.1.4.0.1)** and click **Next**.

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

15. Click **Next**.

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

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

    The **Select Configuration Options** screen appears.

17. Select **Oracle Internet Directory**, **OracleAS Directory Integration and Provisioning**, and **High Availability and Replication** and click **Next**.

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

18. Select **Manual** and click **Next**.

    The **Specify Repository** screen appears.

19. Provide the DBA login and computer information and click **Next**.

    Note: The syntax for the hostname and port field for a RAC database is:

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

    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.

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

    The **Specify ODS Password** screen appears.

21. Specify the ODS password (by default, the ias_admin password) and click **Next**.

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

    The **Specify OID Login** screen appears.

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

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

    The **Summary** screen appears.

24. 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.

25. 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.

26. 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 myWebCenter.com with JAZN-SSO/DAS, 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 APPHOST1 is down, then the Load Balancing Router directs all traffic to the Oracle Internet Directory on APPHOST2 only.
>
> However, there is a10-second interval during which the Load Balancing Router is unaware that the Oracle Internet Directory on APPHOST1 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 APPHOST1.

2.4 Testing the Oracle Internet Directory Instances

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

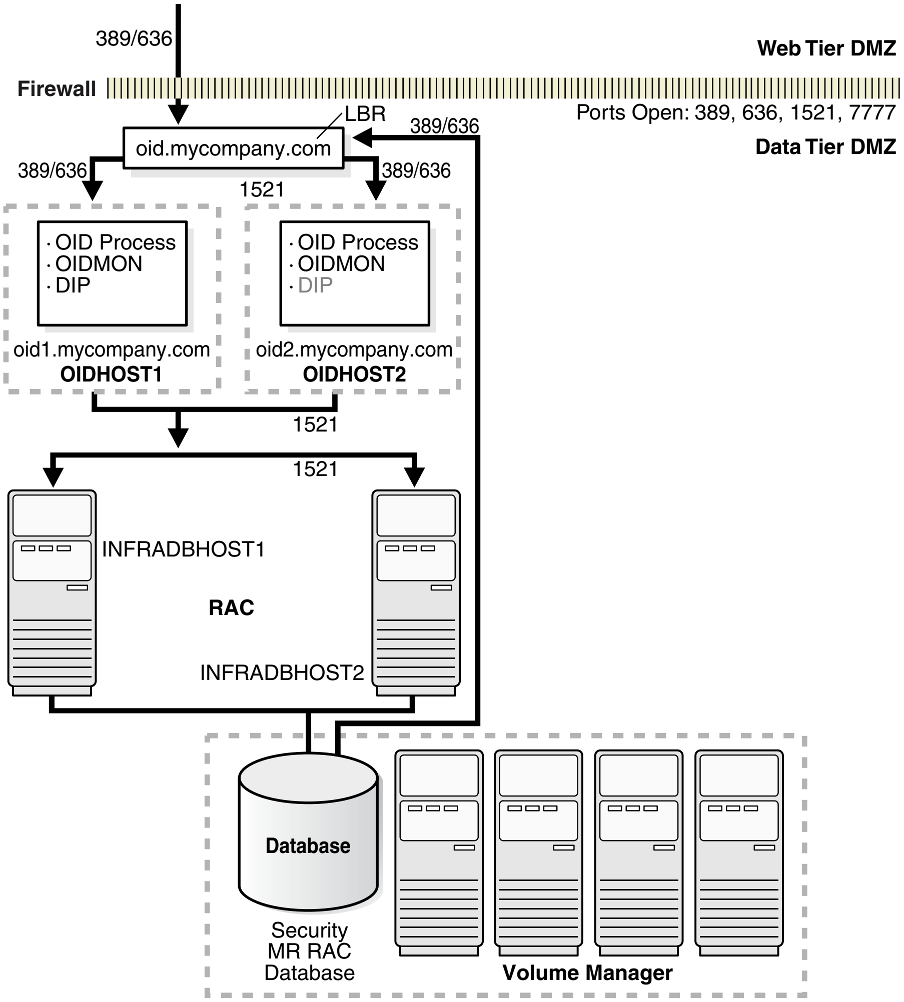
   ```
   ldapbind -p 389 -h OIDHOST1

   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 2–1.

Figure 2–1 Data Tier Configuration



3

Installing and Configuring the myWebCenter Application and Web Tiers

3.1 Installing and Configuring the Web and Application Tiers

The myWebCenterApplication Tier consists of multiple computers hosting middle-tier Oracle Application Server 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.

> **Note:** When the Application Server Control application and the JSSO application are in the same OC4J instance, complex application deployments through the Application Server Control may consume the majority of resources in the JVM, and affect single sign-on. Ideally, the Application Server Control and JSSO should reside in separate OC4J instances.

The Web Tier(WEBHOST1 and WEBHOST2) consists of Oracle HTTP Servers. Figure 1–1, "Enterprise Deployment Architecture for myWebCenter.com with JSSO and Oracle Internet Directory" on page 1-4 shows the Application Tier (APPHOST1 and APPHOST2) and Web tiers.

3.1.1 Installing the Oracle HTTP Servers on WEBHOST1 and WEBHOST2 (and IDMWEBHOST1 and IDMWEBHOST2, for myWebCenter.com with Oracle Application Server Single Sign-On)

Note: These instructions assume installation of Oracle HTTP Server based on Apache 1.3.33 from the Oracle WebCenter Suite from the product CD. However, you may install Oracle HTTP Server based on Apache 2.0 from the Companion CD instead. If you choose to do this, note that the path to the Oracle HTTP Server configuration file for the Oracle HTTP Server from the Companion CD is:

`ORACLE_HOME``/ohs/conf/httpd.conf`

---

1. Ensure that the system, patch, kernel and other requirements are met as specified in the installation guide. You can find this guide in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a local directory, such as TMP. You will provide the path to this file during installation.
3. Edit the `staticport.ini` file to assign the following custom ports:

   ```
   Oracle HTTP Server port = 7777
   ```

Note: Ensure that these ports are not already in use by any other service on the computer. Using the Static Ports feature to install the the Application Server Tier ensures that the port assignments will be consistent, if the ports are correctly specified in the file and the port is not already in use. If a port is incorrectly specified, the Oracle Universal Installer will assign the default port. If a port is already in use, the Oracle Universal Installer will select the next available port.

---

4. Start the Oracle Universal Installer as follows:

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

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

   The **Oracle Application Server WebCenter 10.1.3.2.0** installation screen appears.
5. Specify an installation directory for the instance.
6. Select **Advanced Installation**.
7. Click **Next**.

   A confirmation dialog appears.
8. Click **Yes**.

   A progress dialog appears, then the **Select Installation Type** screen appears.
9. Select **Oracle HTTP Server** and click **Next**.

   The **Specify Port Configuration Options** screen appears.
10. Select **Manual**, specify the location of the `staticports.ini` file, and click **Next**.

The **Specify Instance Name** screen appears.

11. Specify the instance name and click **Next**.

    The **Cluster Topology Configuration** screen appears.

12. Check the box to configure the instance to be part of an Oracle Application Server cluster.

13. Specify the multicast address and port.

    > **Note:** An example of a multicast address is `225.0.0.20`, with port `8001`. The address and port should be the same for each computer in a farm.

14. Click **Install**.

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

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

17. Verify that the installation was successful by viewing the Oracle HTTP Server instance. Start a browser and access:

    `http://`*`WEBHOST1`*`:7777` or

    `http://`*`WEBHOST2`*`:7777`

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

3.1.2 Renaming Apache 2.0 Web Server Instances (Optional)

If you installed the Oracle HTTP Server based on Apache 2.0 from the Companion CD on WEBHOST1 and WEBHOST2, the instance name on both computers will be the default name assigned by the installer. In a cluster, you will want the instance names to be unique when you view the instances with the `opmnctl @cluster status` command. Follow these steps to rename an instance:

1. Stop the instance by issuing this command:

    ```
    opmnctl stopall
    ```

2. Modify the *`ORACLE_HOME`*`/opmn/conf/opmn.xml` file to change the instance id and name as shown:

    ```
    <ias-instance id="IAS-1
     name="IAS-1">
    ```

    Replace both occurrences of the existing instance name (IAS-1 in the example) with a unique instance name.

3. Save and close the file.

4. Restart the instance by issuing this command:

    ```
    opmnctl startall
    ```

3.1.3 Installing the WebCenter Framework 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 using one of these commands:
   - On UNIX, issue this command: **`runInstaller`**
   - On Windows, double-click **`setup.exe`**

   The **Oracle WebCenter Suite 10.1.3.2.0** installation screen appears.
3. Specify an installation directory for the instance, or leave the default.
4. Select **Advanced Installation** and click **Next**.

   A confirmation dialog appears.
5. Click **Yes**.

   A progress dialog appears, then the **Select Installation Type** screen appears.
6. Select **Oracle WebCenter Framework** and click **Next**.

   The **Specify Port Configuration Options** screen appears.
7. Select **Automatic** and click **Next**.

   The **Administration Settings** screen appears.
8. Specify the instance name, provide and confirm the administrator password, and on the APPHOST1 installation only, select the **Start ASControl in this instance home** checkbox and click **Next**.

   The **Cluster Topology Configuration** screen appears.
9. Check the box to configure the instance to be part of an Oracle Application Server cluster, and check the box to access the instance from a separate Oracle HTTP Server.
10. Specify the multicast address and port.

    Note: An example of a multicast address is `225.0.0.20`, with port `8001`. The address and port should be the same for each computer in a farm.

11. Click **Install**.
12. The **Configuration Assistants** screen appears. When the configuration process completes, the **End of Installation** screen appears.
13. Click **Exit**, and then confirm your choice to exit.

3.1.4 Specifying an Oracle Metadata Services (MDS) Location

WebCenter application customizations are stored in MDS on the file system. When you predeploy a WebCenter Application, you must specify an MDS location on APPHOST1 and APPHOST2. A shared file system is used for high availability (see Figure 1–1, Figure 1–2 and Figure 1–3). The locations must be identical. You can use any location on the file system, observing these conditions:

- On Microsoft Windows, the drive letter must be the same on both systems: for example, system 1 and system 2 must both refer to the location as `X:\mds`; it cannot be `D:\mds` on one system and and `E:\mds` on the other system.
- On UNIX, the mount point must be identical: system 1 and system 2 must refer to the same directory, such as `/oracle/webcenter`.
- In a clustered environment, you need only execute the predeployment tool once to produce the target EAR file, and then you deploy that EAR file on other OC4J instances. For more information about the predeployment for deploying WebCenter applications, see the *Oracle WebCenter Framework Developer's Guide*.

3.1.5 About Portlet Preference Stores

WebCenter applications can consume portlets such as Web Services for Remote Portlets (WSRP) or Portal Developer Kit (PDK-Java) portlets hosted by a portlet producer. The portlet producers store portlet customizations, or preferences, in a preference store that resides in a database or on a file system. In an enterprise deployment, you put the preference store on a database that is configured for high availability, such as a Real Application Clusters database or a cold failover cluster database.

A portlet preference store is different from MDS in purpose and implementation. MDS stores application metadata and can reside only on a file system, as described in Section 3.1.4, "Specifying an Oracle Metadata Services (MDS) Location".

3.1.6 Configuring OC4J to Run Portlet Producers on APPHOST1 and APPHOST2

By default, the PDK-Java and WSRP producers that are located in the OC4J_WebCenter instances are configured to use the file-based preference store. For high availability, you configure the preference store to use a database. To do this, you must set up a schema for the preference store in the database, configure the producer, and map preference store connection details to a JDBC data source.

3.1.6.1 Creating the Producer Schemas User and JPDK and WSRP Schemas

1. Navigate to the *`ORACLE_HOME`*`/bin` directory.
2. Connect to SQL*Plus using the SYS account and SYSDBA database administrator role.
3. Issue this command (substituting the Oracle home path):

   ```
   @ORACLE_HOME/j2ee/home/database/wsrp/dbprefstore.sql
   ```

4. When prompted, create a user name and password for the WSRP and PDK-Java preference store database schema. This user name and password will be used in the command in Section 3.1.6.2, "Creating the WebClipping Schema".

   A database preference store is created and the schema populated with the required database objects.

3.1.6.2 Creating the WebClipping Schema

1. Create the schema by issuing this command (shown on multiple lines for readability):

   ```
   ORACLE_HOME/jdk/bin/java
     -classpath ORACLE_HOME/lib/xmlparserv2.jar:ORACLE_
   HOME/jdbc/lib/ojdbc14.jar:ORACLE_HOME/portal/jlib/wce.jar
     oracle.portal.wcs.Installer -installSchema
     -username preference store schema user
     -password preference store schema user password
     -dburl jdbc:oracle:thin:@//database host:database port/database service name
   ```

   Substitute Oracle home values, user name, password, and database information where indicated with italics.

3.1.6.3 Configuring WSRP Producers to use a Database Preference Store

1. Add a new data source entry that maps the connection details for the preference store schema to a JDBC data source. You can use any data source that has its JNDI location set to `jdbc/portletPrefs`.

   a. Access the Application Server Control Console at `http://`*`hostname`*`:`*`port`*`/em/` and log in with the oc4jadmin password set during installation.

      The **Cluster Topology** page appears.

   b. Click the link for the OC4J_WebCenter instance.

   c. Click **Administration**.

      The **Administration Tasks** list appears.

   d. Click the **Go to Task** icon for **JDBC Resources** under the **Services** task.

      The **JDBC Resources** page appears.

      Click **Create** in the **Connection Pools** section.

      The **Create Connection Pool - Application** page appears.

   e. Click **Continue** (leave the default selections).

      The **Create Connection Pool** page appears.

   f. Specify the following values:

      Name: The name of the connection pool, for example, `OracleWSRPPool`.

      Connection Factory Class: Leave the default value.

      JDBC URL: The JDBC URL for the Oracle database that contains the schema for the application. For example:

      ```
      jdbc:oracle:thin:@//custdbhost.mycompany.com:1521/service name
      ```

      Username: The username for the database that contains the schema for this application.

      Use Cleartext Password/Password: N/A

      Use Indirect Password/Indirect Password: Select this radio button and provide the indirect password for the database that contains the schema for this application.

   g. Click **Finish**.

The JDBC Resources page appears.

h. Click the **Test Connection** icon for the newly created connection.

i. Click **Create** in the **Data Sources** section.

   The **Create Data Source - Application & Type** page appears.

j. Click **Continue** (leave the defaults).

   The **Create Data Source - Managed Data Source** page appears.

k. Specify the following values:

   Name: The name of the data source, for example, `WSRP_PREF_DS`.

   JNDI Location: `jdbc/portletPrefs`

   Transaction Level: Leave the default.

   Connection Pool: `OracleWSRPPool`(created in prior step)

   Login Timeout: Leave the default.

l. Click **Finish**.

2. Edit the *`ORACLE_HOME`*`/j2ee/`*`OC4J_instance`*`/applications/`*`application name`*`/`*`optional web module name`*`/WEB-INF/web.xml` file to specify a database preference store for each application (replace *OC4J_instance*, *application name*, and, if applicable, *optional web module name* with the applicable names). Modify (or, if necessary, add under the `web-app` tag) the `env-entry-value` as shown in the example:

```
<env-entry>
<env-entry-name>oracle/portal/wsrp/server/persistentStore</env-entry-name>
<env-entry-type>java.lang.String</env-entry-type>
<env-entry-value>Database</env-entry-value>
</env-entry>
```

3. Access the Application Server Control Console at http://hostname:port/em/ and log in with the oc4jadmin password set during installation.

   The **Cluster Topology** page appears.

   Check the box in the **Select** column for the OC4J_WebCenter instance.

4. Click **Restart**.

3.1.6.4 Configuring PDK-Java Producers to use a Database Preference Store

1. Map the connection details for the preference store schema to a JDBC data source. You can use any data source that has its JNDI location set to `jdbc/portletPrefs`.

   a. Access the Application Server Control Console at `http://`*`hostname`*`:`*`port`*`/em/` and log in with the oc4jadmin password set during installation.

      The **Cluster Topology** page appears.

   b. Click the link for the **home** instance.

   c. Click **Administration**.

      The **Administration Tasks** list appears.

   d. Click the **Go to Task** icon for **JDBC Resources** under the **Services** task.

The **JDBC Resources** page appears.

Click **Create** in the **Connection Pools** section.

The **Create Connection Pool - Application** page appears.

e. Click **Continue** (leave the default selections).

   The **Create Connection Pool** page appears.

f. Specify the following values:

   Name: The name of the connection pool, for example, `OracleWSRPPool`.

   Connection Factory Class: Leave the default value.

   JDBC URL: The JDBC URL for the Oracle database that contains the schema for the application. For example:

   ```
   jdbc:oracle:thin:@//custdbhost.mycompany.com:1521/service name
   ```

   Username: The username for the database that contains the schema for this application.

   Use Cleartext Password/Password: N/A

   Use Indirect Password/Indirect Password: Select this radio button and provide the indirect password for the database that contains the schema for this application.

g. Click **Finish**.

   The **JDBC Resources** page appears.

h. Click the **Test Connection** icon for the newly created connection.

i. Click **Create** in the **Data Sources** section.

   The **Create Data Source - Application & Type** page appears.

j. Click **Continue** (leave the defaults).

   The **Create Data Source - Managed Data Source** page appears.

k. Specify the following values:

   Name: The name of the data source, for example, `PDK_PREF_DS`.

   JNDI Location: `jdbc/portletPrefs`

   Transaction Level: Leave the default.

   Connection Pool: `OraclePDKPool`(created in prior step)

   Login Timeout: Leave the default.

l. Click **Finish**.

2. Update the OmniPortlet producer to use a database preference store:

   a. Open the *`ORACLE_HOME`*`/j2ee/OC4J_WebCenter/applications/portalTools/omniPortlet/WEB-INF/providers/omniPortlet/provider.xml` file.

   b. Modify the the `preferenceStore` tag to use the database preference store.

```
<preferenceStore
class="oracle.portal.provider.v2.preference.DBPreferenceStore">
<name>omniPortletprefStore</name>
<connection>jdbc/PooledConnection</connection>
</preferenceStore>
```

3. Update the PDK-Java sample producers to use a database preference store.

   a. Open the *`ORACLE_HOME`*`/j2ee/OC4J_WebCenter/applications/jpdk/jpdk/WEB-INF/providers/`*`provider name`*`/provider.xml` file.

   b. Modify the the `preferenceStore` tag to use the database preference store, substituting *provider name* with the application name.

```
<preferenceStore
class="oracle.portal.provider.v2.preference.DBPreferenceStore">
<name>provider name</name>
<connection>jdbc/PooledConnection</connection>
</preferenceStore>
```

4. Update the WebClipping producers to use a database repository (by default, it uses MDS, a file-based storage location, as its repository).

   a. Open the *`ORACLE_HOME`*`/j2ee/OC4J_WebCenter/applications/portalTools/webClipping/WEB-INF/providers/webClipping/provider.xml` file.

   b. Update the repositoryInfo tag as shown, substituting current values for *mysid*, *webclipping user*, and *password* (these are the same values provided when creating the schema for the preference store in Section 3.1.6.2) and, if necessary, the customer database host and port:

```
<repositoryInfo
class="oracle.portal.wcs.provider.info.DatabaseInformation">
   <useRAA>false</useRAA>
   <databaseHost>custdbhost.mycompany.com</databaseHost>
   <databasePort>1521</databasePort>
   <databaseSid>mysid</databaseSid>
   <databaseUsername>webclipping user</databaseUsername>
   <databasePassword>password</databasePassword>
   <useASO>false</useASO>
</repositoryInfo>
```

5. Access the Application Server Control Console at http://hostname:port/em/ and log in with the oc4jadmin password set during installation.

   The **Cluster Topology** page appears.

   Check the box in the **Select** column for the OC4J_WebCenter instance.

6. Click **Restart**.

3.1.6.5 Configuring Java Object Cache Communication on APPHOST1 and APPHOST2

When Java Object Cache is configured in a clustered environment, it requires a list of all cluster members' IP addresses and port numbers to share objects and coordinate across the cluster. This list must be specified in the `discoverer` attribute of the `javacache.xml` file. All caches cooperating in the same cache system must specify exactly the same set of IP addresses and port numbers, in the same order. To configure this, perform the following steps:

1. Modify the *ORACLE_HOME*`/portal/conf/javacache.xml` file and the *ORACLE_HOME*`/javacache/admin/javacache.xml` file to configure or add the `isDistributed` and `discoverer` elements as shown in Example 3–1.

Example 3–1 javacache.xml file communication element

```
<communication>
  <isDistributed>true</isDistributed>
  <discoverer ip="APPHOST1 IP address"
     discovery-port="APPHOST1 discovery port"/>
  <discoverer ip="APPHOST2 IP address"
     discovery-port="APPHOST2 discovery port"/>
</communication>
```

2. Access the Application Server Control Console at http://hostname:port/em/ and log in with the oc4jadmin password set during installation.

   The **Cluster Topology** page appears.

3. Check the box in the **Select** column for the OC4J_WebCenter instance.
4. Click **Restart**.
5. Check the box in the **Select** column for the OC4J_Apps instance.
6. Click **Restart**.
7. Check the box in the **Select** column for the **home** instance.
8. Click **Restart**.

3.1.7 Configuring Corporate Proxy Server Settings for OmniPortlet and OracleAS Web Clipping on APPHOST1 and APPHOST2 (Optional)

1. Configure the HTTP proxy for OmniPortlet and OracleAS Web Clipping by performing the following steps (the Load Balancing Router must already be configured):

   a. Open the `provider.xml` file, located at:

      OmniPortlet:

      ORACLE_HOME`/j2ee/OC4J_WebCenter/applications/portalTools/omniPortlet/WEB-INF/providers/omniPortlet/provider.xml`

      WebClipping:

      ORACLE_HOME`/j2ee/OC4J_WebCenter/applications/portalTools/webClipping/WEB-INF/providers/webClipping/provider.xml`

b. Update the `proxyInfo` tag as shown:

```
<proxyInfo class="oracle.portal.provider.v2.ProxyInformation">
   <httpProxyHost>proxy.mycompany.com</httpProxyHost>
   <httpProxyPort>80</httpProxyPort>
   <dontProxyFor>*.mycompany.com</dontProxyFor>
   <proxyUseAuth>true</proxyUseAuth>
   <proxyType>Basic</proxyType>
   <proxyRealm>realm1</proxyRealm>
   <proxyUseGlobal>false</proxyUseGlobal>
   <proxyUser>scott</proxyUser>
   <proxyPassword>!tiger</proxyPassword>
</proxyInfo>
```

2. Access the Application Server Control Console at http://*hostname*:*port*/em/ and log in with the oc4jadmin password set during installation.

   The **Cluster Topology** page appears.

   Check the box in the **Select** column for the OC4J_WebCenter instance.

3. Click **Restart**.

4. Verify that OmniPortlet and the OracleAS Web Clipping providers work properly through the Load Balancing Router, by accessing the test pages at these URLs:

   `http://mywebcenter.com/portalTools/omniPortlet/providers/omniPortlet`

   > **Note:** If the "No Portlets Available" message appears under the Portlet Information section in the OmniPortlet Provider test page, then OmniPortlet is not configured correctly. If OmniPortlet is configured correctly, then the OmniPortlet and Simple Parameter Form portlets are available on the test page.

   `http://mywebcenter.com/portalTools/webClipping/providers/webClipping`

3.1.8 Oracle Content DB Limitations

In this release, there are some limitations to Oracle Content DB functionality:

- Oracle Content DB does not provide single sign-on support. In Oracle Content DB server failover situations, users will have to log in to the servers again.
- Any in-flight transactions (such as uploading a file) or transactions that require multiple steps (such as creation of a group) will be lost in the event of server failure, and will have to be restarted.
- Users will need to re-launch the user interface in the event of server failure (the session established on the failed server is no longer valid).
- Oracle Content DB agents can only be run on one computer. If the computer operating the agent fails, the system administrator must manually start the agents on the other computer. These agents perform housekeeping tasks for the Oracle Content DB server. Their failure does not cause Oracle Content DB server failure, but over time, with out the agents operating, the server's performance and scalability will be degraded.

3.1.9 Installing the Oracle Content DB Instances on CTHOST1 and CTHOST2

Before you install the Oracle Content DB instances, review the "Requirements for Oracle Content Database" section in the installation guide for the platform you are using.

The procedures for the Oracle Content DB instances on CTHOST1 and CTHOST2 differ slightly; this section contains a separate procedure for each. The directions for CTHOST2 apply to any additional instances installed.

> **Note:** Before you begin installing the Oracle Content DB instances, a Real Application Clusters (RAC) database must be installed and configured on CUSTDBHOST1 and CUSTDBHOST2, and the database character set must be ALT32UTF8. If it is not, an error occurs and installation cannot proceed.

3.1.9.1 Installing the First Oracle Content DB Instance on CTHOST1

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 using one of these commands:
   - On UNIX, issue this command: **`runInstaller`**
   - On Windows, double-click **`setup.exe`**

   The **WebCenter Suite 10.1.3.2.0 Installation** screen appears.
3. Specify an installation directory for the instance, or leave the default.
4. Select **Advanced Installation** and click **Next**.

   A confirmation dialog appears.
5. Click **Yes**.

   A progress dialog appears, then the **Select Installation Type** screen appears.
6. Select **Oracle Content Database** and click **Next**.

   The Specify **Port Configuration Options** screen appears.
7. Select **Manual**, provide a path to the `staticports.ini` file, and click **Next**.

   The **Administration Settings** screen appears.
8. 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 CTDB1 as the instance name and the host name is `server1.mycompany.com`, the instance name will be `CTDB1.server1.mycompany.com`.

9. Specify and confirm the administrator password for the application server instance.
10. Click **Next**.

    The **Specify Database Information** screen appears.

11. Provide the SYS password, the hostname and port (in RAC database format *CUSTDBHOST1*:1521^*CUSTDBHOST2*:1521), and the service name, and click **Next**.

    The **Specify Content Database Schema Password** screen appears.

12. Establish and confirm the Oracle Content DB schema password and click **Next**.

    The **Specify User Repository Info** screen appears.

13. Select **Directory Based**, select **Oracle Internet Directory** (or any LDAP service available), provide the connection information, and click **Next**.

    The **Cluster Topology** screen appears.

14. Enter 225.0.0.1 for the IP Address and 8001 for the port and click **Next**.

    The **Summary** screen appears.

15. Click **Install**.

    The **Preparing to Install** dialog appears, then the **Install** screen appears.

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

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

3.1.9.2 Installing the Second Oracle Content DB Instance on CTHOST2

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 using one of these commands:

    - On UNIX, issue this command: **`runInstaller`**
    - On Windows, double-click **`setup.exe`**

    The **WebCenter Suite 10.1.3.2.0 Installation** screen appears.

3. Specify an installation directory for the instance, or leave the default.

4. Select **Advanced Installation** and click **Next**.

    A confirmation dialog appears.

5. Click **Yes**.

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

6. Select **Oracle Content Database** and click **Next**.

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

7. Select **Manual** and click **Next**.

    The **Administration Settings** screen appears.

8. 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 CTDB2 as the instance name and the host name is `server1.mycompany.com`, the instance name will be `CTDB2.server1.mycompany.com`.

9. Specify and confirm the administrator password for the application server instance.

10. Click **Next**.

    The **Specify Database Information** screen appears.

11. Provide the SYS password, the hostname and port (in RAC database format *CUSTDBHOST1*:1521^*CUSTDBHOST2*:1521), and the service name, and click **Next**.

    The **Specify Content Database Schema Password** screen appears.

12. Provide the schema password and click **Next**.

    The **Specify User Repository Info** screen appears.

13. Provide the user name and password for the selected LDAP service, and click **Next**.

    The **Cluster Topology** page appears.

14. Enter 225.0.0.1 for the IP Address and 8001 for the port and click **Next**.

    The **Summary** screen appears.

15. Click **Install**.

    The **Preparing to Install** dialog appears, then the **Install** page appears.

16. The **Configuration Assistants** page appears. When the configuration process completes, the **End of Installation** page appears.

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

3.1.10 Configuring the Load Balancing Router

Configure a virtual IP address on the Load Balancing Router that listens on port 80 and maps to Oracle HTTP Server on WEBHOST1 and WEBHOST2, with no stick session enabled.

3.1.11 Disabling the Oracle HTTP Server in the Oracle Content DB Instances on CTHOST1 and CTHOST2

1. Open the `ORACLE_HOME/opmn/conf/opmn.xml` file.

2. Edit the file to disable the Oracle HTTP Server as shown:

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

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

   ```
   opmnctl stopall
   ```

   ```
   opmnctl startall
   ```

   Oracle Content DB now receives requests from the Oracle HTTP Servers on WEBHOST1 and WEBHOST2.

3.1.12 Defining the Virtual Hosts on WEBHOST1 and WEBHOST2 (and IDMWEBHOST1 and IDMWEBHOST2, for myWebCenter.com with Oracle Application Server Single Sign-On)

1. Open the Oracle HTTP Server configuration file:

   Apache 1.3:

   ORACLE_HOME/Apache/Apache/conf/httpd.conf

   Apache 2.0:

   ORACLE_HOME/ohs/conf/httpd.conf

2. Perform the following steps:

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

   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
   ```

   b. Add the lines shown to create a NameVirtualHost directive and a VirtualHost container for mywebcenter.mycompany.com and port 80.

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

The LoadModule rewrite_module directive must appear before the LoadModule certheaders_module directive.

c. Add the lines shown to create a NameVirtualHost directive and a VirtualHost container for ctdb.mycompany.com and port 80.

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

d. Add the lines shown to create a NameVirtualHost directive and a VirtualHost container for portlets.mycompany.com and port 80.

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

3. Save the httpd.conf file.

4. Restart the Oracle HTTP Server using these commands in *ORACLE_HOME*/opmn/bin:

```
opmnctl stopall
```

```
opmnctl startall
```

5. Verify that you can access this URL:

```
https://mywebcenter.mycompany.com/content/
```

Note: When producers are registered, the address is:

```
http://mywebcenter-producers.com:7777/...
```

3.1.13 Updating Domain Properties for Applications

1. Access the Oracle Enterprise Manager 10*g* Application Server Control Console at:

```
https://mywebcenter.com/em
```

2. Select the instance.
3. Select **OC4J_Content**.
4. On the **Applications** tab, select the content link.
5. Select **Content DB Extension**.
6. On the **Administration** tab, select **Go to Task** next to **Domain Properties**.
7. Update the `IFS.DOMAIN.APPLICATION.ApplicationHost` to the Load Balancing Router Virtual IP host name.
8. Update the `IFS.DOMAIN.APPLICATION.ApplicationPort` to the Load Balancing Router Virtual IP port.
9. Update the `IFS.DOMAIN.APPLICATION.ApplicationUseHttps` to `true`.
10. Issue these commands in *ORACLE_HOME*/`opmn/bin`:

    ```
    opmnctl stopall
    ```

    ```
    opmnctl startall
    ```

11. Access this URL:

    ```
    http://mywebcenter.com/content
    ```

12. Log in as the administrator (`orcladmin` user, Oracle Internet Directory administrator password).

3.1.14 Configuring the Oracle Content DB Instances on CTHOST1 and CTHOST2

1. Access the Application Server Control Console at `http://`*APPHOST*`:`*port*`/em/` and log in with the oc4jadmin password set during installation.

   The **Cluster Topology** page appears.

2. Select the Oracle Content DB instance.
3. Select the OC4J_Content instance.
4. Click **Applications**.
5. Click **Content**.
6. Click **Go to Task** next to **Domain Properties**.
7. Update the `IFS.DOMAIN.APPLICATION.ApplicationHost` to the Load Balancing Router virtual IP name and `IFS.DOMAIN.APPLICATION.ApplicationPort` to the Load Balancing Router virtual IP port.
8. Issue this command in *CONTENT_DB_ORACLE_HOME*/`opmn/bin` on CTHOST1 and CTHOST2:

   ```
   opmnctl reload
   ```

3.1.15 Disabling Application Server Control Console on APPHOST2 (Optional)

Application Server Control Console stores certain local state information that does not get replicated to another active Application Server Control Console. This includes things such as JMX Notification Subscriptions and Received Notifications. If you use JMX notifications, you may wish to disable the second Application Server Control Console so that Oracle HTTP Server does not route requests to it. This will ensure that notifications subscriptions are not changed or deleted on the instance receiving requests (causing the two instances to be out of synchronization). You can disable routing to one of the Application Server Control Consoles by setting the `ohs-routing` tag in the `default-web-site.xml` file for the second Application Server Control Console to `false` as shown:

```
<web-app application="ascontrol" load-on-startup="true" name="ascontrol"
ohs-routing="false" root="/em"/>
```

You can set `ohs-routing` to `true` if you need to use the secondary Application Server Control Console for failover. You will need to use some backup and recovery procedure in order to restore the state of notification subscriptions and received notifications from the primary Application Server Control Console to the secondary.

If you have two Application Server Control Consoles active, be aware of the following:

- If you change the administrator password on the managed OC4J instances, you will have to make the same change to the stored administrator password on all Application Server Control Console instances. When Oracle HTTP Server directs requests to an Application Server Control Console that does not have the correct password, attempts to connect to the managed instance will fail and Application Server Control Console will prompt for the new administrator password.

  On login, Application Server Control Console displays a warning on the Cluster Topology page that there are multiple instances running.

3.1.16 Listing Occupied Ports

Use the `netstat` command to identify occupied ports:

```
netstat -an
```

The AJP port range is 12501-12600. Note the port numbers in this range that do not appear in the output of the `netstat` command; these are the ports you can assign to OC4J instances.

3.1.17 Configuring the Firewall for the Application Tier

After you have installed all of the components on the Application Tier, you will be able to identify the port numbers that need to be opened on the firewall. This depends on the number of application server instances and types of components installed. In general, the process of configuring the firewall involves these steps:

1. For each installed instance, determine the component types and their designated port ranges (for example, the home instance and any instances you create) by examining the `ORACLE_HOME/opmn/conf/opmn.xml/opmn.xml` file. Example 3–2 shows components and default ports in the `opmn.xml` file. In the example, the OC4J `Admin` instance is listening on port 12501. Another instance, `Apps`, occupies port 12502.
2. Determine the ports in use with the `netstat` command:

   ```
   netstat -an
   ```

3. Configure the firewall to open only the ports in use.

Example 3–2 Oracle Application Server components and port ranges in opmn.xml

```
<opmn xmlns="http://www.oracle.com/ias-instance">
 <log path="$ORACLE_HOME\opmn\logs\opmn.log" comp="internal;ons;pm"
 rotation-size="1500000" />
 <debug path="$ORACLE_HOME\opmn\logs\opmn.dbg" comp="internal"
```

```
 rotation-size="1500000" />
 <notification-server>
 <port local="6100" remote="6200" request="6003" />
 <ssl enabled="true" wallet-file="$ORACLE_HOME\opmn\conf\ssl.wlt\default" />
 <topology>
 <discover list="*225.0.0.20:8001" />
 </topology>
 </notification-server>
...
       <ias-component id="OC4J">
         <process-type id="Admin" module-id="OC4J" status="enabled">
             ...
             <port id="default-web-site" range="*12501*" protocol="ajp"/>
             ...
         </process-type>
         <process-type id="OC4J_WP" module-id="OC4J" status="enabled">
             ...
             <port id="default-web-site" range="*12502*" protocol="ajp"/>
         </process-type>
       </ias-component>
...
```

Note that the AJP ports used by applications fall within the range 12501-12600. Ensure that all of the AJP ports used by OC4J applications are open on the firewall between the Web server and the application. If a port is not open, the following error occurs when access to the application from the Web tier is attempted (that is, when the URL ***web host:port/application*** is requested):

```
mod_oc4j: request to OC4J apphost1.us.oracle.com:12501 failed:
Connect failed (errno=110)
```

This error creates an entry in a log file in the `ohs/logs` directory.

3.1.18 Configuring the Cluster Gateway

Because there is a firewall between the instances clustered on the Web tier and the instances clustered on the Application tier, you must configure a cross-topology gateway to enable communication between the clusters. In the gateway configuration, one server on each side of the firewall is an entry point into the cluster. These instructions designate APPHOST1 and WEBHOST1 as the gateway servers, but any server may be designated the gateway server. The remote port is used for communication with the gateway server; it is designated in the `<gateway>` subelement in `opmn.xml` as shown in bold.

Follow these steps to specify gateway servers on the Application Tier and the Web Tier:

1. Open the *`APPHOST1_ORACLE_HOME`*`/opmn/conf/opmn.xml` file.
2. Create the `<gateway>` subelement as shown in the example:

```
<notification-server>
  <port local="6101" remote="6201" request="6004"/>
  <ssl enabled="true" wallet-file="$ORACLE_HOME\opmn\conf\ssl.wlt\default"/>
   <topology>
   <discover list="*225.0.0.20:8001"/>
    <gateway
list="apphost1.mycompany.com:6200&amp;apphost2.mycompany.com:6200&amp;webhost1.
mycompany.com:6200&amp;webhost2.mycompany.com:6200/"/>
   </topology>
</notification-server>
```

```
...
```

Note: 6201 is the OPMN remote port onAPPHOST1, and 6202 is the OPMN remote port on WEBHOST1. You must view the `opmn.xml` file on each server to determine the port values needed for the configuration.

---

3. Issue this command in *`APPHOST1_ORACLE_HOME`*`/opmn/bin`:

   `opmnctl reload`

4. Copy the `<gateway>` subelement to:

   - The *`WEBHOST1_ORACLE_HOME`*`/opmn/conf/opmn.xml` file
   - The *`WEBHOST2_ORACLE_HOME`*`/opmn/conf/opmn.xml` file
   - The *`APPHOST1_ORACLE_HOME`*`/opmn/conf/opmn.xml` file

5. Issue the **`opmnctl reload`** command in:

   - *`WEBHOST1_ORACLE_HOME`*`/opmn/bin`
   - *`WEBHOST2_ORACLE_HOME`*`/opmn/bin`
   - *`APPHOST1_ORACLE_HOME`*`/opmn/bin`

Note: For more information, see "Configuring Cross-Topology Gateways" in the *Oracle Containers for J2EE Configuration and Administration Guide*.

3.1.19 Creating the OC4J_Apps Instance and Associating it with Oracle Internet Directory

1. Access the Application Server Control Console at `http://`*`hostname`*`:`*`port`*`/em/` and log in with the oc4jadmin password set during installation.

   The **Cluster Topology** page appears.

2. Click the application server instance link.

   The **Application Server** page appears.

3. Click **Create OC4J Instance**.

   The **Create OC4J Instance** page appears.

4. Name the instance `OC4J_Apps` and leave the default group selection.

5. Check the **Start this OC4J instance after creation** checkbox.

6. Click **Create**.

   The **Processing: Create OC4J Instance** page appears with a progress message, then the Application Server page appears with the newly created instance.

7. Click the link for the OC4J_Apps instance.

   The **OC4J:OC4J_Apps** page appears.

8. Click **Administration**.

The **Administration** page appears.

9. Click the icon for the **Identity Management** task (in the **Security** section).

   The Identity Management page appears.

10. Click **Configure**.

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

11. Specify the Load Balancing Router (oid.mycompany.com) for the Oracle Internet Directory host, cn=orcladmin for the Oracle Internet Directory User DN, and 389 for the non-SSL Oracle Internet Directory port.

12. Click **Next**.

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

13. Click the **Use Oracle Identity Management Security Provider** checkbox.

14. Click **Next**.

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

15. Click **Configure**.

    The Identity Management page appears with a confirmation message that the OC4J_Apps instance was successfully associated with Oracle Internet Directory, and a prompt to restart OC4J_Apps.

16. Click **Restart**.

    A warning message appears.

17. Click **Yes**.

    A status message appears, then the **Cluster Topology** page reappears with a message that the instance was restarted.

> **Note:** If the application uses JAAS permissions (for example, if it uses ADF Security authorization) then the permissions need to be migrated to Oracle Internet Directory. See the *Oracle WebCenter Framework Developer's Guide*, "Using the OracleAS JAAS Provider Migration Tool".

3.1.20 Deploying WebCenter Applications on APPHOST1 or APPHOST2

1. Predeploy the application by issuing this command (shown on multiple lines for readability):

```
ORACLE_HOME/jdk/bin/java
  -jar ORACLE_HOME/adfp/lib/portlet-client-deploy.jar
  -predeploy -source myWebCenterArchive.ear
  -target target.ear
  -configuration config.xml
-profile Template
```

   Substitute Oracle home values where indicated with italics, and substitute the EAR file name for *myWebCenterArchive.ear* and *target.ear*.

2. Deploy the application by following these steps:

   a. Click the link for the OC4J_Apps instance.

      The **OC4J: OC4J_Apps** page appears.

b. Click **Applications**.

   The **Applications** page appears.

c. Click **Deploy**.

   The **Deploy: Select Archive** page appears.

d. Provide the location of the EAR file you predeployed and click **Next**.

   The **Deploy: Application Attributes** page appears.

e. Provide the application name and click **Next**.

   The **Deploy: Deployment Settings** page appears.

f. Click the icon for the **Select Security Provider** task.

   The **Deployment Settings: Select Security Provider** page appears.

g. Select **Oracle Identity Management** from the Security Provider drop-down list.

h. Click **OK**.

   The Deploy: Deployment settings page appears with an information message that the deployment plan was updated successfully.

i. Click **Cancel**.

   The **OC4J: OC4J_Apps** page appears.

3. Migrate security information:

   a. Create an LDIF file by issuing this command (shown on multiple lines for readability):

```
java oracle.security.jazn.tools.JAZNMigrationTool
  -D binddn
  -w password
  -h host name
  -p 389
  -sr jazn.com
  -st xml
  -dt ldap
  -sf ORACLE_HOME/j2ee/OC4J_
Apps/applications/webCenterArchive1/adf/META-INF/app-jazn-data.xml
  -df ORACLE_HOME/temp/migrate.ldif
  -m all
```

   Substitute password, host name, and Oracle home values where indicated with italics.

   b. Import the LDIF file into Oracle Internet Directory by issuing this command (shown on multiple lines for readability):

```
ldapmodify
  -h host name
  -p 389
  -D jazn.com
  -w password
  -f ORACLE_HOME/temp/migrate.ldif
  -v -c -o ORACLE_HOME/temp errors_ldiffile
```

   Substitute host name, password, host name, and Oracle home values where indicated with italics.

4. Configure role mapping manually in the deployed ORACLE_HOME/j2ee/OC4J_Apps/application-deployments/application name/orion-application.xml file:

   a. Set `jaas-mode` to `doASPrivileged` as follows:

   ```
   <jazn provider="LDAP" jaas-mode="doAsPrivileged"/>
   ```

   b. Set security-role-mapping to `users` as follows:

   ```
   <security-role-mapping name="users">
   <group name="users" />
   </security-role-mapping>
   ```

5. Access the Application Server Control Console at http://hostname:port/em/ and log in with the oc4jadmin password set during installation.

   The **Cluster Topology** page appears.

   Check the box in the **Select** column for the OC4J_Apps instance.

6. Click **Restart**.

3.2 Configuring Session State Replication for the OC4J_Apps and OC4J_WebCenter Instance

1. Access the Application Server Control Console at `http://`*`hostname`*`:`*`port`*`/em/` and log in with the oc4jadmin password set during installation.

   The **Cluster Topology** page appears.

2. Select the **OC4J_Apps** instance.

   The **OC4J:OC4J_Apps** page appears.

3. Click **Applications**.

4. Click the default application.

   The **Application: default** page appears.

5. Click **Administration**.

6. Click the icon for **Clustering Properties** in the **Properties** section.

   The **Clustering Properties** page appears showing that the parent application is not clustered.

7. Click the radio button for **Override parent application clustering settings** and select Enable from the drop-down list.

   The Replication Properties selections appear with Peer-Peer Replication selected as the default.

8. Leave the default and click **OK**.

   The **Application: default** page appears with a confirmation message that the changes were applied.

9. Return to the **Cluster Topology** page and select the **OC4J_WebCenter** instance.

   The **OC4J:OC4J_WebCenter** page appears.

10. Click **Applications**.

11. Click the default application.

    The **Application: default** page appears.

12. Click **Administration**.

13. Click the icon for **Clustering Properties** in the **Properties** section.

    The **Clustering Properties** page appears showing that the parent application is not clustered.

14. Click the radio button for **Override parent application clustering settings** and select **Enable** from the drop-down list.

    The **Replication Properties** selections appear with **Peer-Peer Replication** selected as the default.

15. Leave the default and click **OK**.

    The **Application: default** page appears with a confirmation message that the changes were applied.

16. Add an empty `<distributable/>` tag to:

    ORACLE_HOME/j2ee/OC4J_Apps/applications/*application name*/*web module name*/WEB-INF/web.xml

    ORACLE_HOME/j2ee/OC4J_WebCenter/applications/*application name*/*web module name*/WEB-INF/web.xml

    The tag must be added for all Web modules that are part of a clustered application.

17. Return to the Cluster Topology page and restart the **OC4J_Apps** and **OC4J_WebCenter** instances.

3.3 Configuring APPHOST1 and APPHOST2 for the RAC Database

1. Open the *ORACLE_HOME*/opmn/conf/opmn.xml file.

2. Add the RAC database hostname and remote port identifiers:

```
<notification-server>
  <port local="6100" remote="6200" request="6003"/>
  <ssl enabled="false" wallet-file="$ORACLE_HOME\opmn\conf\ssl.wlt\default"/>
  <topology>
  <nodeslist="apphost1:6200,apphost2:6200,webhost1:6200,webhost2:6200,infradbho
st1:6200,infradbhost2:6200"/>
  </topology>
</notification-server>
```

3. Save and close the file.

4. Open the *ORACLE_HOME*/j2ee/OC4J_WebCenter/config/data-sources.xml file.

5. Add the RAC node information:

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<data-sources xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://xmlns.oracle.com/oracleas/schema/data-sou
rces-10_1.xsd" schema-major-version="10" schema-minor-version="1">
     <managed-data-source connection-pool-name="Example Connection Pool"
jndi-name="jdbc/OracleDS" name="OracleDS"/>
     <managed-data-source connection-pool-name="OracleWSRPPool"
jndi-name="jdbc/portletPrefs" name="WSRP_PREF_DS"/>
     <connection-pool name="Example Connection Pool">
       <connection-factory factory-class="oracle.jdbc.pool.OracleDataSource"
user="scott" password="tiger" url="jdbc:oracle:thin:@//localhost:1521/ORCL"/>
     </connection-pool>
     <connection-pool name="OracleWSRPPool">
        <connection-factory factory-class="oracle.jdbc.pool.OracleDataSource"
user="pref1" password="pref1" url="jdbc:oracle:thin:@//(DESCRIPTION =(ADDRESS
= (PROTOCOL = TCP)(HOST = infradbhost1)(PORT = 1521))(ADDRESS = PROTOCOL =
TCP)(HOST = infradbhost2)(PORT = 1521))(LOAD_BALANCE=yes)(CONNECT_DATA=(SERVER
= DEDICATED)(SERVICE_NAME = stork)))"/>
     </connection-pool>
</data-sources>
```

6. Save and close the file.
7. Issue this command in *ORACLE_HOME*/opmn/bin:

   opmnctl reload

3.4 Configuring Network Communication

After the installation and configuration is complete, configure the network communication as described in this section. Table 3–1 lists the ports open on each firewall.

Configure the Load Balancing Router to:

- Receive requests on http://webcenter.mycompany.com, port 443
- Receive requests on http://ctdb.mycompany.com, port 443
- Receive requests on http://portlets.mycompany.com, port 443
- Receive requests on http://portlets.mycompany.com, port 7777
- Receive requests on http://sso.mycompany.com, port 443
- Balance requests with SSL acceleration to WEBHOST1, WEBHOST2 on port 7777

Configure the firewall for communication into DMZ1:

- http://WEBHOST1:7777
- http://WEBHOST2:7777
- ONS remote port 6200 on WEBHOST1 and WEBHOST2

Configure the firewall for communication into and out of DMZ2:

- http://APPHOST1 (J2EE with WebCenter components) AJP ports 12501-12510
- http://APPHOST2 (J2EE with WebCenter components) AJP ports 12501-12510
- ONS remote port 6200 on APPHOST1 and APPHOST2
- NIP/NAP ports for Oracle COREid Access and Identity (default values are 6021 and 6022) for communication from WEBHOST1 and WEBHOST2 to IDMHOST1 and IDMHOST2.

Configure the firewall for communication into DMZ3:

- INFRADBHOST1 INFRADBHOST2 database with listener on port 1521

Table 3–1 Open ports between firewall zones

Firewall Zones	Ports	Purpose
DMZ1 to DMZ2	12510-12510	WEBHOST1 and WEBHOST2, to access APPHOST1 and APPHOST2 AJP ports
DMZ1 to DMZ2	6200, 6201	OPMN cluster gateway
DMZ2 to DMZ1	7777	Communication to Oracle Content DB
DMZ1 to DMZ2	6021, 6022	WEBHOST1 and WEBHOST2 to IDMHOST1 and IDMHOST2
DMZ2 to DMZ1	6021, 6022	IDMHOST1 and IDMHOST2 to WEBHOST1 and WEBHOST2
DMZ2 to DMZ3	1521	Database access
DMZ2 to DMZ3	389, 636	Oracle Internet Directory server access

3.4.1 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.

3.5 Configuring Application Authentication and Authorization

The tasks you have to perform depend on the authentication method you will use for myWebCenter. If you want user login sessions to persist after a failover event, you will need to use single sign-on.

myWebCenter with JSSO and Oracle Internet Directory

Perform these steps:

1. "Steps to Use the Oracle Identity Management Security Provider" and "Settings for Authentication Method with Oracle Identity Management" in the *Oracle Containers for J2EE Security Guide*, Chapter 8.
2. Section 3.5.1, "Configuring Java SSO on APPHOST1 and APPHOST2".

myWebCenter with Oracle Application Server Single Sign-On

Perform these steps:

1. "Steps to Use the Oracle Identity Management Security Provider" and "Settings for Authentication Method with Oracle Identity Management" in the *Oracle Containers for J2EE Security Guide*, Chapter 8.
2. Chapter 5, "Installing and Configuring OracleAS Single Sign-On and Oracle Delegated Administration Services".

3.5.1 Configuring Java SSO on APPHOST1 and APPHOST2

You will need to follow these steps on both Oracle Application Server instances (APPHOST1 and APPHOST2), to configure Java SSO for the `ascontrol` (for Application Server Control Console) application in the home instances:

Access the Oracle Enterprise Manager 10*g* Application Server Control Console and perform these steps:

1. Click the link for the home instance.

   The **OC4J:home** page appears.

2. Click **Applications**.

   The applications are listed.

3. Click **Expand All**.

4. Select the `javasso` application and click **Start**.

   This warning message appears:

   ```
   Java SSO is not properly configured. This is often caused
   when you are running multiple Java SSO applications in the
   cluster that use different shared symmetric keys. Please
   configure all Java SSO applications in the cluster to use the
   same shared symmetric key. You can do this from Java SSO
   Configuration page.
   ```

5. Click **Configure Java SSO**.

   A confirmation message appears that the SSO configuration was completed and will take effect after the instances are restarted.

6. Click **Restart**.

   A confirmation message appears.

7. Click **Yes**.

   The instance is restarted. When configuring the home instance, the system terminates your login session and you must log back in to continue the setup.

8. Scroll to the Administration section and click **Java SSO Configuration**.

   The Java SSO Configuration page appears.

9. Click **Participating Applications**.

   The applications are listed.

10. Click the check box for the applications to be Java SSO enabled.

11. Click **Apply**.

3.6 WebCenter Application Deployment and Migration Utilities (Optional)

There are several migration utilities available that can help you deploy WebCenter applications:

- *Oracle WebCenter Framework Developer's Guide*, "Using Lifecycle Tools to Predeploy an Existing .ear File
- *Oracle WebCenter Framework Developer's Guide*, "Using the OracleAS JAAS Provider Migration Tool"
- *Oracle WebCenter Framework Developer's Guide*, "Usage Notes for the OracleAS JAAS Provider Migration Tool"
- *Oracle WebCenter Framework Developer's Guide*, "OracleAS JAAS Provider Migration Tool Command Syntax and Options"

- *Oracle WebCenter Framework Developer's Guide*, "Using the PDK-Java Preference Store Migration and Upgrade Utility"

4

Installing and Configuring Oracle COREid Access and Identity

4.1 Understanding Oracle COREid Access and Identity Components

The Oracle COREid Access and Identity authentication and authorization services are provided by the components described in this section. The components are shown in Figure 1–2, "Enterprise Deployment Architecture for myWebCenter.com with Oracle COREid Access and Identity".

> **Note:** The WebPass and AccessManager components are not available on Windows at the time of publication. Therefore, WEBHOST1, WEBHOST2 and ADMINHOST in the myWebCenter Oracle COREid Access and Identity configuration must be servers with operating systems other than Microsoft 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 COREid Access and Identity server. Every web server instance that communicates with a Oracle COREid Access and Identity server must be configured with WebPass. WebPass is also required on each computer hosting an Access Manager.

Oracle COREid Access and Identity, 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 COREid Access and Identity 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.

4.2 The myWebCenter Oracle COREid Access and Identity Authentication and Authorization Process

This section describes the sequence for authentication and authorization for J2EE applications using Oracle COREid Access and Identity 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 fetches extra roles from the Access Server.

4.3 Preparing to Install Oracle COREid Access and Identity Components

Before you install the Oracle COREid Access and Identity 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 COREid Access and Identity 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 COREid Access and Identity components.
- Define the Master Identity Administrator user account (this user has access to all Oracle COREid Access and Identity functionality).
- Have a user account with administrator privileges on all computers.
- On Windows, ensure that the user account used to install the Oracle COREid Access and Identity server and Access Server has the privilege to log on as a service. The Oracle COREid Access and Identity 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, "Configuring the Data Tier".

4.4 Installing the First Identity Server on IDMHOST1

1. Log in to IDMHOST1 as an administrator.
2. Issue one of these commands 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
   ```

   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 COREid Access and 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 4.16.

   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 **Open** 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 COREid Access and Identity 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**.

    The Identity Server Configuration screen appears with these options:

    - Directory Server hosting user data is in SSL
    - Directory Server hosting Oracle data is in SSL

14. Leave the checkboxes clear (do not select an option) and click **Next**.

    You are prompted to select the directory server type from the drop-down list.

15. Select **Oracle Internet Directory** and click **Next**.

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

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

18. 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 COREid Access and Identity branches of the directory information tree (DIT). Oracle COREid Access and Identity will access the directory server as this account.

    Documentation references and contact information appears.

19. Click **Next**.

    An installation summary appears.

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

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

    Windows:

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

    Linux:

    Issue this command in `*Oracle COREid Access and Identity installation directory*/identity/oblix/apps/common/bin`:

    ```
    start_ois_server
    ```

4.5 Installing WebPass on WEBHOST1

1. Log in to the computer as an administrator.

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

   Linux console installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_linux_OHS_WebPass
   ```

   or

   ```
   ./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_WebPass
   ```
   [1]

   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] 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 4.16.

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 `Open` 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 COREid Access and Identity 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`*`/Apache/Apache/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 COREid Access and Identity installation directory*/oblix/apps/common/bin directory:

    stop_ois_server

19. Start the Identity server service by issuing the following command in the *Oracle COREid Access and Identity 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 COREid Access and Identity system console at this URL:

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

       The Oracle COREid Access and Identity system main page appears.

4.6 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 COREid Access and Identity 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**. (You do not need to do anything because the schema was updated during installation.)

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 **Open**.

   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 COREid Access and Identity 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 the **Auto Configure objectclass** box, then 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 COREid Access and Identity 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 COREid Access and Identity 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 COREid Access and Identity 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.

4.7 Installing the Second Identity Server on IDMHOST2

1. Log in to IDMHOST2 as an administrator.

2. Issue one of these commands 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
   ```

   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 4.16.

   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 **Open** 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** and click **Next**.

    The documentation references and contact information appear.

14. Click **Next**.

    An installation summary appears.

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

16. Start the Identity Server by doing one of the following:

    Windows:

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

    Linux:

    Issue this command:

    ```
    Identity Server installation
    directory/identity/oblix/apps/common/bin/start_ois_server
    ```

4.8 Installing WebPass on WEBHOST2

Follow the steps in Section 4.5, "Installing WebPass on WEBHOST1" on page 4-6 to install WebPass on WEBHOST2, specifying the host name and port for the Identity Server on IDMHOST2. 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.

4.9 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 4.6.

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.

4.10 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 myWebCenter with Oracle COREid Access and Identity, 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

4.10.1 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 3.1.1, "Installing the Oracle HTTP Servers on WEBHOST1 and WEBHOST2 (and IDMWEBHOST1 and IDMWEBHOST2, for myWebCenter.com with Oracle Application Server Single Sign-On)" on page 3-2 to install a Web Server on ADMINHOST for use with the Policy Manager.

4.10.2 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 4.5, "Installing WebPass on WEBHOST1" on page 4-6 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.

4.10.3 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 these commands to start the installation (according to platform and installation option):

   Windows:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_NSAPI_Policy_
   Manager.exe
   ```

   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. 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 4.16.

   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 the Configure Directory Server for Policy Data screen appears with the **Directory Server Type** drop down list.

9. Select **Oracle Internet Directory**.

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

10. Select the **Open** option.

    A progress message appears, then the Configure Directory Server for Policy Data screen appears with the **Directory Server Type** drop down list.

11. Select **Oracle Internet Directory**, then click **Next**.

    You are prompted to specify whether policy data is in a separate directory server than the directory containing Oracle configuration data or user data, and if so, whether you would like the installer to automatically configure the directory server containing policy data.

12. Select **No** and click **Next**.

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

14. Click **Next**.

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

15. Stop the Policy Manager web server instance.

16. Stop and then start the Identity Server instance.

17. Start the Policy Manager web server instance.

18. Click **Next**.

    Read Me information appears.

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

    A message appears informing you that the installation was successful.

20. Click **Finish**.

4.10.4 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. Stop and then start the Identity Server service for the WebPass.
23. Restart the WebPass/Policy Manager web server instance.
24. After the Web server reastarts, click **Done**.

    The Policy Manager home page appears.

25. 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.

4.10.5 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 `Open` (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 these commands 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 4.16.

    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 `Open` 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 4.10.5, "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.

4.10.6 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 computer level or the virtual web server level. However, do not install at both the computer 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 WEBHOST1 or WEBHOST2 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 `Open` (the transport security mode must be the same between all Access Servers and WebGates).

   In the **Preferred HTTP Host** field, specify the host on which the web server is running.

   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 these commands 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
   ```

Linux console installation:

```
./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_WebGate
```

Linux GUI installation:

```
./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_WebGate -gui
```

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:

   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 4.16.

   On Linux systems, this prompt appears:

   ```
   To proceed with installation of Oracle COREid Access and Identity 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:

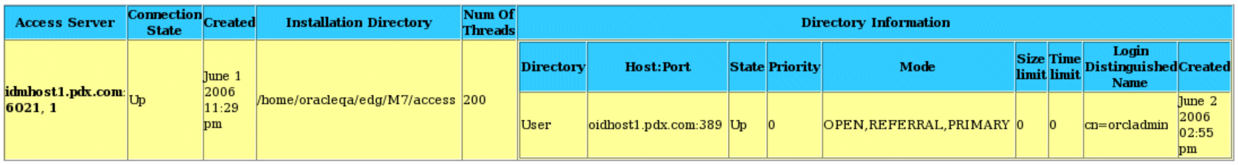
    a. Ensure that the Identity Server, WebPass, and Access Server are running.

    b. Access this URL:

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

       The WebGate page appears as shown in Figure 4–1.

Figure 4–1 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.

4.11 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`.

4.12 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]`.

For a comprehensive discussion of the Access SDK, see Chapter 5 of the *Oracle Identity Management Application Developer's Guide*.

4.12.1 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.

4.12.2 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 4.16.

   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 COREid Access and Identity 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.

4.12.3 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 `Open` (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 preceding steps 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 COREid Access and Identity are deployed.

4.13 Configuring Oracle COREid Access and Identity Single Sign-On for OC4J Applications

After you have installed the Oracle COREid Access and Identity, WebGate and Access Server SDK, complete the procedures in this section to integrate WebCenter components with Oracle COREid Access and Identity.

4.13.1 Configuring Access to WebCenter Components

1. Update the `opmn.xml` file to set the `LD_ASSUME_KERNEL` environment variable to `2.4.19`, as shown in Example 4–1.

Example 4–1 opmn.xml File Updates

```
<process-type id="OC4J_WebCenter" module-id="OC4J" status="enabled">
               <environment>
                 <variable id="LD_ASSUME_KERNEL" value="2.4.19"/>
               </environment>
               <module-data>
                  <category id="start-parameters">
                     <data id="java-options" value="-server -XX:MaxPermSize=128M
-ms512M -mx1024M -XX:AppendRatio=3
-Djava.library.path=/product/oracle/AccessServerSDK/oblix/lib
-Djava.security.policy=$ORACLE_HOME/j2ee/home/config/java2.policy
-Djava.awt.headless=true -Dhttp.webdir.enable=false
...
```

2. Copy the Access Server /oblix/lib/jobaccess.jar file to the *ORACLE_HOME*/j2ee/home/lib/ext directory. For example:

   ```
   cp product/oracle/AccessServerSDK/oblix/lib/jobaccess.jar ORACLE_
   HOME/j2ee/home/lib/ext
   ```

3. Restart the OC4J_WebCenter instance by issuing these commands:

   opmnctl reload

   opmnctl restartproc process-type=OC4J_WebCenter

4. Create the file *ORACLE_HOME*/ohs/htdocs/login/login.html. The variable names for username and password match the plug-ins defined for COREidSSOform and COREidSSONoPwd in the next step.

   > **Note:** If you need detailed information, see the *Oracle Containers for J2EE Security Guide*, Chapter 11, section titled "Create a Login Form".

5. Create authentication schemes, resource types and action URL protection in the Access Server console, as follows:

   Create COREidSSOform, a form-based authentication scheme. For instructions, see the *Oracle Containers for J2EE Security Guide*, Chapter 11, section titled "Define Form-Based Authentication in Policy Manager".

   Create COREidSSONoPwd, for authentication without password. For instructions, see the *Oracle Containers for J2EE Security Guide*, Chapter 11, section titled "Define Basic Authentication in Policy Manager".

   Create myresourcetype, to be used in the login-modules section of the system-jazn-data.xml file. For instructions, see the *Oracle Containers for J2EE Security Guide*, Chapter 11, section titled "Configure the Name and Operation of the Resource Type".

   Protect the action URL in the login.html file with COREidSSONoPwd. For instructions, see the *Oracle Containers for J2EE Security Guide*, Chapter 11, section titled "Protect the Action URL".

   > **Note:** The plug-ins in COREidSSOform and COREidSSONoPwd must match the variables in the login.html file.

4.13.2 Configuring the Login Protected by Oracle COREid Access and Identity

1. Use the Access Server console and the instructions in *Oracle COREid Access and Identity Access Administration Guide* to create policy domains to protect the URLS with COREidSSOform, for example:

   /em

2. Visit the protected URLs created in Step 1.

   The login is not fully functional at this point; attempting to access the URLs causes a redirect to the /login/login.html page.

3. Locate the application section in the jazn-loginconfig section of the *ORACLE_HOME*/j2ee/OC4J_WebCenter/config/system-jazn-data.xml file. The application section is shown in bold in Example 4–2.

Example 4–2 Additions to <application> section of system-jazn-data.xml

```
<grant>
     <grantee>
           <principals>
                <principal>
                     <class>oracle.security.jazn.realm.CoreIDPrincipal</class>
                            <name>page-viewer</name>
                </principal>
           </principals>
     </grantee>
     <permissions>
                        ... ...
                     <class>oracle.security.jazn.realm.CoreIDPrincipal</class>
                            <name>page-customizer</name>
                        ... ...
                     <class>oracle.security.jazn.realm.CoreIDPrincipal</class>
                            <name>page-personalizer</name>
                        ... ...
```

4. Replace the application name with the application name of the component to authorize. For example, for Application Server Control Console, it is `ascontrol`.

5. If necessary, create an application section for each component to authorize by copying and pasting an existing application section, and replacing the `name` value with the name of the application.

6. Add `COREIDSSO` as the authentication method to *`ORACLE_HOME`*`/j2ee/OC4J_WebCenter/application-deployments/`*`application name`*`/orion-application.xml`. For example, replace:

```
<jazn provider="XML" default-realm="jazn.com" jaas-mode="doAsPrivileged"/>
```

Note: The `jaas-mode` setting is the value required by the particular application. When the application is developed, the `jaas-mode="doAsPrivileged"` would have been set through the use of the ADF Security Wizard in JDeveloper at design time. It can always be set manually thereafter.

with the following, shown in bold (note also that the slash following `doASPrivileged` must be removed):

```
<jazn provider="XML" default-realm="jazn.com" jaas-mode="doAsPrivileged">
<jazn-web-app auth-method="COREIDSSO"/>
</jazn>
```

Caution: Edit the file with care, making certain that the XML is well-formed. If it is not, restarting the application with the `opmnctl` utility can remove the application from the `server.xml` file. This causes the application to become undeployed.

7. Ensure that the appropriate roles and users are populated in Oracle COREid Access and Identity for use with Oracle Internet Directory by adding `oc4jadmin` to the `oc4j-administrators` and `ascontrol_admin` groups in Oracle Internet Directory. For instructions on adding users to groups, see the Oracle Internet Directory documentation set. It is available in the Oracle Identity Management 10g (10.1.4.0.1) documentation library. Click **View Library, Identity and Access Management** at:

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

8. Restart the OC4J instance.
9. Access a protected URL to verify that the login is working.

4.13.3 Configuring the Logout

1. Copy the `logout.html` file from the WebGate directory `access/oblix/lang/en-us/` to *`ORACLE_HOME`*`/ohs/htdocs`.
2. Navigate to **Access System Console, Access System Configuration, Server Settings, Configure SSO logout URL**.
3. Set the URL to `/logout.html`.
4. Restart the Oracle HTTP Server for the Policy Manager.
5. Perform one of the following steps to cause Oracle COREid Access and Identity to reread the configuration:
   - Restart the Oracle COREid Access and Identity server.
   - Clear the cache in the Identity System Console by selecting **System Configuration, Server settings, Cache**.
6. In the *`ORACLE_HOME`*`/j2ee/OC4J_WebCenter/config/jazn.xml` file, update `custom.sso.url.logout` property to:

```
<property name="custom.sso.url.logout" value="/logout.html"/>
```

7. Restart the OC4J instance by issuing these commands:

```
opmnctl reload
```

```
opmnctl restartproc process-type=OC4J_WebCenter
```

   The logout for all components will now redirect to this logout page.

4.14 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

4.14.1 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.

4.15 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

4.15.1 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.

4.16 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.$$
```

4.17 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 4–1 lists the components, data stores, and configuration methods.

Table 4–1 Supported Failover Configurations for Directory Servers

Component	Data Store	Operation	Configuration Method
Identity Server	User	Read/Write	Directory Profile See Section 4.17.1, "Configuring Directory Failover for User Data"
Identity Server	Oracle	Read/Write	Directory Profile and XML Configuration Files See Section 4.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Server	User	Read/Write[1]	Directory Profile See Section 4.17.1, "Configuring Directory Failover for User Data"
Access Server	Oracle	Read/Write[2]	`ConfigureAAAServer` command line tool Section 4.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Server	Policy	Read/Write[3]	`ConfigureAAAServer` command line tool Section 4.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Manager	User	Read	Directory Profile XML Configuration Files
Access Manager	Oracle	Read/Write[4]	Section 4.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Manager	Policy	Read/Write[5]	XML configuration files Section 4.17.2, "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.

4.17.1 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 reestablish 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.

4.17.2 Configuring Directory Failover for Oracle and Policy Data

This section explains how to configure failover in the Identity Server for Oracle and Policy data.

4.17.2.1 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 4–3 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

4.17.2.1.1 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 4–3 as a guide (server information and encrypted password shown in bold).

   > **Note:** Instructions for obtaining the encrypted password are provided in Section 4.17.2.1.3, "Creating the Encrypted Password for the Bind DN" on page 4-38.

3. Save the `sample_failover.xml` file as `failover.xml`.

Example 4–3 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>
```

4.17.2.1.2 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 4.17.1, "Configuring Directory Failover for User Data".

4.17.2.1.3 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.

4.18 Configuring Access Server Directory Failover for Oracle and Policy Data

Perform the procedures in this section to configure directory failover for the Access Server.

4.18.1 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`

4.19 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.

4.20 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.

4.20.1 Creating a Directory Server Profile for the Identity Servers

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

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

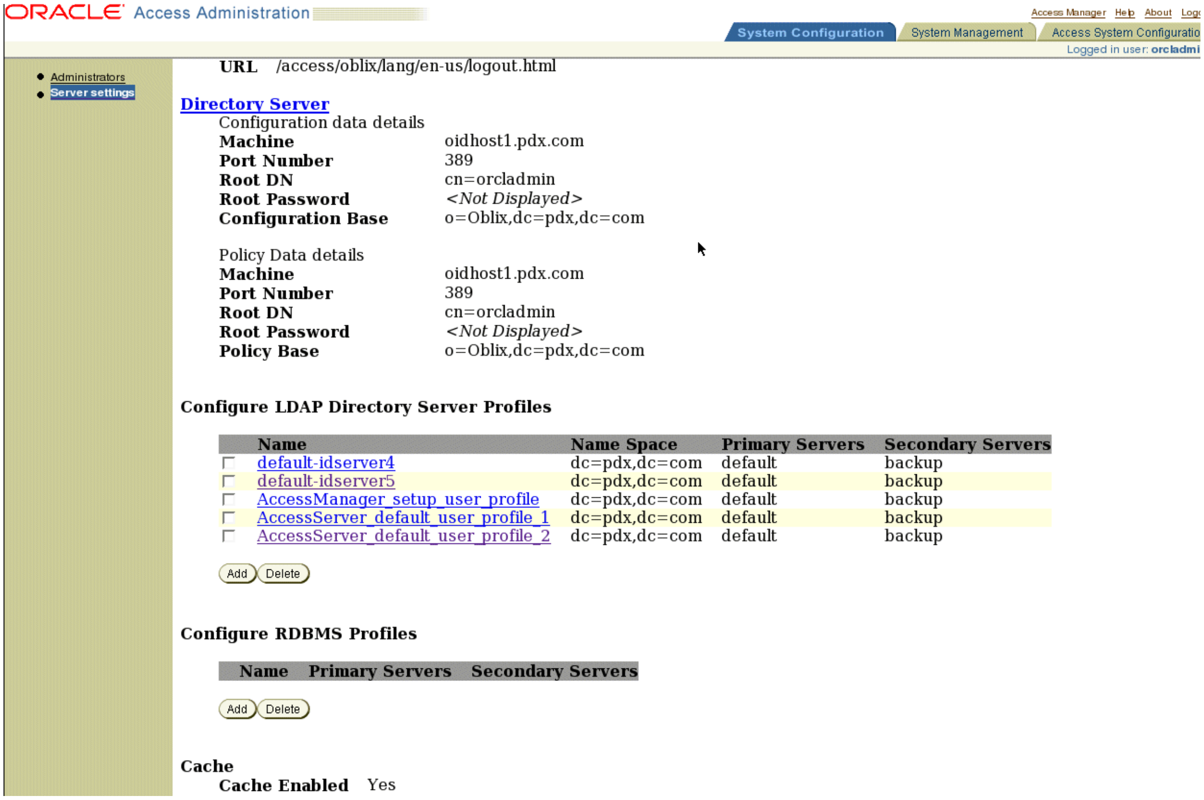
    The **Identity Administration** page appears.
2. Select **Identity System Console**.

    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 4–2.

Figure 4–2 Oracle Access Administration Configure Profiles Screen



URL /access/oblix/lang/en-us/logout.html

Directory Server

Configuration data details

Machine	oidhost1.pdx.com
Port Number	389
Root DN	cn=orcladmin
Root Password	*<Not Displayed>*
Configuration Base	o=Oblix,dc=pdx,dc=com

Policy Data details

Machine	oidhost1.pdx.com
Port Number	389
Root DN	cn=orcladmin
Root Password	*<Not Displayed>*
Policy Base	o=Oblix,dc=pdx,dc=com

Configure LDAP Directory Server Profiles

	Name	Name Space	Primary Servers	Secondary Servers
☐	default-idserver4	dc=pdx,dc=com	default	backup
☐	default-idserver5	dc=pdx,dc=com	default	backup
☐	AccessManager_setup_user_profile	dc=pdx,dc=com	default	backup
☐	AccessServer_default_user_profile_1	dc=pdx,dc=com	default	backup
☐	AccessServer_default_user_profile_2	dc=pdx,dc=com	default	backup

Configure RDBMS Profiles

Name	Primary Servers	Secondary Servers

Cache

Cache Enabled Yes

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.

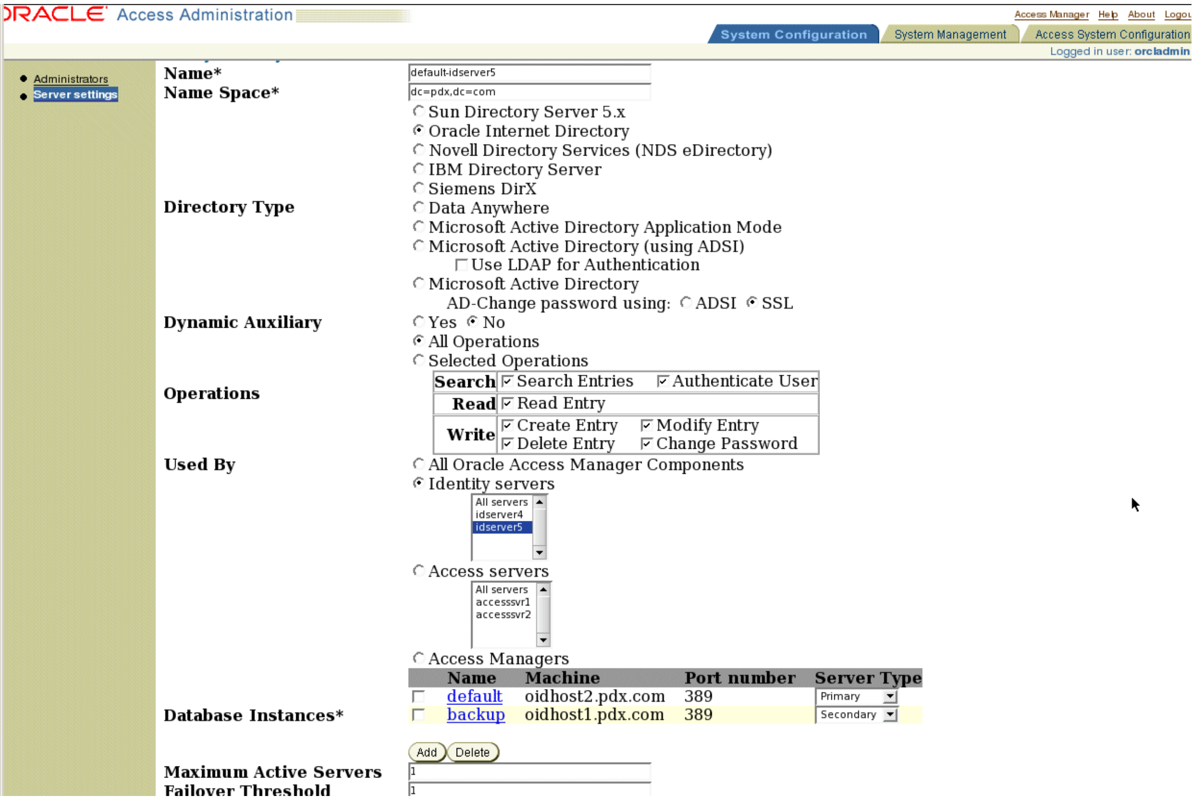
11. Specify *oidhost1.mycompany.com*, and select **Secondary** from the Server Type drop-down list.

12. Click **Save**.

    The **Modify Directory Server Profile** screen appears.

13. Restart both Identity Servers.

Figure 4–3 Oracle Access Administration Create Directory Server Profile Screen



Name* default-idserver5

Name Space* dc=pdx,dc=com

Directory Type
- ○ Sun Directory Server 5.x
- ● Oracle Internet Directory
- ○ Novell Directory Services (NDS eDirectory)
- ○ IBM Directory Server
- ○ Siemens DirX
- ○ Data Anywhere
- ○ Microsoft Active Directory Application Mode
- ○ Microsoft Active Directory (using ADSI)
  - □ Use LDAP for Authentication
- ○ Microsoft Active Directory
  - AD-Change password using: ○ ADSI ● SSL

Dynamic Auxiliary ○ Yes ● No

Operations
- ● All Operations
- ○ Selected Operations

Search	☑ Search Entries	☑ Authenticate User
Read	☑ Read Entry	
Write	☑ Create Entry ☑ Delete Entry	☑ Modify Entry ☑ Change Password

Used By
- ○ All Oracle Access Manager Components
- ● Identity servers: All servers, idserver4, idserver5 (selected: idserver5)
- ○ Access servers: All servers, accesssvr1, accesssvr2
- ○ Access Managers

Database Instances*

	Name	Machine	Port number	Server Type
□	default	oidhost2.pdx.com	389	Primary
□	backup	oidhost1.pdx.com	389	Secondary

Maximum Active Servers 1

Failover Threshold 1

4.20.2 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 4–2.

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.

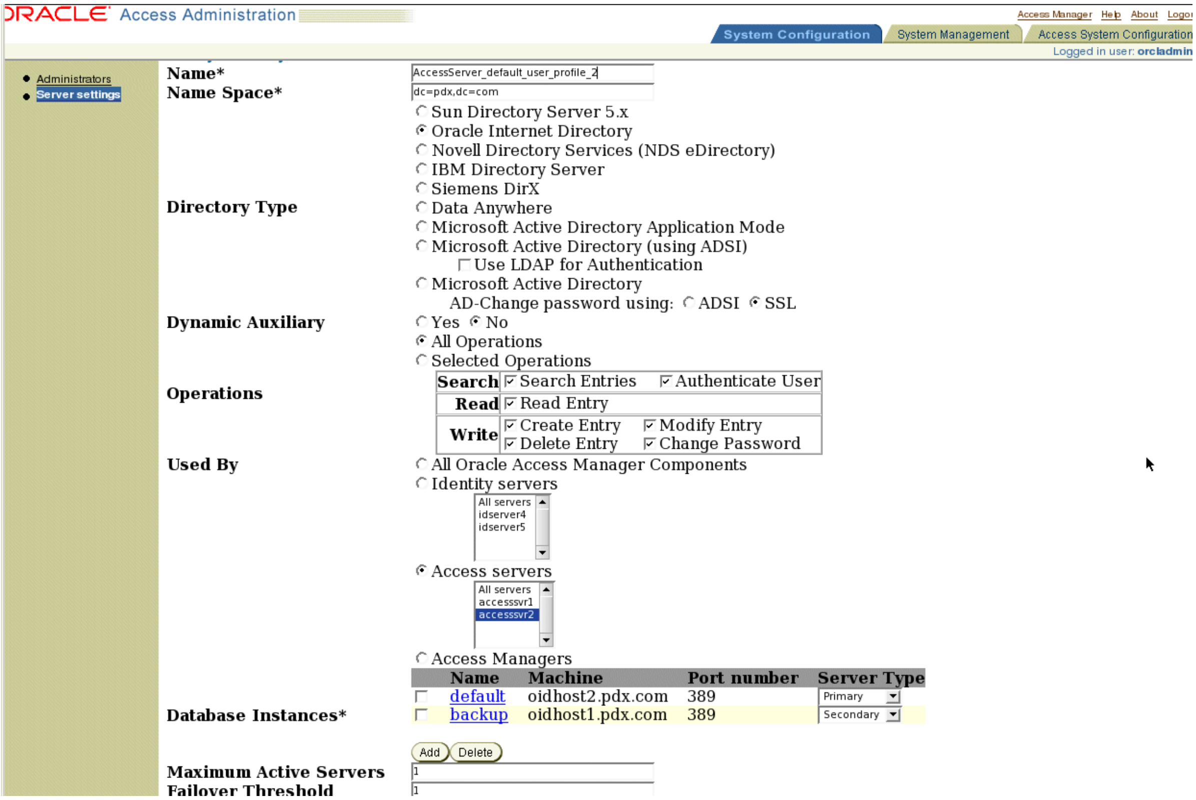
10. Click **Save**.

    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 4–4 Oracle Access Administration Create Directory Server Profile Screen



Name*: AccessServer_default_user_profile_2

Name Space*: dc=pdx,dc=com

Directory Type:
○ Sun Directory Server 5.x
● Oracle Internet Directory
○ Novell Directory Services (NDS eDirectory)
○ IBM Directory Server
○ Siemens DirX
○ Data Anywhere
○ Microsoft Active Directory Application Mode
○ Microsoft Active Directory (using ADSI)
□ Use LDAP for Authentication
○ Microsoft Active Directory
AD-Change password using: ○ ADSI ● SSL

Dynamic Auxiliary: ○ Yes ● No

Operations:
● All Operations
○ Selected Operations

Search	☑ Search Entries	☑ Authenticate User
Read	☑ Read Entry	
Write	☑ Create Entry ☑ Delete Entry	☑ Modify Entry ☑ Change Password

Used By:
○ All Oracle Access Manager Components
○ Identity servers
All servers
idserver4
idserver5
● Access servers
All servers
accesssvr1
accesssvr2
○ Access Managers

Database Instances*:

	Name	Machine	Port number	Server Type
□	default	oidhost2.pdx.com	389	Primary
□	backup	oidhost1.pdx.com	389	Secondary

Maximum Active Servers: 1

Failover Threshold: 1

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.

4.21 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.

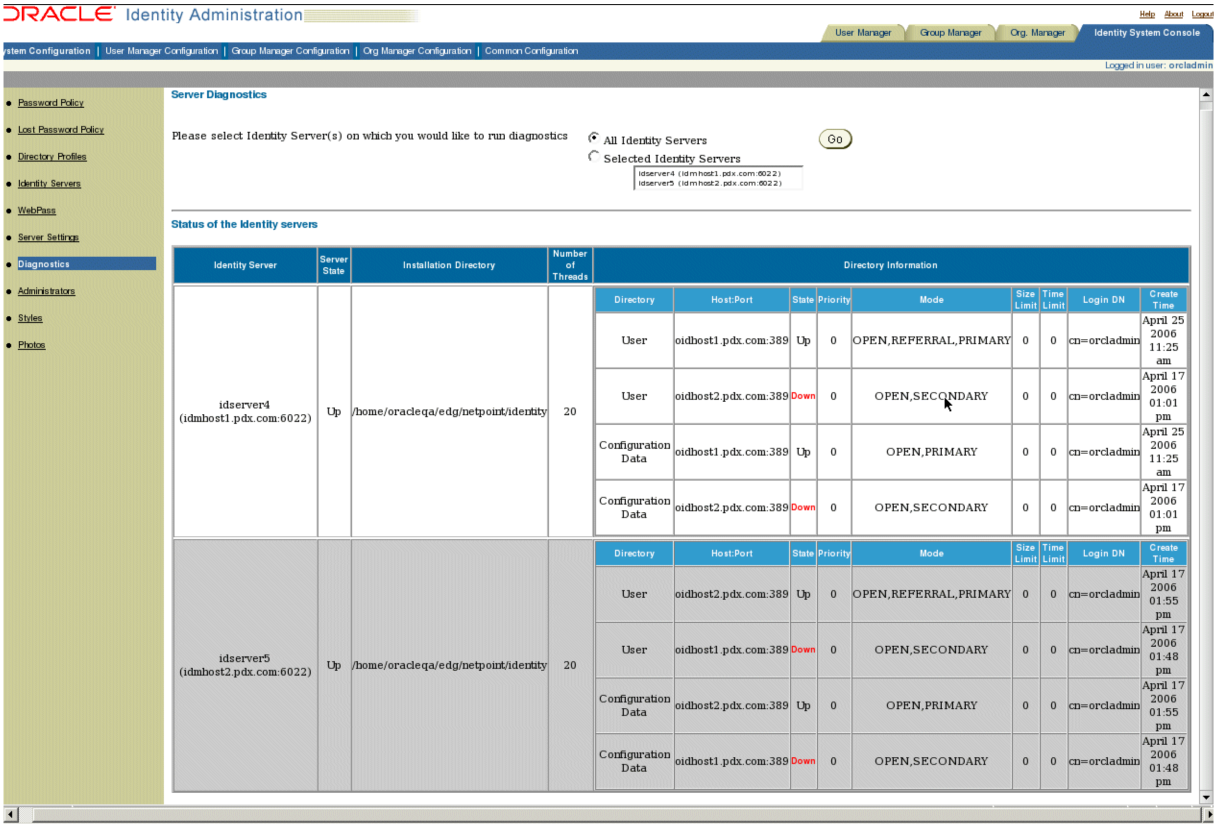
3. Provide the user ID and password and click **Login**.

   The **System Configuration** page appears.

4. Click **System Configuration**, then **Diagnostics**.

   The **Server Diagnostics** screen appears as shown in Figure 4–2.

Figure 4–5 Oracle Identity Administration Server Diagnostics Screen



Server Diagnostics

Please select Identity Server(s) on which you would like to run diagnostics

● All Identity Servers

○ Selected Identity Servers

idserver4 (idmhost1.pdx.com:6022)
idserver5 (idmhost2.pdx.com:6022)

Status of the Identity servers

Identity Server	Server State	Installation Directory	Number of Threads	Directory Information								
				Directory	Host:Port	State	Priority	Mode	Size Limit	Time Limit	Login DN	Create Time
idserver4 (idmhost1.pdx.com:6022)	Up	/home/oracleqa/edg/netpoint/identity	20	User	oidhost1.pdx.com:389	Up	0	OPEN,REFERRAL,PRIMARY	0	0	cn=orcladmin	April 25 2006 11:25 am
				User	oidhost2.pdx.com:389	Down	0	OPEN,SECONDARY	0	0	cn=orcladmin	April 17 2006 01:01 pm
				Configuration Data	oidhost1.pdx.com:389	Up	0	OPEN,PRIMARY	0	0	cn=orcladmin	April 25 2006 11:25 am
				Configuration Data	oidhost2.pdx.com:389	Down	0	OPEN,SECONDARY	0	0	cn=orcladmin	April 17 2006 01:01 pm
idserver5 (idmhost2.pdx.com:6022)	Up	/home/oracleqa/edg/netpoint/identity	20	Directory	Host:Port	State	Priority	Mode	Size Limit	Time Limit	Login DN	Create Time
				User	oidhost2.pdx.com:389	Up	0	OPEN,REFERRAL,PRIMARY	0	0	cn=orcladmin	April 17 2006 01:55 pm
				User	oidhost1.pdx.com:389	Down	0	OPEN,SECONDARY	0	0	cn=orcladmin	April 17 2006 01:48 pm
				Configuration Data	oidhost2.pdx.com:389	Up	0	OPEN,PRIMARY	0	0	cn=orcladmin	April 17 2006 01:55 pm
				Configuration Data	oidhost1.pdx.com:389	Down	0	OPEN,SECONDARY	0	0	cn=orcladmin	April 17 2006 01:48 pm

4.22 Configuring Oracle WebCenter Services User Roles for Oracle COREid Access and Identity

You must update the system `system-jazn-data.xml` file to include specific user roles: `page-customizer`, `page-personalizer` and `page-viewer`. In the `system-jazn-data.xml` file, the difference between a file-based security provider and Oracle COREid Access and Identity is that the `grantee` element does not have `realm-name` and `type` subelements, and if the name is simply `users` (as opposed to `jazn.com/users`). The grant in Example 4–4 is configured for Oracle COREid Access and Identity. Note also that the class `oracle.security.jazn.spi.xml.XMLRealmRole` is changed to `oracle.security.jazn.realm.CoreIDPrincipal`.

Example 4–4 system-jazn-data.xml file for use with Oracle COREid Access and Identity

```
<grant>
    <grantee>
      <principals>
        <principal>
        <class>oracle.security.jazn.realm.CoreIDPrincipal</class>
        <name>page-viewer</name>
        </principal>
      </principals>
    </grantee>
    <permissions>
      <permission>
        <class>oracle.adf.share.security.authorization.MethodPermission</class>
        <name>testjcr.getItems</name>
        <actions>invoke</actions>
      </permission>
      <permission>
        <class>oracle.adf.share.security.authorization.MethodPermission</class>
        <name>testjcr.advancedSearch</name>
         <actions>invoke</actions>
      </permission>
      <permission>
        <class>oracle.adf.share.security.authorization.RegionPermission</class>
        <name>view.pageDefs.PortalExtAppPageDef</name>
        <actions>view</actions>
      </permission>
       ...
    </permissions>
</grant>
```

5

Installing and Configuring OracleAS Single Sign-On and Oracle Delegated Administration Services

5.1 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 sso.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.

5.2 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.

5.2.1 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
```

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.

11. Select OracleAS Infrastructure 10g and click **Next**.

    The **Select Installation Type** screen appears.

12. Select **Identity Management** 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.

14. Select **OracleAS Single Sign-On, Oracle Delegated Administration Services**, and **High Availability and Replication**

    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.

16. Select **OracleAS Cluster (Identity Management)** and click **Next**.

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

17. Select **Create a New OracleAS Cluster** and click **Next**.

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

18. Complete the **New OracleAS Cluster Name** field with a name for the cluster 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.

19. Enter the name of the Load Balancing Router, the SSL port, and the non-SSL port.

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.

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.

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.

5.2.2 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. Stop all components on OIDHOST2, using this command:

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

5. Ensure that all components on OIDHOST1 are running:

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

6. Access the following URL:

   https://IDMHOST2.mycompany.com/pls/orasso

5.2.3 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
```

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.

11. Select **OracleAS Infrastructure 10**g, and click **Next**.

    The **Select Installation Type** screen appears.

12. Select **Identity Management** 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.

14. Select **OracleAS Single Sign-On, Oracle Delegated Administration Services**, and **High Availability and Replication**.

15. Click **Next**.

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

16. Select **OracleAS Cluster (Identity Management)** and click **Next**.

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

17. Select **Join an Existing OracleAS Cluster** and click **Next**.

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

18. Complete the **Existing OracleAS Cluster Name** field with the name you provided for the cluster when installing the first instance and click **Next**.

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

19. Enter the name of the Load Balancing Router, the SSL port, and the non-SSL port.

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.

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.

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.

5.3 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 sso.mycompany.com 443
   ```

   In the preceding command, *sso.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 sso.mycompany.com:443

   -remote_midtier

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

   -mod_osso_url https://sso.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 **sso.mycompany.com** and port **443**.

Apache 1.3:

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

Apache 2.0:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName sso.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.

5.4 Testing the Identity Management Tier Components

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

1. Stop all components on IDMHOST1, using this command:

   ```
   ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

2. Ensure that all components on IDMHOST2 are running, using this command:

   ```
   ORACLE_HOME/opmn/bin/opmnctl status
   ```

3. Access the following URLs from two browsers:

   ```
   https://sso.mycompany.com/pls/orasso
   ```

   ```
   https://sso.mycompany.com/oiddas
   ```

4. Start all components from IDMHOST1, using this command:

```
ORACLE_HOME/opmn/bin/opmnctl startall
```

5. Stop all components on IDMHOST2, using this command:

   ```
   ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

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

5.5 Configuring Session State Replication for the OC4J_SECURITY Instance

1. Access the Application Server Control Console at `http://`*`hostname`*`:`*`port`*`/em/` and log in with the oc4jadmin password set during installation.

   The **Cluster Topology** page appears.

2. Select the OC4J_SECURITY instance.

   The OC4J_SECURITY page appears.

3. Click **Applications**.

   The applications for the instance appear.

4. Select the `default` application.

   The **Application: default** page appears.

5. Click **Administration**.

   The administration tasks are listed.

6. Click the **Go To Task** icon for Clustering Properties.

   The Clustering Properties page appears.

7. Select **Enable** from the **Clustering** drop-down list.

   The Replication Protocol choices appear.

8. Select **Peer-Peer**.

9. Scroll downward and click the **+** before **Replication Properties**.

   The replication properties are listed.

10. If applicable, select and specify replication properties.

11. Click **OK**.

    The Application: default page appears with a confirmation message that the changes were applied.

12. Click the **Cluster Topology** link.

    The Cluster Topology page appears.

13. Select the checkbox next to the OC4J_SECURITY instance and click **Restart**.

    A confirmation message appears.

14. Click **Yes**.

    A progress message appears, then the Cluster Topology page appears with a message that the instance was restarted.

5.6 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

6
Maintaining the WebCenter Suite

6.1 Managing the WebCenter Suite

Common administration operations are listed in Table 6–1. You can monitor and manage the system using consoles or command line tools.

Table 6–1 System administration tasks, tools, and related documentation

Task or operation	Tool	Where documented
Access the Application Server Control Console	Application Server Control Console	*Oracle Application Server Administrator's Guide*
Start and stop Oracle Application Server	Application Server Control Console	*Oracle Application Server Administrator's Guide*
Create and delete OC4J instances	Application Server Control Console	*Oracle Application Server Administrator's Guide*
List and view log files	Application Server Control Console	*Oracle Application Server Administrator's Guide*
Back up and restore instances	Command line	*Oracle Application Server Administrator's Guide*
Change hostname, domain name, or IP address	Command line	*Oracle Application Server Administrator's Guide*
Manage wallets and Certificate Revocation Lists	Command line	*Oracle Application Server Administrator's Guide*

6.2 Enabling Disaster Recovery

For recommendations and instructions on enabling disaster recovery, see the *Oracle Application Server High Availability Guide*

Index