Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle Business Intelligence

11*g* Release 1 (11.1.1)

E15722-03

June 2011

ORACLE®

Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence, 11*g* Release 1 (11.1.1)

E15722-03

Contents

6   Scaling Out the Oracle Business Intelligence System

10   Managing Enterprise Deployments

Index

Preface

This preface describes the audience, contents, and conventions used in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence*.

Audience

This document is intended for system administrators who are responsible for installing and configuring Oracle Business Intelligence enterprise deployments.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For related information, see the following documents in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1) documentation set:

- *Oracle Fusion Middleware Release Notes* for your platform

- *Oracle Fusion Middleware High Availability Guide*

- *Oracle Fusion Middleware Administrator's Guide*

- *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Real-Time Decisions*

- *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence*

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

- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher*

Conventions

The following text conventions are used in this document:

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

1

Enterprise Deployment Overview

This chapter provides an overview of the enterprise topology for Oracle Business Intelligence.

> **Important:** Oracle strongly recommends that you read *Oracle Fusion Middleware Release Notes* for any additional installation and deployment considerations before starting the setup process.

This chapter contains the following topics:

1.1 What Is an Enterprise Deployment?

This Enterprise Deployment Guide defines an architectural blueprint that captures Oracle's recommended best practices for a highly available and secure Oracle Business Intelligence deployment. The best practices described in this blueprint use Oracle products from across the technology stack, including Oracle Database, Oracle Fusion Middleware, and Oracle Enterprise Manager. The resulting enterprise deployment can be readily scaled out to support increasing capacity requirements.

In particular, an Oracle Business Intelligence enterprise deployment:

- Considers various business service level agreements (SLAs) to make high-availability best practices as widely applicable as possible
- Leverages database grid servers and storage grids with low-cost storage to provide highly resilient, lower-cost infrastructure
- Uses results from extensive performance impact studies for different configurations to ensure that the high-availability architecture is optimally configured to perform and scale to business needs
- Enables control over the length of time to recover from an outage and the amount of acceptable data loss from a natural disaster
- Uses Oracle best practices and recommended architecture that are independent of hardware and operating systems

For more information on high availability practices, go to:

> **Note:** This document focuses on enterprise deployments in Linux environments, but enterprise deployments can also be implemented in UNIX and Windows environments.

1.2 Terminology

The following terms are used in this document:

- **Oracle home:** Contains installed files necessary to host a specific product. For example, the Oracle Business Intelligence Oracle home contains a directory that contains binary and library files for Oracle Business Intelligence. An Oracle home resides within the directory structure of the Middleware home. Each Oracle home can be associated with multiple Oracle instances or Oracle WebLogic Server domains.

- **WebLogic Server home:** Contains installed files necessary to host an Oracle WebLogic Server. The WebLogic Server home directory is a peer of the Oracle home directories and resides within the directory structure of the Middleware home.

- **Middleware home:** Consists of the WebLogic Server home, and, optionally, one or more Oracle homes. A Middleware home can reside on a local file system or on a remote shared disk that is accessible through NFS.

- **Oracle instance:** Contains one or more active middleware system components, such as Oracle BI Server, Oracle BI Presentation Services, Oracle HTTP Server, or Oracle Internet Directory. You determine which components are part of an instance, either at install time or by creating and configuring an instance at a later time. An Oracle instance contains files that can be updated, such as configuration files, log files, and temporary files.

- **failover:** The process that occurs when a member of a high availability system fails unexpectedly (unplanned downtime), so that the system can continue offering services to its consumers. If the system is an active-passive system, the passive member is activated during the failover operation and consumers are directed to it instead of the failed member. The failover process can be performed manually, or it can be automated by setting up hardware cluster services to detect failures and move cluster resources from the failed node to the standby node. If the system is an active-active system, the failover is performed by the load balancer entity serving requests to the active members. If an active member fails, the load balancer detects the failure and automatically redirects requests for the failed member to the surviving active members. See *Oracle Fusion Middleware High Availability Guide* for information on active-active and active-passive systems.

- **failback:** The process that occurs after a system undergoes a successful failover operation. In the failback process, the original failed member is repaired over time and is then reintroduced into the system as a standby member. Optionally, a failback process can be initiated to activate this member and deactivate the other. This process reverts the system back to its pre-failure configuration.

- **hardware cluster:** A collection of computers that provides a single view of network services (for example, an IP address) or application services (for example, databases and Web servers) to clients of these services. Each node in a hardware cluster is a standalone server that runs its own processes. These processes can

communicate with one another to form what looks like a single system that cooperatively provides applications, system resources, and data to users.

A hardware cluster achieves high availability and scalability with specialized hardware (cluster interconnect, shared storage) and software (health monitors, resource monitors). (The cluster interconnect is a private link used by the hardware cluster for heartbeat information to detect node death.) Due to the need for specialized hardware and software, hardware clusters are commonly provided by hardware vendors such as Sun, HP, IBM, and Dell. While the number of nodes that can be configured in a hardware cluster is vendor dependent, for the purpose of Oracle Fusion Middleware high availability, only two nodes are required. Hence, this document assumes a two-node hardware cluster for high availability solutions employing a hardware cluster.

- **cluster agent:** The software that runs on a node member of a hardware cluster that coordinates availability and performance operations with other nodes. Clusterware provides resource grouping, monitoring, and the ability to move services. A cluster agent can automate the service failover.

- **clusterware:** Software that manages the operations of the members of a cluster as a system. It enables you to define a set of resources and services to monitor through a heartbeat mechanism between cluster members and to move these resources and services to a different member in the cluster as efficiently and transparently as possible.

- **shared storage:** The storage subsystem that is accessible by all the computers in the enterprise deployment. Among other things, the following is located on the shared disk:

  - Middleware home software

  - Administration Server domain home

  - JMS

  - Tlogs (where applicable)

  Managed Server homes can also be optionally located in the shared disk. The shared storage can be a Network Attached Storage (NAS), a Storage Area Network (SAN), or any other storage system that multiple nodes can access simultaneously and can read/write.

- **primary node:** The node that is actively running an Oracle Fusion Middleware instance at any given time and has been configured to have a backup/secondary node. If the primary node fails, the applicable Oracle Fusion Middleware components are failed over to the secondary node. This failover can be manual, or automated using the Clusterware for Administration Server. For a server migration-based scenario, WebLogic Whole Server Migration is used for automated failover.

- **secondary node:** The node that is the backup node for an Oracle Fusion Middleware instance. This is where the active instance fails over when the primary node is no longer available. See the definition for primary node in this section.

- **network host name:** A name assigned to an IP address either through the /etc/hosts file or through DNS resolution. This name is visible in the network where the computer to which it refers is connected. Often, the network host name and physical host name are identical. However, each computer has only one physical host name, but may have multiple network host names. Thus, a computer's network host name may not always be its physical host name.

- **physical host name:** The "internal name" of the current computer. On UNIX, this is the name returned by the hostname command. Note that this document differentiates between the terms physical host name and network host name.

  Oracle Fusion Middleware uses the physical host name to reference the local host. During installation, the installer automatically retrieves the physical host name from the current computer and stores it in the Oracle Fusion Middleware configuration metadata on disk.

- **physical IP:** The IP address of a computer on the network. In most cases, it is normally associated with the physical host name of the computer (see the definition for physical host name). In contrast to a virtual IP, it is always associated with the same computer when on a network.

- **switchover:** A process that occurs during normal operation when active members of a system might require maintenance or upgrading. A switchover process can be initiated to enable a substitute member to take over the workload performed by the member that requires maintenance or upgrading, which undergoes planned downtime. The switchover operation ensures continued service to consumers of the system.

- **switchback:** The process that occurs after a system undergoes a successful switchover operation, in which a member of the system is deactivated for maintenance or upgrading. When the maintenance or upgrade is completed, the system can undergo a switchback operation to activate the upgraded member and bring the system back to the pre-switchover configuration.

- **virtual host name:** A network addressable host name that maps to one or more physical computers through a load balancer or a hardware cluster. For load balancers, the name "virtual server name" is used interchangeably with virtual host name in this document. A load balancer can hold a virtual host name on behalf of a set of servers, and clients communicate indirectly with the computers using the virtual host name. A virtual host name in a hardware cluster is a network host name assigned to a cluster virtual IP. Because the cluster virtual IP is not permanently attached to any particular node of a cluster, the virtual host name is not permanently attached to any particular node either.

  > **Note:** Whenever the term "virtual host name" is used in this document, it is assumed to be associated with a virtual IP address. In cases where just the IP address is needed or used, it is explicitly stated.

- **virtual IP:** A virtual IP address that can be assigned to a hardware cluster or load balancer. To present a single system view of a cluster to network clients, a virtual IP serves as an entry point IP address to the group of servers which are members of the cluster. A virtual IP can be assigned to a server load balancer or a hardware cluster. Virtual IP is also called cluster virtual IP and load balancer virtual IP.

  A hardware cluster uses a cluster virtual IP to present to the outside world the entry point into the cluster (it can also be set up on a standalone computer). The hardware cluster's software manages the movement of this IP address between the two physical nodes of the cluster while clients connect to this IP address without the need to know which physical node this IP address is currently active on. In a typical two-node hardware cluster configuration, each computer has its own physical IP address and physical host name, while there could be several cluster IP addresses. These cluster IP addresses float or migrate between the two nodes. The node with current ownership of a cluster IP address is active for that address.

A load balancer also uses a virtual IP as the entry point to a set of servers. These servers tend to be active at the same time. This virtual IP address is not assigned to any individual server but to the load balancer which acts as a proxy between servers and their clients.

In addition to the terms defined in this section, this Enterprise Deployment Guide assumes knowledge of general Oracle Fusion Middleware and Oracle WebLogic Server concepts and architecture. See *Oracle Fusion Middleware Administrator's Guide* for more information.

1.3 Benefits of Oracle Recommendations

The Oracle Fusion Middleware configurations discussed in this document are designed to ensure security of all invocations, maximize hardware resources, and provide a reliable, standards-compliant system for Oracle Business Intelligence.

The security and high availability benefits of the Oracle Fusion Middleware configurations are realized through isolation in firewall zones and replication of software components.

This section contains the following topics:

- Section 1.3.1, "Built-in Security"
- Section 1.3.2, "High Availability"

1.3.1 Built-in Security

The Enterprise Deployment architectures are secure because every functional group of software components is isolated in its own demilitarized zone (DMZ), and all traffic is restricted by protocol and port. A DMZ is a perimeter network that exposes external services to a larger untrusted network.

The following characteristics ensure security at all needed levels and a high level of standards compliance:

- External load balancers are configured to redirect all external communication received on port 80 to port 443.

  > **Note:**   You can find a list of validated load balancers and their configuration on the Oracle Technology Network at:
  >
  > http://www.oracle.com/technology/products/ias/hi_av/Tested_ LBR_FW_SSLAccel.html

- 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 is allowed.

- Components are separated in different protection zones: 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.

- Identity Management components are in a separate subnet.

- All communication between components across protection zones is restricted by port and protocol, according to firewall rules.

1.3.2 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.

1.4 Hardware Requirements

Typical hardware requirements for the Enterprise Deployment on Linux operating systems are listed in Table 1–1.

For detailed requirements, or for requirements for other platforms, see the *Oracle Fusion Middleware Installation Guide* for that platform.

Table 1–1   Typical Hardware Requirements

Server	Processor	Disk	Memory	TMP Directory	Swap
Database	4 or more X Pentium, 1.5 GHz or greater	nXm n = number of disks, at least 4 (striped as one disk) m = size of the disk (minimum of 30 GB)	6-8 GB	Default	Default
WEBHOST*n*	2 or more X Pentium, 1.5 GHz or greater	10 GB	4 GB	Default	Default
APPHOST*n*	1 dual-core Pentium, 2.8 GHz or greater	20 GB or more	8 GB	Default	Default

1.5 Enterprise Deployment Reference Topology

The instructions and diagrams in this document describe a reference topology, to which variations may be applied.

This document provides configuration instructions for a reference enterprise topology that uses Oracle Business Intelligence with Oracle Access Manager, as shown in Figure 1–1.

Figure 1–1   MyBICompany Topology with Oracle Access Manager
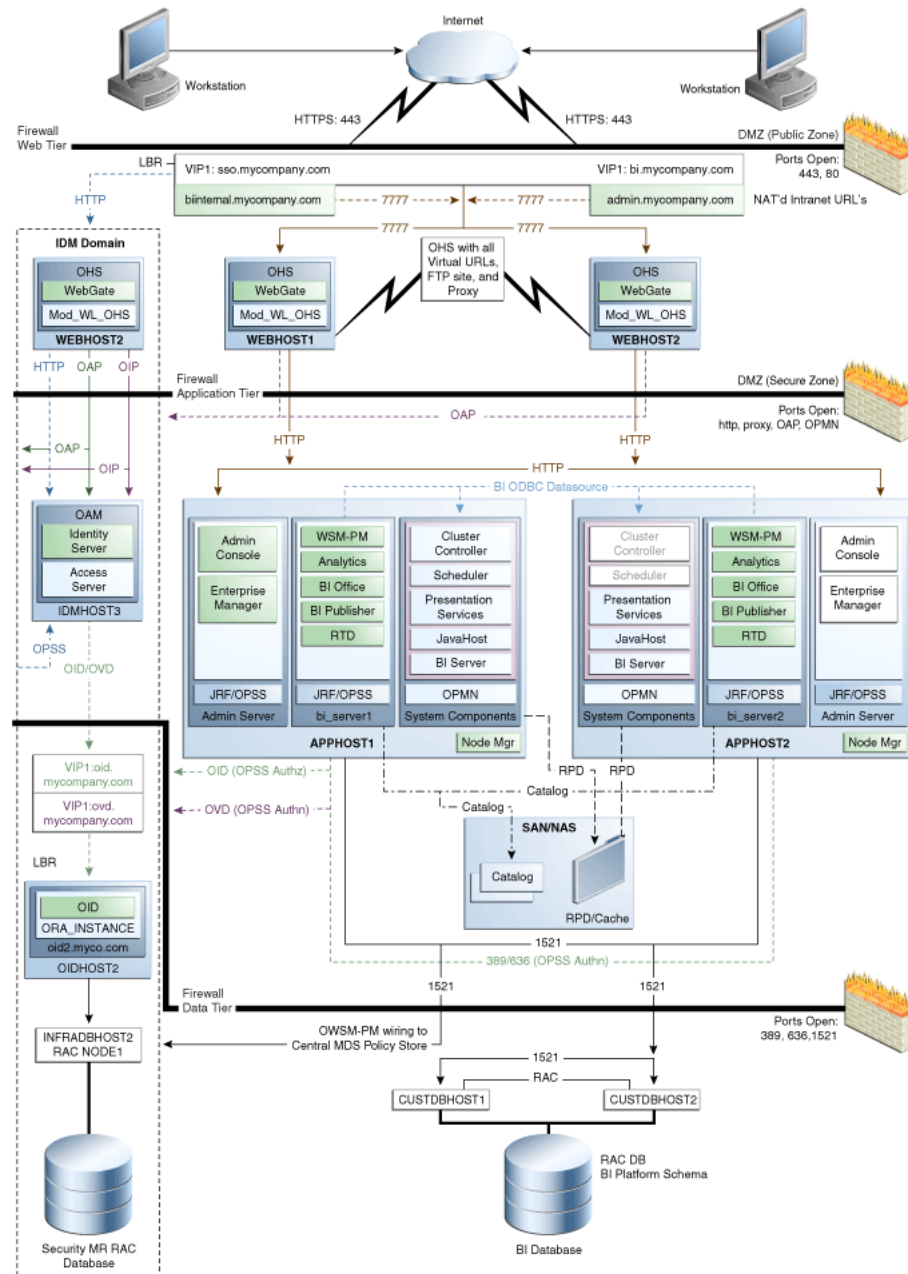
This section covers the following topics:

- Section 1.5.1, "Oracle Identity Management"

- Section 1.5.2, "Web Tier"

- Section 1.5.3, "Application Tier"

- Section 1.5.4, "Data Tier"

- Section 1.5.5, "What to Install"

- Section 1.5.6, "Unicast Requirement"

1.5.1 Oracle Identity Management

Integration with the Oracle Identity Management system is an important aspect of the enterprise deployment architecture. This integration provides features such as single sign-on, integration with OPSS, centralized identity and credential store, authentication for the WebLogic domain, and so on. The IDM (Identity Management) EDG is separate from this EDG and exists in a separate domain by itself. For more information on identity management in an enterprise deployment context, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

The primary interface to the IDM EDG is the LDAP traffic to the LDAP servers, the OAP (Oracle Access Protocol) to the OAM Access Servers, and the HTTP redirection of authentication requests.

1.5.2 Web Tier

Nodes in the Web tier are located in the DMZ public zone.

In this tier, two nodes, WEBHOST1 and WEBHOST2, run Oracle HTTP Server configured with WebGate and mod_wl_ohs.

Through mod_wl_ohs, which allows requests to be proxied from Oracle HTTP Server to Oracle WebLogic Server, Oracle HTTP Server forwards the requests to Oracle WebLogic Server running in the application tier.

WebGate (which is an Oracle Access Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running on OAMHOST2, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.

The Web tier also includes a load balancer router to handle external requests. External requests are sent to the virtual host names configured on the load balancer. The load balancer then forwards the requests to Oracle HTTP Server.

The WebGate module in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager to perform operations such as querying user groups.

On the firewall protecting the Web tier, only the HTTP ports are open: 443 for HTTPS, and 80 for HTTP.

1.5.2.1 Load Balancer Requirements

This enterprise topology uses an external load balancer. This external load balancer should have the following features:

- Ability to load-balance traffic to a pool of real servers through a virtual host name

  Clients access services using the virtual host name (instead of using actual host names). The load balancer can then load balance requests to the servers in the pool.

- Port translation configuration

  This feature is necessary so that incoming requests on the virtual host name and port are directed to a different port on the back-end servers.

- Monitoring of ports on the servers in the pool to determine the availability of a service

- Ability to configure virtual server names and ports

  Note the following requirements:

- The load balancer should allow configuration of multiple virtual servers. For each virtual server, the load balancer should allow configuration of traffic management on multiple ports. For example, for Oracle HTTP Server in the Web tier, the load balancer must be configured with a virtual server and ports for HTTP and HTTPS traffic.

  - The virtual server names must be associated with IP addresses and be part of your DNS. Clients must be able to access the external load balancer through the virtual server names.

- Ability to detect node failures and immediately stop routing traffic to the failed node

- Fault-tolerant mode

  It is highly recommended that you configure the load balancer to be in fault-tolerant mode.

- Ability to configure the virtual server to return immediately to the calling client

  It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the back-end services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client computer.

- Sticky routing capability

  Sticky routing capability is the ability to maintain sticky connections to components. Examples of this include cookie-based persistence, IP-based persistence, and so on.

- SSL acceleration

  The load balancer should be able to terminate SSL requests at the load balancer and forward traffic to the back-end real servers using the equivalent non-SSL protocol (for example, HTTPS to HTTP). Typically, this feature is called SSL acceleration and it is required for this EDG.

1.5.3 Application Tier

Nodes in the application tier are located in the DMZ secure zone.

APPHOST1 and APPHOST2 run the Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control, but in an active-passive configuration. You can fail over the Administration Server manually (see Section 5.14, "Manually Failing Over the Administration Server to APPHOST2"); alternatively you can configure the Administration Console with CFC/CRS to fail over automatically on a separate hardware cluster (not shown in this architecture).

The Oracle Business Intelligence Cluster Controller and Oracle BI Scheduler system components run on APPHOST1 and APPHOST2 in an active-passive configuration. The other Oracle Business Intelligence system components, Oracle BI Server, Oracle BI JavaHost, and Oracle BI Presentation Services, run on APPHOST1 and APPHOST2 in an active-active configuration. All system components are managed by OPMN and do not run in the Managed Servers.

The Oracle Business Intelligence Java components, including Oracle Real-Time Decisions, Oracle BI Publisher, Oracle BI for Microsoft Office, and the Oracle BI Enterprise Edition Analytics application, run in the two Managed Servers on APPHOST1 and APPHOST2. Oracle Web Services Manager (Oracle WSM) is another Java component that provides a policy framework to manage and secure Web services

in the EDG topology. WSM Policy Manager runs in active-active configuration in the two Managed Servers in APPHOST1 and APPHOST2.

1.5.4 Data Tier

Nodes in the data tier are located in the most secured network zone (the intranet).

In this tier, an Oracle RAC database runs on the nodes CUSTDBHOST1 and CUSTDBHOST2. The database contains the schemas needed by the Oracle Business Intelligence components. The Oracle Business Intelligence components running in the application tier access this database.

On the firewall protecting the data tier, the database listener port (typically, 1521) is required to be open. The LDAP ports (typically, 389 and 636) are also required to be open for the traffic accessing the LDAP storage in the IDM EDG.

1.5.5 What to Install

Table 1–2 identifies the source for installation of each software component. For more information, see *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence*.

Table 1–2   Components and Installation Sources

Component	Distribution Medium
Oracle Database 10*g* or 11*g*	Oracle Database CD (in 10*g* series, 10.2.0.4 or higher; in 11*g* series, 11.1.0.7 or higher)
Repository Creation Utility (RCU)	Oracle Fusion Middleware Repository Creation Utility 11*g* (11.1.1.1.0) DVD
Oracle WebLogic Server (WLS)	Oracle Weblogic Server (10.3.1) DVD
Oracle HTTP Server	Oracle Fusion Middleware WebTier and Utilities 11*g* (11.1.1.1.0) DVD
Oracle Business Intelligence	Oracle Business Intelligence 11*g* (11.1.1.5.0) DVD
Oracle Access Manager 10*g* Webgate	Oracle Access Manager 10*g* Webgates (10.1.4.3.0) DVD; OAM OHS 11*g* Webgates per platform
Oracle Virtual Directory (OVD)	Oracle Identity Management 11*g* (11.1.1.1.0) DVD

1.5.6 Unicast Requirement

Oracle recommends that the nodes in the MyBICompany topology communicate using unicast. Unlike multicast communication, unicast does not require cross-network configuration and it reduces potential network errors that can occur from multicast address conflicts as well.

The following considerations apply when using unicast to handle cluster communications:

- All members of a WebLogic cluster must use the same message type. Mixing between multicast and unicast messaging is not allowed.

- Individual cluster members cannot override the cluster messaging type.

- The entire cluster must be shut down and restarted to change the message modes (from unicast to multicast or from multicast to unicast).

- JMS topics configured for multicasting can access WebLogic clusters configured for unicast because a JMS topic publishes messages on its own multicast address that is independent of the cluster address. However, the following considerations apply:

  - The router hardware configurations that allow unicast clusters may not allow JMS multicast subscribers to work.

  - JMS multicast subscribers must be in a network hardware configuration that allows multicast accessibility. (That is, JMS subscribers must be in a multicast-enabled network to access multicast topics.)

2

Database and Environment Preconfiguration

This chapter describes database and network environment preconfiguration required by the Oracle Business Intelligence enterprise topology, as well as recommendations for shared storage and directory structure.

> **Important:** Oracle strongly recommends that you read *Oracle Fusion Middleware Release Notes* for any additional installation and deployment considerations before starting the setup process.

This chapter contains the following topics:

- Section 2.1, "Database Environment Preconfiguration"
- Section 2.2, "Network Environment Preconfiguration"
- Section 2.3, "Shared Storage and Recommended Directory Structure"
- Section 2.4, "Clock Synchronization"

2.1 Database Environment Preconfiguration

You must install a database and then load the Oracle Business Intelligence schemas into it before you can configure the Oracle Fusion Middleware components. You load the Oracle Business Intelligence schemas using the Repository Creation Utility (RCU).

For the enterprise topology, an Oracle Real Application Clusters (Oracle RAC) database is highly recommended to achieve a highly available data tier. When you install Oracle Business Intelligence, the installer prompts you to enter the information for connecting to the database that contains the required schemas.

This section covers the following topics:

- Section 2.1.1, "Setting Up the Database"
- Section 2.1.2, "Loading the Oracle Business Intelligence Schemas in the Oracle RAC Database"
- Section 2.1.3, "Backing Up the Database"

2.1.1 Setting Up the Database

Before loading the Oracle Business Intelligence schemas into your database, ensure that the database meets the requirements described in the following sections:

- Section 2.1.1.1, "Database Host Requirements"
- Section 2.1.1.2, "Supported Database Versions"

- Section 2.1.1.3, "Database Services"

2.1.1.1 Database Host Requirements

On the hosts CUSTDBHOST1 and CUSTDBHOST2 in the data tier, note the following requirements:

- Oracle Clusterware

  For 11*g* Release 1 (11.1) for Linux, refer to *Oracle Clusterware Installation Guide for Linux.*

- Oracle Real Application Clusters

  For 11*g* Release 1 (11.1) for Linux, refer to *Oracle Real Application Clusters Installation Guide for Linux and UNIX*. For 10*g* Release 2 (10.2) for Linux, refer to *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux*.

- Automatic Storage Management (optional)

  ASM is installed for the node as a whole. It is recommended that you install it in a separate Oracle home from the Oracle Database Oracle home. You can select this option when running the runInstaller. In the Select Configuration page, select the **Configure Automatic Storage Management** option to create a separate Oracle home for ASM.

2.1.1.2 Supported Database Versions

Oracle Business Intelligence requires the presence of a supported database and schemas. To check if your database is certified or to see all certified databases, refer to the "Oracle Fusion Middleware 11g Release 1 (11.1.1.x)" product area on the Oracle Fusion Middleware Supported System Configurations page on the Oracle Technology Network at:

http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html

To check the release of your database, you can query the PRODUCT_COMPONENT_VERSION view as follows:

Example 2–1

```
SQL> SELECT VERSION FROM SYS.PRODUCT_COMPONENT_VERSION WHERE PRODUCT LIKE
'%Oracle%';
```

> **Note:** The database you use as the Oracle Business Intelligence supporting database (either Oracle Database 10*g* or 11*g*) must support the AL32UTF8 character set. Check the database documentation for information on choosing a character set for the database.

2.1.1.3 Database Services

Oracle recommends using the Oracle Enterprise Manager Cluster Managed Services Page to create database services that client applications can use to connect to the database. For complete instructions on creating database services, see the chapter on workload management in the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*.

You can also use SQL*Plus to configure the database services, as follows:

1. Use the `CREATE_SERVICE` subprogram to create the biedg.mycompany.com database service. Log onto SQL*Plus as the SYSDBA user and run the following command:

```
SQL> EXECUTE DBMS_SERVICE.CREATE_SERVICE (SERVICE_NAME =>
'biedg.mycompany.com', NETWORK_NAME => 'biedg.mycompany.com');
```

2. Add the service to the database and assign it to the instances using srvctl:

```
prompt> srvctl add service -d custdb -s biedg -r custdb1,custdb2
```

3. Start the service using srvctl:

```
prompt> srvctl start service -d custdb -s biedg
```

> **Note:** For more information about the SRVCTL command, see *Oracle Real Application Clusters Administration and Deployment Guide*.

Oracle recommends that a specific database service be used for a product suite even when they share the same database. It is also recommended that the database service used is different than the default database service. In this case, the database is custdb.mycompany.com and the default service is one with the same name. The Oracle Business Intelligence installer is configured to use the service biedg.mycompany.com.

2.1.2 Loading the Oracle Business Intelligence Schemas in the Oracle RAC Database

Perform these steps to load the Oracle Business Intelligence schemas into your database:

1. Insert the Repository Creation Utility (RCU) DVD, and then start RCU from the bin directory in the RCU home directory.

```
prompt> cd RCU_HOME/bin
prompt> ./rcu
```

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

3. In the Create Repository screen, select **Create** to load component schemas into a database. Click **Next**.

4. In the Database Connection Details screen, enter connect information for your database:

   - **Database Type**: Select **Oracle Database**.

   - **Host Name**: Specify the name of the node on which the database resides. For the Oracle RAC database, specify the VIP name or one of the node names as the host name: CUSTDBHOST1-VIP.

   - **Port**: Specify the listen port number for the database: 1521.

   - **Service Name**: Specify the service name of the database (biedg.mycompany.com).

   - **Username**: Specify the name of the user with DBA or SYSDBA privileges: SYS.

   - **Password**: Enter the password for the SYS user.

   - **Role**: Select the database user's role from the list: SYSDBA (required by the SYS user).

   Click **Next**.

5. In the Select Components screen, do the following:

■ Select **Create a new Prefix**, and then enter a prefix to use for the database schemas (for example, `DEV` or `PROD`). You can specify up to six characters as a prefix. Prefixes are used to create logical groupings of multiple repositories in a database. For more information, see *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

> **Tip:** Note the name of the schema, because the upcoming steps require this information.

■ Select the following components:

– **AS Common Schemas: Metadata Services** (automatically selected)

– **Oracle Business Intelligence: Business Intelligence Platform**

Click **Next**.

Figure 2–1 shows the Select Components screen.

Figure 2–1   Repository Creation Utility Select Components Screen

6. In the Schema Passwords screen, enter passwords for the main schema users, and click **Next**.

You can choose either **Use same passwords for all schemas** or **Specify different passwords for all schemas**, depending on your requirements.

Do not select **Use main schema passwords for auxiliary schemas**. The auxiliary passwords are derived from the passwords of the main schema users.

> **Tip:** Note the names of the schema passwords, because the upcoming steps require this information.

7. In the Map Tablespaces screen, choose the tablespaces for the selected components, and click **Next**.

8. In the Summary screen, click **Create**.

9. In the Completion Summary screen, click **Close**.

> **Note:** Oracle recommends using the database used for identity management (see Chapter 9, "Integrating with Oracle Identity Management") to store the Oracle WSM policies. It is therefore expected that you will use the identity management database information for the OWSM MDS schemas, which will be different from the one used for the rest of the BI schemas. To create the required schemas in the identity management database, repeat the preceding steps using the identity management database information, but select only "AS Common Schemas: Metadata Services" in the Select Components screen (step 5).

2.1.3 Backing Up the Database

After you have loaded the Oracle Business Intelligence schemas in your database, you should make a backup.

Backing up the database enables you to quickly recover from any issues that may occur in subsequent steps. You can choose to use your database backup strategy for this purpose, or you can simply make a backup using operating system tools or Oracle Recovery Manager (RMAN). It is recommended that you use RMAN for the database, particularly if the database was created using Oracle ASM. If possible, you can also perform a cold backup using operating system tools such as tar.

2.2 Network Environment Preconfiguration

You must ensure that every computer where you plan to run Oracle Business Intelligence can access (ping) the primary host computer of your cluster using its fully qualified domain name. For the installation to succeed, every computer on which you scale out your installation must be able to support bidirectional communication with the Administration Server on the cluster's primary host.

This section contains the following topics:

- Section 2.2.1, "Virtual Server Names"
- Section 2.2.2, "Load Balancers"
- Section 2.2.3, "IPs and Virtual IPs"
- Section 2.2.4, "Firewalls and Ports"

2.2.1 Virtual Server Names

The BI enterprise topology uses the following virtual server names:

- bi.mycompany.com
- admin.mycompany.com

■ biinternal.mycompany.com

Ensure that the virtual server names are associated with IP addresses and are part of your DNS. The nodes running Oracle Fusion Middleware must be able to resolve these virtual server names.

2.2.1.1 bi.mycompany.com

bi.mycompany.com is a virtual server name that acts as the access point for all HTTP traffic to the run-time Oracle BI components. Traffic to SSL is configured. Clients access this service using the address bi.mycompany.com:443. This virtual server is defined on the load balancer.

2.2.1.2 admin.mycompany.com

admin.mycompany.com is a virtual server name that acts as the access point for all internal HTTP traffic that is directed to administration services such as Oracle WebLogic Administration Server Console and Oracle Enterprise Manager.

The incoming traffic from clients is not SSL-enabled. Clients access this service using the address admin.mycompany.com:80 and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2. This virtual server is defined on the load balancer.

2.2.1.3 biinternal.mycompany.com

biinternal.mycompany.com is a virtual server name used for internal invocation of BI services. This URL is not exposed to the internet and is only accessible from the intranet.

The incoming traffic from clients is not SSL-enabled. Clients access this service using the address biinternal.mycompany.com:80 and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2. This virtual server is defined on the load balancer.

2.2.2 Load Balancers

This enterprise topology uses an external load balancer. For more information on load balancers, see Chapter 4, "Configuring the Web Tier."

> **Note:** The Oracle Technology Network (http://www.oracle.com/technology) provides a list of validated load balancers and their configuration at:
>
> http://www.oracle.com/technology/products/ias/hi_av/Tested_
> LBR_FW_SSLAccel.html

Configuring the Load Balancer
Perform these steps to configure the load balancer:

1. Create a pool of servers. You will assign this pool to virtual servers.

2. Add the addresses of the Oracle HTTP Server hosts to the pool. For example:

   ■ WEBHOST1:7777

   ■ WEBHOST2:7777

3. Configure a virtual server in the load balancer for bi.mycompany.com:443.

   ■ For this virtual server, use your system's frontend address as the virtual server address (for example, bi.mycompany.com). The frontend address is the

externally facing host name used by your system and that will be exposed in the Internet.

- Configure this virtual server with port 80 and port 443. Any request that goes to port 80 should be redirected to port 443.

- Specify HTTP as the protocol.

- Enable address and port translation.

- Enable reset of connections when services and/or nodes are down.

- Assign the pool created in step 1 to the virtual server.

- Create rules to filter out access to `/console` and `/em` on this virtual server.

4. Configure a virtual server in the load balancer for `admin.mycompany.com:80`.

- For this virtual server, use your internal administration address as the virtual server address (for example, `admin.mycompany.com`). This address is typically not externalized.

- Specify HTTP as the protocol.

- Enable address and port translation.

- Enable reset of connections when services and/or nodes are down.

- Optionally, create rules to allow access only to /console and /em on this virtual server.

- Assign the pool created in step 1 to the virtual server.

5. Configure a virtual server in the load balancer for `biinternal.mycompany.com:80`.

- For this virtual server, use your internal administration address as the virtual server address (for example, `biinternal.mycompany.com`). This address is typically not externalized.

- Specify HTTP as the protocol.

- Enable address and port translation.

- Enable reset of connections when services and/or nodes are down.

- Assign the pool created in step 1 to the virtual server.

- Optionally, create rules to filter out access to `/console` and `/em` on this virtual server.

6. Configure monitors for the Oracle HTTP Server nodes to detect failures in these nodes.

- Set up a monitor to regularly ping the "/" URL context.

   Tip: Use `GET /\n\n` instead if the Oracle HTTP Server's document root does not include `index.htm` and Oracle WebLogic Server returns a 404 error for "/".

- For the ping interval, specify a value that does not overload your system. You can try 5 seconds as a starting point.

- For the timeout period, specify a value that can account for the longest response time that you can expect from your BI system, that is, specify a value greater than the longest period of time any of your requests to HTTP servers can take.

2.2.3 IPs and Virtual IPs

Table 2–1 describes the various virtual hosts.

Table 2–1   Virtual Hosts

Virtual IP	VIP Maps to...	Description
VIP1	ADMINVHN	ADMINVHN is the virtual host name that is the listen address for the Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running (APPHOST1 by default).
VIP2	APPHOST1VHN1	APPHOST1VHN1 is the virtual host name that maps to the listen address for bi_server1 and fails over with server migration of this Managed Server. It is enabled on the node where the bi_server1 process is running (APPHOST1 by default).
VIP3	APPHOST2VHN1	APPHOST2VHN1 is the virtual host name that maps to the listen address for bi_server2 and fails over with server migration of this Managed Server. It is enabled on the node where the bi_server2 process is running (APPHOST2 by default).

2.2.3.1 Enabling Virtual IPs for the Managed Servers

The BI domain uses virtual host names as the listen addresses for the Oracle Business Intelligence Managed Servers. You must enable the VIPs, mapping each of these host names on the two BI computers (VIP2 on APPHOST1 and VIP3 on APPHOST2), and they must correctly resolve to the virtual host names in the network system used by the topology (either by DNS Server or hosts resolution).

Before the Managed Servers can be configured to listen on a virtual IP Address, one of the network interface cards on the host running the Managed Server must be configured to listen on this virtual IP Address.

Perform the following steps once on each host to enable the appropriate virtual IP Address (VIP2 on APPHOST1 and VIP3 on APPHOST2). In an UNIX environment, the command must be run as the root user:

1. On the appropriate host (APPHOST1 or APPHOST2), run the `ifconfig` command to get the value of the netmask. In a UNIX environment, run this command as the root user. For example, on APPHOST1:

   ```
   [root@APPHOST1 ~] # /sbin/ifconfig
   eth0    Link encap:Ethernet  HWaddr 00:11:43:D7:5B:06
       inet addr:139.185.140.51  Bcast:139.185.140.255  Mask:255.255.255.0
       inet6 addr: fe80::211:43ff:fed7:5b06/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:10626133 errors:0 dropped:0 overruns:0 frame:0
       TX packets:10951629 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:4036851474 (3.7 GiB)  TX bytes:2770209798 (2.5 GiB)
       Base address:0xecc0 Memory:dfae0000-dfb00000
   ```

2. Bind the virtual IP Address to the network interface card using `ifconfig`. In a UNIX environment, run this command as the root user. Use a netmask value that was obtained in Step 1.

   The syntax and usage for the `ifconfig` command is as follows:

   ```
   /sbin/ifconfig networkCardInterface Virtual_IP_Address netmask netMask
   ```

For example:

```
/sbin/ifconfig eth0:1 100.200.140.206 netmask 255.255.255.0
```

3. Update the routing table using `arping`. In a UNIX environment, run this command as the root user.

```
/sbin/arping -q -U -c 3 -I networkCardInterface Virtual_IP_Address
```

For example:

```
/sbin/arping -q -U -c 3 -I eth0 100.200.140.206
```

See also Section 5.5.1, "Enabling ADMINVHN on APPHOST1" for information about enabling VIP1 for the Administration Server on APPHOST1.

2.2.4 Firewalls and Ports

Many Oracle Fusion Middleware components and services use ports. As an administrator, you must know the port numbers used by these services, and ensure that the same port number is not used by two services on a host.

Most port numbers are assigned during installation.

Table 2–2 lists the ports used in the Oracle BI topology, including the ports that you must open on the firewalls in the topology.

Firewall notation:

- FW0 refers to the outermost firewall.

- FW1 refers to the firewall between the Web tier and the application tier.

- FW2 refers to the firewall between the application tier and the data tier.

Table 2–2   Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Browser request	FW0	80	HTTP / Load Balancer	Inbound	Timeout depends on all HTML content and the type of process model used for BI.
Browser request	FW0	443	HTTPS / Load Balancer	Inbound	Timeout depends on all HTML content and the type of process model used for BI.
Load balancer to Oracle HTTP Server	n/a	7777	HTTP	n/a	See Section 2.2.2, "Load Balancers."
Oracle HTTP Server registration with Administration Server	FW1	7001	HTTP/t3	Inbound	Set the timeout to a short period (5-10 seconds).
Oracle HTTP Server management by Administration Server	FW1	OPMN port (6701) and Oracle HTTP Server Admin Port (7779)	TCP and HTTP, respectively	Outbound	Set the timeout to a short period (5-10 seconds).

Table 2–2   (Cont.) Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
BI Server access	FW1	9704	HTTP/bi_server$n$	Inbound	Timeout varies based on the type of process model used for BI.
Communication between BI Cluster members	n/a	9704	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Session replication within a WebLogic Server cluster	n/a	n/a	n/a	n/a	By default, this communication uses the same port as the server's listen address.
Oracle WebLogic Server Administration Console access	FW1	7001	HTTP / Administration Server and Enterprise Manager	Both	You should tune this timeout based on the type of access to the Administration Console (whether you plan to use the Administration Console from application tier clients, or from clients external to the application tier).
Node Manager	n/a	9556	TCP/IP	n/a	n/a
					For actual values, see "Firewall and Port Configuration" in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.
Access Server access	FW1	6021	OAP	Inbound	For actual values, see "Firewall and Port Configuration" in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.
Identity Server access	FW1	6022	OAP	Inbound	n/a
Database access for BI Server and BI Publisher JDBC data sources	FW1	Listening port for client connections to the listener	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for BI
Database access	FW2	1521	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for BI.

Table 2–2   (Cont.) Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Oracle Internet Directory access	FW2	389	LDAP	Inbound	You should tune the directory server's parameters based on load balancer, and not the other way around.
Oracle Internet Directory access	FW2	636	LDAP SSL	Inbound	You should tune the directory server's parameters based on load balancer, and not the other way around.
JOC for OWSM	n/a	9991	TCP/IP	n/a	n/a

> **Note:**   The firewall ports depend on the definition of TCP/IP ports.

2.3 Shared Storage and Recommended Directory Structure

This section details the directories and directory structure that Oracle recommends for the reference enterprise deployment topology in this guide. Other directory layouts are possible and supported, but the model adopted in this guide was chosen for maximum availability and provides the best isolation of components and symmetry in the configuration, as well as facilitating backup and disaster recovery. The rest of the document uses this directory structure and directory terminology.

This section contains the following topics:

- Section 2.3.1, "Terminology for Directories and Directory Environment Variables"
- Section 2.3.2, "Recommended Locations for the Different Directories"
- Section 2.3.3, "Shared Storage Configuration"
- Section 2.3.4, "Ensuring That Shared Network Files Are Accessible in Windows Environments"

2.3.1 Terminology for Directories and Directory Environment Variables

This enterprise deployment guide uses the following references to directory locations:

- **ORACLE_BASE:** This environment variable and related directory path refers to the base directory under which Oracle products are installed.
- **MW_HOME:** This environment variable and related directory path refers to the location where Oracle Fusion Middleware resides.
- **WL_HOME:** This environment variable and related directory path contains installed files necessary to host an Oracle WebLogic Server.
- **ORACLE_HOME:** This environment variable and related directory path refers to the directory where the binaries required to run Oracle Business Intelligence are installed.
- **ORACLE_COMMON_HOME:** This environment variable and related directory path refers to the Oracle home that contains the binary and library files required for Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).

- **Domain directory:** This directory path refers to the location where the Oracle WebLogic domain information (configuration artifacts) is stored. Different WLS Servers can use different domain directories even when in the same node.

- **ORACLE_INSTANCE:** An Oracle instance directory contains configuration files, log files, and temporary files for one or more Oracle system components (such as Oracle BI Server, Oracle BI Presentation Services, Oracle HTTP Server, and so on).

> **Tip:** You can simplify directory navigation by using environment variables as shortcuts to the locations in this section. For example, you could use an environment variable called $ORACLE_BASE in Linux to refer to /u01/app/oracle (that is, the recommended ORACLE_BASE location). In Windows, you would use %ORACLE_BASE% and use Windows-specific commands.

2.3.2 Recommended Locations for the Different Directories

Oracle Business Intelligence 11*g* supports the deployment and instantiation of multiple processes (such as Managed Servers, BI Servers, and Presentation Services servers) from a single binary installation. This capability simplifies lifecycle operations like patching, upgrade, and test-to-production, as well as scale-out operations for an Oracle Business Intelligence deployment. However, for maximum availability, Oracle recommends using redundant binary installations. In the EDG model, two Oracle Fusion Middleware homes (*MW_HOME*), each of which has a *WL_HOME* and an *ORACLE_HOME* for each product suite, are installed in a shared storage. Additional servers (when scaling out or up) of the same type can use either one of these two locations without requiring more installations. Ideally, users should use two different volumes (referred to as VOL1 and VOL2 in subsequent text) for redundant binary location, thus isolating as much as possible the failures in each volume. For additional protection, Oracle recommends that these volumes are disk-mirrored. If multiple volumes are not available, Oracle recommends using mount points to simulate the same mount location in a different directory in the shared storage. Although this does not guarantee the protection that multiple volumes provide, it does allow protection from user deletions and individual file corruption.

When an *ORACLE_HOME* or a *WL_HOME* is shared by multiple servers on different computers, you should keep the Oracle Inventory (oraInventory) and Middleware home list on those computers up-to-date. Doing so ensures consistency when you perform future installations or apply patches. To update the oraInventory on a computer and "attach" an installation in a shared storage to it, use *ORACLE_HOME*/oui/bin/attachHome.sh. To update the Middleware home list to add or remove a WL_HOME, edit the *user_home*/bea/beahomelist file. This is required for any additional computers where Oracle Business Intelligence is installed, in addition to the two computers used in this EDG.

Oracle recommends also separating the domain directory used by the Administration Server from the domain directory used by the Managed Servers. This allows a symmetric configuration for the domain directories used by Managed Servers, and isolates the failover of the Administration Server. The domain directory for the Administration Server must reside in a shared storage to allow failover to another computer with the same configuration. The domain directories of the Managed Servers can reside in a local or shared storage.

You can use a shared domain directory for all Managed Servers on different computers, or use one domain directory for each computer. Sharing domain directories for Managed Servers facilitates the scale-out procedures. In this case, the

deployment should conform to the requirements (if any) of the storage system to facilitate multiple computers mounting the same shared volume.

All procedures that apply to multiple local domains apply to a single shared domain. Hence, this enterprise deployment guide uses a model where one domain directory is used for each computer. The directory can be local or reside in shared storage. Based on the preceding assumptions, the following paragraphs describe the directories recommended. Wherever a shared storage location is directly specified, it is implied that shared storage is required for that directory. When using local disk or shared storage is optional, the mount specification is qualified with "if using a shared disk." The shared storage locations are examples and can be changed as long as the provided mount points are used. However, Oracle recommends this structure in the shared storage device for consistency and simplicity.

ORACLE_BASE:

/u01/app/oracle

MW_HOME (Application Tier):

ORACLE_BASE/product/fmw

- Mount point: *ORACLE_BASE*/product/fmw

- Shared storage location: *ORACLE_BASE*/product/fmw (VOL1 and VOL2)

- Mounted from: Nodes alternatively mount VOL1 or VOL2 in such a way that at least half the nodes use an installation and the other half use the other one. In the EDG for Oracle Business Intelligence, APPHOST1 mounts VOL1 and APPHOST2 mounts VOL2. When only one volume is available, nodes mount two different directories in shared storage alternatively (that is, for example, APPHOST1 would use *ORACLE_BASE*/product/fmw1 as shared storage location and APPHOST2 would use *ORACLE_BASE*/product/fmw2 as shared storage location).

> **Note:** When there is just one volume available in the shared storage, you can provide redundancy using different directories to protect from accidental file deletions and for patching purposes. Two *MW_HOME*s would be available; at least one at *ORACLE_BASE*/product/fmw1, and another at *ORACLE_BASE*/product/fmw2. These *MW_HOME*s are mounted on the same mount point in all nodes.

MW_HOME (Web tier):

ORACLE_BASE/product/fmw/web

- Mount point: *ORACLE_BASE*/product/fmw

- Shared storage location: *ORACLE_BASE*/product/fmw (VOL1 and VOL2)

- Mounted from: For shared storage installations, nodes alternatively mount VOL1 or VOL2 in such a way that at least half the nodes use an installation and the other half use the other one. In the EDG for BI, WEBHOST1 would mount VOL1 and WEBHOST2 would mount VOL2. When only one volume is available, nodes mount the two suggested directories in shared storage alternatively (that is, for example, WEBHOST1 would use *ORACLE_BASE*/product/fmw1 as shared storage location and WEBHOST2 would use *ORACLE_BASE*/product/fmw2 as shared storage location).

> **Note:** Web tier installation is usually performed on local storage to the WEBHOST nodes. When using shared storage, appropriate security restrictions for access to the storage device across tiers must be considered.

WL_HOME:

MW_HOME/wlserver_10.3

ORACLE_HOME:

MW_HOME/Oracle_BI1

ORACLE_COMMON_HOME:

MW_HOME/oracle_common

ORACLE_INSTANCE:

ORACLE_BASE/admin/*instance_name*

- If you are using a shared disk, the mount point on the system is *ORACLE_BASE*/admin/*instance_name* mounted to *ORACLE_BASE*/admin/*instance_name* (VOL1).

  > **Note:** (VOL1) is optional; you could also use (VOL2).

Domain Directory for Admin Directory:

ORACLE_BASE/admin/*domain_name*/aserver/*domain_name* (the last "domain_name" is added by the Configuration Assistant).

- Mount point on system: *ORACLE_BASE*/admin/*domain_name*/aserver
- Shared storage location: *ORACLE_BASE*/admin/*domain_name*
- Mounted from: Only the node where the Administration Server is running needs to mount this directory. When the Administration Server is relocated (failed over) to a different node, the node then mounts the same shared storage location on the same mount point. The remaining nodes in the topology do not need to mount this location.

Domain Directory for Managed Server:

ORACLE_BASE/admin/*domain_name*/mserver/*domain_name*

- If you are using a shared disk, the mount point on the system is *ORACLE_BASE*/admin/*domain_name*/mserver mounted to *ORACLE_BASE*/admin/*domain_name*/Node*n*/mserver/ (each node uses a different domain directory for Managed Servers).

  > **Note:** This procedure is really shared storage dependent. The example in the preceding bullet point is specific to NAS, but other storage types may provide this redundancy with different types of mappings.

Location for JMS file-based stores and Tlogs:

ORACLE_BASE/admin/*domain_name*/*cluster_name*/jms

ORACLE_BASE/admin/*domain_name*/*cluster_name*/tlogs

- Mount point: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

- Shared storage location: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

- Mounted from: All nodes running BI components must mount this shared storage location so that transaction logs and JMS stores are available when server migration to another node takes place.

Location for Oracle BI Presentation Catalog:

ORACLE_BASE/admin/*domain_name*/*cluster_name*/catalog/*customCatalog* (where customCatalog is an example of the catalog name)

- Mount point: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

- Shared storage location: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

- Mounted from: All nodes containing the instances of Presentation Services in the cluster mount this location (all nodes must have read and write access).

Note that the Oracle BI Presentation Catalog is called Presentation Service Repository in Fusion Middleware Control.

Location for Repository Publishing Directory:

ORACLE_BASE/admin/*domain_name*/*cluster_name*/ClusterRPD

- Mount point: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

- Shared storage location: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

- Mounted from: All nodes containing the instances of BI Server in the cluster mount this location. The master BI Server must have read and write access to this directory. All other BI Servers must have read access.

Note that the repository publishing directory is identified as the Shared Location for the BI Server Repository in Fusion Middleware Control.

Location for BI Server Global Cache:

ORACLE_BASE/admin/*domain_name*/*cluster_name*/GlobalCache

- Mount point: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

  Shared storage location: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

  Mounted from: All nodes containing the instances of BI Server in the cluster mount this location. The master BI Server must have read and write access to this directory. All other BI Servers must have read access.

Location for BI Publisher Configuration Folder:

ORACLE_BASE/admin/*domain_name*/*cluster_name*/bipublisher/config

- Mount point: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

- Shared storage location: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

- Mounted from: All nodes containing the instances of BI Publisher in the cluster mount this location with read/write access.

Location for BI Publisher Scheduler Temp Directory:

ORACLE_BASE/admin/*domain_name*/*cluster_name*/bipublisher/temp

- Mount point: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

- Shared storage location: *ORACLE_BASE*/admin/*domain_name*/*cluster_name*

■ Mounted from: All nodes containing the instances of BI Publisher in the cluster mount this location with read/write access.

Location for Application Directory for Administration Server:

ORACLE_BASE/admin/*domain_name*/aserver/applications

■ Mount point: *ORACLE_BASE*/admin/*domain_name*/aserver/applications

■ Shared storage location: *ORACLE_BASE*/admin/*domain_name*/aserver

Location for Application Directory for Managed Server:

ORACLE_BASE/admin/*domain_name*/mserver/applications

> **Note:** This directory is local in the context of the EDG for Oracle Business Intelligence.

Figure 2–2 shows the recommended directory structure.

Figure 2–2 EDG Directory Structure for Oracle Business Intelligence
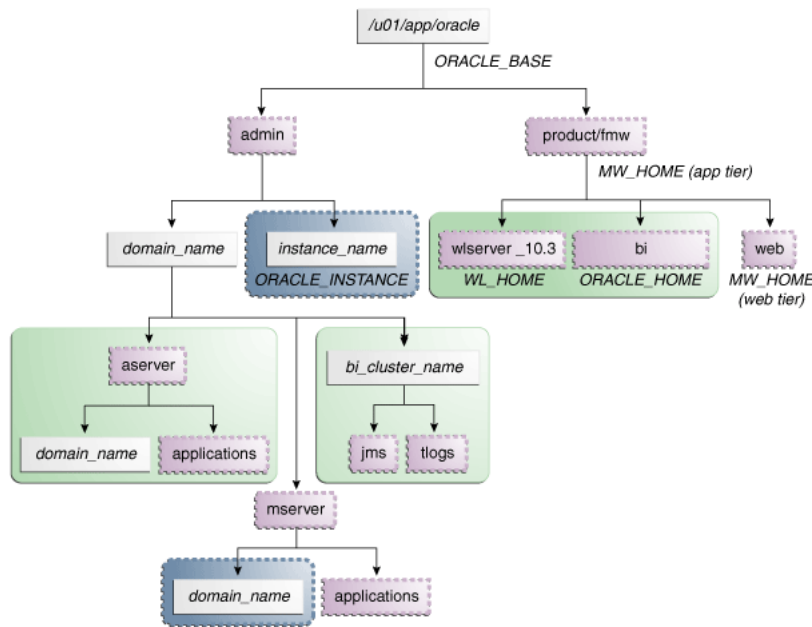
Note that the directory structure in Figure 2–2 does not show other required internal directories such as `oracle_common`. It also does not show shared component directories; see Section 2.3.3, "Shared Storage Configuration" for information about shared directories.

Table 2–3 explains what the various color-coded elements in Figure 2–2 mean.

Table 2–3 Directory Structure Elements

Element	Explanation
⬭	The Administration Server domain directories, applications, deployment plans, file adapter control directory, JMS and TX logs, and the entire *MW_HOME* are on a shared disk.

Table 2–3   (Cont.) Directory Structure Elements

Element	Explanation
	The Managed Server domain directories can be on a local disk or a shared disk. To share the Managed Server domain directories on multiple computers, you must mount the same shared disk location across the computers. The *instance_name* directory for the Web tier can be on a local disk or a shared disk.
	Fixed name.
	Installation-dependent name.

2.3.3 Shared Storage Configuration

The following steps show to create and mount shared storage locations so that APPHOST1 and APPHOST2 can see the same location for binary installation in two separate volumes.

"nasfiler" is the shared storage filer.

From APPHOST1:

```
APPHOST1> mount nasfiler:/vol/vol1/u01/app/oracle/product/fmw
/u01/app/oracle/product/fmw -t nfs
```

From APPHOST2:

```
APPHOST2> mount nasfiler:/vol/vol2/u01/app/oracle/product/fmw
/u01/app/oracle/product/fmw -t nfs
```

If only one volume is available, users can provide redundancy for the binaries by using two different directories in the shared storage and mounting them to the same dir in the APPHOST servers:

From APPHOST1:

```
APPHOST1> mount nasfiler:/vol/vol1/u01/app/oracle/product/fmw1
/u01/app/oracle/product/fmw -t nfs
```

From APPHOST2:

```
APPHOST2> mount nasfiler:/vol/vol2/u01/app/oracle/product/fmw2
/u01/app/oracle/product/fmw -t nfs
```

The following commands show how to share the BI TX logs location across different nodes:

```
APPHOST1> mount nasfiler:/vol/vol1/u01/app/oracle/stores/bifoundation_domain/
bi_cluster/tlogs /u01/app/oracle/stores/bifoundation_domain/
bi_cluster/tlogs -t nfs

APHOST2> mount nasfiler:/vol/vol1/u01/app/oracle/stores/bifoundatin_domain/
bi_cluster/tlogs /u01/app/oracle/stores/bifoundation_domain/
bi_cluster/tlogs -t nfs
```

> **Note:** The shared storage can be a NAS or SAN device. The following illustrates an example of creating storage for a NAS device from APPHOST1. The options may differ.
>
> ```
> APPHOST1> mount nasfiler:/vol/vol1/fmw11shared ORACLE_BASE/wls -t
> nfs -o rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsize=32768,
> wsize=32768
> ```
>
> Contact your storage vendor and computer administrator for the correct options for your environment.

2.3.4 Ensuring That Shared Network Files Are Accessible in Windows Environments

In Windows environments, shared storage is typically specified using Universal Naming Convention (UNC). UNC is a PC format for specifying locations of resources on a local area network. UNC uses the following format:

```
\\server_name\shared_resource_path_name
```

In addition, you must use named users to run OPMN processes in Windows environments so that the shared network files are accessible.

To run OPMN processes using a named user:

1. Open the Services dialog. For example, select **Start > Programs > Administrative Tools > Services**.

2. Right-click **OracleProcessManager_instance*n*** and then select **Properties**.

3. Select the Log On tab.

4. Select **This account**, and then provide a user name and password.

5. Click **OK**.

2.4 Clock Synchronization

The clocks of all servers participating in the cluster must be synchronized to within one second difference. To accomplish this, use a single network time server and then point each server to that network time server.

The procedure for pointing to the network time server is different on different operating systems. Refer to your operating system documentation for more information.

3

Installing the Software

This chapter describes the software installations required for the enterprise deployment reference topology for Oracle Business Intelligence. The installation is divided into two parts. The first part covers the required Web tier installation, while the second part addresses the required Oracle Fusion Middleware components. Later chapters describe the required configuration steps to create the reference topology for Oracle Business Intelligence.

> **Important:**   Oracle strongly recommends that you read *Oracle Fusion Middleware Release Notes* for any additional installation and deployment considerations before starting the setup process.

This chapter contains the following topics:

- Section 3.1, "Software Installation Summary"
- Section 3.2, "Installing Oracle HTTP Server"
- Section 3.3, "Installing Oracle Fusion Middleware"

3.1 Software Installation Summary

Table 3–1 shows what software should be installed on each host or be accessible from each host.

Table 3–1   Software To Be Installed on Each Host or Accessible From Each Host

Hosts	OHS	WLS	BI
WEBHOST1	Yes	No	No
WEBHOST2	Yes	No	No
APPHOST1	No	Yes	Yes
APPHOST2	No	Yes	Yes

Table 3–2 shows the software versions used.

Table 3–2   Software Versions Used

Software	Name	Version
OHS	Oracle HTTP Server 11*g*	11.1.1.3
WLS	WebLogic Server 11*g*	10.3.5

Table 3–2   (Cont.) Software Versions Used

Software	Name	Version
BI	Oracle Business Intelligence Enterprise Edition 11*g*	11.1.1.5
IDM	Oracle Identity Management 11*g*	11.1.1.3

3.2 Installing Oracle HTTP Server

This section contains the following topics:

- Section 3.2.1, "Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2"
- Section 3.2.2, "Backing Up the Installation"

3.2.1 Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2

Prerequisites

Before installing Oracle HTTP Server (OHS), check that your computers meet the following requirements:

- Ensure that the system, patch, kernel, and other requirements are met as specified in the installation documentation.

- Because Oracle HTTP Server is installed on port 7777 by default, you must ensure that port 7777 is not used by any service on the nodes. To check if this port is in use, run the following command before installing Oracle HTTP Server:

  ```
  netstat -an | grep 7777
  ```

  You must free port 7777 if it is in use.

- On Linux platforms, if the /etc/oraInst.loc file exists, check that its contents are correct. Specifically, check that the inventory directory is correct and that you have write permissions for that directory. If the /etc/oraInst.loc file does not exist, you can skip this step.

- Before starting the installation, ensure that the following environment variables are not set:

  - LD_ASSUME_KERNEL
  - ORACLE_INSTANCE

Procedure

As described in Section 2.3, "Shared Storage and Recommended Directory Structure," you install Oracle Fusion Middleware in at least two storage locations for redundancy.

1. Start the installer for Oracle HTTP Server from the installation media:

   ```
   ./runInstaller
   ```

2. In the Specify Inventory Directory screen, do the following:

   a. Enter *HOME*/**oraInventory**, where *HOME* is the home directory of the user performing the installation (this is the recommended location).

   b. Enter the OS group for the user performing the installation.

   c. Click **OK**.

Follow the instructions on screen to execute /createCentralInventory.sh as root.

Click **OK**.

This screen is displayed only during the first installation of Oracle products on a system.

3. In the Welcome screen, click **Next**.

4. In the Select Installation Type screen, select **Install Software - Do Not Configure**, and click **Next**.

5. In the Prerequisite Checks screen, verify that all checks complete successfully, and click **Next**.

6. In the Specify Installation Location screen, specify the following values:

   ■ **Oracle Middleware Home**: *ORACLE_BASE*/product/fmw

   ■ **Oracle Home Directory:** Oracle_WT1

   Click **Next**.

7. In the Specify Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your e-mail address.

8. In the Installation Summary screen, review the selections to ensure they are correct. If they are not, click **Back** to modify selections on previous screens. When you are ready, click **Install**.

   On UNIX systems, if prompted to run the oracleRoot.sh script, make sure you run it as the root user.

   The Oracle HTTP Server software is installed.

9. In the Installation Progress screen, click **Next**.

10. In the Installation Complete screen, click **Finish** to exit.

3.2.2 Backing Up the Installation

Back up the Middleware home (make sure to stop the server first):

```
WEBHOST1> tar -cvpf fmwhomeback.tar ORACLE_BASE/product/MW_HOME/oraInventory
```

3.3 Installing Oracle Fusion Middleware

This section describes how to install the required Oracle Fusion Middleware software for the enterprise deployment reference topology for Oracle Business Intelligence. The software components to be installed consist of the WebLogic Server home (*WL_HOME*) and Oracle home (*ORACLE_HOME*). As described in Section 2.3, "Shared Storage and Recommended Directory Structure," you install Oracle Fusion Middleware in at least two storage locations for redundancy.

> **Important:**   Oracle strongly recommends that you read *Oracle Fusion Middleware Release Notes* for any additional installation and deployment considerations before starting the setup process.

This section covers the following topics:

■ Section 3.3.1, "Installing Oracle WebLogic Server and Creating the Middleware Home"

- Section 3.3.2, "Installing Oracle Business Intelligence"
- Section 3.3.3, "Backing Up the Installation"

3.3.1 Installing Oracle WebLogic Server and Creating the Middleware Home

Perform these steps to install Oracle WebLogic Server on APPHOST1 and APPHOST2:

1. Start the installer for Oracle WebLogic Server from the installation media.

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

3. In the Choose Middleware Home Directory screen, do the following:

   - Select **Create a new Middleware Home**.

   - For Middleware Home Directory, enter *ORACLE_BASE***/product/fmw**.

     Note: *ORACLE_BASE* is the base directory under which Oracle products are installed. The recommended value is `/u01/app/oracle`. See Section 2.3, "Shared Storage and Recommended Directory Structure" for more information.

   Click **Next**.

4. In the Register for Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your e-mail address.

   Click **Next**.

5. In the Choose Install Type screen, select **Typical** and click **Next**.

6. In the Choose Product Installation Directories screen, accept the directory *ORACLE_BASE***/product/fmw/wlserver_10.3**. Also accept the default directory for Oracle Coherence (*ORACLE_BASE***/product/fmw/coherence_3.6**).

7. Click **Next**.

8. In the Installation Summary screen, click **Next**.

   The Oracle WebLogic Server software is installed.

9. In the Installation Complete screen, clear the **Run Quickstart** option and click **Done**.

3.3.2 Installing Oracle Business Intelligence

Perform the steps described in this section to install Oracle Business Intelligence on APPHOST1 and APPHOST2. Note that because the installation is performed on a shared storage, the *MW_HOME* is accessible and used by the Oracle BI servers in APPHOST1 and APPHOST2.

1. On Linux platforms, if the /etc/oraInst.loc file exists, check that its contents are correct. Specifically, check that the inventory directory is correct and that you have write permissions for that directory. If the /etc/oraInst.loc file does not exist, you can skip this step.

2. Start the installer for Oracle Business Intelligence from the installation media:

   ```
   ./runInstaller
   ```

3. In the Specify Inventory Directory screen, do the following:

    a. Enter *HOME*/**oraInventory**, where *HOME* is the home directory of the user performing the installation (this is the recommended location).

    b. Enter the OS group for the user performing the installation.

    c. Click **Next**.

    Follow the instructions on screen to execute /createCentralInventory.sh as root.

    Click **OK**.

4. In the Welcome screen, click **Next**.

5. In the Install Software Updates screen, choose whether to skip software updates, search My Oracle Support for software updates, or search your local directory for updates. When you are ready to proceed, click **Next**.

6. In the Select Installation Type screen, select **Software Only Install** and click **Next**.

7. In the Prerequisite Checks screen, verify that all checks complete successfully, and click **Next**.

8. In the Specify Installation Location screen, select the previously installed Middleware home from the drop-down list. For the Oracle home directory, enter the directory name (**Oracle_BI1**).

    Click **Next**.

9. In the Specify Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your e-mail address and click **Next**.

10. In the Summary screen, click **Install**.

    The Oracle Business Intelligence software is installed.

11. In the Installation Progress screen, click **Next**.

12. In the Complete screen, click **Finish**.

3.3.3 Backing Up the Installation

At this point, back up the Middleware home. Make sure to stop the servers first.

To back up the Middleware home, run the following command:

```
APPHOST1> tar -cvpf fmwhomeback.tar ORACLE_BASE/product/fmw
```

This command creates a backup of the installation files for both Oracle WebLogic Server and the Oracle Fusion Middleware components, including Oracle Business Intelligence.

4

Configuring the Web Tier

This chapter describes how to configure the Oracle Web tier to support the Oracle Business Intelligence enterprise deployment.

> **Important:** Oracle strongly recommends that you read *Oracle Fusion Middleware Release Notes* for any additional installation and deployment considerations before starting the setup process.

This chapter contains the following topics:

- Section 4.1, "Configuring the Oracle Web Tier"
- Section 4.2, "Validating the Installation"
- Section 4.3, "Configuring Oracle HTTP Server with the Load Balancer"
- Section 4.4, "Configuring Virtual Hosts"

4.1 Configuring the Oracle Web Tier

Prior to configuration, the Oracle Web tier software must be installed on WEBHOST1 and WEBHOST2, as described in Section 3.2, "Installing Oracle HTTP Server." The steps for configuring the Oracle Web tier are the same for both WEBHOST1 and WEBHOST2.

Perform these steps to configure the Oracle Web tier:

1. Change the directory to the location of the Oracle Fusion Middleware Configuration Wizard:

    ```
    WEBHOSTn> cd ORACLE_HOME/bin
    ```

2. Start the Configuration Wizard:

    ```
    WEBHOSTn> ./config.sh
    ```

3. In the Welcome screen, click **Next**.

4. In the Configure Components screen, select **Oracle HTTP Server** and deselect **Associate Selected Components with WebLogic Domain**. Ensure that Oracle Web Cache is *not* selected.

    Click **Next**.

5. In the Specify Component Details screen, specify the following values:

    - Instance Home Location: *ORACLE_BASE*/admin/web*n*

- Instance Name: web*n*

- OHS Component Name: ohs*n*

(where *n* is a sequential number for your installation; for example, 1 for WEBHOST1, 2 for WEBHOST2, and so on.)

Click **Next**.

6. In high-availability implementations, although it is not mandatory, it is simpler if all ports used by the various components are synchronized across hosts. You can bypass automatic port configuration by specifying the ports you want to use in a file.

In the Configure Ports screen, select a file name and then click **View/Edit**. The file looks similar to the following:

```
[OHS]
#Listen port for OHS component
OHS Port = 7777

[OPMN]
#Process Manager Local port no
OPMN Local Port = 1880
```

You can find a sample staticports.ini file in the /Disk1/stage/Response/ directory.

Click **Next**.

7. In the Specify Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your e-mail address.

8. In the Installation Summary screen, review the selections to ensure they are correct. If they are not, click **Back** to modify selections on previous screens. When you are ready, click **Configure**.

9. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, click **Next**, and the Installation Complete screen appears.

10. In the Installation Complete screen, click **Finish** to exit.

4.2 Validating the Installation

After the installation is complete, check that it is possible to access the Oracle HTTP Server home page using the following URLs:

```
http://webhost1.mycompany.com:7777/
```

```
http://webhost2.mycompany.com:7777/
```

4.3 Configuring Oracle HTTP Server with the Load Balancer

Configure your load balancer to route all HTTP requests to the hosts running Oracle HTTP Server (WEBHOST1, WEBHOST2). You do not need to enable sticky sessions (insert cookie) on the load balancer when Oracle HTTP Server is front-ending Oracle WebLogic Server. You need sticky sessions if you are going directly from the load balancer to Oracle WebLogic Server, which is not the case in the topology described in this guide. Also, you should set monitors for HTTP.

4.4 Configuring Virtual Hosts

For Oracle Business Intelligence to work with the load balancer, a virtual host must be created in the Oracle HTTP Server configuration. Edit the httpd.conf file located at *ORACLE_INSTANCE*/config/OHS/*component_name* and add the following virtual host sections:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
   ServerName https://bi.mycompany.com:443
   RewriteEngine On
   RewriteOptions inherit
</VirtualHost>

NameVirtualHost *:7777
<VirtualHost *:7777>
   ServerName admin.mycompany.com:80
   ServerAdmin you@your.address
   RewriteEngine On
   RewriteOptions inherit
</VirtualHost>

NameVirtualHost *:7777
<VirtualHost *:7777>
   ServerName biinternal.mycompany.com:80
   ServerAdmin you@your.address
   RewriteEngine On
   RewriteOptions inherit
</VirtualHost>
```

> **Note:**   Perform this step for both WEBHOST1 and WEBHOST2.

After modifying the httpd.conf file, you must restart both Oracle HTTP Servers, as follows:

```
WEBHOST> cd ORACLE_BASE/admin/instance_name/bin
WEBHOST> opmnctl stopall
WEBHOST> opmnctl startall
```

Access the following URLs to ensure that your load balancer and Oracle HTTP Server are configured properly:

- http://bi.mycompany.com/index.html

- http://admin.mycompany.com/index.html

- http://biinternal.mycompany.com/index.html

5

Creating a Domain with the Administration Server and First Managed Server

This chapter describes how to create a domain and the first Oracle Business Intelligence Managed Server using the Oracle Business Intelligence Configuration Assistant, Oracle WebLogic Server Administration Console, and Oracle Enterprise Manager Fusion Middleware Control. Later, you will scale out the domain to add additional components. This is addressed in later chapters in this document.

> **Important:** Oracle strongly recommends that you read *Oracle Fusion Middleware Release Notes* for any additional installation and deployment considerations before starting the setup process.

This chapter contains the following topics:

- Section 5.1, "Creating a Domain and the bi_server1 Managed Server on APPHOST1"
- Section 5.2, "Configuring JMS for Oracle BI Publisher"
- Section 5.3, "Creating boot.properties for the Administration Server on APPHOST1"
- Section 5.4, "Starting the Administration Server on APPHOST1"
- Section 5.5, "Enabling Administration Server High Availability"
- Section 5.6, "Validating the Administration Server"
- Section 5.7, "Setting the Listen Address for bi_server1 Managed Server"
- Section 5.8, "Disabling Host Name Verification for the bi_server1 Managed Server"
- Section 5.9, "Validating Oracle Business Intelligence on APPHOST1"
- Section 5.10, "Configuring Oracle HTTP Server"
- Section 5.11, "Registering Oracle HTTP Server with Oracle WebLogic Server"
- Section 5.12, "Setting the Frontend URL for the Administration Console"
- Section 5.13, "Validating Access Through Oracle HTTP Server"
- Section 5.14, "Manually Failing Over the Administration Server to APPHOST2"
- Section 5.15, "Backing Up the Installation"

5.1 Creating a Domain and the bi_server1 Managed Server on APPHOST1

Run the Oracle Business Intelligence Configuration Assistant from the Oracle home directory to create a domain containing the Administration Server and the first Managed Server with Oracle Business Intelligence components.

1. Ensure that the database where you installed the Business Intelligence Platform schemas is running. For an Oracle RAC database, it is recommended that you ensure that all instances are running, so that the validation check that is performed in later steps is more reliable.

2. Change the directory to the location of the Configuration Assistant (created in Chapter 3, "Installing the Software"):

   ```
   APPHOST1> cd ORACLE_HOME/bin
   ```

3. Start the Configuration Assistant:

   ```
   APPHOST1> ./config.sh
   ```

4. In the Welcome screen, click **Next**.

5. In the Prerequisite Checks screen, verify that all checks complete successfully, and then click **Next**.

6. The Create, Scale Out or Extend screen is displayed. In this screen, select **Create New BI System**, then enter the following:

   - **User Name:** weblogic
   - **User Password:** *your_password*
   - **Domain Name:** *bifoundation_domain*

   Click **Next**.

7. In the Specify Installation Location screen, enter:

   - **Middleware Home:** *ORACLE_BASE*/product/fmw (dimmed)
   - **Oracle Home:** *ORACLE_BASE*/product/fmw/Oracle_BI1 (dimmed)
   - **WebLogic Server Home:** *ORACLE_BASE*/product/fmw/wlserver_10.3 (dimmed)
   - **Domain Home:** *ORACLE_BASE*/admin/*domain_name*/aserver/*domain_name*

     The Domain Home must end with the domain name.
   - **Instance Home:** *ORACLE_BASE*/admin/instance1
   - **Instance Name:** instance1

   Click **Next**.

8. In the Configure Components screen, select the following:

   - Oracle Business Intelligence
     - Business Intelligence Enterprise Edition
     - Business Intelligence Publisher
     - Real-Time Decisions

   Click **Next**.

9. In the RPD Encryption Password screen, provide the following information:

- **RPD Password**

- **Confirm RPD Password**

This password is used for the sample repository called SampleAppLite.rpd that is included with the installed files.

Click **Next**.

10. In the BIPLATFORM Schema screen, provide the following information:

- **Database Type:** Oracle Database

- **Connect String:** CUSTDBHOST1:1521:CUSTDB1^CUSTDBHOST2:1521:CUSTDB2@BIEDG.MYCOMPANY.COM

- **BIPLATFORM Schema Username:** *prefix*_BIPLATFORM

- **BIPLATFORM Schema Password:** *your_password*

Click **Next**.

11. In the MDS Schema screen, verify the information. For example:

- **Database Type:** Oracle Database

- **Connect String:** CUSTDBHOST1:1521:CUSTDB1^CUSTDBHOST2:1521:CUSTDB2@BIEDG.MYCOMPANY.COM

- **MDS Schema Username:** *prefix*_MDS

- **MDS Password:** *your_password*

Click **Next**.

12. In the Configure Ports screen, select one the following:

- Auto Port Configuration

- Specify Ports using Configuration File

Click **Next**.

13. In the Specify Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your e-mail address.

Click **Next**.

14. In the Summary screen, click **Configure**.

15. In the Configuration Progress screen, verify that all the Configuration Tools have completed successfully and click **Next**.

16. In the Complete screen, click **Finish**.

Usually, Node Manager is started automatically when config.sh completes. If Node Manager is not running for some reason, run these commands to start it on APPHOST1:

```
APPHOST1> cd WL_HOME/server/bin
APPHOST1> ./startNodeManager.sh
```

5.2 Configuring JMS for Oracle BI Publisher

You must configure the location for all persistence stores to a directory visible from both nodes. Change all persistent stores to use this shared base directory.

1. Log into the Administration Console.

2. In the Domain Structure window, expand the **Services** node and then click the **Persistent Stores** node. The Summary of Persistent Stores page is displayed.

3. In the Change Center, click **Lock & Edit**.

4. Click **BipJmsStore** and enter a directory that is located in the shared storage. This shared storage is accessible from both APPHOST1 and APPHOST2:

   ORACLE_BASE/admin/*domain_name*/bi_cluster/jms

5. Click **Save** and then click **Activate Changes**.

6. The changes will not take effect until the Managed Server is restarted. Restart the Managed Server.

5.3 Creating boot.properties for the Administration Server on APPHOST1

Create a boot.properties file for the Administration Server on APPHOST1. This file enables the Administration Server to start without prompting you for the administrator username and password.

1. Go to the following directory:

   ```
   ORACLE_BASE/admin/domain_name/aserver/domain_name/servers/AdminServer/security
   ```

2. In this directory, create a file called boot.properties using a text editor and enter the following lines in the file:

   ```
   username=Admin_Username
   password=Admin_Password
   ```

   > **Note:** When you start the Administration Server, the username and password entries in the file get encrypted. You start the Administration Server in Section 5.4, "Starting the Administration Server on APPHOST1." For security reasons, you want to minimize the time the entries in the file are left unencrypted. After you edit the file, you should start the server as soon as possible so that the entries get encrypted.

3. Save the file and close the editor.

5.4 Starting the Administration Server on APPHOST1

The Administration Server is started and stopped using Node Manager. However, the first start of the Administration Server with Node Manager requires changing the default username and password that the Configuration Assistant set for Node Manager. Follow these steps to start the Administration Server using Node Manager:

1. Use the Administration Console to update the Node Manager credentials:

   a. Open a Web browser and go to http://APPHOST1:7001/console.

   b. Log in as the administrator.

   c. In the Change Center, click **Lock & Edit** to enable configuration changes.

   d. Click *domain_name*, then **Security**, then **General**, and then expand the **Advanced** options at the bottom.

      e. Enter a new username for Node Manager, or make a note of the existing one and update the Node Manager password.

      f. Click **Save**.

      g. Click **Activate Changes**.

2. Stop the Administration Server process using one of the following methods:

- Use Ctrl+C in the shell where it was started

- Use the standard process identification and kill commands in the operating system

- Log in to the Administration Console and click **Servers** under the Environment heading, then click the **Control** tab. Select **AdminServer(admin)** and click **Shutdown**.

3. Stop and restart Node Manager and enable dynamic registration, as follows:

      a. Stop the running NodeManager process.

      b. Run the setNMProps.sh script, which is located in the *ORACLE_COMMON_HOME*/common/bin directory, to set the StartScriptEnabled property to 'true' before starting Node Manager:

```
APPHOST1> cd ORACLE_COMMON_HOME/common/bin
APPHOST1> ./setNMProps.sh
```

> **Note:** You must use the StartScriptEnabled property to avoid class loading failures.

      c. Restart Node Manager and enable dynamic registration using the following commands:

```
APPHOST1> cd WL_HOME/server/bin
APPHOST1> export JAVA_OPTIONS=-DDomainRegistrationEnabled=true
APPHOST1> ./startNodeManager.sh
```

> **Note:** It is important that you set -DDomainRegistrationEnabled=true whenever you start a Node Manager which must manage the Administration Server. If there is no Administration Server on this computer, and if this computer is not an Administration Server failover node, then Node Manager can be started as follows:
>
> ```
> APPHOST1> ./startNodeManager.sh
> ```

4. Start the Oracle WebLogic Scripting Tool (WLST) and connect to Node Manager with `nmconnect` and the credentials set in step 1, and start the Administration Server using `nmstart`:

```
APPHOST1> cd ORACLE_COMMON_HOME/common/bin
APPHOST1> ./wlst.sh
```

In the WLST shell, execute the following command:

```
wls:/offline>nmConnect('Admin_User','Admin_Pasword', 'APPHOST1','9556',
'domain_name','Domain_Home')


wls:/nm/domain_name> nmStart('AdminServer')
```

For example:

```
wls:/offline>nmConnect('weblogic', 'my_password', 'APPHOST1' , '9556',
'bifoundation_domain' ,'/u01/app/oracle/admin/bifoundation_domain/aserver/
bifoundation_domain')

wls:/nm/bifoundation_domain> nmStart('AdminServer')
```

> **Note:** APPHOST1 is the address of the node where the domain was created, not the listen address of the Administration Server. Also, the username and password are only used to authenticate connections between Node Manager and clients. They are independent from the server admin ID and password, and are stored in the *ORACLE_BASE*/admin/*domain_name*/aserver/*domain_name*/config/nodemanager/nm_password.properties file.

5.5 Enabling Administration Server High Availability

The Oracle WebLogic Server Administration Server is a singleton application, so it cannot be deployed in an active-active configuration. By default, the Administration Server is only available on the first installed node, and for this enterprise topology, it is available only on APPHOST1. If this node becomes unavailable, then the Administration Console and Fusion Middleware Control also become unavailable. To avoid this scenario, the Administration Server and the applications deployed to it must be enabled for high availability. The enterprise deployment architecture in this guide calls for the deploying the Administration Server on a disk shared between APPHOST1 and APPHOST2.

The process described in this guide initially deploys the Administration Server and the bi_server1 Managed Server on the shared disk mounted on APPHOST1, and then manually migrates the bi_server1 Managed Server domain information to the local file system. This process is necessary to overcome certain design constraints in the Oracle Universal Installer.

This section contains the following topics:

- Section 5.5.1, "Enabling ADMINVHN on APPHOST1"

- Section 5.5.2, "Create a Machine for the Administration Server"

- Section 5.5.3, "Enabling the Administration Server to Listen on the Virtual IP Address"

- Section 5.5.4, "Creating a Separate Domain Directory for the bi_server1 Managed Server"

- Section 5.5.5, "Enabling Fusion Middleware Control Failover"

5.5.1 Enabling ADMINVHN on APPHOST1

The Administration Server must be configured to listen on a virtual IP Address to enable it to seamlessly failover from one host to another. In case of a failure, the Administration Server, along with the virtual IP Address, can be migrated from one host to another.

However, before the Administration Server can be configured to listen on a virtual IP Address, one of the network interface cards on the host running the Administration

Server must be configured to listen on this virtual IP Address. The steps to enable a virtual IP Address are completely dependent on the operating system.

Follow the steps in this section to enable a virtual IP Address on APPHOST1. In a UNIX environment, the command must be run as the root user:

1. On APPHOST1, run the `ifconfig` command to get the value of the netmask. In a UNIX environment, run this command as the root user. For example:

```
[root@APPHOST1 ~] # /sbin/ifconfig
eth0     Link encap:Ethernet  HWaddr 00:11:43:D7:5B:06
     inet addr:139.185.140.51  Bcast:139.185.140.255  Mask:255.255.255.0
     inet6 addr: fe80::211:43ff:fed7:5b06/64 Scope:Link
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:10626133 errors:0 dropped:0 overruns:0 frame:0
     TX packets:10951629 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:4036851474 (3.7 GiB)  TX bytes:2770209798 (2.5 GiB)
     Base address:0xecc0 Memory:dfae0000-dfb00000
```

2. On APPHOST1, bind the virtual IP Address to the network interface card using `ifconfig`. In a UNIX environment, run this command as the root user. Use a netmask value that was obtained in Step 1.

   The syntax and usage for the `ifconfig` command is as follows:

   ```
   /sbin/ifconfig networkCardInterface Virtual_IP_Address netmask netMask
   ```

   For example:

   ```
   /sbin/ifconfig eth0:1 100.200.140.206 netmask 255.255.255.0
   ```

3. Update the routing table using `arping`. In a UNIX environment, run this command as the root user.

   ```
   /sbin/arping -q -U -c 3 -I networkCardInterface Virtual_IP_Address
   ```

   For example:

   ```
   /sbin/arping -q -U -c 3 -I eth0 100.200.140.206
   ```

See also Section 2.2.3.1, "Enabling Virtual IPs for the Managed Servers" for information about enabling VIP2 and VIP3 for the Managed Servers on APPHOST1 and APPHOST2.

5.5.2 Create a Machine for the Administration Server

Create a new machine and assign the Administration Server to the new machine using the Administration Console.

1. Log in to the Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. In the Environment section of the Home page, click **Machines**.

4. On the Summary of Machines page, select the Machine that is associated with the Administration Server from under the Machines table and click **Clone**. For example: APPHOST1.MYCOMPANY.COM.

5. On the Clone a Machine page, enter the Name of the Machine under the Machine Identity section and click **OK**. For example, enter ADMINHOST as the machine name.

6. On the Summary of Machines page, click the newly created Machine link.

7. On the Settings page for the ADMINHOST machine, select the **Servers** tab.

8. Click **Add** under the Servers table.

9. On the Add a Server to Machine page, choose **Select an existing server, and associate it with this machine option**.

10. Choose the AdminServer from the drop-down menu.

11. Click **Finish** to associate the Administration Server with the Machine.

12. In the Change Center, click **Activate Changes**.

5.5.3 Enabling the Administration Server to Listen on the Virtual IP Address

Ensure that you have performed the steps described in Section 5.5.1, "Enabling ADMINVHN on APPHOST1" before setting the Administration Server listen address.

Perform these steps to set the Administration Server listen address:

1. Log in to the Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. Expand the **Environment** node in the Domain Structure window.

4. Click **Servers**. The Summary of Servers page is displayed.

5. Select **AdminServer(admin)** in the Names column of the table. The Setting page for AdminServer(admin) is displayed.

6. Set the **Listen Address** to ADMINVHN.

7. Click **Save**.

8. Click **Activate Changes**.

9. The changes will not take effect until the Administration Server is restarted. Follow these steps to restart the Administration Server:

   a. In the Summary of Servers page, select the **Control** tab.

   b. Select **AdminServer(admin)** in the table and then click **Shutdown**.

   c. Start the Administration Server again from the command line, as follows:

   ```
   APPHOST1> cd ORACLE_COMMON_HOME/common/bin
   APPHOST1> ./wlst.sh
   wls:/offline> nmConnect
   ('Admin_User','Admin_Password','APPHOST1','9556','domain_name','DOMAIN
   home')
   wls:/nm/domain_name> nmStart ('AdminServer')
   ```

5.5.4 Creating a Separate Domain Directory for the bi_server1 Managed Server

Use the pack and unpack commands to separate the domain directory used by the Administration Server from the domain directory used by the bi_server1 Managed Server in APPHOST1.

1. Run the pack command on APPHOST1 to create a template pack using the following command. Make sure to pass managed=true to pack just the bi_server1 Managed Server domain information.

   ```
   APPHOST1> cd ORACLE_HOME/common/bin
   APPHOST1> ./pack.sh -managed=true -domain=path_to_installer_created_domain
   ```

```
-template=templateName.jar -template_name=templateName
```

For example:

```
APPHOST1> cd ORACLE_HOME/common/bin
APPHOST1> ./pack.sh -managed=true -domain=
ORACLE_BASE/admin/bifoundation_domain/aserver/bifoundation_domain
-template=/tmp/managedServer.jar -template_name=ManagedServer_Template
```

2. Run the unpack command on APPHOST1 to unpack the template to the domain directory of the Managed Server using the following command:

```
APPHOST1> cd ORACLE_HOME/common/bin
APPHOST1> ./unpack.sh -domain=path_to_domain_on_LocalFileSystem
-template=templateName.jar -app_dir=path_to_applications_dir_on_LocalFileSystem
```

For example:

```
APPHOST1> cd ORACLE_HOME/common/bin
APPHOST1>./unpack.sh -domain=
ORACLE_BASE/admin/bifoundation_domain/mserver/bifoundation_domain
-template=/tmp/managedServer.jar -app_dir=
ORACLE_BASE/admin/bifoundation_domain/mserver/applications
```

3. Restart the bi_server1 Managed Server on APPHOST1, as follows (ensure that Node Manager is up and running):

   a. Log in to the Administration Console.

   b. Expand the **Environment** node in the Domain Structure window.

   c. Click **Servers**. The Summary of Servers page is displayed.

   d. On the Summary of Servers page, select the **Control** tab.

   e. Select **bi_server1** in the table and then click **Start**.

5.5.5 Enabling Fusion Middleware Control Failover

To enable Fusion Middleware Control failover, copy the em.ear file from the *MW_HOME*/user_projects/applications/bifoundation_domain directory to the equivalent directory on all nodes where Administration Server HA might be performed. In some cases, you might need to create the *MW_HOME*/user_projects/applications/bifoundation_domain directory on the other nodes.

5.6 Validating the Administration Server

Perform these steps to ensure that the Administration Server is properly configured:

1. Open a Web browser and go to http://ADMINVHN:7001/console.

2. Log in as the administrator.

3. Check that you can access Fusion Middleware Control at:

   http://ADMINVHN:7001/em

4. Log in to Fusion Middleware Control with the username and password you specified in Section 5.3, "Creating boot.properties for the Administration Server on APPHOST1."

5.7 Setting the Listen Address for bi_server1 Managed Server

Ensure that you have performed the steps described in Section 2.2.3.1, "Enabling Virtual IPs for the Managed Servers" before setting the bi_server1 listen address.

Perform these steps to set the listen address for the Managed Server:

1. Log in to the Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. Expand the **Environment** node in the Domain Structure window.

4. Click **Servers**. The Summary of Servers page is displayed.

5. Select **bi_server1** in the Names column of the table. The Setting page for bi_server1 is displayed.

6. Set the **Listen Address** to APPHOST1VHN1.

7. Click **Save**.

8. Click **Activate Changes**.

9. The changes will not take effect until the bi_server1 Managed Server is restarted (ensure that Node Manager is up and running):

   a. On the Summary of Servers page, select the **Control** tab.

   b. Select **bi_server1** in the table and then click **Shutdown**.

   c. After the server has shut down, select **bi_server1** in the table and then click **Start**.

10. Restart the Oracle Business Intelligence system components, as follows:

    ```
    cd ORACLE_BASE/admin/instances/instance1/bin
    ./opmnctl restartproc
    ```

5.7.1 Updating the Oracle BI Publisher Scheduler Configuration

Follow the steps in this section to update the WebLogic JNDI URL for the Oracle BI Publisher Scheduler.

To update the Oracle BI Publisher Scheduler configuration:

1. Log in to Oracle BI Publisher at the following URL:

   http://APPHOST1VHN1:9704/xmlpserver

2. Click the **Administration** link.

3. Click **Scheduler Configuration** under System Maintenance. The Scheduler Configuration screen is displayed.

4. Update the **WebLogic JNDI URL** under JMS Configuration, as follows:

   t3://APPHOST1VHN1:9704

5. Click **Test JMS**.

   You should receive a confirmation message that JMS tested successfully.

6. Click **Apply**. The changes are sent to the cluster to be applied at run time.

7. Check the Scheduler status from the Scheduler Diagnostics tab.

5.8 Disabling Host Name Verification for the bi_server1 Managed Server

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server (see Chapter 7, "Setting Up Node Manager"). If you have not configured the server certificates, you will receive errors when managing the different Oracle WebLogic Server. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again after the EDG topology configuration is complete as described in Chapter 7, "Setting Up Node Manager."

Perform these steps to disable host name verification:

1. Log in to the Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. Expand the **Environment** node in the Domain Structure window.

4. Click **Servers**. The Summary of Servers page is displayed.

5. Select **bi_server1** in the Names column of the table. The settings page for the server is displayed.

6. Open the SSL tab.

7. Expand the **Advanced** section of the page.

8. Set **Hostname Verification** to 'None'.

9. Click **Save**.

10. Click **Activate Changes**.

11. The change will not take effect until the bi_server1 Managed Server is restarted (ensure that Node Manager is up and running):

    a. On the Summary of Servers page, select the **Control** tab.

    b. Select **bi_server1** in the table and then click **Shutdown**.

    c. Select **bi_server1** in the table and then click **Start**.

12. Restart the Oracle Business Intelligence system components, as follows:

    ```
    cd ORACLE_BASE/admin/instance1/bin
    ./opmnctl stopall
    ./opmnctl startall
    ```

5.9 Validating Oracle Business Intelligence on APPHOST1

Access the following URLs:

- Access `http://APPHOST1VHN1:9704/analytics` to verify the status of bi_server1.

- Access `http://APPHOST1VHN1:9704/wsm-pm` to verify the status of Web Services Manager. Click **Validate Policy Manager**. A list of policies and assertion templates available in the data is displayed.

    Note: The configuration is incorrect if no policies or assertion templates appear.

- Access `http://APPHOST1VHN1:9704/xmlpserver` to verify the status of the Oracle BI Publisher application.

- Access `http://APPHOST1VHN1:9704/ui` to verify the status of the Oracle Real-Time Decisions application.

- Access `http://APPHOST1VHN1:9704/bioffice/about.jsp` to verify the status of the Oracle BI for Microsoft Office application.

5.10 Configuring Oracle HTTP Server

This section covers how to configure Oracle HTTP Server for the Administration Server and for the bi_server1 Managed Server.

This section contains the following topics:

- Section 5.10.1, "Configuring Oracle HTTP Server for the Administration Server"
- Section 5.10.2, "Configuring Oracle HTTP Server for the bi_servern Managed Servers"
- Section 5.10.3, "Important Security Considerations"

5.10.1 Configuring Oracle HTTP Server for the Administration Server

To enable Oracle HTTP Server to route to the Administration Server, you must set the corresponding mount points in your HTTP server configuration:

1. For each of the Web servers on WEBHOST1 and WEBHOST2, create a file called admin.conf in the following directory:

   ORACLE_INSTANCE/config/OHS/*component*/moduleconf

   Then, add the following lines to this file:

```
NameVirtualHost *:80
<VirtualHost *:80>
   ServerName admin.mycompany.com:80
   ServerAdmin you@your.address
   RewriteEngine On
   RewriteOptions inherit

   # Admin Server and EM
   <Location /console>
     SetHandler weblogic-handler
     WebLogicHost ADMINVHN
     WeblogicPort 7001
     WLProxySSL ON
     WLProxySSLPassThrough ON
   </Location>

   <Location /consolehelp>
     SetHandler weblogic-handler
     WebLogicHost ADMINVHN
     WeblogicPort 7001
     WLProxySSL ON
     WLProxySSLPassThrough ON
   </Location>

   <Location /em>
     SetHandler weblogic-handler
     WebLogicHost ADMINVHN
     WeblogicPort 7001
     WLProxySSL ON
     WLProxySSLPassThrough ON
   </Location>
</VirtualHost>
```

Note that the value for the VirtualHost parameters depends on how the LBR virtual host was set up. You might need to use a different value than the one shown, such as 7777.

2. Restart Oracle HTTP Server on both WEBHOST1 and WEBHOST2, as follows:

```
WEBHOST1> ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc
ias-component=ohs1

WEBHOST2> ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc
ias-component=ohs2
```

5.10.2 Configuring Oracle HTTP Server for the bi_server*n* Managed Servers

To enable Oracle HTTP Server to route to bi_cluster, which contains the bi_server*n* Managed Servers, you must set the WebLogicCluster parameter to the list of nodes in the cluster:

1. On WEBHOST1 and WEBHOST2, add the following lines to the *ORACLE_BASE*/admin/*instance_name*/config/OHS/*component_name*/mod_wl_ohs.conf file:

```
#redirect browser requests that omit document/dir
RedirectMatch 301 /analytics$ /analytics/
RedirectMatch 301 /bimiddleware$ /bimiddleware/
RedirectMatch 301 /xmlpserver$ /xmlpserver/
RedirectMatch 301 /ui$ /ui/

# WSM-PM
<Location /wsm-pm>
    SetHandler weblogic-handler
    WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# BIEE Analytics
<Location /analytics>
    SetHandler weblogic-handler
    WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

<Location /analytics-ws>
    SetHandler weblogic-handler
    WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

<Location /bimiddleware>
    SetHandler weblogic-handler
    WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# MapViewer
<Location /mapviewer>
    SetHandler weblogic-handler
```

```
        WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
        WLProxySSL ON
        WLProxySSLPassThrough ON
</Location>

# BI Publisher
<Location /xmlpserver>
        SetHandler weblogic-handler
        WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
        WLProxySSL ON
        WLProxySSLPassThrough ON
</Location>

# Oracle RTD
<Location /ui>
        SetHandler weblogic-handler
        WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
        WLProxySSL ON
        WLProxySSLPassThrough ON
</Location>

<Location /rtis>
        SetHandler weblogic-handler
        WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
        WLProxySSL ON
        WLProxySSLPassThrough ON
</Location>

<Location /schema>
        SetHandler weblogic-handler
        WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
        WLProxySSL ON
        WLProxySSLPassThrough ON
</Location>

<Location /ws>
        SetHandler weblogic-handler
        WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
        WLProxySSL ON
        WLProxySSLPassThrough ON
</Location>

# BI Office
<Location /bioffice>
        SetHandler weblogic-handler
        WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
        WLProxySSL ON
        WLProxySSLPassThrough ON
</Location>

<Location /biofficeclient>
        SetHandler weblogic-handler
        WebLogicCluster APPHOST1VHN1:9704,APPHOST2VHN1:9704
        WLProxySSL ON
        WLProxySSLPassThrough ON
</Location>
```

Note: Add other resources as appropriate (such as analyticsRes or ActionSamples to support functionality in SampleApp.rpd).

2. Make sure the httpd.conf file located in the same directory as the mod_wl_ohs file contains the following lines:

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

NameVirtualHost *:7777

<VirtualHost *:7777>
    ServerName admin.mycompany.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit
</VirtualHost>
```

> **Note:** Values such as bi.mycompany.com:443, admin.mycompany.com:80 and you@your.address that are noted in this document serve as examples only. Enter values based on the actual environment.

3. Restart Oracle HTTP Server on both WEBHOST1 and WEBHOST2, as follows:

```
WEBHOST1> ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc
ias-component=ohs1
WEBHOST2> ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc
ias-component=ohs2
```

The servers specified in the WebLogicCluster parameters are only important at startup time for the plug-in. The list must provide at least one running cluster member for the plug-in to discover other members in the cluster. The listed cluster member must be running when Oracle HTTP Server is started. Oracle WebLogic Server and the plug-in work together to update the server list automatically with new, failed, and recovered cluster members.

Sample scenarios include:

- **Example 1:** If you have a two-node cluster and then add a third member, you do not need to update the configuration to add the third member. The third member will be discovered dynamically at run time.

- **Example 2:** You have a three-node cluster, but only two nodes are listed in the configuration. However, if both listed nodes are down when you start Oracle HTTP Server, then the plug-in would fail to route to the cluster. You must ensure that at least one of the listed nodes is running when you start Oracle HTTP Server.

If you list all the members of the cluster, then you guarantee you can route to the cluster, assuming at least one member is running when Oracle HTTP Server is started. For more information on configuring the WebLogic Server plug-in, see *Oracle Fusion Middleware Using Web Server Plug-Ins with Oracle WebLogic Server*.

5.10.3 Important Security Considerations

For security purposes, and because the load balancer terminates SSL requests (Oracle HTTP Server routes the requests as non-SSL to WebLogic Server), after SSL is

configured for the load balancer, turn on the WebLogic Plugin Enabled flag for the domain. To do this, follow these steps:

1. Log in to the Administration Console.

2. Click the domain name in the navigation tree on the left.

3. Click the **Web Applications** tab.

4. In the Change Center, click **Lock & Edit**.

5. Select **WebLogic Plugin Enabled**.

6. Click **Save**, then click **Activate Changes**.

7. Restart the Administration Server and Managed Server.

5.11 Registering Oracle HTTP Server with Oracle WebLogic Server

For Fusion Middleware Control to be able to manage and monitor Oracle HTTP Server instances, they must be registered with the domain. To do this, you must register Oracle HTTP Server with Oracle WebLogic Server using the following command:

```
WEBHOST1> cd ORACLE_INSTANCE/bin
WEBHOST1> ./opmnctl registerinstance -adminHost ADMINVHN -adminPort 7001
-adminUsername weblogic
```

You must also run this command from WEBHOST2 for OHS2.

> **Note:** After registering Oracle HTTP Server, it should appear as a manageable target in Fusion Middleware Control. To verify this, log in to Fusion Middleware Control. The WebTier item in the navigation tree should show that Oracle HTTP Server has been registered.

5.12 Setting the Frontend URL for the Administration Console

The Administration Console application tracks changes made to ports, channels and security using the console. When changes made through the console are activated, the console validates its current listen address, port, and protocol. If the listen address, port, and protocol are still valid, the console redirects the HTTP request replacing the host and port information with the Administration Server's listen address and port. When the Administration Console is accessed using a load balancing router (LBR), it is required to change the Administration Server's frontend URL so that the user's Web browser is redirected to the appropriate LBR address. To do this, follow these steps:

1. Log in to the Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. Expand the **Environment** node in the Domain Structure window.

4. Click **Servers**. The Summary of Servers page is displayed.

5. Select **AdminServer(admin)** in the Names column of the table. The settings page for AdminServer(admin) is displayed.

6. Click the **Protocols** tab.

7. Click the **HTTP** tab.

8. Set the **Frontend Host** field to admin.mycompany.com (your LBR address).

9. Set the **Frontend HTTP Port** to 80.

10. Click **Save**, then click **Activate Changes**.

To eliminate redirections, it is recommended that you disable the Administration Console's "Follow changes" feature. To do this, log in to the Administration Console and click **Preferences**, and then **Shared Preferences**. Clear the **Follow Configuration Changes** option, and then click **Save**.

5.13 Validating Access Through Oracle HTTP Server

Verify that the server status is reported as 'Running' in the Administration Console. If the server is shown as 'Starting' or 'Resuming,' wait for the server status to change to 'Started.' If another status is reported (such as 'Admin' or 'Failed'), check the server output log files for errors.

This section contains the following topics:

- Section 5.13.1, "Validating the Administration Console and Fusion Middleware Control"
- Section 5.13.2, "Validating bi_cluster"

5.13.1 Validating the Administration Console and Fusion Middleware Control

Validate the Administration Console and Fusion Middleware Control through both Oracle HTTP Server instances using the following URLs:

- http://WEBHOST*n*:7777/console
- http://WEBHOST*n*:7777/em

> **Note:** After setting the frontend URL to the LBR address, the access to the console through the WEBHOST*n* addresses will be redirected by the console to the frontend URL, thus validating the correct configuration of both Oracle HTTP Server and the LBR device.

- http://admin.mycompany.com/console
- http://admin.mycompany.com/em

For information on configuring system access through the load balancer, see Section 2.2.2, "Load Balancers."

5.13.2 Validating bi_cluster

Validate bi_cluster through Oracle HTTP Server using the following URLs (for both WEBHOST1 and WEBHOST2):

- http://WEBHOST*n*:7777/analytics
- http://WEBHOST*n*:7777/mapviewer
- http://WEBHOST*n*:7777/xmlpserver
- http://WEBHOST*n*:7777/ui
- http://WEBHOST*n*:7777/wsm-pm
- http://WEBHOST*n*:7777/bioffice/about.jsp

For information on configuring system access through the load balancer, see Section 2.2.2, "Load Balancers."

5.14 Manually Failing Over the Administration Server to APPHOST2

In case a node fails, you can fail over the Administration Server to another node. This section describes how to fail over the Administration Server from APPHOST1 to APPHOST2, and contains the following topics:

- Section 5.14.1, "Assumptions and Procedure"
- Section 5.14.2, "Validating Access to APPHOST2 Through Oracle HTTP Server"
- Section 5.14.3, "Failing the Administration Server Back to APPHOST1"

5.14.1 Assumptions and Procedure

Note the following assumptions:

- The Administration Server is configured to listen on ADMINVHN, and not on ANY address.
- The Administration Server is failed over from APPHOST1 to APPHOST2, and the two nodes have these IP addresses:
  - APPHOST1: 100.200.140.165
  - APPHOST2: 100.200.140.205
  - ADMINVHN: 100.200.140.206. This is the VIP where the Administration Server is running, assigned to eth*X:Y*, available in APPHOST1 and APPHOST2.
- The domain directory where the administration server is running in APPHOST1 is on a shared storage and is mounted also from APPHOST2.
- Oracle WebLogic Server and Oracle Fusion Middleware components have been installed in APPHOST2 (that is, the same paths for *ORACLE_HOME* and *MW_HOME* that exist on APPHOST1 are also available on APPHOST2).

Procedure

The following procedure shows how to fail over the Administration Server to a different node (APPHOST2):

1. Stop the Administration Server, if it is running.

2. Migrate the IP address to the second node:

   a. Run the following command as root on APPHOST1 (where *X:Y* is the current interface used by ADMINVHN):

   ```
   APPHOST1> /sbin/ifconfig ethX:Y down
   ```

   b. Run the following command on APPHOST2:

   ```
   APPHOST2> /sbin/ifconfig interface:index IP_address netmask netmask
   ```

   For example:

   ```
   APPHOST2> /sbin/ifconfig eth0:1 10.200.140.206 netmask 255.255.255.0
   ```

   Note: Make sure that the netmask and interface to be used match the available network configuration in APPHOST2.

   ---

   c. Update the routing tables using `arping`. For example:

```
APPHOST2> /sbin/arping -b -A -c 3 -I eth0 100.200.140.206
```

3. Start Node Manager in APPHOST2, using the instructions given in Step 3 of Section 5.4, "Starting the Administration Server on APPHOST1."

4. Start the Administration Server on APPHOST2, using the instructions given in Step 4 of Section 5.4, "Starting the Administration Server on APPHOST1."

5. Test that you can access the Administration Server on APPHOST2, as follows:

   a. Ensure that you can access the Administration Console at http://ADMINVHN:7001/console.

   b. Check that you can access and verify the status of components in Fusion Middleware Control at http://ADMINVHN:7001/em.

5.14.2 Validating Access to APPHOST2 Through Oracle HTTP Server

Perform the steps described in Section 5.13, "Validating Access Through Oracle HTTP Server" to check that you can access the Administration Server when it is running on APPHOST2.

5.14.3 Failing the Administration Server Back to APPHOST1

This step checks that you can fail back the Administration Server; that is, stop it on APPHOST2 and run it on APPHOST1 again. To do this, migrate ADMINVHN back to the APPHOST1 node as follows:

1. Make sure the Administration Server is not running.

2. Run the following command as root on APPHOST2.

   ```
   APPHOST2> /sbin/ifconfig ethX:Y down
   ```

3. Run the following command on APPHOST1:

   ```
   APPHOST1> /sbin/ifconfig interface:index IP_Address netmask netmask
   ```

   For example:

   ```
   APPHOST1> /sbin/ifconfig eth0:1 100.200.140.206 netmask 255.255.255.0
   ```

   > **Note:** Make sure that the netmask and interface you use matches the available network configuration in APPHOST1.

4. Update the routing tables using `arping`. For example:

   ```
   APPHOST1> /sbin/arping -b -A -c 3 -I ethZ 100.200.140.206
   ```

5. Start the Administration Server again on APPHOST1, as described in Step 4 of Section 5.4, "Starting the Administration Server on APPHOST1."

6. Test that you can access the Administration Console at http://ADMINVHN:7001/console.

7. Check that you can access and verify the status of components in Fusion Middleware Control at http://ADMINVHN:7001/em.

If you encounter problems with Administration Server failover, see Section 10.6.2, "Administration Server Fails to Start After a Manual Failover" for additional information.

5.15 Backing Up the Installation

After you have verified that the extended domain is working, back up the installation. This is a quick backup for the express purpose of immediate restore in case of problems in the further steps. The backup destination is the local disk. This backup can be discarded after the enterprise deployment setup is complete. At that point, the regular deployment-specific backup and recovery process can be initiated. *Oracle Fusion Middleware Administrator's Guide* provides further details. For information on describing the Oracle HTTP Server data that must be backed up and restored, refer to the "Backup and Recovery Recommendations for Oracle HTTP Server" section in that guide. For information on how to recover components, see the "Recovering Components" and "Recovering After Loss of Component Host" sections in the guide. For recommendations specific to recovering from the loss of a host, see the "Recovering Oracle HTTP Server to a Different Host" section in the guide. Also refer to *Oracle Database Backup and Recovery User's Guide* for information on database backup.

Perform these steps to back up the installation at this point:

1. Back up the Web tier:

   a. Shut down the instance using `opmnctl`:

   ```
   WEBHOSTn> ORACLE_BASE/admin/instance_name/bin/opmnctl stopall
   ```

   b. Back up the Middleware home on the Web tier using the following command (as root):

   ```
   WEBHOSTn> tar -cvpf BACKUP_LOCATION/web.tar MW_HOME
   ```

   c. Back up the Oracle instance on the Web tier using the following command:

   ```
   WEBHOSTn> tar -cvpf BACKUP_LOCATION/web_instance_name.tar ORACLE_INSTANCE
   ```

   d. Start the instance using `opmnctl`:

   ```
   WEBHOSTn> cd ORACLE_BASE/admin/instance_name/bin
   WEBHOSTn> opmnctl startall
   ```

   Repeat this step for WEBHOST2.

2. Back up the database. This is a full database backup (either hot or cold) using Oracle Recovery Manager (recommended) or operating system tools such as tar for cold backups if possible.

3. Back up the BI Instance in the application tier, as follows:

   a. Shut down the instance using opmnctl:

   ```
   APPHOST1> ORACLE_INSTANCE/bin/opmnctl stopall
   ```

   b. Back up the Middleware home on the application tier using the following command (as root):

   ```
   APPHOST1> tar -cvpf BACKUP_LOCATION/bi.tar MW_HOME
   ```

   c. Back up the Oracle instance on the application tier using the following command:

   ```
   APPHOST1> tar -cvpf BACKUP_LOCATION/bi_instance_name.tar ORACLE_INSTANCE
   ```

   d. Start the instance using opmnctl:

   ```
   APPHOST1> ORACLE_INSTANCE/bin/opmnctl startall
   ```

4. Back up the Administration Server and Managed Server domain directories to save your domain configuration. The configuration files all exist in the *ORACLE_ BASE*/admin/ *domain_name* directory. Run the following command to create the backup:

```
APPHOST1> tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
```

6

Scaling Out the Oracle Business Intelligence System

This chapter describes how to scale out the Oracle Business Intelligence system using the Configuration Assistant. It is assumed that an Oracle Business Intelligence *ORACLE_HOME* (binaries) has already been installed and is available from APPHOST1 and APPHOST2, and that a domain with an Administration Server has been created. This is the domain that will be extended in this chapter to support Oracle Business Intelligence components.

> **Important:** Oracle strongly recommends that you read *Oracle Fusion Middleware Release Notes* for any additional installation and deployment considerations before starting the setup process.

This chapter contains the following topics:

- Section 6.1, "Scaling Out the BI System on APPHOST2"
- Section 6.2, "Scaling Out the System Components"
- Section 6.3, "Configuring Secondary Instances of Singleton System Components"
- Section 6.4, "Configuring the bi_server2 Managed Server"
- Section 6.5, "Performing Additional Configuration for Oracle Business Intelligence Availability"
- Section 6.6, "Configuring a Default Persistence Store for Transaction Recovery"
- Section 6.7, "Starting and Validating Oracle Business Intelligence on APPHOST2"
- Section 6.8, "Validating Access Through Oracle HTTP Server"
- Section 6.9, "Configuring Node Manager for the Managed Servers"
- Section 6.10, "Configuring Server Migration for the Managed Servers"
- Section 6.11, "Backing Up the Installation"

6.1 Scaling Out the BI System on APPHOST2

This section explains how to scale out Oracle Business Intelligence on APPHOST2. Perform the steps in the following sections:

- Section 6.1.1, "Setting Up Oracle BI Enterprise Edition Shared Files"
- Section 6.1.2, "Using the Configuration Assistant to Scale Out the BI System"

6.1.1 Setting Up Oracle BI Enterprise Edition Shared Files

This section contains the following topics:

6.1.1.1 Setting the Location of the Shared Oracle BI Repository

When you specify a repository publishing directory for the Oracle BI repository, each Oracle BI Server instance loads the repository from the shared network location.

Perform the following steps in Oracle Enterprise Manager Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

2. Expand the **Business Intelligence** node in the Farm_*domain_name* window.

3. Click **coreapplication**.

4. Click **Deployment**, then click **Repository**.

5. Click **Lock and Edit Configuration**.

6. Select **Share Repository** and specify the **Shared Location** for the Oracle BI Repository.

   In a Windows environment, you must specify a UNC path name.

7. If you already have a repository deployed locally in your system, upload the repository again so that it gets copied to the shared location. Otherwise, you can skip this step.

8. Click **Apply**.

9. Click **Activate Changes**.

6.1.1.2 Setting the Location of the Shared Oracle BI Presentation Catalog

Each Presentation Services instance loads the Oracle BI Presentation Catalog from the catalog location specified in Fusion Middleware Control.

Perform the following steps:

1. Copy your existing (locally published) Oracle BI Presentation Catalog to the shared location. An example of a locally published catalog is:

   ```
   ORACLE_INSTANCE/bifoundation/OracleBIPresentationServicesComponent/
   coreapplication_obipsn/catalog/SampleAppLite
   ```

   You must perform this step before designating the **Catalog Location** from Fusion Middleware Control.

2. Log in to Fusion Middleware Control.

3. Expand the **Business Intelligence** node in the Farm_*domain_name* window.

4. Click **coreapplication**.

5. Click **Deployment**, then click **Repository**.

6. Click **Lock and Edit Configuration**.

7. Specify the **Catalog Location** for the shared Oracle BI Presentation Catalog.

   In a Windows environment, you must specify a UNC path name.

8. Click **Apply**.

9. Click **Activate Changes**.

6.1.1.3 Setting the Location of the Global Cache

The global cache resides on a shared file system storage device and stores purging events, seeding events (often generated by Agents), and result sets associated with seeding events. Note that each Oracle BI Server still maintains its own local query cache for regular queries.

Perform the following steps in Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

2. Expand the **Business Intelligence** node in the Farm_*domain_name* window.

3. Click **coreapplication**.

4. Click **Capacity Management**, then click **Performance**.

5. Click **Lock and Edit Configuration**.

6. In the Global Cache section, specify the shared location for storing purging and seeding cache entries in the **Global cache path** field. In a Windows environment, you must specify a UNC path name.

7. Enter a value for **Global cache size** to specify the maximum size of the global cache (for example, 250 MB).

8. Click **Apply**.

9. Click **Activate Changes**.

10. Click **Restart to apply recent changes**.

11. Click **Restart** under Manage System.

12. Click **Yes** in the confirmation dialog.

6.1.2 Using the Configuration Assistant to Scale Out the BI System

Run the Configuration Assistant from the *ORACLE_HOME* directory to scale out the BI system, as follows:

1. Change the directory to location of the Configuration Assistant, as follows:

```
APPHOST2> cd ORACLE_HOME/bin
```

2. Start the Oracle Business Intelligence Configuration Assistant:

```
APPHOST2> ./config.sh
```

3. In the Welcome screen, click **Next**.

4. In the Prerequisite Checks screen, verify that all checks complete successfully, and then click **Next**.

5. In the Create, Scale Out, or Extend screen, select **Scale Out BI System** and enter the following:

- **Host Name:** ADMINVHN

- **Port:** 7001

- **User name:** weblogic

- **User Password:** *your_password*

Click **Next**.

6. In the Scale Out BI System Details screen, enter the following:

   - **Middleware Home:** *ORACLE_BASE*/product/fmw (dimmed)

   - **Oracle Home:** *ORACLE_BASE*/product/fmw/Oracle_BI1 (dimmed)

   - **WebLogic Server Home:** *ORACLE_BASE*/product/fmw/wlserver_10.3 (dimmed)

   - **Domain Home:** *ORACLE_BASE*/admin/*domain_name*/mserver/*domain_name*

   - **Applications Home:** *ORACLE_BASE*/admin/*domain_name*/mserver/applications

   - **Instance Home:** *ORACLE_BASE*/admin/instance2

   - **Instance Name:** instance2 (dimmed)

   Click **Next**.

7. In the Configure Ports screen, select one of the following:

   - Auto Port Configuration

   - Specify Ports using Configuration File

   Click **Next**.

8. In the Specify Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your e-mail address.

   Click **Next**.

9. In the Summary screen, click **Configure**.

10. In the Configuration Progress screen, verify that all the Configuration Tools have completed successfully and click **Next**.

11. In the Complete screen, click **Finish**.

Usually, Node Manager is started automatically when config.sh completes. If Node Manager is not running for some reason, run these commands to start it on APPHOST2:

1. Run the setNMProps.sh script, which is located in the *ORACLE_COMMON_HOME*/common/bin directory, to set the StartScriptEnabled property to 'true' before starting Node Manager:

   ```
   APPHOST2> cd ORACLE_COMMON_HOME/common/bin
   APPHOST2> ./setNMProps.sh
   ```

   > **Note:** You must use the StartScriptEnabled property to avoid class loading failures.

2. Start Node Manager:

   ```
   APPHOST2> cd WL_HOME/server/bin
   APPHOST2> ./startNodeManager.sh
   ```

6.2 Scaling Out the System Components

Perform the following steps in Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

2. Expand the **Business Intelligence** node in the Farm_*domain_name* window.

3. Click **coreapplication**.

4. Click **Capacity Management**, then click **Scalability**.

5. Click **Lock and Edit Configuration**.

6. For the APPHOST2 instance2 Oracle instance, increment the Oracle Business Intelligence components by 1:

   ■ BI Servers

   ■ Presentation Servers

   ■ JavaHosts

7. Change the **Port Range From** and **Port Range To** to be the same as the APPHOST1 instance1 Oracle instance.

8. Click **Apply**.

9. Click **Activate Changes**.

You do not need to restart at this point, because you will perform a restart after completing the steps in Section 6.3.

6.3 Configuring Secondary Instances of Singleton System Components

The Oracle BI Cluster Controllers and Oracle BI Scheduler are singleton components that operate in active/passive mode. Configure a secondary instance of these components so that they are distributed for high availability.

Perform the following steps in Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

2. Expand the **Business Intelligence** node in the Farm_*domain_name* window.

3. Click **coreapplication**.

4. Click **Capacity Management**, then click **Availability**.

5. Click **Lock and Edit Configuration** to activate the Primary/Secondary Configuration section of the Availability tab.

6. Specify the Secondary Host/Instance for BI Scheduler and BI Cluster Controller.

7. Click **Apply**.

   Under Potential Single Points of Failure, it should report **No problems - all components have a backup**.

8. Click **Activate Changes**.

9. Click **Restart to apply recent changes**.

10. Click **Restart** under Manage System.

11. Click **Yes** in the confirmation dialog.

6.4 Configuring the bi_server2 Managed Server

This section explains how to configure the bi_server2 Managed Server, and contains the following topics:

- Section 6.4.1, "Setting the Listen Address for the bi_server2 Managed Server"
- Section 6.4.2, "Disabling Host Name Verification for the bi_server2 Managed Server"

6.4.1 Setting the Listen Address for the bi_server2 Managed Server

Ensure that you have performed the steps described in Section 2.2.3.1, "Enabling Virtual IPs for the Managed Servers" before setting the bi_server2 listen address.

Perform these steps to set the listen address for the Managed Server:

1. Log in to the Oracle WebLogic Server Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. Expand the **Environment** node in the Domain Structure window.

4. Click **Servers**. The Summary of Servers page is displayed.

5. Select **bi_server2** in the Names column of the table. The settings page for bi_server2 is displayed.

6. Set the **Listen Address** to APPHOST2VHN1.

7. Click **Save**.

8. Click **Activate Changes**.

   The changes will not take effect until the bi_server2 Managed Server is restarted.

6.4.2 Disabling Host Name Verification for the bi_server2 Managed Server

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server (see Chapter 7, "Setting Up Node Manager"). If you have not configured the server certificates, you will receive errors when managing the different Oracle WebLogic Servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again after the EDG topology configuration is complete as described in Chapter 7, "Setting Up Node Manager."

Perform these steps to disable host name verification:

1. Log in to the Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. Expand the **Environment** node in the Domain Structure window.

4. Click **Servers**. The Summary of Servers page is displayed.

5. Select **bi_server2** in the Names column of the table. The settings page for the server is displayed.

6. Open the SSL tab.

7. Expand the **Advanced** section of the page.

8. Set host name verification to 'None'.

9. Click **Save**.

10. Click **Activate Changes**.

11. The change will not take effect until the bi_server2 Managed Server is restarted (ensure that Node Manager is up and running):

    a. In the Summary of Servers screen, select the **Control** tab.

    b. Select **bi_server2** in the table and then click **Shutdown**.

    c. Select **bi_server2** in the table and then click **Start**.

12. Restart the BI System Components on APPHOST2, as follows:

    a. Log in to Fusion Middleware Control.

    b. Expand the **Business Intelligence** node in the Farm_*domain_name* window.

    c. Click **coreapplication**.

    d. On the Business Intelligence Overview page, click **Restart**.

6.5 Performing Additional Configuration for Oracle Business Intelligence Availability

This section describes additional high availability configuration tasks for Oracle BI Scheduler, Oracle Real-Time Decisions, Oracle BI Publisher, and Oracle BI for Microsoft Office. It contains the following topics:

- Section 6.5.1, "Additional Configuration Tasks for Oracle BI Scheduler"
- Section 6.5.2, "Additional Configuration Tasks for Oracle Real-Time Decisions"
- Section 6.5.3, "Additional Configuration Tasks for Oracle BI Publisher"
- Section 6.5.4, "Additional Configuration Tasks for Oracle BI for Microsoft Office"

6.5.1 Additional Configuration Tasks for Oracle BI Scheduler

If you use server-side scripts with Oracle BI Scheduler, it is recommended that you configure a shared directory for the scripts so that they can be shared by all Oracle BI Scheduler components in a cluster.

Perform these steps only if you are using server-side scripts.

To share Oracle BI Scheduler scripts:

1. Copy the default Oracle BI Scheduler scripts (for example, *ORACLE_ INSTANCE*/bifoundation/OracleBISchedulerComponent/coreapplication_ obisch1/scripts/common) and custom Oracle BI Scheduler scripts (for example, *ORACLE_ INSTANCE*/bifoundation/OracleBISchedulerComponent/coreapplication_ obisch1/scripts/scheduler) to the shared BI Scheduler scripts location.

2. Update the SchedulerScriptPath and DefaultScriptPath elements of the Oracle BI Scheduler instanceconfig.xml file, as follows:

- SchedulerScriptPath: Refers to the path where Oracle BI Scheduler-created job scripts are stored. Change this to the path of the shared BI Scheduler scripts location.

- DefaultScriptPath: Specifies the path where user-created job scripts (not agents) are stored. Change this to the path of the shared BI Scheduler scripts location.

In a Windows environment, you must specify a UNC path name.

3. Restart the Oracle BI Scheduler component, as follows:

```
opmnctl stopproc ias-component=coreapplication_obisch1
opmnctl startproc ias-component=coreapplication_obisch1
```

The instanceconfig.xml file for Oracle BI Scheduler is located in *ORACLE_INSTANCE*/config/OracleBISchedulerComponent/coreapplication_obisch*n*. You must update this file for each Oracle BI Scheduler component in the deployment.

6.5.2 Additional Configuration Tasks for Oracle Real-Time Decisions

This section contains the following topics:

- Section 6.5.2.1, "Configuring Oracle Real-Time Decisions Clustering Properties"
- Section 6.5.2.2, "Adding System Properties to the Server Start Tab"

6.5.2.1 Configuring Oracle Real-Time Decisions Clustering Properties

Perform the following steps in Fusion Middleware Control to set up cluster-specific configuration properties for Oracle RTD.

You only need to perform these steps for the first node in your deployment. You do not need to set cluster-specific configuration properties for Oracle RTD for subsequent nodes.

1. Log in to Fusion Middleware Control.

2. Expand the **Application Deployments** node in the Farm_*domain_name* window.

3. Click **OracleRTD(11.1.1)(bi_cluster)**.

4. Click any node under it. For example, **OracleRTD(11.1.1)(bi_server1)**.

5. In the right pane, click **Application Deployment**, and then select **System MBean Browser**.

6. In the System MBean Browser pane, expand **Application Defined MBeans**.

7. For any one of the servers under OracleRTD, navigate to the **SDClusterPropertyManager -> Misc** MBean and set the **DecisionServiceAddress** attribute to http://bi.mycompany.com. Other servers automatically get updated with the value you set.

8. Click **Apply**.

6.5.2.2 Adding System Properties to the Server Start Tab

After scaling out Oracle RTD, use the Administration Console to add three system properties to the **Server Start** tab of each Managed Server.

In the Administration Console, choose **Environment > Servers > bi_server<1,2> > Server Start > Arguments** and then add these three properties:

```
-Drtd.clusterRegistryJobIntervalMs=12000
-Drtd.clusterDepartureThresholdMs=50000
-Drtd.clusterDepartureThreshold2Ms=50000
```

Performing this task enables an instance of Oracle RTD to be migrated successfully from one host to another in the event of a failure of a Managed Server.

Even after these changes, if the server migration finishes in less than 50 seconds, the Oracle RTD batch framework will be in an inconsistent state.

If the enterprise has deployed any RTD Inline Services that host Batch Job implementations, and if after a server migration the batch console command, "batch-names", or its brief name, "bn", shows no registered batch jobs, then the Oracle

RTD Batch Manager service must be stopped and restarted. To do this, follow these steps:

1. In Fusion Middleware Control, expand the **WebLogic Domain** node in the left pane. Then, right-click **bifoundation_domain** and select **System MBean Browser**.

2. Locate the **BatchManager** MBean, under either **Application Defined MBeans > OracleRTD > Server:bi_server1 > Server** or under **Application Defined MBeans > OracleRTD > Server:bi_server2> Server**.

   It should be in one of these locations, but not both.

3. Locate the corresponding MBean attribute **BatchManagerEnabled** under **SDPropertyManager > Misc**. For example, if the BatchManager MBean is located in bi_server1, then select **Application Defined MBeans > OracleRTD > Server:bi_server1 > SDPropertyManager > Misc : BatchManagerEnabled**.

4. Set the BatchManagerEnabled attribute to **false** and click **Apply**.

5. Set the BatchManagerEnabled attribute back to **true** and click **Apply**. Performing this task causes the Batch Manager to stop and be restarted.

   When it restarts, it will be running on either the same server as before, or on a different server.

6. After restarting Batch Manager, note that the corresponding MBean does not always immediately get refreshed on the server where Batch Manager comes back up, so this is not a concern. Instead, verify that Batch Manager is now operational by using the Batch Console tool, as follows:

   a. Locate the zip file for the Oracle RTD client tools in the following location:

   ```
   ORACLE_HOME/clients/rtd/rtd_client_11.1.1.zip
   ```

   b. Because most Oracle RTD client tools do not run on UNIX, unzip this file in a location on a Windows computer (referred to here as *RTD_HOME*). Then, locate the batch console jar file in:

   ```
   RTD_HOME/client/Batch/batch-console.jar
   ```

   c. Change to this directory and execute the jar, passing to it the URL and port of either the Managed Server, or of the cluster proxy:

   ```
   java -jar batch-console.jar -url http://SERVER:PORT
   ```

   d. When prompted, enter the user name and password of a user who is a member of the Administrator role, BI_Adminstrator role, or some other role authorized to administer Oracle RTD batch jobs.

   e. When prompted for a command, enter bn:

   ```
   Checking server connection...
   command: bn
       CrossSellSelectOffers
   command:quit
   ```

   If Batch Manager has successfully restarted, then the "bn" command lists the names of all batch implementations hosted by all deployed RTD Inline Services.

   The commonly deployed example, CrossSell, hosts a batch implementation named CrossSellSelectOffers, shown in the preceding example.

6.5.3 Additional Configuration Tasks for Oracle BI Publisher

This section contains the following topics:

6.5.3.1 Setting the Location of the Shared Oracle BI Publisher Configuration Folder

Follow these steps to set server configuration options for Oracle BI Publisher:

1. Copy the contents of the *DOMAIN_HOME*/config/bipublisher/repository directory to the shared configuration folder location.

2. On either APPHOST1 or APPHOST2, log in to BI Publisher with Administrator credentials and select the **Administration** tab.

3. Under System Maintenance, select **Server Configuration**.

4. In the **Path** field under Configuration Folder, enter the shared location for the Configuration Folder.

5. Apply your changes and restart your BI Publisher application, as follows:

    a. Log in to the Administration Console.

    b. Click **Deployments** in the Domain Structure window.

    c. Select **bipublisher(11.1.1)**.

    d. Click **Stop**.

    e. After the application has stopped, click **Start**.

6. Because Oracle BI Publisher reads its configuration from the Administration Server central location rather than from the Managed Server's configuration directory when the Managed Servers are restarted, you must copy the XML configuration file for Oracle BI Publisher from the Managed Server to the Administration Server location.

    To do this, on APPHOST1, copy the file xmlp-server-config.xml from:

    ```
    ORACLE_BASE/admin/domain_name/mserver/domain_name/config/bipublisher
    ```

    to:

    ```
    ORACLE_BASE/admin/domain_name/aserver/domain_name/config/bipublisher
    ```

6.5.3.2 Setting Scheduler Configuration Options

Follow these steps to set Scheduler configuration options:

1. On APPHOST1, log in to BI Publisher with Administrator credentials and select the **Administration** tab.

2. Under System Maintenance, select **Scheduler Configuration**.

3. Select **Quartz Clustering** under the Scheduler Selection.

4. Click **Apply**.

6.5.3.3 Configuring Integration with Oracle BI Presentation Services

Follow these steps to configure Oracle BI Publisher integration with Oracle BI Presentation Services:

1. Log into Oracle BI Publisher with Administrator credentials and select the **Administration** tab.

2. Under **Integration**, select **Oracle BI Presentation Services**.

3. Verify and update the following:

- **Server Protocol:** HTTP
- **Server:** biinternal.mycompany.com
- **Port:** 80
- **URL Suffix:** analytics-ws/saw.dll

4. Click **Apply**.

5. Restart your Oracle BI Publisher application.

6.5.3.4 Setting the Oracle BI EE Data Source

The Oracle BI EE Data Source must point to the clustered Oracle BI Servers through the Cluster Controllers. Perform this task in Oracle BI Publisher.

To set the Oracle BI EE data source in Oracle BI Publisher:

1. Log in to Oracle BI Publisher with Administrator credentials and select the **Administration** tab.

2. Under **Data Sources**, select **JDBC Connection**.

3. Update the Oracle BI EE data source setting by changing the **Connection String** parameter to the following:

```
jdbc:oraclebi://primary_cluster_controller_host:primary_cluster_controller_
port/PrimaryCCS=primary_cluster_controller_host;PrimaryCCSPort=primary_cluster_
controller_port;SecondaryCCS=secondary_cluster_controller_host;
SecondaryCCSPort=secondary_cluster_controller_port;
```

For example:

```
jdbc:oraclebi://APPHOST1:9706/PrimaryCCS=APPHOST1;PrimaryCCSPort=9706;
SecondaryCCS=APPHOST2;SecondaryCCSPort=9706;
```

4. Deselect **Use System User** and specify administrator credentials for **Username** and **Password** (for example, weblogic).

5. Click **Test Connection**. You should receive a "Connection established successfully" message.

6. Click **Apply**.

6.5.3.5 Configuring JMS for Oracle BI Publisher

You must configure the location for all persistence stores to a directory visible from both nodes. Change all persistent stores to use this shared base directory.

1. Log into the Administration Console.

2. In the Domain Structure window, expand the **Services** node and then click the **Persistent Stores** node. The Summary of Persistent Stores page is displayed.

3. In the Change Center, click **Lock & Edit**.

4. Click **New**, and then **Create File Store**.

5. Enter a name (for example, BipJmsStore2) and target BI_SERVER2. Enter a directory that is located in shared storage so that it is accessible from both APPHOST1 and APPHOST2:

   ORACLE_BASE/admin/*domain_name*/bi_cluster/jms

6. Click **OK** and **Activate Changes**.

7. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Servers** node. The Summary of JMS Servers page is displayed.

8. In the Change Center, click **Lock & Edit**.

9. Click **New**.

10. Enter a name (for example, BipJmsServer2) and in the **Persistence Store** drop-down list, select **BipJmsStore2** and click **Next**.

11. Select **BI_SERVER2** as the target.

12. Click **Finish** and **Activate Changes**.

13. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Modules** node. The JMS Modules page is displayed.

14. In the Change Center, click **Lock & Edit**.

15. Click **BipJmsResource** and then click the Subdeployments tab.

16. Select **BipJmsSubDeployment** under Subdeployments.

17. Add the new Oracle BI Publisher JMS Server, **BipJmsServer2**, as an additional target for the subdeployment.

18. Click **Save** and **Activate Changes**.

To validate the JMS configuration performed for Oracle BI Publisher, perform the steps in Section 6.5.3.6, "Updating the Oracle BI Publisher Scheduler Configuration."

6.5.3.6 Updating the Oracle BI Publisher Scheduler Configuration

Follow the steps in this section to update the WebLogic JNDI URL and the JMS Shared Temp Directory for the Oracle BI Publisher Scheduler. You only need to perform the steps in this section on one of the APPHOSTS (either APPHOST1 or APPHOST2).

To update the Oracle BI Publisher Scheduler configuration:

1. Log in to Oracle BI Publisher at the one of the following URLs:

   ■ http://APPHOST1VHN1:9704/xmlpserver

   ■ http://APPHOST2VHN1:9704/xmlpserver

2. Click the **Administration** link.

3. Click **Scheduler Configuration** under System Maintenance. The Scheduler Configuration screen is displayed.

4. Update the **WebLogic JNDI URL** under JMS Configuration, as follows:

   t3://APPHOST1VHN1:9704,APPHOST2VHN1:9704

5. Update the **Shared Directory** by entering a directory that is located in the shared storage. This shared storage is accessible from both APPHOST1 and APPHOST2.

6. Click **Test JMS**.

You should receive a confirmation message that JMS tested successfully.

7. Click **Apply**.

8. Check the Scheduler status from the Scheduler Diagnostics tab.

6.5.4 Additional Configuration Tasks for Oracle BI for Microsoft Office

This section contains the following topics:

- Section 6.5.4.1, "Configuring Oracle BI for Microsoft Office Properties"
- Section 6.5.4.2, "Validating Oracle BI for Microsoft Office Configuration"

6.5.4.1 Configuring Oracle BI for Microsoft Office Properties

Follow these steps to perform additional configuration tasks for Oracle BI for Microsoft Office:

1. Validate the Oracle BI EE Office Server setup by accessing the following URLs:

- http://APPHOST1VHN1:9704/bioffice/about.jsp
- http://APPHOST2VHN1:9704/bioffice/about.jsp

The About Oracle BI EE Office Server page is displayed, as shown in Figure 6–1.

Figure 6–1   About Oracle BI EE Office Server Page
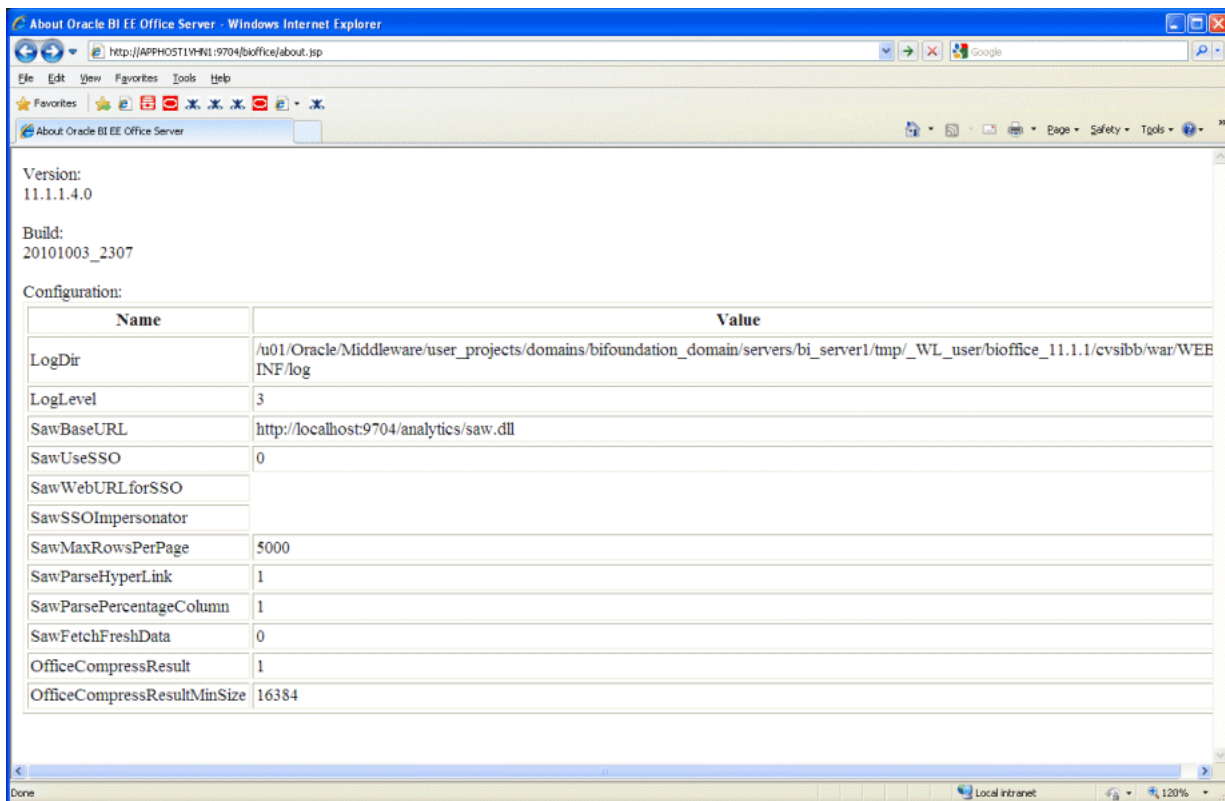
2. Go to the Oracle BI EE Office Server directory. For example:

DOMAIN_HOME/servers/*managed_server*/tmp/_WL_user/bioffice_
11.1.1/cvsibb/war/WEB-INF

If you are not sure how to locate the Oracle BI EE Office Server directory, check the
LogDir parameter on the About Oracle BI EE Office Server page. The Oracle BI EE
Office Server directory is the parent directory of the log directory.

3. On both APPHOST1 and APPHOST2, open bioffice.xml for editing and modify
the properties shown in Table 6–1.

Table 6–1   Properties in bioffice.xml

Property Name	Valid Value	Description
SawBaseURL	https://bi.mydomain.com:443 /analytics/saw.dll or https://bi.mydomain.com:443 /analytics-ws/saw.dll	Load Balancer Virtual Server Name URL for Oracle BI Presentation Services. **Important:** If SSO is enabled, then enter the URL for the protected analytics servlet that you deployed when configuring Oracle BI for Microsoft Office to integrate with the SSO-enabled Oracle BI Server. The URL that is specified for this property is used for Web services requests between the BI Office Server and Presentation Services.
SawUseSSO	0 = No (Default) 1 = Yes	Set this property to 1 if the Oracle Business Intelligence implementation is enabled for SSO.
SawWebURLforSSO	https://bi.mydomain.com:443 /analytics/saw.dll	When SSO is enabled, use this property to enter the public URL that allows external users to access Oracle Business Intelligence using SSO from Oracle BI for Microsoft Office.

4. Restart the Oracle BI for Microsoft Office application, as follows:

   a. Log in to the Administration Console.

   b. Click **Deployments** in the Domain Structure window.

   c. Select **bioffice(11.1.1)**.

   d. Click **Stop**.

   e. After the application has stopped, click **Start**.

5. Validate that the **SawBaseURL** parameter has been updated on the About Oracle
BI EE Office Server page.

6.5.4.2 Validating Oracle BI for Microsoft Office Configuration

Follow these steps to validate configuration for Oracle BI for Microsoft Office:

1. Log in to Oracle BI Presentation Services at:

   https://bi.mydomain.com:443/analytics

2. In the lower left pane, under the Get Started heading, select **Download BI
Desktop Tools** and then select **Oracle BI for MS Office**.

3. Install Oracle BI for Microsoft Office by running the Oracle BI Office InstallShield
Wizard.

4. Open Microsoft Excel or Microsoft Powerpoint.

5. From the **Oracle BI** menu, select **Preferences**.

6. In the Connections tab, select **New**.

7. Enter values for the following fields:

- **Server Name:** Provide a name for the connection.

- **BI Office Server:** Provide the URL for the Oracle BI EE Office Server.

- **Application Name:** Enter the Application Name that you defined for the Oracle BI EE Office Server when you deployed the Oracle BI EE Office Server application to WLS. The default name is **bioffice**.

- **Port:** Enter the Oracle BI EE Office Server port number.

Figure 6–2 shows the New Connection dialog.

Figure 6–2   New Connection Dialog for Oracle BI for Microsoft Office
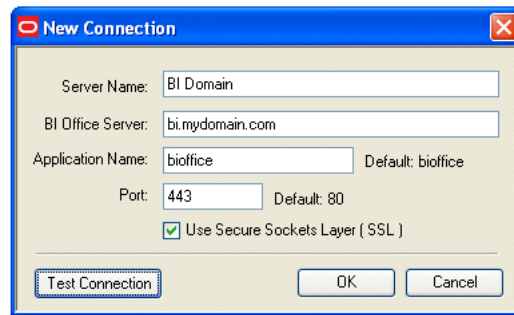
8. Click **Test Connection** to test the connection between the add-in and the Oracle BI EE Office Server.

Successful connections receive a Test connection successful message, as shown in Figure 6–3.

Figure 6–3   Test Connection Successful Message
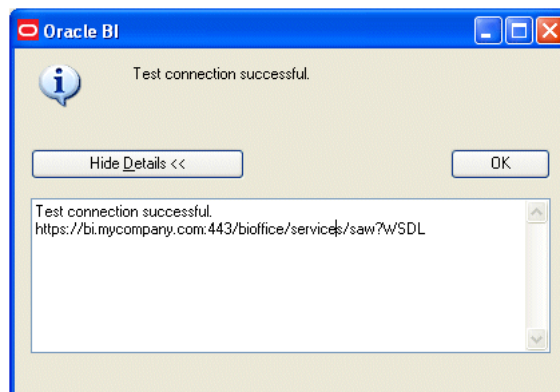
9. Log in as an Administrator (for example, weblogic) and validate that you can access the Oracle BI Task Pane, as shown in Figure 6–4.

Figure 6–4   Oracle BI Task Pane in Microsoft Excel
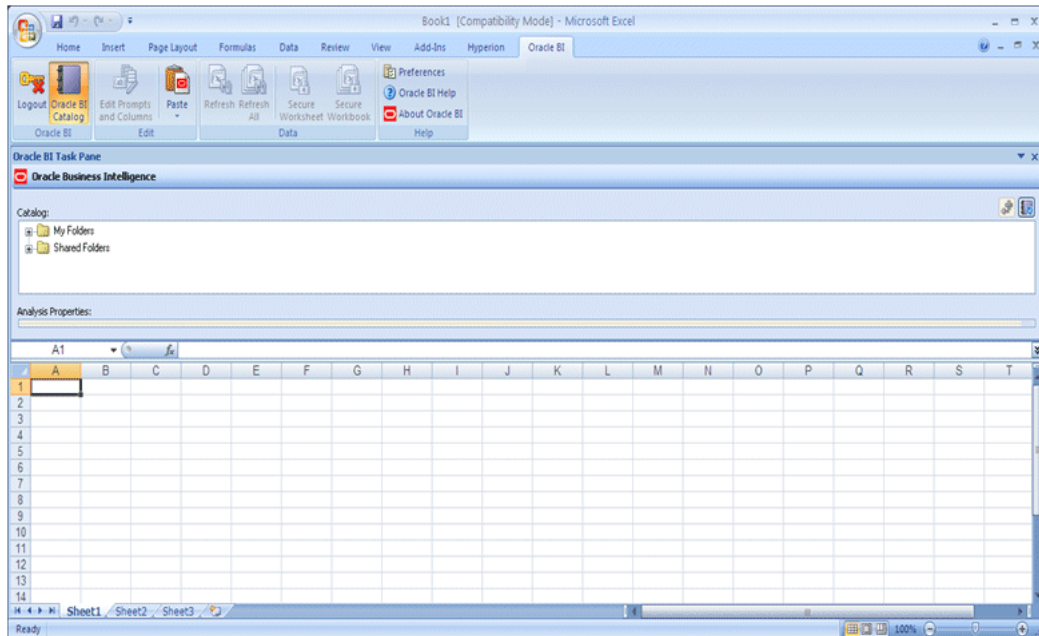
6.6 Configuring a Default Persistence Store for Transaction Recovery

Each server has a transaction log that stores information about committed transactions that are coordinated by the server that may not have been completed. The WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the servers within a cluster, store the transaction log in a location accessible to a server and its backup servers.

> **Note:**   Preferably, this location should be a dual-ported SCSI disk or on a Storage Area Network (SAN).

Perform these steps for each Managed Server to set the location for the default persistence store:

1. Log in to the Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node. The Summary of Servers page is displayed.

4. Click the name of the server (represented as a hyperlink) in the Names column of the table. The Settings page for the selected server is displayed, and defaults to the Configuration tab.

5. Open the **Services** tab.

6. In the Default Store section of the page, enter the path to the folder where the default persistent stores will store its data files. The directory structure of the path is as follows:

   ORACLE_BASE/admin/*domain_name*/*bi_cluster_name*/tlogs

Use the same path for each Managed Server. When the Managed Servers are restarted, subdirectories are created for each one.

7. Click **Save** and **Activate Changes**.

> **Note:** To enable migration of the Transaction Recovery service, specify a location on a persistent storage solution that is available to other servers in the cluster. Both bi_server1 and bi_server2 must be able to access this directory.

6.7 Starting and Validating Oracle Business Intelligence on APPHOST2

This section contains the following topics:

- Section 6.7.1, "Starting the bi_server2 Managed Server"
- Section 6.7.2, "Starting the Oracle Business Intelligence System Components"
- Section 6.7.3, "Validating Oracle Business Intelligence URLs"

6.7.1 Starting the bi_server2 Managed Server

Perform these steps to start the bi_server2 Managed Server:

1. Start the bi_server2 Managed Server using the Administration Console, as follows:

   a. Expand the **Environment** node in the Domain Structure window.

   b. Click **Servers**. The Summary of Servers page is displayed.

   c. Click the **Control** tab.

   d. Select **bi_server2** and then click **Start**.

2. Verify that the server status is reported as 'Running' in the Administration Console. If the server is shown as 'Starting' or 'Resuming,' wait for the server status to change to 'Started.' If another status is reported (such as 'Admin' or 'Failed'), check the server output log files for errors.

6.7.2 Starting the Oracle Business Intelligence System Components

You can control Oracle Business Intelligence system components using opmnctl commands.

To start the Oracle Business Intelligence system components using the opmnctl command-line tool:

1. Go to the directory that contains the OPMN command-line tool, located in *ORACLE_INSTANCE*/bin.

2. Run the opmnctl command to start the Oracle Business Intelligence system components:

   - opmnctl startall

     Starts OPMN and all Oracle Business Intelligence system components.

   - opmnctl start

     Starts OPMN only.

   - opmnctl startproc ias-component=*component_name*

Starts a particular system component. For example, where coreapplication_obips2 is the Presentation Services component:

opmnctl startproc ias-component=coreapplication_obips2

3. Check the status of the Oracle Business Intelligence system components:

opmnctl status

6.7.3 Validating Oracle Business Intelligence URLs

Access the following URLs:

- Access `http://APPHOST2VHN1:9704/analytics` to verify the status of bi_server1.

- Access `http://APPHOST2VHN1:9704/wsm-pm` to verify the status of Web Services Manager. Click **Validate Policy Manager**. A list of policies and assertion templates available in the data is displayed.

  Note: The configuration is incorrect if no policies or assertion templates appear.

- Access `http://APPHOST2VHN1:9704/xmlpserver` to verify the status of the Oracle BI Publisher application.

- Access `http://APPHOST2VHN1:9704/ui` to verify the status of the Oracle Real-Time Decisions application.

- Access `http://APPHOST2VHN1:9704/mapviewer` to verify the status of Oracle MapViewer.

6.8 Validating Access Through Oracle HTTP Server

You should verify URLs to ensure that the appropriate routing and failover is working from Oracle HTTP Server to bi_cluster. Perform these steps to verify the URLs:

1. While bi_server2 is running, stop bi_server1 using the Administration Console.

2. Access the following URLs to verify that routing and failover is functioning properly:

   - http://WEBHOST1:7777/analytics

   - http://WEBHOST1:7777/xmlpserver

   - http://WEBHOST1:7777/ui

3. Start bi_server1 from the Administration Console.

4. Stop bi_server2 from the Administration Console.

5. Access the following URLs to verify that routing and failover is functioning properly:

   - http://WEBHOST1:7777/analytics

   - http://WEBHOST1:7777/xmlpserver

   - http://WEBHOST1:7777/ui

6. Start bi_server2 from the Administration Console.

6.9 Configuring Node Manager for the Managed Servers

Oracle recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for

the different addresses communicating with the Administration Server and other servers. See Chapter 7, "Setting Up Node Manager" for further details. The procedures in that chapter must be performed twice using the information provided in Table 6–2.

Table 6–2   Details for Host Name Verification for Node Manager and Servers

Run	Host Name (HOST)	Server Name (WLS_SERVER)
Run1:	APPHOST1	bi_server1
Run2:	APPHOST2	bi_server2

6.10 Configuring Server Migration for the Managed Servers

Server Migration is required for proper failover of the Oracle BI Publisher components in the event of failure in any of the APPHOST1 and APPHOST2 nodes. See Chapter 8, "Configuring Server Migration" for further details.

6.11 Backing Up the Installation

After you have verified that the scaled out domain is working, back up the installation. This is a quick backup for the express purpose of immediate restore in case of problems in the further steps. The backup destination is the local disk. This backup can be discarded after the enterprise deployment setup is complete. At that point, the regular deployment-specific backup and recovery process can be initiated. *Oracle Fusion Middleware Administrator's Guide* provides further details. For information on describing the Oracle HTTP Server data that must be backed up and restored, refer to the "Backup and Recovery Recommendations for Oracle HTTP Server" section in that guide. For information on how to recover components, see the "Recovering Components" and "Recovering After Loss of Component Host" sections in the guide. For recommendations specific to recovering from the loss of a host, see the "Recovering Oracle HTTP Server to a Different Host" section in the guide. Also refer to *Oracle Database Backup and Recovery User's Guide* for information on database backup.

Perform these steps to back up the installation at this point:

1. Back up the Web tier:

   a. Shut down the instance using `opmnctl`:

      ```
      WEBHOSTn> ORACLE_BASE/admin/instance_name/bin/opmnctl stopall
      ```

   b. Back up the Middleware home on the Web tier using the following command (as root):

      ```
      WEBHOSTn> tar -cvpf BACKUP_LOCATION/web.tar MW_HOME
      ```

   c. Back up the Oracle instance on the Web tier using the following command:

      ```
      WEBHOSTn> tar -cvpf BACKUP_LOCATION/web_instance_name.tar ORACLE_INSTANCE
      ```

      Repeat this step for WEBHOST2.

   d. Start the instance using `opmnctl`:

      ```
      WEBHOSTn> cd ORACLE_BASE/admin/instance_name/bin
      WEBHOSTn> opmnctl startall
      ```

2. Back up the database. This is a full database backup (either hot or cold) using Oracle Recovery Manager (recommended) or operating system tools such as tar for cold backups if possible.

3. Back up the BI Instance in the application tier, as follows:

    a. Shut down the instance using opmnctl:

```
APPHOST1> ORACLE_INSTANCE/bin/opmnctl stopall
```

    b. Back up the Middleware home on the application tier using the following command (as root):

```
APPHOST1> tar -cvpf BACKUP_LOCATION/bi.tar MW_HOME
```

    c. Back up the Oracle instance on the application tier using the following command:

```
APPHOST1> tar -cvpf BACKUP_LOCATION/bi_instance_name.tar ORACLE_INSTANCE
```

    d. Start the instance using opmnctl:

```
APPHOST1> ORACLE_INSTANCE/bin/opmnctl startall
```

4. Back up the Administration Server and Managed Server domain directories to save your domain configuration. The configuration files all exist in the *ORACLE_BASE*/admin/ *domain_name* directory. Run the following command to create the backup:

```
APPHOST1> tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
```

Note: Create backups on all computers in the application tier by following the steps shown in this section.

7

Setting Up Node Manager

This chapter describes how to configure Node Manager in accordance with the EDG recommendations.

> **Important:** Oracle strongly recommends that you read *Oracle Fusion Middleware Release Notes* for any additional installation and deployment considerations before starting the setup process.

This chapter contains the following topics:

- Section 7.1, "About Setting Up Node Manager"
- Section 7.2, "Changing the Location of the Node Manager Log"
- Section 7.3, "Enabling Host Name Verification Certificates for Node Manager"
- Section 7.4, "Starting Node Manager"

7.1 About Setting Up Node Manager

Node Manager enables you to start and stop the Administration Server and the Managed Servers.

Process

The procedures described in this chapter must be performed for various components of the enterprise deployment topology outlined in Section 1.5, "Enterprise Deployment Reference Topology." The following variables are used in this chapter to distinguish between component-specific items:

- **WLS_SERVER:** Refers to an Oracle WebLogic Server Managed Server for the enterprise deployment component (for example, bi_server1).

- **HOST:** Refers to a host computer for the enterprise deployment component (for example, APPHOST1).

- **VIP:** Refers to a virtual IP for the enterprise deployment component (for example, APPHOST1VHN1).

The values to be used for these variables are provided in the component-specific chapters in this EDG. Note that the procedures in this chapter must be performed multiple times for each VIP-and-IP pair using the information provided in the component-specific chapters.

Recommendations

Oracle provides two main recommendations for Node Manager configuration in enterprise deployment topologies:

1. Oracle recommends placing the Node Manager log file in a location different from the default one (which is inside the Middleware home where Node Manager resides). See Section 7.2, "Changing the Location of the Node Manager Log" for further details.

2. Oracle also recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses used in the domain. This chapter explains the steps for configuring certificates in the hosts for host name verification. See Section 7.3, "Enabling Host Name Verification Certificates for Node Manager" for further details.

> **Note:** The passwords used in this guide are provided only as examples. Use secure passwords in a production environment. For example, use passwords that consist of random sequences of both uppercase and lowercase characters as well as numbers.

7.2 Changing the Location of the Node Manager Log

Change the location of the Node Manager log by editing the nodemanager.properties file, located in the *MW_HOME*/wlserver_10.3/common/nodemanager directory. Add the new location for the log file using the following line:

```
LogFile=ORACLE_BASE/admin/nodemanager.log
```

Oracle recommends that this location be outside the *MW_HOME* directory and inside the admin directory for the EDG.

Restart Node Manager for the change to take effect.

7.3 Enabling Host Name Verification Certificates for Node Manager

Setting up host name verification certificates for communication between Node Manager and the Administration Server consists of the following steps:

- Step 1: Generating Self-Signed Certificates Using the utils.CertGen Utility
- Step 2: Creating an Identity Keystore Using the utils.ImportPrivateKey Utility
- Step 3: Creating a Trust Keystore Using the Keytool Utility
- Step 4: Configuring Node Manager to Use the Custom Keystores
- Step 5: Configuring Managed Servers to Use the Custom Keystores
- Step 6: Changing the Host Name Verification Setting for the Managed Servers

7.3.1 Generating Self-Signed Certificates Using the utils.CertGen Utility

The certificates added in this chapter (as an example) address a configuration where Node Manager listens on a physical host name (HOST.mycompany.com) and a Managed Server listens on a virtual host name (VIP.mycompany.com). Whenever a Managed Server is using a virtual host name, it is implied that the Managed Server can be migrated from one node to another. Consequently, the directory where keystores and trust keystores are maintained ideally must reside on a shared storage that is

accessible from the failover. If additional host names are used in the same or different nodes, the steps in this example will need to be extended to:

- Add the required host names to the certificate stores (if they are different from HOST.mycompany.com and VIP.mycompany.com).

- Change the identity and trust store location information for Node Manager (if the additional host names are used by Node Manager) or for the servers (if the additional host names are used by Managed Servers).

Follow these steps to create self-signed certificates on HOST. These certificates should be created using the network name or alias. For information on using trust CA certificates instead, see "Configuring Identity and Trust" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

The following examples configure certificates for HOST.mycompany.com and VIP.mycompany.com; that is, it is assumed that both a physical host name (HOST) and a virtual host name (VIP) are used in HOST. It is also assumed that HOST.mycompany.com is the address used by Node Manager, and VIP.mycompany.com is the address used by a Managed Server or the Administration Server. This is the common situation for nodes hosting an Administration Server and an Oracle Fusion Middleware component, or for nodes where two Managed Servers coexist with one server listening on the physical host name and one server using a virtual host name (which is the case for servers that use migration servers).

1. Set up your environment by running the *WL_HOME*/server/bin/setWLSEnv.sh script. In the Bourne shell, run the following commands:

   ```
   HOST> cd WL_HOME/server/bin
   HOST> ../setWLSEnv.sh
   ```

   Verify that the `CLASSPATH` environment variable is set:

   ```
   HOST> echo $CLASSPATH
   ```

2. Create a user-defined directory for the certificates. For example, create a directory called 'certs' under the *ORACLE_BASE*/admin/*domain_name*/*cluster_name* directory. Note that certificates can be shared across WLS domains.

   ```
   HOST> cd ORACLE_BASE/admin/domain_name/cluster_name
   HOST> mkdir certs
   ```

   > **Note:** The directory where keystores and trust keystores are maintained must be on shared storage that is accessible from all nodes so that when the servers fail over (manually or with server migration), the appropriate certificates can be accessed from the failover node. Oracle recommends using central or shared stores for the certificates used for different purposes (such as SSL set up for HTTP invocations).

3. Change the directory to the directory that you just created:

   ```
   HOST> cd certs
   ```

4. Run the utils.CertGen tool from the user-defined directory to create the certificates for both HOST.mycompany.com and VIP.mycompany.com.

   Syntax (all on a single line):

   ```
   java utils.CertGen Key_Passphrase Cert_File_Name Key_File_Name
   [export | domestic] [Host_Name]
   ```

Examples:

```
HOST> java utils.CertGen welcome1 HOST.mycompany.com_cert
HOST.mycompany.com_key domestic HOST.mycompany.com

HOST> java utils.CertGen welcome1 VIP.mycompany.com_cert
VIP.mycompany.com_key domestic VIP.mycompany.com
```

Sample output for the command shown in the first example is:

```
...... Will generate certificate signed by CA from CertGenCA.der file
...... With Domestic Key Strength
...... Common Name will have Hostname HOST.mycompany.com
...... Issuer CA name is CN=CertGenCAB,OU=FOR TESTING ONLY,O=MyOrganization,
L=MyTown,ST=MyState,C=US
```

7.3.2 Creating an Identity Keystore Using the utils.ImportPrivateKey Utility

Follow these steps to create an identity keystore on HOST:

1. Create a new identity keystore called appIdentityKeyStore using the utils.ImportPrivateKey utility. Create this keystore under the same directory as the certificates (that is, *ORACLE_BASE*/admin/*domain_name*/aserver/*domain_name*/certs).

> **Note:** The identity store is created (if none exists) when you import a certificate and the corresponding key into the identity store using the utils.ImportPrivateKey utility.

2. Import the certificate and private key for both HOST.mycompany.com and VIP.mycompany.com into the identity store. Make sure that you use a different alias for each of the certificate/key pairs imported.

Syntax (all on a single line):

```
java utils.ImportPrivateKey Keystore_File Keystore_Password
Certificate_Alias_to_Use Private_Key_Passphrase
Certificate_File Private_Key_File [Keystore_Type]
```

Examples:

```
HOST> java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1
appIdentity1 welcome1 ORACLE_BASE/admin/domain_name/aserver/domain_name/
certs/HOST.mycompany.com_cert.pem ORACLE_BASE/admin/domain_name/
aserver/domain_name/certs/HOST.mycompany.com_key.pem

HOST> java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1
appIdentity2 welcome1 ORACLE_BASE/admin/domain_name/aserver/
domain_name/certs/VIP.mycompany.com_cert.pem ORACLE_BASE/admin/
domain_name/aserver/domain_name/certs/VIP.mycompany.com_key.pem
```

7.3.3 Creating a Trust Keystore Using the Keytool Utility

You only need to perform the steps in this section for the first Managed Server.

Follow these steps to create the trust keystore on HOST1:

1. Copy the standard Java keystore to create the new trust keystore because it already contains most of the root CA certificates needed. Oracle does not recommend

modifying the standard Java trust keystore directly. Copy the standard Java keystore CA certificates located under the *WL_HOME*/server/lib directory to the same directory as the certificates. For example:

```
HOST> cp WL_HOME/server/lib/cacerts ORACLE_BASE/admin/domain_
name/aserver/domain_name/certs/appTrustKeyStore.jks
```

2. The default password for the standard Java keystore is 'changeit'. Oracle recommends always changing the default password. Use the keytool utility to do this. The syntax is (all on a single line):

```
APPHOST1> keytool -storepasswd -new New_Password -keystore Trust_Keystore
-storepass Original_Password
```

For example:

```
HOST> keytool -storepasswd -new welcome1 -keystore appTrustKeyStore.jks
-storepass changeit
```

3. The CA certificate CertGenCA.der is used to sign all certificates generated by the utils.CertGen tool. It is located in the *WL_HOME*/server/lib directory. This CA certificate must be imported into the appTrustKeyStore using the keytool utility. The syntax is (all on a single line):

```
HOST> keytool -import -v -noprompt -trustcacerts -alias Alias_Name
-file CA_File_Location -keystore Keystore_Location -storepass Keystore_Password
```

For example:

```
HOST> keytool -import -v -noprompt -trustcacerts -alias clientCACert -file
WL_HOME/server/lib/CertGenCA.der -keystore appTrustKeyStore.jks -storepass
welcome1
```

7.3.4 Configuring Node Manager to Use the Custom Keystores

To configure Node Manager to use the custom keystores, add the following lines to the end of the nodemanager.properties file located in the *WL_HOME*/common/nodemanager directory:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity_Keystore
CustomIdentityKeyStorePassPhrase=Identity_Keystore_Password
CustomIdentityAlias=Identity_Keystore_Alias
CustomIdentityPrivateKeyPassPhrase=Private_Key_Used_When_Creating_Certificate
```

Make sure to use the correct value for `CustomIdentityAlias` on each node. For example, on HOST2, use appIdentity2.

For example:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=ORACLE_BASE/admin/domain_name/aserver/domain_name/
certs/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=welcome1
CustomIdentityAlias=appIdentity2
CustomIdentityPrivateKeyPassPhrase=welcome1
```

The passphrase entries in the nodemanager.properties file get encrypted when you start Node Manager as described in Section 7.4, "Starting Node Manager." For security reasons, you want to minimize the time the entries in the nodemanager.properties file are left unencrypted. After you edit the file, you should start Node Manager as soon as possible so that the entries get encrypted.

7.3.5 Configuring Managed Servers to Use the Custom Keystores

You must perform the steps in this section for the Administration Server and all Managed Servers.

To configure the identity and trust keystores:

1. Log in to the Oracle WebLogic Server Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. Expand the **Environment** node in the Domain Structure window.

4. Click **Servers**. The Summary of Servers page is displayed.

5. Click the name of the server for which you want to configure the identity and trust keystores (WLS_SERVER). The settings page for the selected server is displayed.

6. Select **Configuration**, and then select **Keystores**.

7. In the **Keystores** field, change to the **Custom Identity and Custom Trust** method for storing and managing private keys/digital certificate pairs and trusted CA certificates.

8. In the Identity section, define attributes for the identity keystore as follows:

   a. **Custom Identity Keystore:** Enter the fully qualified path to the identity keystore:

      ```
      ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/
      appIdentityKeyStore.jks
      ```

   b. **Custom Identity Keystore Type:** Ensure that this field is blank. Do not keep the default value of JKS.

   c. **Custom Identity Keystore Passphrase:** Enter the keystore password (*Keystore_Password*) you provided in Section 7.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."

      This attribute might be optional or required, depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. Oracle WebLogic Server only reads from the keystore, so whether you need to define this property depends on the requirements of the keystore.

9. In the Trust section, define properties for the trust keystore:

   a. **Custom Trust Keystore:** Enter the fully qualified path to the trust keystore:

      ```
      ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/
      appTrustKeyStore.jks
      ```

   b. **Custom Trust Keystore Type:** This field defaults to **JKS**. You must explicitly remove the default value so that the field is blank.

   c. **Custom Trust Keystore Passphrase:** Enter the password you provided for *New_Password* in Section 7.3.3, "Creating a Trust Keystore Using the Keytool Utility."

      This attribute might be optional or required, depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. Oracle WebLogic Server only reads from the keystore, so whether you define this property depends on the requirements of the keystore.

10. Click **Save**.

11. In the Change Center, click **Activate Changes**.

12. Select **Configuration**, then select **SSL**.

13. In the Change Center, click **Lock & Edit**.

14. In the **Private Key Alias** field, enter the alias you used for the host name on which the Managed Server listens.

    In the **Private Key Passphrase** and the **Confirm Private Key Passphrase** fields, enter the password for the keystore that you created in Section 7.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."

15. Click **Save**.

16. In the Change Center, click **Activate Changes**.

7.3.6 Changing the Host Name Verification Setting for the Managed Servers

After the steps in the previous sections have been performed, you should set host name verification for the affected Managed Servers to **Bea Host Name Verifier**. To do this, perform the following steps for all Managed Servers:

1. Log in to the Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. Expand the **Environment** node in the Domain Structure window.

4. Click **Servers**. The Summary of Servers page is displayed.

5. Select the Managed Server in the **Names** column of the table. The settings page for the server is displayed.

6. Open the **SSL** tab.

7. Expand the **Advanced** section of the page.

8. Set **Hostname Verification** to **BEA Hostname Verifier**.

9. Click **Save**.

10. In the Change Center, click **Activate Changes**.

11. Restart the Managed Server for which the changes have been applied.

7.4 Starting Node Manager

When using a common/shared storage installation for *MW_HOME*, Node Manager is started from different nodes using the same base configuration (nodemanager.properties). In that case, it is required to add the certificate for all the nodes that share the binaries to the appIdentityKeyStore.jks identity store. To do this, create the certificate for the new node and import it to appIdentityKeyStore.jks as described in Section 7.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility." After the certificates are available in the store, each Node Manager must point to a different identity alias to send the correct certificate to the Administration Server. To do this, set different environment variables before starting Node Manager in the different nodes:

```
HOST> cd WL_HOME/server/bin
HOST> export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityX
```

> **Note:** Make sure to specify the custom identity alias specifically assigned to each host. For example, specify appIdentity1 for HOST1 and appIdentity2 for HOST2.

If you are not using a common/shared storage installation for *MW_HOME*, run these commands to restart Node Manager on HOST:

1. Stop the Node Manager process by using CTRL-C in the shell where it was started, or by process identification and kill in the operating system.

2. Start Node Manager, as follows:

   ```
   HOST> cd WL_HOME/server/bin
   HOST> ./startNodeManager.sh
   ```

   > **Note:** If you have not configured and started Node Manager for the first time, run the *ORACLE_COMMON_HOME*/common/bin/setNMProps.sh script. This will enable the use of the start script, which is required for Oracle Business Intelligence.

8

Configuring Server Migration

In this enterprise topology, you must configure server migration for the bi_server1 and bi_server2 Managed Servers. To do this, you configure the bi_server1 Managed Server to restart on APPHOST2 should a failure occur, and you configure the bi_server2 Managed Server to restart on APPHOST1 should a failure occur. For this configuration, the bi_server1 and bi_server2 servers listen on specific floating IPs that are failed over by WLS Server Migration.

> **Important:** Oracle strongly recommends that you read *Oracle Fusion Middleware Release Notes* for any additional installation and deployment considerations before starting the setup process.

This chapter contains the following topics:

- Section 8.1, "Setting Up a User and Tablespace for the Server Migration Leasing Table"

- Section 8.2, "Creating a Multi-Data Source Using the Administration Console"

- Section 8.3, "Enabling Host Name Verification Certificates"

- Section 8.4, "Editing the Node Manager Properties File"

- Section 8.5, "Setting Environment and Superuser Privileges for the wlsifconfig.sh Script"

- Section 8.6, "Configuring Server Migration Targets"

- Section 8.7, "Testing the Server Migration"

8.1 Setting Up a User and Tablespace for the Server Migration Leasing Table

The first step is to set up a user and tablespace for the server migration leasing table:

1. Create a tablespace called 'leasing'. For example, log on to SQL*Plus as the sysdba user and run the following command:

```
SQL> create tablespace leasing logging datafile 'DB_
HOME/oradata/orcl/leasing.dbf' size 32m autoextend on next 32m maxsize 2048m
extent management local;
```

2. Create a user named 'leasing' and assign to it the leasing tablespace:

```
SQL> create user leasing identified by welcome1;
SQL> grant create table to leasing;
```

```
SQL> grant create session to leasing;
SQL> alter user leasing default tablespace leasing;
SQL> alter user leasing quota unlimited on LEASING;
```

3. Create the leasing table using the leasing.ddl script:

   a. Copy the leasing.ddl file located in either the *WL_HOME*/server/db/oracle/ 817 or the *WL_HOME*/server/db/oracle/920 directory to your database node.

   b. Connect to the database as the leasing user.

   c. Run the leasing.ddl script in SQL*Plus:

      ```
      SQL> @Copy_Location/leasing.ddl;
      ```

8.2 Creating a Multi-Data Source Using the Administration Console

The second step is to create a multi-data source for the leasing table from the Oracle WebLogic Server Administration Console. You create a data source to each of the Oracle RAC database instances during the process of setting up the multi-data source, both for these data sources and the global leasing multi-data source. Note the following considerations when creating a data source:

- Make sure that this is a non-XA data source.

- The names of the multi-data sources are in the format of *<MultiDS>-rac0*, *<MultiDS>-rac1*, and so on.

- Use Oracle's Driver (Thin) Version 9.0.1, 9.2.0, 10, 11.

- Data sources do not require support for global transactions. Therefore, do *not* use any type of distributed transaction emulation/participation algorithm for the data source (do not choose the **Supports Global Transactions** option, or the **Logging Last Resource**, **Emulate Two-Phase Commit**, or **One-Phase Commit** suboptions), and specify a service name for your database.

- Target these data sources to the bi_cluster.

- Make sure the initial connection pool capacity of the data sources is set to 0 (zero). To do this, select **Services**, and then **Data Sources**. In the Data Sources list, click the name of the data source, and then click the **Connection Pool** tab and enter **0** (zero) in the **Initial Capacity** field.

Creating a Multi-Data Source

Perform these steps to create a multi-data source:

1. In the Domain Structure window in the Administration Console, expand the **Services** node, then click **Data Sources**. The Summary of JDBC Data Sources page is displayed.

2. In the Change Center, click **Lock & Edit**.

3. Click **New**, then select **Multi Data Source**. The Create a New JDBC Multi Data Source page is displayed.

4. For **Name**, enter leasing.

5. For **JNDI Name**, enter jdbc/leasing.

6. For **Algorithm Type**, select **Failover** (the default).

7. Click **Next.**

8. On the Select Targets page, select **bi_cluster** as the target.

9. Click **Next**.

10. On the Select Data Source Type page, select **non-XA driver** (the default).

11. Click **Next**.

12. Click **Create a New Data Source**.

13. For **Name**, enter leasing-rac0. For **JNDI Name**, enter jdbc/leasing-rac0. For **Database Type**, select **Oracle**.

> **Note:** When creating the multi-data sources for the leasing table, enter names in the format of *<MultiDS>*-rac0, *<MultiDS>*-rac1, and so on.

14. Click **Next**.

15. For **Database Driver**, select **Oracle's Driver (Thin) for RAC Service-Instance connections; Versions:10 and later**.

16. Click **Next**.

17. Deselect **Supports Global Transactions**.

18. Click **Next**.

19. Enter the leasing schema details, as follows:

   - **Service Name:** Enter the service name of the database.

   - **Database name:** Enter the Instance Name for the first instance of the Oracle RAC database.

   - **Host Name:** Enter the name of the node that is running the database. For the Oracle RAC database, specify the first instance's VIP name or the node name as the host name.

   - **Port:** Enter the port number for the database (1521).

   - **Database User Name:** Enter leasing.

   - **Password:** Enter the leasing password.

20. Click **Next**.

21. Click **Test Configuration** and verify that the connection works.

22. Click **Next**.

23. On the Select Targets page, select **bi_cluster** as the target.

24. Click **Finish**.

25. Click **Create a New Data Source** for the second instance of your Oracle RAC database, target it to the bi_cluster, repeating the steps for the second instance of your Oracle RAC database.

26. On the Add Data Sources page, add **leasing-rac0** and **leasing-rac1** to your datasource by moving them to the **Chosen** list.

27. Click **Finish**.

28. Click **Activate Changes**.

8.3 Enabling Host Name Verification Certificates

The third step is to create the appropriate certificates for host name verification between Node Manager and the Administration Server. This procedure is described in Section 7.3, "Enabling Host Name Verification Certificates for Node Manager." If you have not yet created these certificates, perform the steps in this section to create certificates for host name verification between Node Manager and the Administration Server.

8.4 Editing the Node Manager Properties File

The fourth step in configuring server migration is to edit the Node Manager properties file. This task must be performed for the Node Managers in both nodes where server migration is being configured:

```
Interface=eth0
NetMask=255.255.255.0
UseMACBroadcast=true
```

- **Interface:** This property specifies the interface name for the floating IP (for example, eth0).

  Do not specify the sub-interface, such as `eth0:1` or `eth0:2`. This interface is to be used without `:0` or `:1`. Node Manager scripts traverse the different :*X*-enabled IPs to determine which to add or remove. For example, the valid values in Linux environments are eth0, eth1, eth2, eth3, eth*n*, depending on the number of interfaces configured.

- **NetMask:** This property specifies the net mask for the interface for the floating IP. The net mask should be the same as the net mask on the interface; 255.255.255.0 is used as an example in this document.

- **UseMACBroadcast:** This property specifies whether to use a node's MAC address when sending ARP packets, or in other words, whether to use the -b flag in the `arping` command.

Verify in the Node Manager output (the shell where Node Manager is started) that these properties are being used, or problems may arise during migration. You should see something like this in the Node Manager output:

```
...
StateCheckInterval=500
Interface=eth0
NetMask=255.255.255.0
...
```

> **Note:** The following steps are not required if the server properties (start properties) have been properly set and Node Manager can start the servers remotely.

1. Set the following property in the nodemanager.properties file:

   - **StartScriptEnabled:** Set this property to 'true'. This is required for Node Manager to start the Managed Servers using start scripts.

2. Start Node Manager on APPHOST1 and APPHOST2 by running the startNodeManager.sh script, which is located in the *WL_HOME*/server/bin directory.

> **Note:** When running Node Manager from a shared storage installation, multiple nodes are started using the same nodemanager.properties file. However, each node may require different NetMask or Interface properties. In this case, specify individual parameters on a per-node basis using environment variables. For example, to use a different interface (eth3) in *HOSTn*, use the Interface environment variable as follows:
>
> ```
> HOSTn> export JAVA_OPTIONS=-DInterface=eth3
> ```
>
> Then, start Node Manager after the variable has been set in the shell.

8.5 Setting Environment and Superuser Privileges for the wlsifconfig.sh Script

The fifth step for server migration is to set environment and superuser privileges for the wlsifconfig.sh script:

1. Ensure that your PATH environment variable includes these files:

Table 8–1   Files Required for the PATH Environment Variable

File	Located in this directory
wlsifconfig.sh	*ORACLE_BASE*/admin/*domain_name*/mserver/*domain_name*/bin/server_migration
wlscontrol.sh	*WL_HOME*/common/bin
nodemanager.domains	*WL_HOME*/common/nodemanager

2. Grant sudo configuration for the wlsifconfig.sh script.

   - Configure sudo to work without a password prompt.

   - For security reasons, sudo should be restricted to the subset of commands required to run the wlsifconfig.sh script. For example, perform these steps to set the environment and superuser privileges for the wlsifconfig.sh script:

     a. Grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the /sbin/ifconfig and /sbin/arping binaries.

     b. Make sure the script is executable by the WebLogic user ('oracle'). The following is an example of an entry inside /etc/sudoers granting sudo execution privilege for `oracle` and also over `ifconfig` and `arping`:

     ```
     oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
     ```

> **Note:** Ask the system administrator for the sudo and system rights as appropriate to this step.

8.6 Configuring Server Migration Targets

The sixth step is to configure server migration targets. You first assign all the available nodes for the cluster's members and then specify candidate machines (in order of preference) for each server that is configured with server migration. Follow these steps to configure cluster migration in a migration in a cluster:

1. Log in to the Administration Console (http://*Host*:*Admin_Port*/console). Typically, *Admin_Port* is 7001 by default.

2. In the Domain Structure window, expand **Environment** and select **Clusters**. The Summary of Clusters page is displayed.

3. Click the cluster for which you want to configure migration (bi_cluster) in the Name column of the table.

4. Click the **Migration** tab.

5. In the Change Center, click **Lock & Edit**.

6. In the **Available** field, select the machine to which to allow migration and click the right arrow. In this case, select **APPHOST1** and **APPHOST2**.

7. Select the data source to be used for automatic migration. In this case, select the leasing data source.

8. Click **Save**.

9. Click **Activate Changes**.

10. Set the candidate machines for server migration. You must perform this task for all of the Managed Servers as follows:

    a. In the Domain Structure window of the Administration Console, expand **Environment** and select **Servers**.

    Tip: Click **Customize this table** in the Summary of Servers page and move Current Machine from the Available window to the Chosen window to view the machine on which the server is running. This will be different from the configuration if the server gets migrated automatically.

    b. Click the server for which you want to configure migration.

    c. Click the **Migration** tab.

    d. In the Change Center, click **Lock & Edit**.

    e. In the Migration Configuration section, for **Candidate Machines**, select the machines to which you want to enable migration and click the right arrow. For **bi_server1**, select **APPHOST2**. For **bi_server2**, select **APPHOST1**.

    f. Select **Automatic Server Migration Enabled**. This enables Node Manager to start a failed server on the target node automatically.

    g. Click **Save**.

    h. Click **Activate Changes**.

    i. Restart the Administration Server, Node Managers, Managed Servers, and the system components for which server migration has been configured.

8.7 Testing the Server Migration

The eighth and final step is to test the server migration. Perform these steps to verify that server migration is working properly:

From APPHOST1:

1. Stop the bi_server1 Managed Server. To do this, run this command:

```
APPHOST1> kill -9 pid
```

where *pid* specifies the process ID of the Managed Server. You can identify the pid in the node by running this command:

HOST1> ps -ef | grep bi_server1

2. Watch the Node Manager console. You should see a message indicating that bi_server1's floating IP has been disabled.

3. Wait for Node Manager to try a second restart of bi_server1. It waits for a fence period of 30 seconds before trying this restart.

4. After Node Manager restarts the server, stop it again. Node Manager should now log a message indicating that the server will not be restarted again locally.

From APPHOST2:

1. Watch the local Node Manager console. After 30 seconds since the last try to restart bi_server1 on node 1, Node Manager on node 2 should prompt that the floating IP for bi_server1 is being brought up and that the server is being restarted in this node.

2. Access one of the applications (for example, BI Publisher) using the same IP.

Verification From the Administration Console

Migration can also be verified in the Administration Console:

1. Log in to the Administration Console.

2. Click **Domain** on the left console.

3. Click the **Monitoring** tab and then the **Migration** subtab.

   The Migration Status table provides information on the status of the migration, as shown in Figure 8–1.

Figure 8–1 Migration Status Table in the Administration Console

> **Note:** After a server is migrated, to fail it back to its original node/computer, stop the Managed Server from the Administration Console and then start it again. The appropriate Node Manager will start the Managed Server on the computer to which it was originally assigned.

9

Integrating with Oracle Identity Management

This chapter describes how to integrate Oracle Business Intelligence with Oracle Identity Management.

Before you perform the steps in this chapter, you must have successfully completed the installation and configuration steps described in both of the following:

- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*
- The previous chapters of this guide

> **Important:** Oracle strongly recommends that you read *Oracle Fusion Middleware Release Notes* for any additional installation and deployment considerations before starting the setup process.

This chapter contains the following topics:

- Section 9.1, "Configuring the Credential and Policy Store"
- Section 9.2, "Oracle Access Manager Integration"

9.1 Configuring the Credential and Policy Store

This section contains the following topics:

- Section 9.1.1, "Overview of Credential and Policy Store Configuration"
- Section 9.1.2, "Configuring the Credential Store"
- Section 9.1.3, "Configuring the Policy Store"
- Section 9.1.4, "Reassociating Credentials and Policies"
- Section 9.1.5, "Regenerating User GUIDs After Identity Store Reassociation"

9.1.1 Overview of Credential and Policy Store Configuration

Oracle Fusion Middleware allows using different types of credentials and policy stores in a WebLogic domain. Domains can use stores based on an XML file or on different types of LDAP providers. When a domain uses an LDAP store, all policy and credential data is kept and maintained in a centralized store. However, when using XML policy stores, the changes made on Managed Servers are not propagated to the Administration Server unless they use the same domain home. Because the Oracle Business Intelligence EDG topology uses different domain homes for the Administration Server and the Managed Server, Oracle requires the use of an LDAP store as policy and credential store for integrity and consistency.

By default, Oracle WebLogic Server domains use an XML file for the policy store. The following sections describe the steps required to change the default store to Oracle Internet Directory LDAP for credentials or policies.

> **Note:** The back-end repository for the policy store and the credential store must use the same kind of LDAP server. To preserve this coherence, note that reassociating one store implies reassociating the other one, that is, the reassociation of both credential and the policy stores is accomplished as a unit using Oracle Enterprise Manager Fusion Middleware Control or the WLST command `reassociateSecurityStore`.

9.1.2 Configuring the Credential Store

This section explains how to configure the credential store and contains the following topics:

- Section 9.1.2.1, "Creating Users and Groups"
- Section 9.1.2.2, "Backing Up Configuration Files"
- Section 9.1.2.3, "Configuring the Identity Store to Use LDAP"
- Section 9.1.2.4, "Setting the Order of Providers"
- Section 9.1.2.5, "Moving the WebLogic Administrator to LDAP"

9.1.2.1 Creating Users and Groups

Create the users and groups you need in Oracle Internet Directory, if you have not done so already. See *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for more information.

9.1.2.2 Backing Up Configuration Files

To be safe, first back up the relevant configuration files:

- *ORACLE_BASE*/admin/*domain_name*/mserver/*domain_name*/config/config.xml
- *ORACLE_BASE*/admin/*domain_name*/mserver/*domain_name*/config/fmwconfig/jps-config.xml
- *ORACLE_BASE*/admin/*domain_name*/mserver/*domain_name*/config/fmwconfig/system-jazn-data.xml

Also back up the boot.properties file for the Administration Server.

9.1.2.3 Configuring the Identity Store to Use LDAP

To configure the credential store to use LDAP, set the proper authenticator using the Oracle WebLogic Server Administration Console, as follows:

1. Log in to the Administration Console.

2. Click the **Security Realms** link on the left navigation bar.

3. Click the **myrealm** default realm entry to configure it.

4. Open the **Providers** tab within the realm. Notice that there is a DefaultAuthenticator provider configured for the realm.

5. In the Change Center, click **Lock & Edit**.

6. Click **New** to add a new provider.

7. Enter a name for the provider, such as OIDAuthenticator.

8. Select the **OracleInternetDirectoryAuthenticator** type from the list of authenticators.

9. Click **OK**.

10. In the Providers screen, click the newly created authenticator.

11. Set the control flag to **SUFFICIENT**. This indicates that if a user can be authenticated successfully by this authenticator, then that authentication should be accepted and any additional authenticators should not be invoked. If the authentication fails, it will be passed to the next authenticator in the chain.

    Make sure that all subsequent authenticators also have their control flag set to SUFFICIENT. In particular, check the control flag for the DefaultAuthenticator and set it to SUFFICIENT if necessary.

12. Click **Save**.

13. Open the Provider Specific tab, then enter details specific to your LDAP server, as shown in Table 9–1.

Table 9–1   LDAP Server Details

Parameter	Value	Description
Host	For example: oid.mycompany.com	The host name of the LDAP server.
Port	For example: 636	The LDAP server port number.
Principal	For example: cn=orcladmin	The LDAP user DN used to connect to the LDAP server.
Credential	*your_password*	The password used to connect to the LDAP server.
SSL Enabled	Selected	Specifies whether SSL protocol is used when connecting to the LDAP server.
User Base DN	For example: cn=Users,dc=mycompany, dc=com	Specifies the DN under which your Users start.
Group Base DN	For example: cn=Groups,dc=mycompany, dc=com	Specifies the DN that points to your Groups node.
User Name Attribute	cn	The user name attribute.
Use Retrieved User Name as Principal	Selected	This option must be enabled.

14. Click **Save** when done.

15. Click **Activate Changes** to propagate the changes.

16. Restart the Administration Server and the Managed Servers.

9.1.2.4 Setting the Order of Providers

Reorder the OID Authenticator and Default Authenticator and ensure that the control flags for each authenticator is set as follows:

- OID LDAP Authenticator: SUFFICIENT

- Default Authenticator: SUFFICIENT

Restart the Administration Server.

9.1.2.5 Moving the WebLogic Administrator to LDAP

After LDAP has been configured, all users (including administrative users) should be LDAP users. This must be configured by the LDAP administrator. An administration group should be created with the necessary users. For information about the required steps, see section 8.5 of *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*. Use 'BIAdministrators' for the group name.

After this group is created, you must update the role definition for the WLS Global Admin role in WebLogic Server, as follows:

1. Log in to the Administration Console.

2. Go to the location that defines the Admin role by selecting **Security Realms**, then your realm name, then **Role and Policies**, then **Global Roles**, then **Roles**, and then **Admin**. Click the **View Role Conditions** link.

   By default, you can see that the Administrators group in Oracle Internet Directory defines who has the Admin role in WebLogic Server.

3. Click **Add Conditions** to add a different group name (BIAdministrators). Then, delete the Administrators group, leaving the new one you added.

4. Click **Save**.

5. After making this change, any members of the new group specified will be authorized to administer WebLogic Server.

9.1.2.5.1 Updating the boot.properties File and Restarting the System The boot.properties file for the Administration Server must be updated with the WebLogic admin user created in Oracle Internet Directory. Follow these steps to update the boot.properties file:

1. On APPHOST1, go to the following directory:

   ```
   APPHOST1> cd ORACLE_BASE/admin/domain_name/aserver/domain_
   name/servers/AdminServer/security
   ```

2. Rename the existing boot.properties file:

   ```
   APPHOST1> mv boot.properties boot.properties.backup
   ```

3. Use a text editor to create a file called boot.properties under the security directory. Enter the following lines in the file:

   ```
   username=admin_user
   password=admin_user_password
   ```

4. Save the file.

5. Stop and restart the Administration Server.

9.1.3 Configuring the Policy Store

The domain policy store is the repository of system and application-specific policies. In a given domain, there is one store that stores all policies that all applications deployed in the domain can use. This section provides the steps to configure Oracle

Internet Directory LDAP as the policy store for the Oracle Business Intelligence EDG topology.

To ensure proper access to the Oracle Internet Directory LDAP server directory used as a policy store, you must set a node in the server directory.

An Oracle Internet Directory administrator must follow these steps to create the appropriate node in the Oracle Internet Directory server:

1. Create an LDIF file (jpstestnode.ldif in this example) specifying the following DN and CN entries:

```
dn: cn=jpsroot_bi,dc=mycompany,dc=com
cn: jpsroot_bi
objectclass: top
objectclass: OrclContainer
```

The DN of the root node (jpsroot_bi in the previous step) must be distinct from any other DN. One root node can be shared by multiple WebLogic domains. It is not required that his node be created at the top level, as long as read and write access to the subtree is granted to the Oracle Internet Directory administrator.

2. Import this data into the Oracle Internet Directory server using the command ldapadd, as shown in the following example:

```
OIDHOST1> ORACLE_HOME/bin/ldapadd -h ldap_host -p ldap_port -D cn=orcladmin -w
password -c -v -f jpstestnode.ldif
```

3. Verify that the node has been successfully inserted using the command ldapsearch, as shown in the following example:

```
OIDHOST1> ORACLE_HOME/bin/ldapsearch -h ldap_host -p ldap_port -D cn=orcladmin
-w password -b "cn=jpsroot_bi,dc=mycompany,dc=com" objectclass="orclContainer"
```

4. When using Oracle Internet Directory as the LDAP-Based policy store, run the utility oidstats.sql in the INFRADBHOST to generate database statistics for optimal database performance:

```
OIDHOST1> connect ods/welcome1
OIDHOST1> @ORACLE_HOME/ldap/admin/oidstats.sql
```

Note: The oidstats.sql utility only needs to be run once after the initial provisioning.

9.1.4 Reassociating Credentials and Policies

To reassociate the policy and credential store with Oracle Internet Directory, use the WLST reassociateSecurityStore command, as follows:

1. From APPHOST1, start the wlst shell:

```
APPHOST1> cd ORACLE_HOME/common/bin
APPHOST1> ./wlst.sh
```

2. Connect to the WebLogic Administration Server using the wlst connect command, as follows:

```
connect ("AdminUser", "AdminPassword", "t3://hostname:port")
```

For example:

```
connect ("weblogic", "welcome1", "t3://ADMINHOSTVPN1:7001")
```

3. Run the `reassociateSecurityStore` command, as follows:

```
reassociateSecurityStore(domain="domainName", admin="cn=admin_user_name",
password="orclPassword", ldapurl="ldap://LDAPHOST:LDAPPORT", servertype="OID",
jpsroot="cn=jpsroot_bi")
```

For example:

```
wls:/bifoundation_domain/serverConfig>
reassociateSecurityStore(domain="bifoundation_domain", admin="cn=orcladmin",
password="welcome1", ldapurl="ldap://oid.mycompany.com:389", servertype="OID",
jpsroot="cn=jsproot_bi,dc=mycompany,dc=com")
```

4. Restart the Administration Server after the command completes successfully.

> **Note:** For credential and policy changes to take effect, the servers in the domain must be restarted.

9.1.5 Regenerating User GUIDs After Identity Store Reassociation

This section contains the following topics:

- Section 9.1.5.1, "About User GUIDs"
- Section 9.1.5.2, "About GUID Regeneration"
- Section 9.1.5.3, "Regenerating User GUIDs"

9.1.5.1 About User GUIDs

In Oracle Business Intelligence 11*g* Release 1 (11.1.1), users are recognized by their global unique identifiers (GUIDs), not by their names. GUIDs are identifiers that are completely unique for a given user. Using GUIDs to identify users provides a higher level of security because it ensures that data and metadata is uniquely secured for a specific user, independent of the user name.

Oracle recommends that you follow these two best practices to ensure that GUIDs are consistently applied in each phase of the development to production lifecycle:

- Ensure that a fan-out replica of the identity store is used between development, test, and production systems, so that user GUIDs are consistent and identical across the complete development to production lifecycle. See "Setting Up Replication" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for further information about creating fan-out replicas.

- Wherever possible, secure access to data and metadata using application roles rather than individual users.

9.1.5.2 About GUID Regeneration

GUID regeneration is the process of regenerating any metadata references to user GUIDs in the Oracle BI repository and Oracle BI Presentation Catalog. During the GUID regeneration process, each user name is looked up in the identity store. Then, all metadata references to the GUID associated with that user name are replaced with the GUID in the identity store.

GUID regeneration might be required when Oracle Business Intelligence is reassociated with an identity store that has different GUIDs for the same users. This situation might occur when reassociating Oracle Business Intelligence with a different type of identity store and should be a rare event.

Note that if Oracle best practices are not observed and Oracle Business Intelligence repository data is migrated between systems that have different GUIDs for the same users, GUID regeneration is required for the system to function. This is not a recommended practice, because it raises the risk that data and metadata secured to one user (for example, John Smith, who left the company two weeks ago) becomes accessible to another user (for example, John Smith, who joined last week). Using application roles wherever possible and using GUIDs consistently across the full development production lifecycle prevents this problem from occurring.

9.1.5.3 Regenerating User GUIDs

To regenerate user GUIDs, perform the following steps on APPHOST1 and APPHOST2. Note that GUID regeneration must occur with only one node operating at a time.

1. Stop Oracle BI Server and Presentation Services on all nodes except where you are regenerating the user GUIDs. For example:

```
cd ORACLE_BASE/admin/instancen/bin
./opmnctl stopproc ias-component=coreapplication_obips1
./opmnctl stopproc ias-component=coreapplicaiton_obis1
```

2. Update the `FMW_UPDATE_ROLE_AND_USER_REF_GUIDS` parameter in NQSConfig.INI:

   a. Open NQSConfig.INI for editing at:

   ```
   ORACLE_INSTANCE/config/OracleBIServerComponent/coreapplication_obisn
   ```

   b. Locate the `FMW_UPDATE_ROLE_AND_USER_REF_GUIDS` parameter and set it to `YES`, as follows:

   ```
   FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = YES;
   ```

   c. Save and close the file.

3. Update the Catalog element in instanceconfig.xml:

   a. Open instanceconfig.xml for editing at:

   ```
   ORACLE_INSTANCE/config/OracleBIPresentationServicesComponent/
   coreapplication_obipsn
   ```

   b. Locate the Catalog element and update it as follows:

   ```
   <Catalog>
   <UpgradeAndExit>false</UpgradeAndExit>
   <UpdateAccountGUIDs>UpdateAndExit</UpdateAccountGUIDs>
   </Catalog>
   ```

   c. Save and close the file.

4. Restart the Oracle BI Server and Presentation Services using opmnctl:

   ```
   cd ORACLE_BASE/admin/instancen/bin
   ./opmnctl stopproc ias-component=coreapplication_obips1
   ./opmnctl stopproc ias-component=coreapplication_obis1
   ./opmnctl startproc ias-component=coreapplication_obis1
   ```

   After you confirm that the Oracle BI Server is running, then start Presentation Services:

   ```
   ./opmnctl startproc ias-component=coreapplication_obips1
   ```

5. Set the `FMW_UPDATE_ROLE_AND_USER_REF_GUIDS` parameter in NQSConfig.INI back to `NO`.

   Important: You must perform this step to ensure that your system is secure.

6. Update the Catalog element in instanceconfig.xml to remove the UpdateAccount GUIDs entry.

7. Restart the Oracle Business Intelligence system components using opmnctl:

```
cd ORACLE_BASE/admin/instancen/bin
./opmnctl stopall
./opmnctl startall
```

9.2 Oracle Access Manager Integration

This section describes how to set up Oracle Access Manager 10*g* as a single sign-on solution for the Oracle Business Intelligence topology.

This section contains the following topics:

- Section 9.2.1, "About Oracle Access Manager Integration"
- Section 9.2.2, "Using the Oracle Access Manager Configuration Tool"
- Section 9.2.3, "Updating the Host Identifier"
- Section 9.2.4, "Updating the WebGate Profile"
- Section 9.2.5, "Installing and Configuring WebGate"
- Section 9.2.6, "Setting Up WebLogic Authenticators"
- Section 9.2.7, "Configuring Applications"

9.2.1 About Oracle Access Manager Integration

The instructions for Oracle Access Manager 10*g* assume an existing Oracle Access Manager installation, complete with Access Managers and a policy protecting the Policy manager. For more information about installing and configuring an Oracle Access Manager installation, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

The configuration described in this chapter includes a directory service such as Oracle Internet Directory, either as a standalone component or as part of an Oracle Virtual Directory configuration. This section provides the necessary steps for configuring your Oracle Business Intelligence installation with Oracle Internet Directory.

In addition, the Oracle Access Manager installation should have its own Web server configured with WebGate. This section also provides steps for using the Oracle Access Manager Web server as a delegated authentication server.

9.2.2 Using the Oracle Access Manager Configuration Tool

This section explains how to use the Oracle Access Manager Configuration Tool and contains the following topics:

- Section 9.2.2.1, "About the Oracle Access Manager Configuration Tool"
- Section 9.2.2.2, "Collecting Information for the Oracle Access Manager Configuration Tool"
- Section 9.2.2.3, "Running the Oracle Access Manager Configuration Tool"

- Section 9.2.2.4, "Verifying Successful Creation of the Policy Domain and AccessGate"

9.2.2.1 About the Oracle Access Manager Configuration Tool

The Oracle Access Manager Configuration Tool (oamcfgtool) starts a series of scripts and sets up the required policies. It requires various parameters as inputs. Specifically, it creates the following:

- A Form Authentication scheme in Oracle Access Manager

- Policies to enable authentication in Oracle WebLogic Server

- A WebGate entry in Oracle Access Manager to enable Oracle HTTP Server WebGates (from your Web tier) to protect your configured application

- A Host Identifier, depending on the scenario chosen (a default host identifier would be used, if not provided)

- Policies to protect and unprotect the application-specific URL

9.2.2.2 Collecting Information for the Oracle Access Manager Configuration Tool

Collect or prepare the following information before running the Oracle Access Manager Configuration Tool:

- Password: Create a secure password. This will be used as the password for the WebGate installation performed later.

- LDAP Host: The host name of the Directory Server or load balancer address, for HA/EDG configurations.

- LDAP Port: The port number of the Directory Server.

- LDAP USER DN: The DN of the LDAP administrator user (for example, "cn=orcladmin").

- LDAP password: The password of the LDAP administrator user.

- OAM_AA_HOST: The host name of the Oracle Access Manager instance.

- OAM_AA_PORT: The Oracle Access Manager port number.

9.2.2.3 Running the Oracle Access Manager Configuration Tool

The Oracle Access Manager Configuration Tool is located in the following directory:

MW_HOME/oracle_common/modules/oracle.oamprovider_11.1.1

The tool can be run from any computer with the required installation files. In this case, you run it from APPHOST1.

Run the Oracle Access Manager Configuration Tool, as follows (all on a single line):

```
MW_HOME/jrockit_160_22_D1.1.1-3/bin/java -jar oamcfgtool.jar mode=CREATE
app_domain="bifoundation_domain" protected_uris="$PROTECTED_URI_LIST"
public_uris="$PUBLIC_URI_LIST" ldap_host="oid.mycompany.com" ldap_port=389
ldap_userdn="cn=LDAP_admin_user_name"
ldap_userpassword=LDAP_admin_user_password oam_aaa_host=OAMHOST1
oam_aaa_port=OAMPORT1 oam_aaa_mode=simple
```

For `$PROTECTED_URI_LIST`, use:

```
"/analytics/saw.dll,/xmlpserver,/ui,/bioffice,/em,/console,/ui/adfAuthentication"
```

For `$PUBLIC_URI_LIST`, use:

```
"/analytics,/analytics/saw.dll/wsdl,/xmlpserver/services,/xmlpserver/
report_service,/xmlpserver/ReportTemplateService.xls,/xmlpserver/Guest,
/ui/do/logout,/ui/images,/bioffice/services/saw?WSDL"
```

You will be prompted for the app_agent_password.

> **Note:** If additional URLs need to be protected later, run the Oracle Access Manager Configuration Tool again using the same app_domain. Be sure to include all the URLs that need to be protected, not just the new ones.

9.2.2.4 Verifying Successful Creation of the Policy Domain and AccessGate

This section covers how to validate that the Policy Domain and AccessGate were created successfully.

Verifying the Policy Domain

Follow these steps to verify the policy domain:

1. Log on to Oracle Access Manager at:

   http://*OAMADMINHOST*:*port*/access/oblix

2. Click **Policy Manager**.

3. Click the **My Policy Domains** link on the left panel. A list of all policy domains is displayed, including the domain you just created.

4. Click the link to the policy domain you just created. The General area of the domain is displayed.

5. Click the **Resources** tab. The URIs you specified are displayed. You can also click other tabs to view other settings.

Verifying the AccessGate Configuration

Follow these steps to verify the AccessGate configuration:

1. Click the **Access System Console** link on the top right. Note that this link toggles between Access System Console and Policy Manager when you click it.

2. Click the **Access System Configuration** tab.

3. Click the **AccessGate Configuration** link in the left pane.

4. Enter 'bifoundation_domain' as the search criterion (or another substring in your app_domain), and then click **Go**.

   The AccessGate for the domain you just created is displayed. This result will have the suffix _AG (for example, bifoundation_domain_AG).

5. Click the AccessGate for your domain to see details.

9.2.3 Updating the Host Identifier

The Oracle Access Manager Configuration Tool uses the value of the app_domain parameter to create a host identifier for the policy domain. This host identifier must be updated with all the host name variations for the host so that the configuration works correctly.

Follow these steps to update the host identifier created by the Oracle Access Manager Configuration Tool:

1. Navigate to the Access System Console by entering the following URL in your Web browser:

    http://*hostname*:*port*/access/oblix

    where *hostname* refers to the host where the WebPass Oracle HTTP Server instance is running, and *port* refers to the HTTP port of the Oracle HTTP Server instance.

2. When prompted for a username and password, log in as an administrator. Click **OK**.

3. On the Access System main page, click the **Access System Console** link.

4. On the Access System Console page, click the **Access System Configuration** tab.

5. On the Access System Configuration page, click **Host Identifiers** on the bottom left.

6. On the List all host identifiers page, click the host identifier created by the Oracle Access Manager Configuration Tool. For example, select bifoundation_domain.

7. On the Host Identifier Details page, click **Modify**.

8. On the Modifying host identifier page, add all the possible host name variations for the host. Click the plus and minus symbols to add or delete fields as necessary.

    The Preferred HTTP Host value used in the Access System Configuration must be added as one of the host name variations. For example:

    bifoundation_domain, webhost1.mycompany.com:7777, admin.mycompany.com:7777

9. Select **Update Cache** and then click **Save**.

    The following message is displayed: "Updating the cache at this point will flush all the cache in the system. Are you sure?"

    Click **OK** to finish saving the configuration changes.

10. Verify the changes on the Host Identifier Details page.

9.2.4 Updating the WebGate Profile

The Oracle Access Manager Configuration Tool populates the Preferred_HTTP_Host and hostname attributes for the WebGate profile that is created with the value of the app_domain parameter. Both of these attributes must be updated with the correct values for the configuration to work.

Follow these steps to update the WebGate profile created by the Oracle Access Manager Configuration Tool:

1. Navigate to the Access System Console by entering the following URL in your Web browser:

    http://*hostname*:*port*/access/oblix

    where *hostname* refers to the host where the WebPass Oracle HTTP Server instance is running, and *port* refers to the HTTP port of the Oracle HTTP Server instance.

2. When prompted for a username and password, log in as an administrator. Click **OK**.

3. On the Access System main page, click the **Access System Console** link.

4. On the Access System Console page, click the **Access System Configuration** tab to display the AccessGate Search page.

5. Enter the appropriate search criteria and click **Go** to display a list of AccessGates.

6. Select the AccessGate created by the Oracle Access Manager Configuration Tool. For example: bifoundation_domain_AG

7. On the AccessGate Details page, select **Modify** to display the Modify AccessGate page.

8. On the Modify AccessGate page, update the following:

   ■ **Hostname:** Update the hostname with the name of the computer where WebGate is running. For example: webhost1.mycompany.com

   ■ **Preferred HTTP Host:** Update the Preferred_HTTP_Host with one of the host name variations specified in the previous section. For example: webhost1.mycompany.com:7777

   ■ **Primary HTTP Cookie Domain:** Update the Primary HTTP Cookie Domain with the Domain suffix or the host identifier. For example: mycompany.com

   ■ **Port:** Update the port with the port where WebGate is running. For example: 7777*

   ■ **Maximum Connections:** Set to 4.

9. Click **Save**, then click **OK** to confirm.

10. Verify the values displayed on the Details for AccessGate page to confirm that the updates were successful.

9.2.5 Installing and Configuring WebGate

WebGate must be installed on each of the WEBHOST*n* computers to secure the Web tier. To do this, follow these steps:

1. Launch the WebGate installer using the following command:

   ```
   ./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g_WebGate -gui
   ```

2. The Welcome screen is displayed. Click **Next**.

3. In the Customer Information screen, enter the user name and user group under which the Web server is running. Click **Next** to continue.

4. In the installation target screen, specify the directory where WebGate should be installed. Click **Next** to continue.

5. In the installation summary screen, click **Next**.

6. Download the required GCC runtime libraries for WebGate as instructed in the WebGate configuration screen, and use **Browse** to point to their location on the local computer. Click **Next** to continue.

7. The installer now creates the required artifacts. After that process is complete, click **Next** to continue.

8. In the transport security mode screen, select the same mode that was configured for the BI Access Gate (for example, **Simple**) and click **Next** to continue.

9. In the WebGate Configuration screen, provide the details of the Access Server that will be used. You must provide the following information:

   ■ WebGate ID, as provided when the Oracle Access Manager Configuration Tool was executed

   ■ Password for WebGate

- Access Server ID, as reported by the Oracle Access Manager Access Server configuration

- Access Server host name, as reported by the Oracle Access Manager Access Server configuration

- Access Server port number, as reported by the Oracle Access Manager Access Server configuration

- Global Access Protocol Pass Phrase

You can obtain these details from your Oracle Access Manager administrator. Click **Next** to continue.

10. In the Configure Web Server screen, click **Yes** to automatically update the Web server. Click **Next** to continue.

11. In the next Configure Web Server screen, specify the full path of the directory containing the httpd.conf file. Click **Next** to continue.

12. In the next Configure Web Server page, a message informs you that the Web Server configuration has been modified for WebGate. Click **Yes** to confirm.

13. Stop and start your Web server for the configuration updates to take effect. Click **Next** to continue.

14. In the next Configure Web Server screen, a message about SSL is displayed. Click **Next** to continue.

15. In the next Configure Web Server screen, a message with the location of the document that has information about the rest of the product setup and Web server configuration is displayed. Choose **No** and click **Next** to continue.

16. The final Configure Web Server screen appears with a message to manually launch a browser and open the HTML document for further information on configuring your Web server. Click **Next** to continue.

17. The Oracle COREid Readme screen appears. Review the information on the screen and click **Next** to continue.

18. A message appears, providing details of the installation and informing you that the installation was successful.

9.2.6 Setting Up WebLogic Authenticators

The instructions in this section assume that you have already set up the LDAP Authenticators.

This section contains the following topics:

- Section 9.2.6.1, "Setting Up the Oracle Access Manager ID Asserter"

- Section 9.2.6.2, "Setting the Order of Providers"

9.2.6.1 Setting Up the Oracle Access Manager ID Asserter

To set up the Oracle Access Manager ID Asserter, follow these steps:

1. Log in to the Administration Console.

2. In the Change Center, click **Lock & Edit**.

3. Navigate to SecurityRealms\myrealm\Providers.

4. Click **New** and select **OAM Identity Asserter** from the drop-down menu.

5. Name the asserter (for example: OAM ID Asserter) and click **OK**.

6. Click the newly added asserter to see the configuration screen for OAM Identity Asserter.

7. Set the control flag to **REQUIRED** and click **Save**.

8. Open the Provider Specific tab to configure the following required settings:

   - **Primary Access Server:** Provide the Oracle Access Manager server endpoint information in *HOST*:*PORT* format.

   - **AccessGate Name:** Provide the name of the AccessGate (for example, bifoundation_domain_AG).

   - **AccessGate password:** Provide the password for the AccessGate.

9. Click **Save** when done.

10. Click **Activate Changes** to propagate the changes.

11. Restart the Administration Server and the Managed Servers.

9.2.6.2 Setting the Order of Providers

Reorder the Oracle Access Manager Identity Asserter, Oracle Internet Directory Authenticator, and Default Authenticator by ensuring that the control flag for each authenticator is set, as follows:

- OAM Identity Asserter: REQUIRED

- OID LDAP Authenticator: SUFFICIENT

- Default Authenticator: SUFFICIENT

Then, restart the Administration Server and the Managed Servers.

9.2.7 Configuring Applications

This section explains how to configure applications, and contains the following topics:

- Section 9.2.7.1, "Enabling SSO/Oracle Access Manager for Oracle BI Enterprise Edition"

- Section 9.2.7.2, "Enabling SSO/Oracle Access Manager for Oracle BI Publisher"

- Section 9.2.7.3, "Enabling SSO/Oracle Access Manager for Oracle BI for Microsoft Office"

- Section 9.2.7.4, "Enabling SSO/Oracle Access Manager for Oracle BI Search"

- Section 9.2.7.5, "Enabling SSO/Oracle Access Manager for Oracle Real-Time Decisions"

9.2.7.1 Enabling SSO/Oracle Access Manager for Oracle BI Enterprise Edition

To enable SSO and Oracle Access Manager for Oracle BI Enterprise Edition, follow these steps:

1. Log in to Fusion Middleware Control.

2. Go to **Business Intelligence > coreapplication > Security**.

3. Click **Lock and Edit Configuration**.

4. Choose **Enable SSO** and select Oracle Access Manager for **SSO Provider**.

5. Configure the login/logout information for the Oracle BI Presentation Services processes by entering the logon and logoff URLs in the following fields:

   ■ **The SSO Provider Logon URL:** http://*OAM_host*:*OAM_port*/oamsso/login.html

   ■ **The SSO Provider Logoff URL:** http://*OAM_host*:*OAM_port*/access/oblix/lang/en-us/logout.html

6. Click **Apply**.

7. Click **Activate Changes**.

8. Restart all Oracle Business Intelligence system components using opmnctl or Fusion Middleware Control.

9.2.7.2 Enabling SSO/Oracle Access Manager for Oracle BI Publisher

To enable SSO and Oracle Access Manager for Oracle BI Publisher, follow these steps:

1. In Oracle BI Publisher, go to the **Administration > Security Configuration** page to enable SSO.

2. On the Security Configuration Page, provide the following information in the Single Sign-On section:

   a. Select **Use Single Sign-On**.

   b. For **Single Sign-On Type**, select **Oracle Access Manager**.

   c. For **Single Sign-Off URL**, enter a URL of the following format:

   ```
   http://OAM_host:OAM_port/access/oblix/lang/en-us/logout.html
   ```

   For example:

   ```
   http://bi.mycompany.com:7777/access/oblix/lang/en-us/logout.html
   ```

3. Click **Apply**.

4. Restart the **bipublisher** application from the Administration Console.

9.2.7.3 Enabling SSO/Oracle Access Manager for Oracle BI for Microsoft Office

SSO configuration for Oracle BI for Microsoft Office was covered in Section 6.5.4.1, "Configuring Oracle BI for Microsoft Office Properties." If you have not already enabled SSO for Oracle BI for Microsoft Office, perform the steps in Section 6.5.4.1 to accomplish this task.

9.2.7.4 Enabling SSO/Oracle Access Manager for Oracle BI Search

To enable SSO and Oracle Access Manager for Oracle BI Search, follow these steps:

1. Open the BISearchConfig.properties file for editing. You can find this file at:

   ```
   DOMAIN_HOME/config/fmwconfig/biinstances/coreapplication/
   ```

2. Set the value of BIServerSSOUrl to the following:

   https://bi.mycompany.com/analytics

3. Save and close the file.

9.2.7.5 Enabling SSO/Oracle Access Manager for Oracle Real-Time Decisions

This section provides information about Oracle Real-Time Decisions configuration with Oracle Access Manager.

This section contains the following topics:

- Section 9.2.7.5.1, "Oracle RTD and Oracle Access Manager Logout Guidelines"

- Section 9.2.7.5.2, "Avoiding Problems with Decision Center Logout Redirection"

9.2.7.5.1 Oracle RTD and Oracle Access Manager Logout Guidelines For Oracle RTD to comply with Oracle Access Manager logout guidelines (in particular, invoking a logout through /adfAuthentication?logout=true&end_url=/ui/do/logout), integration with Oracle Access Manager 10*g* requires additional WebGate configuration to handle the end_url. Without this additional configuration, you are logged out, but not redirected to the end URL because Oracle Access Manager 10*g* WebGate does not process end_url.

For information about configuration procedures, see *Oracle Fusion Middleware Application Security Guide*.

9.2.7.5.2 Avoiding Problems with Decision Center Logout Redirection When Webgate 10*g* against Oracle Access Manager (OAM) 11g is configured as the SSO provider for Oracle RTD Decision Center access, logging out of, then back into Decision Center should ask users for their user name and password credentials on the re-login. To ensure that this occurs correctly, you must configure the following Oracle RTD Decision Center resources in OAM/Webgate as public (unprotected or anonymous access):

1. Decision Center logout URI /ui/do/logout

2. Decision Center images /ui/images/*

10

Managing Enterprise Deployments

This chapter provides information about operations that you can perform after you have set up your topology, including monitoring, scaling, and backing up your enterprise deployment.

This chapter contains the following topics:

- Section 10.1, "Starting and Stopping Oracle Business Intelligence"
- Section 10.2, "Monitoring Enterprise Deployments"
- Section 10.3, "Scaling Enterprise Deployments"
- Section 10.4, "Performing Backups and Recoveries"
- Section 10.5, "Patching Enterprise Deployments"
- Section 10.6, "Troubleshooting"
- Section 10.7, "Other Recommendations"

10.1 Starting and Stopping Oracle Business Intelligence

To start Oracle Business Intelligence, you must always start the Managed Servers first, before the system components. In addition, any time the Managed Servers are restarted, the system components must be restarted also.

For additional information, see "Starting and Stopping Oracle Business Intelligence" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

This section contains the following topics:

- Section 10.1.1, "Starting and Stopping Oracle Business Intelligence Managed Servers"
- Section 10.1.2, "Starting and Stopping Oracle Business Intelligence System Components"

10.1.1 Starting and Stopping Oracle Business Intelligence Managed Servers

Follow these steps to stop, start, or restart Oracle Business Intelligence Managed Servers:

1. Log in to the Oracle WebLogic Server Administration Console.

2. Expand the **Environment** node in the Domain Structure window.

3. Click **Servers**. The Summary of Servers page is displayed.

4. Select the Oracle Business Intelligence Managed Server you want to manage (for example, **bi_server1**, **bi_server2**, and so on).

5. Perform one of the following actions:

   - To stop the Managed Server, click **Stop**.

   - To start the Managed Server, click **Start**.

   - To restart the Managed Server, first click **Stop** and wait until the server is completely stopped. Then, select the Managed Server again and click **Start**.

10.1.2 Starting and Stopping Oracle Business Intelligence System Components

Follow these steps to stop, start, or restart Oracle Business Intelligence system components:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control.

2. Expand the **Business Intelligence** node in the Farm_*domain_name* window.

3. Click **coreapplication**.

4. On the Business Intelligence Overview page, click **Stop**, **Start**, or **Restart**.

10.2 Monitoring Enterprise Deployments

For information on monitoring the Oracle Business Intelligence topology, see "Monitoring Service Levels" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

See also "Diagnosing and Resolving Issues in Oracle Business Intelligence" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* for information about Oracle Business Intelligence log files, including rotating and managing logs.

10.3 Scaling Enterprise Deployments

You can scale up or scale out the Oracle Business Intelligence enterprise topology, as follows:

- When you scale up the topology, you add additional system components to one of the existing nodes in your enterprise topology.

- When you scale out the topology, you add a new node to your topology with a Managed Server and set of system components.

This section includes the following topics:

- Section 10.3.1, "Scaling Up the Oracle Business Intelligence Topology"

- Section 10.3.2, "Scaling Out the Oracle Business Intelligence Topology"

> **Note:** To scale out and up the SOA subsystem used by I/PM, refer to the SOA enterprise deployment topology documentation.

10.3.1 Scaling Up the Oracle Business Intelligence Topology

This procedure assumes that you already have an enterprise topology that includes two nodes, with a Managed Server and a full set of system components on each node.

To scale up the topology, you increase the number of system components running on one of your existing nodes.

Note that it is not necessary to run multiple Managed Servers on a given node.

To scale up the Oracle Business Intelligence enterprise topology:

1. Log in to Fusion Middleware Control.

2. Expand the **Business Intelligence** node in the Farm_*domain_name* window.

3. Click **coreapplication**.

4. Click **Capacity Management**, then click **Scalability**.

5. Click **Lock and Edit Configuration**.

6. Change the number of **BI Servers**, **Presentation Servers**, or **JavaHosts** using the arrow keys.

7. Click **Apply**, then click **Activate Changes**.

8. Click **Overview**, then click **Restart**.

10.3.2 Scaling Out the Oracle Business Intelligence Topology

When scaling out the topology, you add a new Managed Server and set of system components to a new node in your topology (APPHOST3). This procedure assumes that you already have an enterprise topology that includes two nodes, with a Managed Server and a full set of system components on each node.

Prerequisites
Before performing the steps in this section, check that you meet these requirements:

- There must be existing nodes running Oracle Business Intelligence Managed Servers within the topology.

- The new node (APPHOST3) can access the existing home directories for Oracle WebLogic Server and Oracle Business Intelligence.

- When an ORACLE_HOME or WL_HOME is shared by multiple servers in different nodes, it is recommended that you keep the Oracle Inventory and Middleware home list in those nodes updated for consistency in the installations and application of patches. To update the oraInventory in a node and "attach" an installation in a shared storage to it, use *ORACLE_HOME*/oui/bin/attachHome.sh. To update the Middleware home list to add or remove a WL_HOME, edit the *MW_HOME*/.home file. See the steps in Section 10.3.2.1, "Scale-out Procedure for Oracle Business Intelligence" for details.

- You must ensure that all shared storage directories are available on the new node. Ensure that all shared directories listed in Section 2.3.2, "Recommended Locations for the Different Directories" are available on all nodes, except for the ORACLE_INSTANCE directory and the domain directory for the scaled out Managed Server.

  Also, if you are using shared storage for the identity keystore and trust keystore that hold your host name verification certificates, ensure that the shared storage directory is accessible from the scaled-out node (APPHOST3). If you are using local directories for your keystores, follow the steps in Section 7.3, "Enabling Host Name Verification Certificates for Node Manager" to create and configure a local identity keystore for the scaled-out node.

  For example, mount the following directories:

- – Transaction Log directory

- – JMS Persistence Store

- – Global Cache

- – BI Presentation Catalog

- – BI Repository Publishing directory

- – BI Publisher Catalog

- – BI Publisher Configuration Keystore (certs)

- – MW_HOME

10.3.2.1 Scale-out Procedure for Oracle Business Intelligence

Perform these steps to scale out Oracle Business Intelligence on APPHOST3:

1. On APPHOST3, mount the existing Middleware home, which should include the Oracle Business Intelligence installation and (optionally, if the domain directory for Managed Servers in other nodes resides on shared storage) the domain directory, and ensure that the new node has access to this directory, just like the rest of the nodes in the domain.

2. To attach *ORACLE_HOME* in shared storage to the local Oracle Inventory, execute the following command:

   ```
   APPHOST3> cd ORACLE_COMMON_HOME/oui/bin/
   APPHOST3> ./attachHome.sh -jreLoc ORACLE_BASE/product/fmw/jrockit_160_<version>
   ```

   To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the *MW_HOME*/.home file and add *ORACLE_ BASE*/product/fmw to it.

3. Run the Configuration Assistant from one of the shared Oracle homes, using the steps in Section 6.1, "Scaling Out the BI System on APPHOST2" as a guide.

4. Scale out the system components on APPHOST3, using the steps in Section 6.2, "Scaling Out the System Components" as a guide.

5. Configure the bi_server3 Managed Server by setting the Listen Address and disabling host name verification, using the steps in Section 6.4, "Configuring the bi_server2 Managed Server" as a guide.

6. Configure JMS for Oracle BI Publisher, as described in Section 6.5.3.5, "Configuring JMS for Oracle BI Publisher."

7. Configure Oracle BI for Microsoft Office on APPHOST3, as described in Section 6.5.4, "Additional Configuration Tasks for Oracle BI for Microsoft Office."

8. Set the location of the default persistence store for bi_server 3, as described in Section 6.6, "Configuring a Default Persistence Store for Transaction Recovery."

9. Configure Oracle HTTP Server for APPHOST3VHN1, using the steps in Section 5.10.2, "Configuring Oracle HTTP Server for the bi_servern Managed Servers" as a guide.

10. Start the bi_server3 Managed Server and the system components running on APPHOST3. See Section 10.1, "Starting and Stopping Oracle Business Intelligence" for details.

11. Set up server migration for the new node, as described in the following sections:

    - Section 8.3, "Enabling Host Name Verification Certificates"

- Section 8.4, "Editing the Node Manager Properties File"

- Section 8.5, "Setting Environment and Superuser Privileges for the wlsifconfig.sh Script"

- Section 8.6, "Configuring Server Migration Targets"

- Section 8.7, "Testing the Server Migration"

12. To validate the configuration, access the following URLs:

   - Access `http://APPHOST3VHN1:9704/analytics` to verify the status of bi_server3.

   - Access `http://APPHOST3VHN1:9704/wsm-pm` to verify the status of Web Services Manager. Click **Validate Policy Manager**. A list of policies and assertion templates available in the data is displayed.

     Note: The configuration is incorrect if no policies or assertion templates appear.

   - Access `http://APPHOST3VHN1:9704/xmlpserver` to verify the status of the Oracle BI Publisher application.

   - Access `http://APPHOST3VHN1:9704/ui` to verify the status of the Oracle Real-Time Decisions application.

13. Oracle recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses communicating with the Administration Server and other servers. See Chapter 7, "Setting Up Node Manager" for further details.

10.4 Performing Backups and Recoveries

See "Backup and Recovery Recommendations for Oracle Business Intelligence" in *Oracle Fusion Middleware Administrator's Guide* for full information about backing up and recovering Oracle Business Intelligence.

10.5 Patching Enterprise Deployments

See "Patching Oracle Business Intelligence Systems" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* for more information about Oracle Business Intelligence patching.

10.6 Troubleshooting

This section covers the following topics:

- Section 10.6.1, "Page Not Found When Accessing BI Applications Through Load Balancer"

- Section 10.6.2, "Administration Server Fails to Start After a Manual Failover"

- Section 10.6.3, "Error While Activating Changes in Administration Console"

- Section 10.6.4, "bi_server Managed Server Not Failed Over After Server Migration"

- Section 10.6.5, "bi_server Managed Server Not Reachable From Browser After Server Migration"

- Section 10.6.6, "OAM Configuration Tool Does Not Remove URLs"

- Section 10.6.7, "Users Redirected to Login Screen After Activating Changes"

-

-

-

-

-

-

10.6.1 Page Not Found When Accessing BI Applications Through Load Balancer

Problem: A 404 "page not found" message is displayed in the Web browser when you try to access Oracle Business Intelligence applications (such as Oracle BI Presentation Services, Oracle BI Publisher, and Oracle Real-Time Decisions) using the load balancer address. The error is intermittent and BI servers appear as "Running" in the Administration Console.

Solution: Even when the BI Managed Servers are up and running, some of the applications contained in them may be in Admin, Prepared, or other states different from Active. The applications might be unavailable while the BI server is running. Check the Deployments page in the Administration Console to verify the status of the affected application. It should be in "Active" state. Check the BI server's output log for errors pertaining to that application and try to start it from the Deployments page in the Administration Console.

10.6.2 Administration Server Fails to Start After a Manual Failover

Problem: Administration Server fails to start after the Administration Server node failed and manual failover to another nodes is performed. The Administration Server output log reports the following:

```
<Feb 19, 2009 3:43:05 AM PST> <Warning> <EmbeddedLDAP> <BEA-171520> <Could not
obtain an exclusive lock for directory: ORACLE_BASE/admin/edg_domain/aserver/edg_
domain/servers/AdminServer/data/ldap/ldapfiles. Waiting for 10 seconds and then
retrying in case existing WebLogic Server is still shutting down.>
```

Solution: When restoring a node after a node crash and using shared storage for the domain directory, you may see this error in the log for the Administration Server due to unsuccessful lock cleanup. To resolve this error, remove the file *ORACLE_BASE*/admin/*domain_name*/aserver/*domain_name*/servers/AdminServer/data/ldap/ldapfiles/EmbeddedLDAP.lok.

10.6.3 Error While Activating Changes in Administration Console

Problem: Activation of changes in Administration Console fails after changes to a server's start configuration have been performed. The Administration Console reports the following when clicking "Activate Changes":

```
An error occurred during activation of changes, please see the log for details.
 [Management:141190]The commit phase of the configuration update failed with an
exception:
In production mode, it's not allowed to set a clear text value to the property:
PasswordEncrypted of ServerStartMBean
```

Solution: This may happen when start parameters are changed for a server in the Administration Console. In this case, provide user name/password information in the server start configuration in the Administration Console for the specific server whose configuration was being changed.

10.6.4 bi_server Managed Server Not Failed Over After Server Migration

Problem: After reaching the maximum restart attempts by local Node Manager, Node Manager in the failover node tries to restart it, but the server does not come up. The server seems to be failed over as reported by Node Manager's output information. The VIP used by the bi_server Managed Server is not enabled in the failover node after Node Manager tries to migrate it (if config in the failover node does not report the VIP in any interface). Executing the command "sudo ifconfig $INTERFACE $ADDRESS $NETMASK" does not enable the IP in the failover node.

Solution: The rights and configuration for `sudo` execution should not prompt for a password. Verify the configuration of `sudo` with your system administrator so that `sudo` works without a password prompt.

10.6.5 bi_server Managed Server Not Reachable From Browser After Server Migration

Problem: Server migration is working (bi_server Managed Server is restarted in the failed over node), but the `Virtual_Hostname:9704/analytics` URL cannot be accessed in the Web browser. The server has been "killed" in its original host and Node Manager in the failover node reports that the VIP has been migrated and the server started. The VIP used by the bi_server Managed Server cannot be pinged from the client's node (that is, the node where the browser is being used).

Solution: The `arping` command executed by Node Manager to update ARP caches did not broadcast the update properly. In this case, the node is not reachable to external nodes. Either update the nodemanager.properties file to include the MACBroadcast or execute a manual arping:

```
/sbin/arping -b -q -c 3 -A -I INTERFACE ADDRESS > $NullDevice 2>&1
```

Where *INTERFACE* is the network interface where the virtual IP is enabled and *ADDRESS* is the virtual IP address.

10.6.6 OAM Configuration Tool Does Not Remove URLs

Problem: The OAM Configuration Tool has been used and a set of URLs was added to the policies in Oracle Access Manager. One of multiple URLs had a typo. Executing the OAM Configuration Tool again with the correct URLs completes successfully; however, when accessing Policy Manager, the incorrect URL is still there.

Solution: The OAM Configuration Tool only adds new URLs to existing policies when executed with the same `app_domain` name. To remove a URL, use the Policy Manager Console in OAM. Log on to the Access Administration site for OAM, click My Policy Domains, and then click the created policy domain (bifoundation_domain). Click the Resources tab, and then remove the incorrect URLs.

10.6.7 Users Redirected to Login Screen After Activating Changes

Problem: After configuring Oracle HTTP Server and LBR to access the Administration Console, some activation changes cause the redirection to the login screen for the Administration Console.

Solution: This is the result of the console attempting to follow changes to port, channel, and security settings as a user makes these changes. For certain changes, the console may redirect to the Administration Server's listen address. Activation is completed regardless of the redirection. It is not required to log in again; users can simply update the URL to `admin.mycompany.com/console/console.portal` and directly access the home page for the Administration Console.

> **Note:** This problem will not occur if you have disabled tracking of the changes described in this section.

10.6.8 Users Redirected to Home Page After Activating Changes

Problem: After configuring OAM, some activation changes cause redirection to the Administration Console home page (instead of the context menu where the activation was performed).

Solution: This is expected when OAM SSO is configured and the Administration Console is set to follow configuration changes (redirections are performed by the Administration Server when activating some changes). Activations should complete regardless of this redirection. For successive changes not to redirect, access the Administration Console, choose Preferences, then Shared Preferences, and deselect the "Follow Configuration Changes" check box.

10.6.9 Configured JOC Port Already in Use

Problem: Attempts to start a Managed Server that uses the Java Object Cache, such as OWSM Managed Servers, fail. The following errors appear in the logs:

```
J2EE JOC-058 distributed cache initialization failure
J2EE JOC-043 base exception:
J2EE JOC-803 unexpected EOF during read.
```

Solution: Another process is using the same port that JOC is attempting to obtain. Either stop that process, or reconfigure JOC for this cluster to use another port in the recommended port range.

10.6.10 Out-of-Memory Issues on Managed Servers

Problem: You are experiencing out-of-memory issues on Managed Servers.

Solution: Increase the size of the memory heap allocated for the Java VM to at least one gigabyte:

1. Log in to the Administration Console.

2. Click **Environment**, then **Servers**.

3. Click a Managed Server name.

4. Open the Configuration tab.

5. Open the Server Start tab in the second row of tabs.

6. Include the memory parameters in the Arguments box, for example:

   ```
   -Xms256m -Xmx1024m -XX:CompileThreshold=8000 -XX:PermSize=128m
   -XX:MaxPermSize=1024m
   ```

> **Note:** The memory parameter requirements may differ between various JVMs (Sun, JRockit, or others).

7. Save the configuration changes.

8. Restart all running Managed Servers.

10.6.11 Missing JMS Instances on Oracle BI Publisher Scheduler Diagnostics Page

In some cases, only one JMS instance is visible on the Oracle BI Publisher Scheduler diagnostics page, rather than all instances in the cluster. This issue is most likely caused by clocks being out of sync. See Section 2.4, "Clock Synchronization" for more information on the importance of synchronizing clocks on all nodes in the cluster.

10.6.12 Oracle BI Publisher Jobs in Inconsistent State After Managed Server Shutdown

Before shutting down the Managed Server on which Oracle BI Publisher is running, it is a best practice (but not mandatory) to wait for all running Oracle BI Publisher jobs to complete, or to cancel any unfinished jobs using the Report Job History page. Otherwise, the shutdown might cause some jobs to incorrectly stay in a running state.

10.6.13 JMS Instance Fails In an Oracle BI Publisher Cluster

On rare occasions, a JMS instance is missing from an Oracle BI Publisher Scheduler cluster. To resolve this issue, restart the Oracle BI Publisher application from the Oracle WebLogic Server Administration Console.

To restart your BI Publisher application:

1. Log in to the Administration Console.

2. Click **Deployments** in the Domain Structure window.

3. Select **bipublisher(11.1.1)**.

4. Click **Stop**.

5. After the application stops, click **Start**.

10.7 Other Recommendations

This section covers the following topics:

- Section 10.7.1, "Preventing Timeouts for SQLNet Connections"
- Section 10.7.2, "Auditing"

10.7.1 Preventing Timeouts for SQLNet Connections

Much of the EDG production deployment involves firewalls. Because database connections are made across firewalls, Oracle recommends that the firewall be configured so that the database connection is not timed out. For Oracle Real Application Clusters (Oracle RAC), the database connections are made on Oracle RAC VIPs and the database listener port. You must configure the firewall to not time out such connections. If such a configuration is not possible, set the*SQLNET.EXPIRE_ TIME=n* parameter in the *ORACLE_HOME*/network/admin/sqlnet.ora file on the database server, where *n* is the time in minutes. Set this value to less than the known

value of the timeout for the network device (that is, a firewall). For Oracle RAC, set this parameter in all of the Oracle home directories.

10.7.2 Auditing

Oracle Fusion Middleware Audit Framework is a new service in Oracle Fusion Middleware 11*g*, designed to provide a centralized audit framework for the middleware family of products. The framework provides audit service for platform components such as Oracle Platform Security Services (OPSS) and Oracle Web Services. It also provides a framework for JavaEE applications, starting with Oracle's own JavaEE components. JavaEE applications will be able to create application-specific audit events. For non-JavaEE Oracle components in the middleware, such as C or JavaSE components, the audit framework also provides an end-to-end structure similar to that for JavaEE applications.

Figure 10–1 is a high-level architectural diagram of the Oracle Fusion Middleware Audit Framework.

Figure 10–1   Audit Event Flow
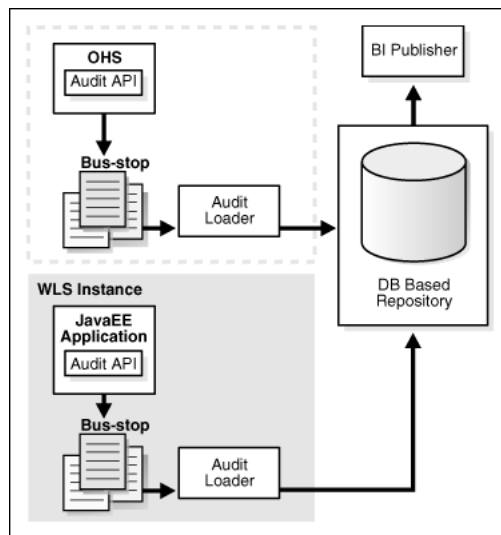
The Oracle Fusion Middleware Audit Framework consists of the following key components:

- **Audit APIs:** These are APIs provided by the audit framework for any audit-aware components integrating with the Oracle Fusion Middleware Audit Framework. During run time, applications may call these APIs, where appropriate, to audit the necessary information about a particular event happening in the application code. The interface allows applications to specify event details such as username and other attributes needed to provide the context of the event being audited.

- **Audit Events and Configuration:** The Oracle Fusion Middleware Audit Framework provides a set of generic events for convenient mapping to application audit events. Some of these include common events such as authentication. The framework also allows applications to define application-specific events.

  These event definitions and configurations are implemented as part of the audit service in Oracle Platform Security Services. Configurations can be updated through Enterprise Manager (UI) and WLST (command-line tool).

- **Audit Bus-stop:** Bus-stops are local files containing audit data before they are pushed to the audit repository. In the event where no database repository is configured, these bus-stop files can be used as a file-based audit repository. The bus-stop files are simple text files that can be queried easily to look up specific audit events. When a DB-based repository is in place, the bus-stop acts as an intermediary between the component and the audit repository. The local files are periodically uploaded to the audit repository based on a configurable time interval.

- **Audit Loader:** As the name implies, the audit loader loads the files from the audit bus-stop into the audit repository. In the case of platform and JavaEE application audit, the audit loader is started as part of the JavaEE container start-up. In the case of system components, the audit loader is a periodically spawned process.

- **Audit Repository:** The audit repository contains a predefined Oracle Fusion Middleware Audit Framework schema, created by Repository Creation Utility (RCU). Once configured, all the audit loaders are aware of the repository and upload data to it periodically. The audit data in the audit repository is expected to be cumulative and will grow over time. Ideally, this should not be an operational database used by any other applications; rather, it should be a standalone RDBMS used for audit purposes only. In a highly available configuration, Oracle recommends that you use an Oracle Real Application Clusters (Oracle RAC) database as the audit data store.

- **Oracle Business Intelligence Publisher:** The data in the audit repository is exposed through predefined reports in Oracle Business Intelligence Publisher. The reports allow users to drill down the audit data based on various criteria. For example:

  - Username

  - Time range

  - Application type

  - Execution context identifier (ECID)

For more introductory information for the Oracle Fusion Middleware Audit Framework, see the "Introduction to Oracle Fusion Middleware Audit Framework" chapter in the *Oracle Fusion Middleware Application Security Guide*.

For information on how to configure the repository for Oracle Fusion Middleware Audit Framework, see the "Configuring and Managing Auditing" chapter in the *Oracle Fusion Middleware Application Security Guide*.

The EDG topology does not include Oracle Fusion Middleware Audit Framework configuration. The ability to generate audit data to the bus-stop files and the configuration of the audit loader will be available after the products are installed. The main consideration is the audit database repository where the audit data is stored. Because of the volume and the historical nature of the audit data, it is strongly recommended that customers use a separate database from the operational store or stores being used for other middleware components.

Index