# Oracle® Fusion Middleware

Disaster Recovery Guide

11*g* Release 1 (11.1.1)

**E15250-01**

December 2009

Oracle Fusion Middleware Disaster Recovery Guide, 11*g* Release 1 (11.1.1)

E15250-01

Primary Author: Bert Rich

Contributing Author: Bharath K. Reddy

Contributors: Pradeep Bhat, Shailesh Dwivedi, Fermin Castro, Kevin Clugage, Bhagat Nainani, Jeff Bryan, Kolpak Kothari , Bo Stern, Sanjay Baldwa, Jeni Ferns, Hui Ye, Brian Fry, Ramaprakash Sathyanarayan, Jingjing Wei, Vasuki Ashok, Pratima Gogineni, Daniel Shih, Ankit Mittal, Shalendra Goel, Patrick Fry, Pushkar Kapasi, Philip Kuhn, Ratheesh Pai, Suresh Mali, Tom Barnes, Vinay Shukla, Shilpa Shree, Prasad Vedurumudi, Premson Rodriguez, Gopal Kirsur

# Contents

## 3 Design Considerations

## 4 Setting Up and Managing Disaster Recovery Sites

## 5 Troubleshooting Disaster Recovery

## A Managing Oracle Inventory

## Index

# Preface

This preface contains these sections:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

## Audience

This document is intended for administrators, developers, and others whose role is to deploy and manage the Oracle Fusion Middleware Disaster Recovery solution using storage replication technology.

## Documentation Accessibility

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

### Accessibility of Code Examples in Documentation

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

### Accessibility of Links to External Web Sites in Documentation

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

### Deaf/Hard of Hearing Access to Oracle Support Services

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

## Related Documents

For more information, see the following documents in the Oracle Fusion Middleware documentation set:

- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide*

## Conventions

The following text conventions are used in this document:

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

# 1 Disaster Recovery Introduction

This chapter provides an introduction to the Oracle Fusion Middleware Disaster Recovery solution.

It contains the following topics:

- Disaster Recovery Overview
- Disaster Recovery for Oracle Fusion Middleware Components

## 1.1 Disaster Recovery Overview

This section provides an overview of Oracle Fusion Middleware Disaster Recovery.

It contains the following topics:

- Problem Description and Common Solutions
- Terminology

### 1.1.1 Problem Description and Common Solutions

Providing Maximum Availability Architecture is one of the key requirements for any Oracle Fusion Middleware enterprise deployment. Oracle Fusion Middleware includes an extensive set of high availability features such as: process death detection and restart, server clustering, server migration, clusterware integration, GridLink, load balancing, failover, backup and recovery, rolling upgrades, and rolling configuration changes, which protect an Enterprise Deployment from unplanned down time and minimize planned downtime.

Additionally, enterprise deployments need protection from unforeseen disasters and natural calamities. One protection solution involves setting up a standby site at a geographically different location than the production site. The standby site may have equal or fewer services and resources compared to the production site. Application data, metadata, configuration data, and security data are replicated to the standby site on a periodic basis. The standby site is normally in a passive mode; it is started when the production site is not available. This deployment model is sometimes referred to as an active/passive model. This model is normally adopted when the two sites are connected over a WAN and network latency does not allow clustering across the two sites.

A core strategy for and a key feature of Oracle Fusion Middleware is hot-pluggability. Built for the heterogeneous enterprise, Oracle Fusion Middleware consists of modular component software that runs on a range of popular platforms and interoperates with middleware technologies and business applications from other software vendors such as IBM, Microsoft, and SAP. For instance, Oracle Fusion Middleware products and technologies such as ADF, Oracle BPEL Process Manager, Oracle Enterprise Service Bus, Oracle Web Services Manager, Adapters, Oracle Access Manager, Oracle Identity Manager, Rules, Oracle TopLink, and Oracle Business Intelligence Publisher can run on non-Oracle containers such as IBM Websphere and JBoss, in addition to running on the Oracle WebLogic Server container.

The Oracle Fusion Middleware Disaster Recovery solution uses storage replication technology for disaster protection of Oracle Fusion Middleware middle tier components. It supports hot-pluggable deployments, and it is compatible with third party vendor recommended solutions.

Disaster protection for Oracle databases that are included in your Oracle Fusion Middleware is provided through Oracle Data Guard.

This document describes how to deploy the Oracle Fusion Middleware Disaster Recovery solution for enterprise deployments on Linux and UNIX operating systems, making use of storage replication technology and Oracle Data Guard technology.

### 1.1.2 Terminology

This section defines the following Disaster Recovery terminology:

- **asymmetric topology**: An Oracle Fusion Middleware Disaster Recovery configuration that is different across tiers on the production site and standby site. For example, an asymmetric topology can include a standby site with fewer hosts and instances than the production site. Section 4.4, "Creating an Asymmetric Standby Site" describes how to create asymmetric topologies.
- **disaster**: A sudden, unplanned catastrophic event that causes unacceptable damage or loss. A disaster is an event that compromises an organization’s ability to provide critical functions, processes, or services for some unacceptable period of time and causes the organization to invoke its recovery plans.
- **Disaster Recovery**: The ability to safeguard against natural or unplanned outages at a production site by having a recovery strategy for applications and data to a geographically separate standby site.
- **alias host name**: This guide differentiates between the terms alias host name and physical host name.

  The alias host name is an alternate way to access the system besides its real network name. Typically, it resolves to the same IP address as the network name of the system. This can be defined in the name resolution system such as DNS, or locally in the local hosts file on each system. Multiple alias host names can be defined for a given system.

  See also the **physical host name** definition later in this section.
- **physical host name**: The physical host name is the host name of the system as returned by the `gethostname()` call or the `hostname` command. Typically, the physical host name is also the network name used by clients to access the system. In this case, an IP address is associated with this name in the DNS (or the given name resolution mechanism in use) and this IP is enabled on one of the network interfaces to the system.

  A given system typically has one physical host name. It can also have one or more additional network names, corresponding to IP addresses enabled on its network interfaces, that are used by clients to access it over the network. Further, each network name can be aliased with one or more alias host names.

  See also the **alias host name** definition earlier in this section.

- **production site setup**: The process of creating the production site. To create the production site using the procedure described in this manual, you must plan and create physical host names and alias host names, create mount points and symbolic links (if applicable) on the hosts to the Oracle home directories on the shared storage where the Oracle Fusion Middleware instances will be installed, install the binaries and instances, and deploy the applications. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes. See Section 3.2.3, "Storage Replication" for more details about symbolic links.
- **site failover**: The process of making the current standby site the new production site after the production site becomes unexpectedly unavailable (for example, due to a disaster at the production site). This book also uses the term "failover" to refer to a site failover.
- **site switchback**: The process of reverting the current production site and the current standby site to their original roles. Switchbacks are planned operations done after the switchover operation has been completed. A switchback restores the original roles of each site: the current standby site becomes the production site and the current production site becomes the standby site. This book also uses the term "switchback" to refer to a site switchback.
- **site switchover**: The process of reversing the roles of the production site and standby site. Switchovers are planned operations done for periodic validation or to perform planned maintenance on the current production site. During a switchover, the current standby site becomes the new production site, and the current production site becomes the new standby site. This book also uses the term "switchover" to refer to a site switchover.
- **site synchronization**: The process of applying changes made to the production site at the standby site. For example, when a new application is deployed at the production site, you should perform a synchronization so that the same application will be deployed at the standby site, also.
- **standby site setup**: The process of creating the standby site. To create the standby site using the procedure described in this manual, you must plan and create physical host names and alias host names, and create mount points and symbolic links (if applicable) to the Oracle home directories on the standby shared storage. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes. See Section 3.2.3, "Storage Replication" for more details about symbolic links.
- **symmetric topology**: An Oracle Fusion Middleware Disaster Recovery configuration that is completely identical across tiers on the production site and standby site. In a symmetric topology, the production site and standby site have the identical number of hosts, load balancers, instances, and applications. The same ports are used for both sites. The systems are configured identically and the applications access the same data. This manual describes how to set up a symmetric Oracle Fusion Middleware Disaster Recovery topology for an enterprise configuration.
- **topology**: The production site and standby site hardware and software components that comprise an Oracle Fusion Middleware Disaster Recovery solution.

## 1.2 Disaster Recovery for Oracle Fusion Middleware Components

This section provides an introduction to setting up Disaster Recovery for a common Oracle Fusion Middleware enterprise deployment.

It contains the following topics:

- Oracle Fusion Middleware Disaster Recovery Architecture Overview
- Components Described in this Document

### 1.2.1 Oracle Fusion Middleware Disaster Recovery Architecture Overview

This section describes the deployment architecture for Oracle Fusion Middleware components.

The product binaries and configuration for Oracle Fusion Middleware components and applications gets deployed in Oracle home directories on the middle tier. Additionally, most of the products also have metadata or run-time data stored in a database repository.

Therefore, the Oracle Fusion Middleware Disaster Recovery solution keeps middle tier file system data and middle tier data stored in databases at the production site synchronized with the standby site.

The Oracle Fusion Middleware Disaster Recovery solution supports these methods of providing data protection for Oracle Fusion Middleware data and database content:

- Oracle Fusion Middleware product binaries, configuration, and metadata files

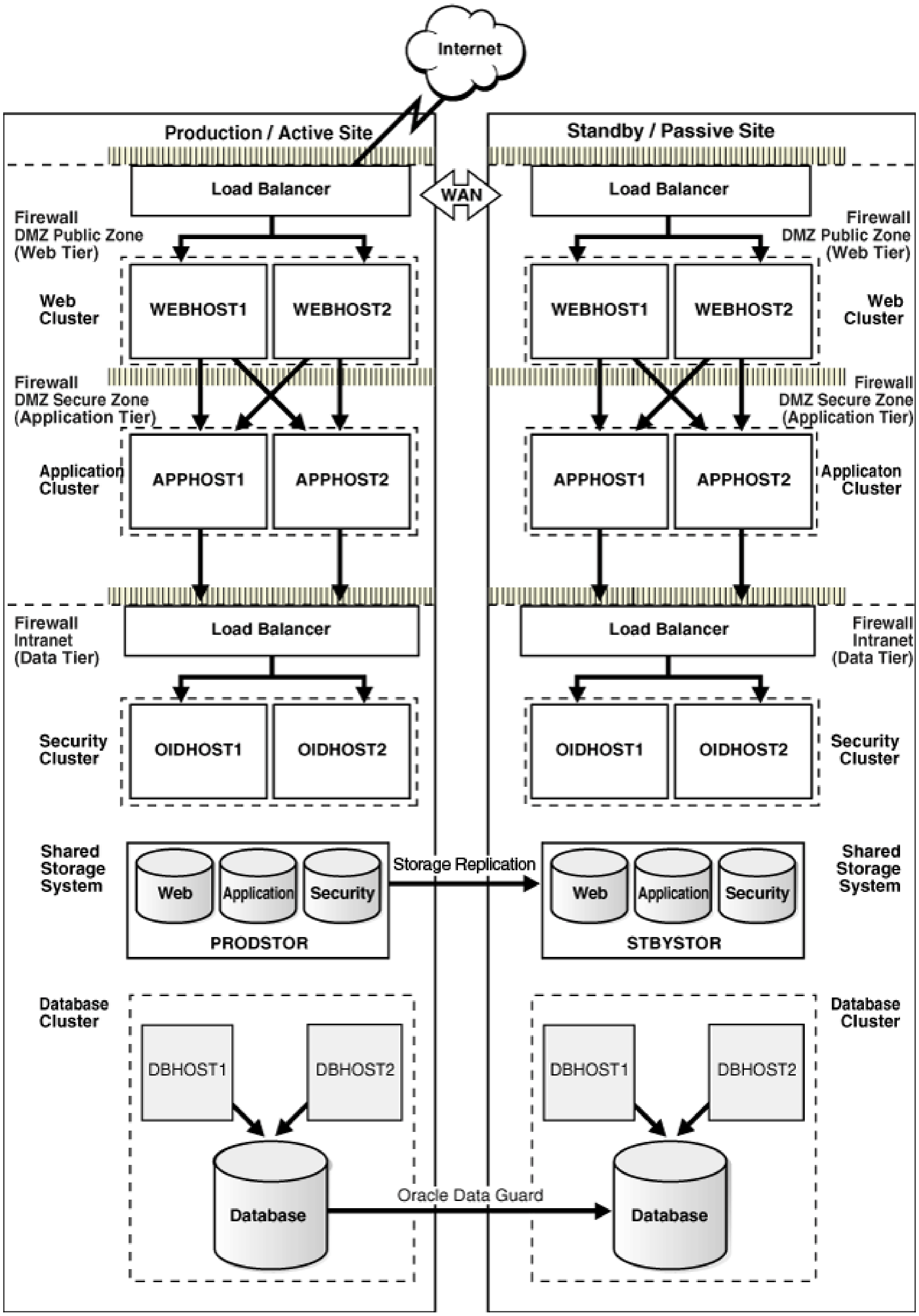
  Use storage replication technologies.

- Database content

  Use Oracle Data Guard for Oracle databases (and vendor-recommended solutions for third party databases).

Figure 1–1 shows an overview of an Oracle Fusion Middleware Disaster Recovery topology:

*Figure 1–1 Production and Standby Site for Oracle Fusion Middleware Disaster Recovery Topology*



Some of the key aspects of the solution in Figure 1–1 are:

- The solution has two sites. The current production site is running and active, while the second site is serving as a standby site and is in passive mode.
- Hosts on each site have mount points defined for accessing the shared storage system for the site.

- On both sites, the Oracle Fusion Middleware components are deployed on the site's shared storage system. This involves creating all the Oracle home directories, which include product binaries and configuration data for middleware components, in volumes on the production site's shared storage and then installing the components into the Oracle home directories on the shared storage. In Figure 1–1, a separate volume is created in the shared storage for each Oracle Fusion Middleware host cluster (note the Web, Application, and Security volumes created for the Web Cluster, Application Cluster, and Security Cluster in each site's shared storage system).
- Mount points must be created on the shared storage for the production site. The Oracle Fusion Middleware software for the production site will be installed into Oracle home directories using the mount points on the production site shared storage. Symbolic links may also need to be set up on the production site hosts to the Oracle Fusion Middleware home directories on the shared storage at the production site. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes. See Section 3.2.3, "Storage Replication" for more details about symbolic links.
- Mount points must be created on the shared storage for the standby site. Symbolic links also need to be set up on the standby site hosts to the Oracle Fusion Middleware home directories on the shared storage at the standby site. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes. See Section 3.2.3, "Storage Replication" for more details about symbolic links. The mount points and symbolic links for the standby site hosts must be identical to those set up for the equivalent production site hosts.
- Storage replication technology is used to copy the middle tier file systems and other data from the production site's shared storage to the standby site's shared storage.
- After storage replication is enabled, application deployment, configuration, metadata, data, and product binary information is replicated from the production site to the standby site.
- It is not necessary to perform any Oracle software installations at the standby site hosts. When the production site storage is replicated at the standby site storage, the equivalent Oracle home directories and data are written to the standby site storage.
- Schedule incremental replications at a specified interval. The recommended interval is once a day for the production deployment, where the middle tier configuration does not change very often. Additionally, you should force a manual synchronization whenever you make a change to the middle tier configuration at the production site (for example, if you deploy a new application at the production site). Some Oracle Fusion Middleware components generate data on the file system, which may require more frequent replication based on recovery point objectives. Please refer to Chapter 2, "Recommendations for Fusion Middleware Components" for detailed Disaster Recovery recommendations for Oracle Fusion Middleware components.
- Before forcing a manual synchronization, you should take a snapshot of the site to capture its current state. This ensures that the snapshot gets replicated to the standby site storage and can be used to roll back the standby site to a previous synchronization state, if desired. Recovery to the point of the previously successful replication (for which a snapshot was created) is possible when a replication fails.

- Oracle Data Guard is used to replicate all Oracle database repositories, including Oracle Fusion Middleware repositories and custom application databases. For information about using Oracle Data Guard to provide disaster protection for Oracle databases, see Section 3.3, "Database Considerations."
- If your Oracle Fusion Middleware Disaster Recovery topology includes any third party databases, use the vendor-recommended solution for those databases.
- User requests are initially routed to the production site.
- When there is a failure or planned outage of the production site, you perform the following steps to enable the standby site to assume the production role in the topology:
  1. Stop the replication from the production site to the standby site (when a failure occurs, replication may have already been stopped due to the failure).
  2. Perform a failover or switchover of the Oracle databases using Oracle Data Guard.
  3. Start the services and applications on the standby site.
  4. Use a global load balancer to re-route user requests to the standby site. At this point, the standby site has assumed the production role.

### 1.2.2 Components Described in this Document

The Oracle Fusion Middleware Disaster Recovery solution supports components from various Oracle product suites, including:

- Oracle WebLogic Server components:

  See Section 2.1, "Recommendations for Oracle WebLogic Server" for Disaster Recovery recommendations for Oracle WebLogic Server components.
- Oracle ADF

  See Section 2.2, "Recommendations for Oracle ADF" for Disaster Recovery recommendations for Oracle Application Development Framework (Oracle ADF).
- Oracle WebCenter components:
  - Oracle WebCenter Spaces
  - Oracle WebCenter Portlets
  - Oracle WebCenter Discussions Server
  - Oracle WebCenter Wiki and Blog Server

  See Section 2.3, "Recommendations for Oracle WebCenter" for Disaster Recovery recommendations for Oracle WebCenter components.
- Oracle SOA Suite components:
  - Oracle SOA Service Infrastructure
  - Oracle BPEL Process Manager
  - Oracle Mediator
  - Oracle Human Workflow
  - Oracle B2B
  - Oracle Web Services Manager
  - Oracle User Messaging Service

  - Oracle JCA Adapters
  - Oracle Business Activity Monitoring

  See Section 2.4, "Recommendations for Oracle SOA Suite" for Disaster Recovery recommendations for Oracle SOA Suite components.

- Oracle Identity Management components:
  - Oracle Internet Directory
  - Oracle Virtual Directory
  - Oracle Directory Integration Platform
  - Oracle Identity Federation
  - Oracle Directory Services Manager
  - Oracle Access Manager

  See Section 2.5, "Recommendations for Oracle Identity Management" for Disaster Recovery recommendations for Oracle Identity Management components.

- Oracle Portal, Forms, Reports, and Business Intelligence Discoverer components:
  - Oracle Portal
  - Oracle Forms
  - Oracle Reports
  - Oracle Business Intelligence Discoverer (Discoverer)

  See Section 2.6, "Recommendations for Oracle Portal, Forms, Reports, and Discoverer" for Disaster Recovery recommendations for these components.

- Oracle Web Tier components:
  - Oracle HTTP Server
  - Oracle Web Cache

  See Section 2.7, "Recommendations for Oracle Web Tier Components" for Disaster Recovery recommendations for Oracle Web Tier components.

# 2 Recommendations for Fusion Middleware Components

This chapter describes the disaster protection requirements for Oracle Fusion Middleware components in different Oracle product suites and also provides recommendations for synchronizing those components. As mentioned previously, use storage replication to synchronize middle tier content, and use Oracle Data Guard to synchronize data in Oracle database repositories or custom application databases included in your Oracle Fusion Middleware Disaster Recovery topology.

This chapter provides Disaster Recovery recommendations for components in the following Oracle product suites:

- Recommendations for Oracle WebLogic Server
- Recommendations for Oracle ADF
- Recommendations for Oracle WebCenter
- Recommendations for Oracle SOA Suite
- Recommendations for Oracle Identity Management
- Recommendations for Oracle Portal, Forms, Reports, and Discoverer
- Recommendations for Oracle Web Tier Components

### Common Artifacts Across Oracle Product Suites

Certain artifacts like the Oracle Inventory, the `beahomelist` file, the `oratab` file and `oraInst.loc` file are common across all Oracle product deployments. These artifacts change very rarely and need not be a part of the regular storage replication and synchronization activity. It is recommended to have the Oracle Inventory, the `beahomelist` file, the `oratab` file, and the `oraInst.loc` file on the local disk of the machines. These artifacts should be manually updated upon creation, as well as upon applying patch updates. If required by your environment, these artifacts can also be on shared storage.

## 2.1 Recommendations for Oracle WebLogic Server

Oracle WebLogic Server is a scalable, enterprise-ready Java Platform, Enterprise Edition (Java EE) application server. The WebLogic Server infrastructure supports the deployment of many types of distributed applications and is an ideal foundation for building applications based on Service Oriented Architectures (SOA).

### Common Artifacts and Considerations for Oracle WebLogic Server

The following artifacts and considerations apply to all the WebLogic Server components along with the component-specific recommendations.

#### Artifacts on the File System

MW_HOME: The Middleware home consists of a WebLogic home that has the WebLogic Server binaries.

Domain home: The domain home contains the configuration data and the applications for the WebLogic domain.

#### Network Artifacts

Oracle recommends using the virtual host name as the listen address for both the Oracle WebLogic Administration Server and Managed Server. As long as this host name can be resolved on both the production and standby site, there is no need to update this value after a Disaster Recovery operation.

If your environment requires whole server migration to be configured, it is recommended to use the virtual host name as the listen address of the Managed Servers that are configured for whole server migration. To avoid manually updating the listen address after a disaster recovery operation, make sure that the host name can be resolved on both the primary and standby sites.

The load balancer virtual hosts used for accessing the WebLogic Server applications should be configured on both the production and standby sites

The rest of this section describes Disaster Recovery recommendations for the following Oracle WebLogic Server components:

- Recommendations for Oracle WebLogic Server JMS and T-Logs
- Recommendations for Oracle Platform Security Services

## 2.1.1 Recommendations for Oracle WebLogic Server JMS and T-Logs

This section describes various Oracle WebLogic Server JMS and transaction log (T-log) artifacts and provides recommendations for disaster recovery.

#### Artifacts on the File System

File-based persistent stores: The file store location for the JMS/T-log when using a file based persistent store.

#### Artifacts in the Database

The schema containing the JMS messages, when using database based persistent stores. The schema containing Logging Last Resource (LLR) transaction log records for WebLogic applications that leverage the JDBC LLR option.

#### Special Considerations

- Messages are lost if they were en-queued after the system restore point time but never processed. Message duplicates are generated for messages enqueued before the restore point time, but dequeued and acknowledged or committed (processed) after this time.
- If the persistent store is a custom store that is dedicated to JMS use, then you can delete the entire store.

- Restoring different parts of the system to different points in time can lead to inconsistent data. This can occur when the message store, transaction log, or application database are synchronized differently. For example, a message may reference a database row that does not exist, or vice-versa. This may delete unprocessed messages in addition to duplicate messages.
- If the store is not dedicated to JMS use, use the Oracle WebLogic Server JMS message management administrative tooling. This tooling can perform import, export, move, and delete operations from the Administration Console, MBeans, and WLST.
- When applications use both queues and topics, make sure to manipulate both the queue and topic subscriptions.

#### Synchronization Recommendations

- If JMS data is critical, it is recommended to synchronize transaction log data and JMS data in real time using synchronous replication. Note that using synchronous replication may have performance implications.
- If data consistency between tiers is important, ensure that the database and application tiers are replicated at the same time. This helps ensure that the different tiers recover to the same exact point in time.
- Use Oracle Data Guard to replicate the primary site and standby site when using database based persistent stores.
- When using a storage device that does not support block-level snapshot capabilities, shut down the JMS server to take a consistent backup. This is to ensure that the persistence store is not being written to while the copy operation is being performed. In a clustered environment, you can do so by shutting down one server at time, backing it up and restarting it. You also can create a script to perform these operations using WLST.

#### Recovery Recommendations

Recover the database schemas containing the persistent store to the most recent point in time, the Administration Server, and the Managed Servers in the WebLogic Server domain.

Also, follow the recovery recommendations below for avoiding duplicate messages.

#### Avoiding Duplicate Messages

Use the following procedure before recovery to drain messages in the JMS queue after persistent-store recovery to avoid processing duplicate messages:

> **Note:** Do not drain and discard messages without first being certain that the messages contain no data that must be preserved. The recovered messages may include unprocessed messages with important application data, in addition to duplicate messages that have already been processed.

1. Log into the Oracle WebLogic Server Administration Console.
2. Before recovery, configure JMS server to pause Production, Insertion, and consumption operations at boot-time to ensure that no new messages are produced or inserted into the destination or consumed from the destination before you drain stale messages. To do this:

   a. Expand **Services**, then **Messaging**, and then **JMS Servers**.
   b. On the Summary of JMS Servers page, click the JMS server you want to configure for message pausing.
   c. On the Configuration: General page, click **Advanced** to define the message pausing options. Select **Insertion Paused At Startup**, **Production Paused At Startup**, and **Consumption Paused At Startup**.
   d. Click **Save**.
   e. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

Use the following procedure after recovery:

1. After recovering the persistent store, start the Managed Servers.
2. Drain the stale messages from JMS destinations by following these steps:
   a. Expand **Services**, then **Messaging**, and then **JMS Modules**.
   b. Select a JMS module, then select a destination.
   c. Select **Monitoring**, then **Show Messages**.
   d. Click **Delete All**.

Resume operations by following these steps:

1. Expand **Services**, then **Messaging**, and then **JMS Servers**.
2. On the Summary of JMS Servers page, click the JMS server you want to configure for message pausing.
3. On the Configuration: General page, click **Advanced**. Select **Insertion Paused At Startup**, **Production Paused At Startup**, and **Consumption Paused At Startup**.
4. Click **Save**.
5. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

## 2.1.2 Recommendations for Oracle Platform Security Services

This section describes various Oracle Platform Security Services artifacts and provides recommendations for disaster recovery.

### Artifacts in the Database

Not applicable because Oracle Platform Security Services does not have any database dependencies.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes and applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

Recover the Administration Server and the Managed Servers in the WebLogic Server domain.

## 2.2 Recommendations for Oracle ADF

Oracle ADF is an end-to-end application framework that builds on Java Platform, Enterprise Edition (Java EE) standards and open-source technologies to simplify and accelerate implementing service-oriented applications. Oracle ADF is suitable for enterprise developers who want to create applications that search, display, create, modify, and validate data using web, wireless, desktop, or web services interfaces

This section describes various Oracle ADF artifacts and provides recommendations for disaster recovery.

### Artifacts on the File System

MW_HOME: The Middleware home consists of a WebLogic home that has the WebLogic Server binaries.

Oracle_Common_Home: The Oracle home that contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).

Domain home: The domain home contains the configuration data and the applications for the Oracle ADF domain.

Custom Applications Directory: This is the stage location for various customer applications and their related libraries.

### Network Artifacts

Oracle recommends using the virtual host name as the listen address for both the Oracle WebLogic Administration Server and Managed Server. As long as this host name can be resolved on both the production and standby site, there is no need to update this value after a Disaster Recovery operation.

The load balancer virtual hosts used for accessing the applications should be configured on both the production and standby sites.

### Artifacts in the Database

Oracle ADF applications may use the MDS repository to persist the application state and configuration data. Persisting data depends on how the application is coded.

Most Oracle ADF applications do not use the MDS repository to store application data, but instead use a separate data store (usually a database) to store application data.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying composites, applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

The database must be recovered to the most recent point in time, along with the Managed Servers running the ADF or WebCenter applications.

## 2.3 Recommendations for Oracle WebCenter

Oracle WebCenter combines the standards-based, declarative development of Java Server Faces (JSF), the flexibility and power of portals, and a set of integrated Web 2.0 services.

### Common Artifacts and Considerations for Oracle WebCenter

The artifacts and considerations below apply to all the Oracle WebCenter products along with the product-specific considerations.

### Artifacts on the File System

MW_HOME: The Middleware home consists of a WebLogic home that has the WebLogic Server binaries and an Oracle home containing the Oracle WebCenter binaries.

Oracle_Common_Home: The Oracle home that contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).

Domain home: The domain home contains the configuration data for the Oracle WebCenter domain.

### Artifacts in the Database

The Oracle WebCenter schema stores data for some of the Oracle WebCenter services and is part of Oracle WebCenter databases, and the MDS repository stores WebCenter metadata and configuration information.

### Network Artifacts

Oracle recommends using the virtual host name as the listen address for both the Oracle WebLogic Administration Server and Managed Server. As long as this host name can be resolved on both the production and standby site, there is no need to update this value after a Disaster Recovery operation.

The load balancer virtual hosts required for accessing the WebCenter products should be configured on both the production and standby sites.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying applications, and applying patches.

Oracle Data Guard should be configured for the Oracle database containing the WebCenter schema and the metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The database containing the Oracle WebCenter schemas must be recovered to the most recent point in time, along with the Managed Servers running the WebCenter applications.

The rest of this section describes Disaster Recovery recommendations for the following Oracle WebCenter products:

- Recommendations for Oracle WebCenter Spaces
- Recommendations for Oracle WebCenter Portlets
- Recommendations for Oracle WebCenter Discussions Server
- Recommendations for Oracle WebCenter Wiki and Blog Server

### 2.3.1 Recommendations for Oracle WebCenter Spaces

Oracle WebCenter Spaces offers a single, integrated, Web-based environment for social networking, communication, collaboration, and personal productivity through a robust set of services and applications.

This section describes various Oracle WebCenter Spaces artifacts and provides recommendations for disaster recovery.

#### Artifacts in the Database

The WebCenter schema stores data for some of the Oracle WebCenter services and is part of the Oracle WebCenter schemas, and the MDS repository stores WebCenter metadata and configuration information.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying applications, and applying patches.

Oracle Data Guard should be configured for the Oracle database containing the WebCenter schema and the metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The database containing the WebCenter schema and MDS repository must be recovered to the most recent point in time, along with the Oracle WebCenter domain.

### 2.3.2 Recommendations for Oracle WebCenter Portlets

Oracle WebCenter Portlets supports deployment and execution of both standards-based portlets (JSR 168, WSRP 1.0 and 2.0), and traditional Oracle PDK-Java based portlets. Oracle WebCenter provides several out-of-the-box producers, such as OmniPortlet, Web Clipping, Rich Text Portlet, and WSRP Tools.

This section describes various Oracle WebCenter Portlets artifacts and provides recommendations for disaster recovery.

### Artifacts in the Database

The Portlet schema stores user customizations and is part of the Oracle WebCenter schemas, and the MDS repository stores Portlet metadata and configuration information.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying applications, and applying patches.

Oracle Data Guard should be configured for the Oracle database containing the WebCenter schema and the metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

The database containing the WebCenter Portlet schema and MDS repository must be recovered to the most recent point in time, along with the Oracle WebCenter domain.

## 2.3.3 Recommendations for Oracle WebCenter Discussions Server

Oracle WebCenter Discussions Server provides the ability to integrate discussion forums and announcements into your applications.

This section describes various Oracle WebCenter Discussions Server artifacts and provides recommendations for disaster recovery.

### Artifacts in the Database

The Discussions schema stores metadata and data and is part of the Oracle WebCenter schemas.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying applications, and applying patches.

Oracle Data Guard should be configured for the Oracle database containing the WebCenter schema and the metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

The database containing the WebCenter Discussions schema must be recovered to the most recent point in time, along with the Oracle WebCenter domain.

## 2.3.4 Recommendations for Oracle WebCenter Wiki and Blog Server

Oracle WebCenter Wiki and Blog server provides the ability to integrate wikis and blogs into your applications. It also supports features that enable application users to create their own wikis and blogs.

This section describes various Oracle WebCenter Wiki and Blog Server artifacts and provides recommendations for disaster recovery.

### Artifacts in the Database

The Wiki schema stores metadata and data and is part of the Oracle WebCenter schemas.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying applications, and applying patches.

Oracle Data Guard should be configured for the Oracle database containing the WebCenter schema and the metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

The database containing the WebCenter Wiki schema must be recovered to the most recent point in time, along with the Oracle WebCenter domain.

## 2.4 Recommendations for Oracle SOA Suite

Oracle SOA Suite is a middleware component of Oracle Fusion Middleware. Oracle SOA Suite provides a complete set of service infrastructure components for designing, deploying, and managing SOA composite applications. Oracle SOA Suite enables services to be created, managed, and orchestrated into SOA composite applications. Composites enable you to easily assemble multiple technology components into one SOA composite application. SOA composite applications consist of:

- Service components: Service components are the basic building blocks of SOA composite applications. Service components implement a part of the overall business logic of the SOA composite application. Oracle BPEL Process Manager, Oracle Mediator, Oracle Human Workflow and Business Rules are examples of service components.
- Binding components: Binding components connect SOA composite applications to external services, applications, and technologies. Binding components are organized into two groups:
  - Services: Provide the outside world with an entry point to the SOA composite application. The WSDL file of the service advertises its capabilities to external applications. The service bindings define how a SOA composite service can be invoked (for example, through SOAP).
  - References: Enable messages to be sent from the SOA composite application to external services (for example, the same functionality that partner links provide for BPEL processes, but at the higher SOA composite application level).

**Note:** In Oracle SOA Suite release 11.1.1.1, the soa-infra and service engine configuration files were stored in local or shared storage files as part of the domain configuration.

Starting in Oracle SOA Suite 11.1.1.2, those files were moved into the metadata repository. Thus, soa-infra and service-engine configuration changes are now immediately propagated across a cluster.

The Disaster Recovery recommendations for Oracle SOA Suite assume that you are using Oracle SOA Suite 11.1.1.2.

Oracle SOA Suite artifacts are stored on the local or shared file system as well as in the metadata repositories. Composite artifacts are stored in the metadata repository, and binaries and domain-related configuration files are stored on a local or shared file system.

### Common Artifacts and Considerations for All SOA Suite Components

The artifacts and considerations below apply to all the SOA Suite components, along with the component-specific considerations.

### Artifacts on the File System

MW_HOME: The Middleware home consists of a WebLogic home that has the WebLogic Server binaries and an Oracle home containing the Oracle SOA Suite binaries.

Oracle_Common_Home: The Oracle home that contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).

Domain Home: The domain home contains the configuration data and SOA composites for the SOA domain.

### Network Artifacts

Oracle recommends using the virtual host name as the listen address for both the Oracle WebLogic Administration Server and Managed Server. As long as this host name can be resolved on both the production and standby site, there is no need to update this value after a Disaster Recovery operation. See *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite* for instructions updating an IP address to a virtual host name.

The load balancer virtual hosts required for accessing the SOA Suite components should be configured on both the production and standby sites.

### Artifacts in the Database

Oracle SOA Suite schemas, Service Infrastructure and Service Engine configurations, and composite definitions are stored in the Oracle SOA Suite database and metadata repository.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making domain-related configuration changes, deploying composites, and applying patches.

Oracle Data Guard should be configured for the Oracle SOA Suite database and metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The database must be recovered to the most recent point in time to ensure that the latest composite definitions and in-flight instances are restored.

In-flight instances require the matching composite definition to continue processing. For this reason, the metadata repository (where composite definitions are stored) and Oracle SOA Suite database (where process state is maintained) must be recovered to the same point in time.

In case of redeployed composites, a database recovery ensures consistency between the dehydrated in-flight processes and their corresponding definition since the process definition is stored in database repository where dehydrated instances are stored.

This section describes Disaster Recovery recommendations for the following Oracle SOA Suite components:

- Recommendations for Oracle SOA Service Infrastructure
- Recommendations for Oracle BPEL Process Manager
- Recommendations for Oracle Mediator
- Recommendations for Oracle Human Workflow
- Recommendations for Oracle B2B
- Recommendations for Oracle Web Services Manager
- Recommendations for Oracle User Messaging Service
- Recommendations for Oracle JCA Adapters
- Recommendations for Oracle Business Activity Monitoring

### 2.4.1 Recommendations for Oracle SOA Service Infrastructure

Oracle SOA Service Infrastructure is a Java EE application that provides the foundation services for running Oracle Fusion Middleware SOA Suite. This Java EE application is a run-time engine that is automatically deployed when Oracle Fusion Middleware SOA Suite is installed. You deploy composites (the basic artifacts in a Service Component Architecture) to the Oracle SOA Infrastructure and it provides the required services for the composites to run. Oracle SOA Infrastructure provides deployment, wiring, and thread management services for the composites. These services sustain the composite's lifecycle and run-time operations.

This section describes various Oracle SOA Service Infrastructure artifacts and provides recommendations for disaster recovery.

#### Artifacts in the Database

Composite definition and configuration files are stored in the MDS repository. The composite instance state persistence is stored in the SOA Service Infrastructure database.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making domain-related configuration changes, deploying composites, and applying patches.

Oracle Data Guard should be configured for the Oracle SOA Suite database and metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

The database must be recovered to the most recent point in time to ensure that the latest composite definitions and in-flight instances are restored.

## 2.4.2 Recommendations for Oracle BPEL Process Manager

The Oracle BPEL Process engine is the service engine running in SOA Service Infrastructure that allows the execution of BPEL Processes. A BPEL process provides the standard for assembling a set of discrete services into an end-to-end process flow, and developing synchronous and asynchronous services into end-to-end BPEL process flows. It provides process orchestration and storage of long running, asynchronous processes.

This section describes various Oracle BPEL Process Manager artifacts and provides recommendations for disaster recovery.

### Artifacts in the Database

Process definition and configuration files are stored in the MDS repository. The BPEL process state persistence is stored in the Oracle SOA Suite database.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making domain-related configuration changes and applying patches.

Oracle Data Guard should be configured for the Oracle SOA Suite database and metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

The database must be recovered to the most recent point in time to ensure that the latest process definitions and in-flight instances are restored. Idempotent Oracle BPEL Process Manager processes are recommended, since no cleanup is required after performing a Disaster Recovery operation. If non-idempotent processes Oracle BPEL Process Manager processes are used, then processes must be cleaned up from the dehydration store after a Disaster Recovery operation is performed, especially when a process is in flight.

### 2.4.3 Recommendations for Oracle Mediator

Oracle Mediator is a service engine within the Oracle SOA Service Infrastructure. Oracle Mediator provides the framework to mediate between various providers and consumers of services and events. The Mediator service engine runs in-place with the SOA Service Infrastructure Java EE application.

This section describes various Oracle Mediator artifacts and provides recommendations for disaster recovery.

#### Artifacts in the Database

The Mediator service engine stores messages in the database for asynchronous routing for parallel routing rules (note that sequential routing rules do not persist their messages into the database as part of the execution). The Mediator component instance state and audit details are also stored in the database.

The metadata repository stores the Mediator component definition as part of the composite definition.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making domain-related configuration changes and applying patches.

Oracle Data Guard should be configured for the Oracle SOA Suite database and metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The database must be recovered to the most recent point in time, along with the Administration Server and the Managed Server running the soa-infra application.

### 2.4.4 Recommendations for Oracle Human Workflow

Oracle Human Workflow is a service engine running in the Oracle SOA Service Infrastructure that allows the execution of interactive human-driven processes. A human workflow provides the human interaction support such as approve, reject, and reassign actions within a process or outside of any process. The Human Workflow service consists of several services that handle various aspects of human interaction with a business process.

This section describes various Oracle Human Workflow artifacts and provides recommendations for disaster recovery.

#### Artifacts in the Database

Human workflow instance data and other worklist data such as vacation rules, group rules, flex field mappings, view definitions are stored in the database.

The metadata repository is used to store shared human workflow service definitions and schemas used by SOA composites.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making domain-related configuration changes and applying patches.

Oracle Data Guard should be configured for the Oracle SOA Suite database and metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

The database must be recovered to the most recent point in time, along with the Managed Server running the soa-infra application. Oracle Human Workflow's engine uses Oracle User Messaging Service to send and receive notifications. See Section 2.4.7, "Recommendations for Oracle User Messaging Service" for details about Oracle User Messaging Service.

## 2.4.5 Recommendations for Oracle B2B

Oracle B2B connects SOA composite applications to external services, applications, and technologies. Oracle B2B offers a multi-protocol gateway that supports industry-recognized B2B standards. Oracle B2B extends Oracle SOA Suite with business protocol standards, such as electronic data interchange (EDI), ebXML, HL7, and RosettaNet. Oracle B2B is implemented as a binding component within the SOA Service Infrastructure.

This section describes various Oracle B2B artifacts and provides recommendations for disaster recovery.

### Artifacts on the File System

JMS Store: The volume containing the file-based JMS persistent store. Table 2–1 shows the JMS queues and topics used internally by Oracle B2B.

*Table 2–1 JMS Queues and Topics Used by Oracle B2B*

| JMS Artifact Name | Type | JNDI Name |
|---|---|---|
| dist_B2BEventQueue_auto | Distributed queue | jms/b2b/B2BEventQueue |
| dist_B2B_IN_QUEUE_auto | Distributed queue | jms/b2b/B2B_IN_QUEUE |
| dist_B2B_OUT_QUEUE_auto | Distributed queue | jms/b2b/B2B_OUT_QUEUE |
| dist_B2BBroadcastTopic_auto | Distributed topic | jms/b2b/B2BBroadcastTopic |

### Artifacts in the Database

Oracle B2B message and message state persistence are stored in the Oracle SOA Suite database along with the partners, documents, and channels definitions. The metadata repository is used for storing Oracle B2B metadata.

### Special Considerations

The external FTP servers and email servers should be available on the standby site if these adapters are used.

### Synchronization Recommendations

For information about Oracle B2B JMS queue synchronization and recovery, refer to Section 2.1.1, "Recommendations for Oracle WebLogic Server JMS and T-Logs."

The application tier must be manually synchronized with the standby site after making domain-related configuration changes and applying patches.

Oracle Data Guard should be configured for the Oracle SOA Suite database and metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The database must be recovered to the most recent point in time, along with the Managed Server running the soa-infra application. Oracle B2B stores state information within JMS queues and the SOA run-time database, so recovering the database and the Managed Server will ensure that the application runs normally.

### 2.4.6 Recommendations for Oracle Web Services Manager

Oracle Web Services Manager (Oracle WSM) provides a policy framework to manage and secure Web services consistently across your organization. It provides capabilities to build, enforce, execute and monitor Web Service policies including security, WSRM, MTOM and addressing policies. Oracle Web Services Manager is made up of the Policy Manager and the Agent.

The Policy Manager reads and writes security and management policies, including predefined and custom policies from the MDS repository. Policy Manager is a stateless Java EE application. It exposes its capabilities through stateless session beans. Although the Policy Manager does not cache any data, the underlying MDS infrastructure does.

The Agent is responsible for policy enforcement, execution and gathering of run-time statistics. The agent is available on all Oracle Fusion Middleware Managed Servers and is configured on the same server as the application which it protects. The agent consists of two pieces: the Policy Access Point (PAP) and the Policy Interceptor

This section describes various Oracle Web Services Manager artifacts and provides recommendations for disaster recovery.

#### Artifacts in the Database

The MDS repository is used for storing the policies.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making domain-related configuration changes and applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The database must be recovered to the most recent point in time, along with the Managed Server running the soa-infra application. All policies are stored in the MDS repository, so recovering the database and the Managed Server will ensure that the application runs normally.

### 2.4.7 Recommendations for Oracle User Messaging Service

Oracle User Messaging Service (Oracle UMS) enables two way communications between users and deployed applications. It has support for a variety of channels, such as email, IM, SMS, and text-to-voice messages. Oracle User Messaging Service is integrated with Oracle Fusion Middleware components such as Oracle BPEL PM, Oracle Human Workflow, Oracle BAM and Oracle WebCenter. It is typically deployed along with Oracle SOA Service Infrastructure. Oracle User Messaging Service is made up of UMS Server, UMS Drivers and UMS Client applications.

This section describes various Oracle User Messaging Service artifacts and provides recommendations for disaster recovery.

#### Artifacts on the File System

JMS Store: The volume containing the file based JMS persistent store. Table 2–2 shows the JMS resources used internally by Oracle User Messaging Service.

*Table 2–2 JMS Resources Used by Oracle User Messaging Service*

| JMS Artifact Name | Type | JNDI Name |
|---|---|---|
| OraSDPMAppDefRcvQ1_auto | Distributed queue | OraSDPM/Queues/OraSDPMAppDefRcvQ1 |
| OraSDPMDriverDefSndQ1_auto | Distributed queue | OraSDPM/Queues/OraSDPMDriverDefSndQ1 |
| OraSDPMEngineCmdQ_auto | Distributed queue | OraSDPM/Queues/OraSDPMEngineCmdQ |
| OraSDPMEngineRcvQ1_auto | Distributed queue | OraSDPM/Queues/OraSDPMEngineRcvQ1 |
| OraSDPMEngineSndQ1_auto | Distributed queue | OraSDPM/Queues/OraSDPMEngineSndQ1 |
| OraSDPMWSRcvQ1_auto | Distributed queue | OraSDPM/Queues/OraSDPMWSRcvQ1 |

#### Artifacts in the Database

Oracle User Messaging Service depends on an external database repository to maintain message and configuration state.

#### Special Considerations

Oracle User Messaging Service uses JMS to deliver messages among messaging applications. By default it is configured to use a file-based persistent JMS store, therefore it depends on the storage device where those files are located.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying additional Oracle User Messaging Service drivers, and applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The database must be recovered to the most recent point in time, along with the Managed Server running the usermessagingserver application. Oracle User Messaging Service maintains message and configuration state in an external database repository along with persisting messages in JMS queues, so recovering the database and the Managed Server ensures that the application functions without any issues. For recommendations on synchronizing JMS data, refer to the "Synchronization Recommendations" subsection in Section 2.1.1, "Recommendations for Oracle WebLogic Server JMS and T-Logs."

### 2.4.8 Recommendations for Oracle JCA Adapters

Oracle JCA Adapters are JCA binding components that allow the Service Infrastructure to communicate to endpoints using different protocols. Oracle JCA Adapters are deployed as a JCA resource (RAR) and are not part of the Oracle SOA Service Infrastructure.

The broad categories of Oracle JCA Adapters are:

- Oracle Technology Adapters
- Legacy Adapters
- Packaged-Application Adapters
- Oracle Adapter for Oracle Applications

See *Oracle Fusion Middleware User's Guide for Technology Adapters* for additional information about the types of Oracle JCA Adapters.

This section describes various Oracle JCA Adapter artifacts and provides recommendations for disaster recovery.

#### Artifacts on the File System

Certain adapters by their nature use local or shared-storage files, for example:

- JMS adapters utilizing WebLogic JMS with file-based persistence store: The persistence store must be synchronized with the standby site to resume processing after failover.
- Inbound and outbound files from either File or FTP adapters: The relevant files must be synchronized with the standby site to resume processing after failover.

Adapter configuration is maintained in the weblogic-ra.xml deployment descriptor for the ear JCA resource (RAR). The file location of each weblogic-ra.xml is determined by the administrator when the file is created, and must be replicated to the standby site.

#### Artifacts in the Database

Adapter artifacts are generated at design time as part of the composite project. These artifacts are stored along with the rest of the composite definition in the metadata repository.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making domain-related configuration changes (that is, adapter configuration changes) and applying patches.

Oracle Data Guard should be configured for the Oracle SOA Suite database and metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The database must be recovered to the most recent point in time, along with the Managed Server running the JCA adapters and the Administration Server.

### 2.4.9 Recommendations for Oracle Business Activity Monitoring

Oracle Business Activity Monitoring (BAM) provides the tools for monitoring business services and processes in the enterprise. It allows correlating of market indicators to the actual business process and to changing business processes quickly or taking corrective actions if the business environment changes. Oracle BAM provides the necessary tools and run-time services for creating dashboards that display real-time data inflow and define rules to send alerts under specified conditions.

This section describes various Oracle BAM artifacts and provides recommendations for disaster recovery.

#### Artifacts in the Database

Oracle BAM data and report metadata is stored in the Oracle BAM database that contains Oracle BAM schemas.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making domain-related configuration changes and applying patches.

Oracle Data Guard should be configured for the Oracle SOA Suite database containing the BAM schema and the metadata repository.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The database must be recovered to the most recent point in time, along with the Managed Server running Oracle BAM.

## 2.5 Recommendations for Oracle Identity Management

The Oracle Identity Management products enable you to configure and manage the identities of users, devices, and services across diverse servers, to delegate administration of these identities, and to provide end users with self-service privileges. These products also enable you to configure single sign-on across applications and to process users' credentials to ensure that only users with valid credentials can log into and access online resources.

#### Common Artifacts and Considerations for all Oracle Identity Management Components

The artifacts and considerations below apply to all the Oracle Identity Management components along with the component-specific considerations.

### Artifacts on the File System

MW_HOME: The Middleware home consists of a WebLogic home that has the WebLogic Server binaries and an Oracle home containing the Oracle Identity Management binaries.

Oracle_Common_Home: The Oracle home that contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).

Domain Home: The domain home contains the Administration Server and Managed Server configuration data and Identity Management applications for the domain.

Oracle Instance: The Oracle instance contains the configuration data for non-J2EE Identity Management applications like Oracle Internet Directory and Oracle Virtual Directory. It also has OPMN configuration and Enterprise Manager Agent configuration data.

### Artifacts in the Database

The Identity Management schemas are in the Identity Management database.

### Network Artifacts

Oracle recommends using the virtual host name as the listen address for both the Oracle WebLogic Administration Server and Managed Server. As long as this host name can be resolved on both the production and standby site, there is no need to update this value after a Disaster Recovery operation.

The load balancer virtual hosts used to access the Identity Management components must be configured on both the production and standby sites.

### Synchronization Recommendations

The directory tier must be manually synchronized with the standby site after making configuration changes, deploying applications, and applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

The database containing the Identity Management schemas must be recovered to the most recent point in time, along with the Identity Management component in question.

The rest of this section describes Disaster Recovery recommendations for the following Oracle Identity Management components:

- Recommendations for Oracle Internet Directory
- Recommendations for Oracle Virtual Directory
- Recommendations for Oracle Directory Integration Platform
- Recommendations for Oracle Identity Federation
- Recommendations for Oracle Directory Services Manager
- Recommendations for Oracle Access Manager

## 2.5.1 Recommendations for Oracle Internet Directory

Oracle Internet Directory is an LDAP Version 3-enabled service that enables fast retrieval and centralized management of information about dispersed users, network configuration, and other resources.

This section describes various Oracle Internet Directory artifacts and provides recommendations for disaster recovery.

### Artifacts in the Database

The ODS and ODSSM schemas used by Oracle Internet Directory are part of the Identity Management database.

### Special Considerations

The load balancer virtual hosts required for the Oracle Internet Directory should be configured on both the production and standby sites.

### Synchronization Recommendations

The directory tier must be manually synchronized with the standby site after making configuration changes and applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

Oracle Internet Directory must be recovered with the ODS and ODSSM schemas to the most recent point in time.

## 2.5.2 Recommendations for Oracle Virtual Directory

Oracle Virtual Directory is an LDAP Version 3-enabled service that provides an abstracted view of one or more enterprise data sources. Oracle Virtual Directory consolidates multiple data sources into a single directory view, enabling you to integrate LDAP-aware applications with diverse directory server data stores.

This section describes various Oracle Virtual Directory artifacts and provides recommendations for disaster recovery.

### Artifacts in the Database

Oracle Virtual Directory does not have any database dependencies.

### Special Considerations

The load balancer virtual hosts required for Oracle Virtual Directory should be configured on both the production and standby sites.

### Synchronization Recommendations

The directory tier must be manually synchronized with the standby site after making configuration changes and applying patches.

### Recovery Recommendations

Recover the Oracle Virtual Directory instance.

## 2.5.3 Recommendations for Oracle Directory Integration Platform

Oracle Directory Integration Platform is a J2EE application that enables you to synchronize data between other directories or databases and Oracle Internet Directory. Oracle Directory Integration Platform includes services and interfaces that allow you to deploy synchronization solutions with other enterprise repositories. It can also be used to provide Oracle Internet Directory interoperability with third party meta-directory solutions.

This section describes various Oracle Directory Integration Platform artifacts and provides recommendations for disaster recovery.

### Artifacts in the Database

The ODS and ODSSM schemas are part of the Identity Management database. Quartz jobs are in the ODSSM schema.

### Synchronization Recommendations

The application tier and data tier must be manually synchronized with the standby site after making configuration changes and applying patches.

### Recovery Recommendations

Oracle Internet Directory must be recovered with the ODS and ODSSM schemas to the most recent point in time, along with the Managed Server running the Oracle Directory Integration Platform application, and the associated Oracle Internet Directory instances.

## 2.5.4 Recommendations for Oracle Identity Federation

Oracle Identity Federation enables companies to provide services and share identities across their respective security domains, while providing protection from unauthorized access.

This section describes various Oracle Identity Federation artifacts and provides recommendations for disaster recovery.

### Artifacts in the Database

Oracle Identity Federation uses the OIF schema, which is part of the Identity Management database. When an RDBMS user store, configuration store, Federation store, message data store, or session store is configured for Oracle Identity Federation, an external database contains those stores.

### Special Considerations

Load balancer virtual hosts for Oracle Identity Federation should be configured on both the production and standby sites.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes and applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories and the data stores.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The databases containing the Oracle Identity Federation schemas and the data stores must be recovered to the most recent point in time, along with the Managed Server running the Oracle Identity Federation application.

### 2.5.5 Recommendations for Oracle Directory Services Manager

Oracle Directory Services Manager is a unified graphical user interface (GUI) for Oracle Virtual Directory and Oracle Internet Directory. Oracle Directory Services Manager simplifies the administration and configuration of Oracle Virtual Directory and Oracle Internet Directory by allowing you to use web-based forms and templates.

This section describes various Oracle Directory Services Manager artifacts and provides recommendations for disaster recovery.

#### Artifacts in the Database

Not applicable because the Oracle Directory Services Manager application does not have any database dependencies.

#### Special Considerations

Load balancer virtual hosts for Oracle Directory Services Manager should be configured on both the production and standby sites.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes and applying patches.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

Recover the Managed Servers running the Oracle Directory Services Manager application, along with the Administration Server.

### 2.5.6 Recommendations for Oracle Access Manager

Oracle Access Manager provides a full range of identity administration and security functions that include Web single sign-on; user self-service and self-registration; sophisticated workflow functionality; auditing and access reporting; policy management; dynamic group management; and delegated administration.

**Note:** The Disaster Recovery solution for Oracle Fusion Middleware 11*g*R1 supports Oracle Access Manager 10.1.4.3. Currently, Oracle Access Manager 10.1.4.3 is the only release of Oracle Access Manager that is supported with Oracle Fusion Middleware 11*g*R1.

This section describes various Oracle Access Manager 10.1.4.3 artifacts and provides recommendations for disaster recovery.

### Artifacts on the File System

Oracle Access Manager install directory: The Oracle Access Manager installation directory contains both configuration data and product binaries for the Oracle Access Manager products. It includes the Oracle home for the Identity Server, Access Server, Policy Manager, and WebPass. The Policy Manager and WebPass share a home with the Oracle HTTP Server instance installed on the OAMADMINHOST.

Oracle HTTP Server Oracle Home: This is the Oracle home for the Oracle HTTP Server instance that front ends the Oracle Access Manager topology.

Oracle HTTP Server Oracle Instance: The Oracle HTTP Server Oracle instance contains the configuration data for the Oracle HTTP Server instance that front ends the Oracle Access Manager topology.

WebGate install directory: The WebGate install directory contains the binaries and configuration data for Oracle WebGate.

### Artifacts in the Database

None.

### LDAP Store

Oracle Access Manager stores configuration information in an LDAP store.

### Special Considerations

Load balancer virtual hosts for Oracle Access Manager should be configured on both the production and standby sites.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes and applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories and the data stores.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

Recover the Oracle Access Manager Identity Server, Access Server, Policy Manager, and WebPass servers, along with the associated Oracle HTTP Server instances.

## 2.6 Recommendations for Oracle Portal, Forms, Reports, and Discoverer

This section describes artifacts and Disaster Recovery recommendations for the following suite of Oracle components:

- Oracle Portal
- Oracle Forms
- Oracle Reports
- Oracle Business Intelligence Discoverer (Discoverer)

### Common Artifacts and Considerations for Oracle Portal, Forms, Reports, and Discoverer

The artifacts and considerations in this section are common to Oracle Portal, Oracle Forms, Oracle Reports, and Discoverer.

#### Artifacts on the File System

MW_HOME: The Middleware home consists of a WebLogic home that has the WebLogic Server binaries and an Oracle home containing the binaries for Oracle Portal, Oracle Forms, Oracle Reports, and Discoverer.

Oracle_Common_Home: The Oracle home that contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).

Domain home: The domain home contains the Administration Server and Managed Server configuration data and the Oracle Portal, Oracle Forms, Oracle Reports, and Discoverer applications for the domain.

Oracle instance: The Oracle instance contains the configuration data for the Oracle Portal, Oracle Forms, Oracle Reports, and Discoverer components. It also contains configuration data for OPMN and the EMAgent.

#### Artifacts in the Database

Database metadata repositories containing the Oracle Portal, Oracle Reports, and Discoverer component schemas and any user-configured databases.

There is no Oracle Forms component schema in the database metadata repository (RCU), but there will likely be customer data in user-configured databases that is being accessed through Oracle Forms.

#### Network Artifacts

Oracle recommends using the virtual host name as the listen address for both the Oracle WebLogic Administration Server and Managed Server. As long as this host name can be resolved on both the production and standby site, there is no need to update this value after a Disaster Recovery operation.

The load balancer virtual hosts used to access Oracle Portal, Oracle Forms, Oracle Reports, and Discoverer must be configured on both the production and standby sites.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying applications, and applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The databases containing the Oracle Portal, Oracle Reports, and Discoverer component schemas must be recovered to the most recent point in time. The Managed Servers running the Oracle Portal, Oracle Forms, Oracle Reports, and Discoverer component applications and the Oracle instances must be restored.

The rest of this section describes Disaster Recovery recommendations for the following components:

- Recommendations for Oracle Portal
- Recommendations for Oracle Forms
- Recommendations for Oracle Reports
- Recommendations for Oracle Business Intelligence Discoverer

## 2.6.1 Recommendations for Oracle Portal

Oracle Portal offers a complete portal framework for building, deploying, and managing portals that are tightly integrated with Oracle Fusion Middleware. Oracle Portal provides a rich, declarative environment for creating a portal Web interface and accessing dynamic data with an extensible framework for Java EE-based enterprise application access.

This section describes various Oracle Portal artifacts and provides recommendations for disaster recovery.

### Artifacts in the Database

The Portal, Portal_Demo, Portal_App, Portal_Public, and Portal_Approval schemas are part of the Oracle Portal metadata repository.

### Special Considerations

Load balancer virtual hosts for accessing the portal should be configured on both the production and standby sites.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying applications, and applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

### Recovery Recommendations

The databases containing the Oracle Portal schemas must be recovered to the most recent point in time. The Managed Server running the Oracle Portal application and the Oracle instance must be restored.

## 2.6.2 Recommendations for Oracle Forms

Oracle Forms is Oracle's long-established technology to design and build enterprise applications quickly and efficiently.

This section describes artifacts that are unique to Oracle Forms and provides recommendations for disaster recovery.

### Artifacts in the Database

Any user configured databases for the Oracle Forms applications.

#### Special Considerations

Load balancer virtual hosts for accessing Oracle Forms should be configured on both the production and standby sites

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying applications, and applying patches.

Oracle Data Guard should be configured for the user configured application databases.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The Managed Server running the Oracle Forms application and the Oracle instance must be restored. If there are any user configured databases, they must be recovered to the most recent point in time.

### 2.6.3 Recommendations for Oracle Reports

Oracle Reports is the reports publishing component of Oracle Fusion Middleware. It is an enterprise reporting service for producing high quality production reports that dynamically retrieve, format, and distribute any data, in any format, anywhere. You can use Oracle Reports to publish in both Web-based and non-Web-based environments.

This section describes various Oracle Reports artifacts and provides recommendations for disaster recovery.

#### Artifacts on the File System

Reports home: This is a user defined location that contains the Report definition files. This may also be under the Oracle instance or Oracle home.

#### Artifacts in the Database

Oracle Reports can be configured to store job-related information, such as scheduled job data, past job data, or job status data in a database. This is a user-configured database.

#### Special Considerations

Load balancer virtual hosts for accessing Oracle Reports should be configured on both the production and standby sites.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes and applying patches.

If the Reports Server is configured to store configuration or user information in other components like Oracle Portal and Oracle Internet Directory, make sure to synchronize these components between the production and standby sites as well.

Oracle Data Guard should be configured for Oracle Reports databases.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The Managed Server running the Oracle Reports application and the Oracle instance must be restored. If there are any user configured databases, they must be recovered to the most recent point in time. Also recover any associated Oracle Portal and Oracle Internet Directory instances.

### 2.6.4 Recommendations for Oracle Business Intelligence Discoverer

Oracle Business Intelligence Discoverer (Discoverer) is a business intelligence tool for analyzing data. It is a key component of Oracle Fusion Middleware. Discoverer provides an integrated business intelligence solution that comprises intuitive ad-hoc query, reporting, analysis, and Web publishing functionality. These tools enable non-technical users to gain immediate access to information from data marts, data warehouses, multidimensional (OLAP) data sources, and online transaction processing systems. Discoverer integrates seamlessly with Oracle Portal and Oracle WebCenter, enabling rapid deployment of Discoverer workbooks and worksheets to Web portals.

This section describes various Discoverer artifacts and provides recommendations for disaster recovery.

#### Artifacts in the Database

The DISCOVERER and DISCOVERER_PS schemas are part of the Discoverer metadata repository.

#### Special Considerations

Load balancer virtual hosts for accessing Discoverer should be configured on both the production and standby sites.

#### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making configuration changes, deploying applications, and applying patches.

Oracle Data Guard should be configured for Oracle database metadata repositories.

It is a best practice recommendation that when the application tier synchronization is initiated on the storage, the standby database is also recovered to be up to the same point in time. This can happen by virtue of Oracle Data Guard being configured in Managed Recovery mode for the database or by explicit user initiation.

#### Recovery Recommendations

The database containing the Discoverer schemas must be restored to the most recent point in time.

The Managed Server running the Discoverer application and the Oracle instance must be restored.

# 2.7 Recommendations for Oracle Web Tier Components

The web tier of a J2EE application server is responsible for interacting with the end users, such as Web browsers primarily in the form of HTTP requests and responses. It is the outermost tier in the HTTP stack, closest to the end user.

This section describes Disaster Recovery recommendations for the following Oracle Web Tier components:

- Recommendations for Oracle HTTP Server
- Recommendations for Oracle Web Cache

## 2.7.1 Recommendations for Oracle HTTP Server

Oracle HTTP Server is the Web server component for Oracle Fusion Middleware. It provides a listener for Oracle WebLogic Server and the framework for hosting static pages, dynamic pages, and applications over the Web.

Oracle HTTP Server is based on the Apache 2.2.x infrastructure, and includes modules developed specifically by Oracle. The features of single sign-on, clustered deployment, and high availability enhance the operation of the Oracle HTTP Server.

This section describes various Oracle HTTP Server artifacts and provides recommendations for disaster recovery.

### Artifacts on the File System

Oracle Home: The Oracle home consists of the Oracle HTTP Server binaries.

Oracle_Common_Home: The Oracle home that contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).

Oracle Instance: The Oracle instance contains the configuration and diagnostic data for Oracle HTTP Server. It also contains configuration data for OPMN and the Enterprise Manager Agent.

Static Content Volume: This volume contains the static content served by the Oracle HTTP Server instance. This volume that contains static HTML content is optional; Oracle Fusion Middleware can operate normally without it.

### Artifacts in the Database

Not applicable because Oracle HTTP Server does not have any database dependencies.

### Special Considerations

These are the special considerations for Oracle HTTP Server:

- Load balancer virtual hosts for accessing the Oracle HTTP Server should be configured on both the production and standby sites.
- This manual directs you to install 11*g* Oracle Fusion Middleware instances (including Oracle HTTP Server instances) on shared storage. When an Oracle instance for Oracle HTTP Server 11*g* is configured on shared storage (for example, NAS storage, NFS storage, or SAN storage) that does not provide reliable file locking, Oracle HTTP Server may experience performance problems.

  Some shared storage systems do not provide the reliable file locking that 11*g* Oracle HTTP Server requires. In these cases, the LockFile directive in the `httpd.conf` file must be changed to point at a local file system.

See the Apache documentation at the following URL for more information about the LockFile directive:

http://httpd.apache.org/docs/2.2/mod/mpm_common.html#acceptmutex

If any 11*g* Oracle HTTP Server instance is installed on shared storage and is experiencing performance problems, perform these steps for the Oracle HTTP Server instance to point the LockFile directive at a local file system:

1. By default, the LockFile directive is in the following format, configured under both the prefork and worker MPM configuration blocks in the `httpd.conf` file:

   ```
   ${ORACLE_INSTANCE}/diagnostics/logs/${COMPONENT_TYPE}/${COMPONENT_
   NAME/http_lock
   ```

2. Edit the `$ORACLE_INSTANCE/config/OHS/<ohs_name>/httpd.conf` file using the appropriate method.
3. Change the LockFile directive under the correct MPM configuration to point to a local file system:

   ```
   LockFile /<local_disk>/<path>/http_lock
   ```

4. Restart the Oracle HTTP Server.

After performing these steps, verify that the `http_lock` file exists in the directory specified by the LockFile directive.

#### Synchronization Recommendations

The Oracle HTTP Server instance must be manually synchronized with the standby site after making configuration changes.

#### Recovery Recommendations

Restore the Oracle HTTP Server instance and related configuration files on the standby site.

### 2.7.2 Recommendations for Oracle Web Cache

Oracle Web Cache is a content-aware server accelerator, or a reverse proxy, for the Web tier. It improves the performance, scalability, and availability of Web sites that run on any Web server or application server, such as Oracle HTTP Server and Oracle WebLogic Server.

Oracle Web Cache is the primary caching mechanism provided with Oracle Fusion Middleware. Caching improves the performance, scalability, and availability of Web sites that run on Oracle Fusion Middleware by storing frequently accessed URLs in memory.

This section describes various Oracle Web Cache artifacts and provides recommendations for disaster recovery.

#### Artifacts on the File System

Oracle Home: The Oracle directory home consists of the Oracle Web Cache binaries.

Oracle_Common_Home: The Oracle home that contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).

Oracle Instance: The Oracle instance contains the configuration data for Oracle Web Cache. It also contains configuration data for OPMN and the Enterprise Manager Agent.

### Artifacts in the Database

Not applicable because Oracle Web Cache does not have any database dependencies.

### Special Considerations

Load balancer virtual hosts for accessing Oracle Web Cache should be configured on both the production and standby sites.

### Synchronization Recommendations

The Oracle Web Cache instance must be manually synchronized with the standby site after making configuration changes.

### Recovery Recommendations

Restore the Oracle Web Cache instance and related configuration files on the standby site.

# 3 Design Considerations

This chapter describes design considerations for an Oracle Fusion Middleware Disaster Recovery solution for an enterprise deployment.

It contains the following topics:

- Network Considerations
- Storage Considerations
- Database Considerations
- Starting Points
- Topology Considerations

This chapter describes detailed instructions for setting up an Oracle Fusion Middleware 11*g* Disaster Recovery production site and standby site for the Linux and UNIX operating systems. It primarily uses the Oracle SOA Suite enterprise deployment shown in Figure 3–1 in the examples of how to set up the Oracle Fusion Middleware 11*g* Disaster Recovery solution for an enterprise deployment. After you understand how to set up Disaster Recovery for the Oracle SOA Suite enterprise topology, you can use the information for other 11g enterprise deployments in this chapter to set up Disaster Recovery for those deployments as well.

**Note:** This chapter describes an Oracle Fusion Middleware 11*g* Disaster Recovery symmetric topology that uses the Oracle SOA Suite enterprise deployment shown in Figure 3–1 at *both* the production site and the standby site. Figure 3–1 shows the deployment for only one site; the high level of detail shown for this deployment precludes showing the deployment for both sites in a single figure.

Figure 1–1 shows a Disaster Recovery symmetric production site and standby site in a single figure.

***Figure 3–1 Deployment Used at Production and Standby Sites for Oracle Fusion Middleware Disaster Recovery***

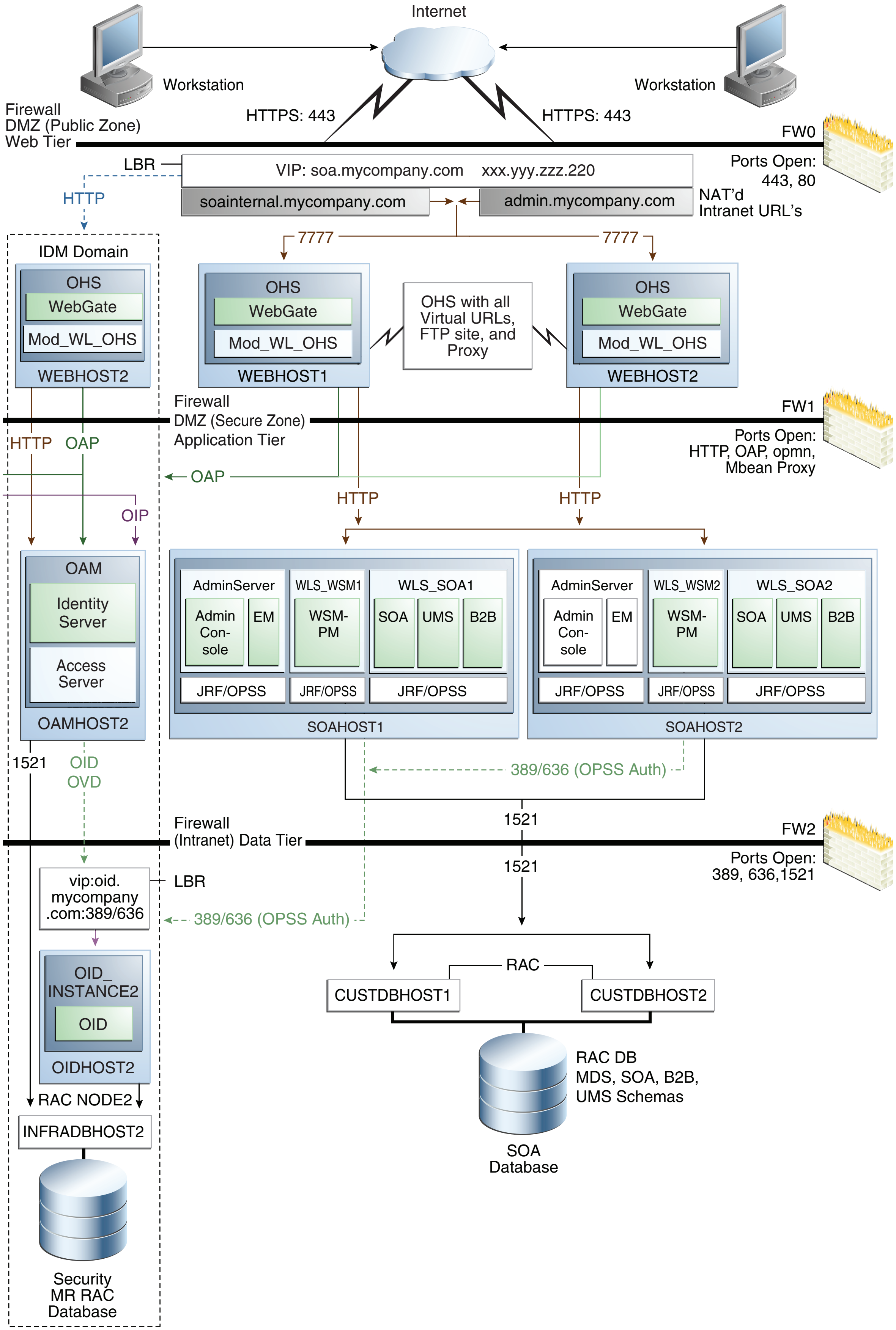

Internet
Workstation
Workstation
HTTPS: 443
HTTPS: 443
Firewall
DMZ (Public Zone)
Web Tier
FW0
Ports Open:
443, 80
LBR
VIP: soa.mycompany.com xxx.yyy.zzz.220
soainternal.mycompany.com
admin.mycompany.com
NAT'd
Intranet URL's
HTTP
7777
7777
IDM Domain
OHS
WebGate
Mod_WL_OHS
WEBHOST2
OHS
WebGate
Mod_WL_OHS
WEBHOST1
OHS with all Virtual URLs, FTP site, and Proxy
OHS
WebGate
Mod_WL_OHS
WEBHOST2
Firewall
DMZ (Secure Zone)
Application Tier
FW1
Ports Open:
HTTP, OAP, opmn,
Mbean Proxy
HTTP
OAP
OAP
OIP
HTTP
HTTP
OAM
Identity Server
Access Server
OAMHOST2
AdminServer
Admin Con-sole
EM
WLS_WSM1
WSM-PM
WLS_SOA1
SOA
UMS
B2B
JRF/OPSS
JRF/OPSS
JRF/OPSS
SOAHOST1
AdminServer
Admin Con-sole
EM
WLS_WSM2
WSM-PM
WLS_SOA2
SOA
UMS
B2B
JRF/OPSS
JRF/OPSS
JRF/OPSS
SOAHOST2
1521
OID
OVD
389/636 (OPSS Auth)
1521
Firewall
(Intranet) Data Tier
FW2
Ports Open:
389, 636,1521
1521
vip:oid.
mycompany
.com:389/636
LBR
389/636 (OPSS Auth)
OID_
INSTANCE2
OID
OIDHOST2
RAC NODE2
INFRADBHOST2
Security
MR RAC
Database
RAC
CUSTDBHOST1
CUSTDBHOST2
RAC DB
MDS, SOA, B2B,
UMS Schemas
SOA
Database

Figure 3–1 shows the mySOACompany with Oracle Access Manager enterprise deployment from the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*. See the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite* for detailed information on installing and configuring this Oracle SOA Suite enterprise deployment.

The Oracle Fusion Middleware Disaster Recovery topology that you design must be symmetric for the following at the production site and standby site.

- Directory names and paths

  Every file that exists at a production site host must exist in the same directory and path at the standby site peer host.

  Thus, Oracle home names and directory paths must be the same at the production site and standby site.

- Port numbers

  Port numbers are used by listeners and for the routing of requests. Port numbers are stored in the configuration and have to be the same at the production site hosts and their standby site peer hosts.

  Section 3.4.1, "Starting with an Existing Site" describes how to check for port conflicts between production site and standby site hosts.

- Security

  The same user accounts must exist at both the production site and standby site. Also, the file system, SSL, and Single Sign-On must be configured identically at the production site and standby site. For example, if the production site uses SSL, the standby site must also use SSL that is configured in exactly the same way as the production site.

- Load balancers and virtual server names

  A front-end load balancer should be set up with virtual server names for the production site, and an identical front-end load balancer should be set up with the same virtual server names for the standby site.

- Software

  The same versions of software must be used on the production site and standby site. Also, the operating system patch level must be the same at both sites, and patches to Oracle or third party software must be made to both the production site and standby site.

## 3.1 Network Considerations

This section describes the following network considerations:

- Planning Host Names
- Load Balancers and Virtual IP Considerations
- Wide Area DNS Operations

### 3.1.1 Planning Host Names

In a Disaster Recovery topology, the production site host names must be resolvable to the IP addresses of the corresponding peer systems at the standby site. Therefore, it is important to plan the host names for the production site and standby site.

This section describes how to plan physical host names and alias host names for the middle tier hosts that use the Oracle Fusion Middleware instances at the production site and standby site. It uses the Oracle SOA Suite enterprise deployment shown in Figure 3–1 for the host name examples. The host name examples in this section assume that a symmetric Disaster Recovery site is being set up, where the production site and standby site have the same number of hosts. Each host at the production site and standby site has a peer host at the other site. The peer hosts are configured the same, for example, using the same ports as their counterparts at the other site.

When configuring each component, use hostname-based configuration instead of IP-based configuration, unless the component requires you to use IP-based configuration. For example, if you are configuring the listen address of an Oracle Fusion Middleware component to a specific IP address such as 123.1.2.113, use the host name SOAHOST1.MYCOMPANY.COM, which resolves to 123.1.2.113.

The following subsections show how to set up host names at the Disaster Recovery production site and standby site for several enterprise deployments.

> **Note:** In this book's examples, IP addresses for hosts at the initial production site have the format 123.1.x.x and IP addresses for hosts at the initial standby site have the format 123.2.x.x.

### Host Names for the Oracle SOA Suite Production Site and Standby Site Hosts

Table 3–1 shows the IP addresses and physical host names that will be used for the Oracle SOA Suite EDG deployment production site hosts. Figure 3–1 shows the configuration for the Oracle SOA Suite EDG deployment at the production site.

***Table 3–1 IP Addresses and Physical Host Names for SOA Suite Production Site Hosts***

| IP Address | Physical Host Name[1] | Alias Host Name |
|---|---|---|
| 123.1.2.111 | WEBHOST1 | None |
| 123.1.2.112 | WEBHOST2 | None |
| 123.1.2.113 | SOAHOST1 | None |
| 123.1.2.114 | SOAHOST2 | None |

[1] See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" and Section 3.1.1.4, "Resolving Host Names Using a Global DNS Server" for information on defining physical host names.

Table 3–2 shows the IP addresses, physical host names, and alias host names that will be used for the Oracle SOA Suite EDG deployment standby site hosts. Figure 3–2 shows the physical host names used for the Oracle SOA Suite EDG deployment at the standby site. The alias host names shown in Table 3–2 should be defined for the SOA Oracle Suite standby site hosts in Figure 3–2.

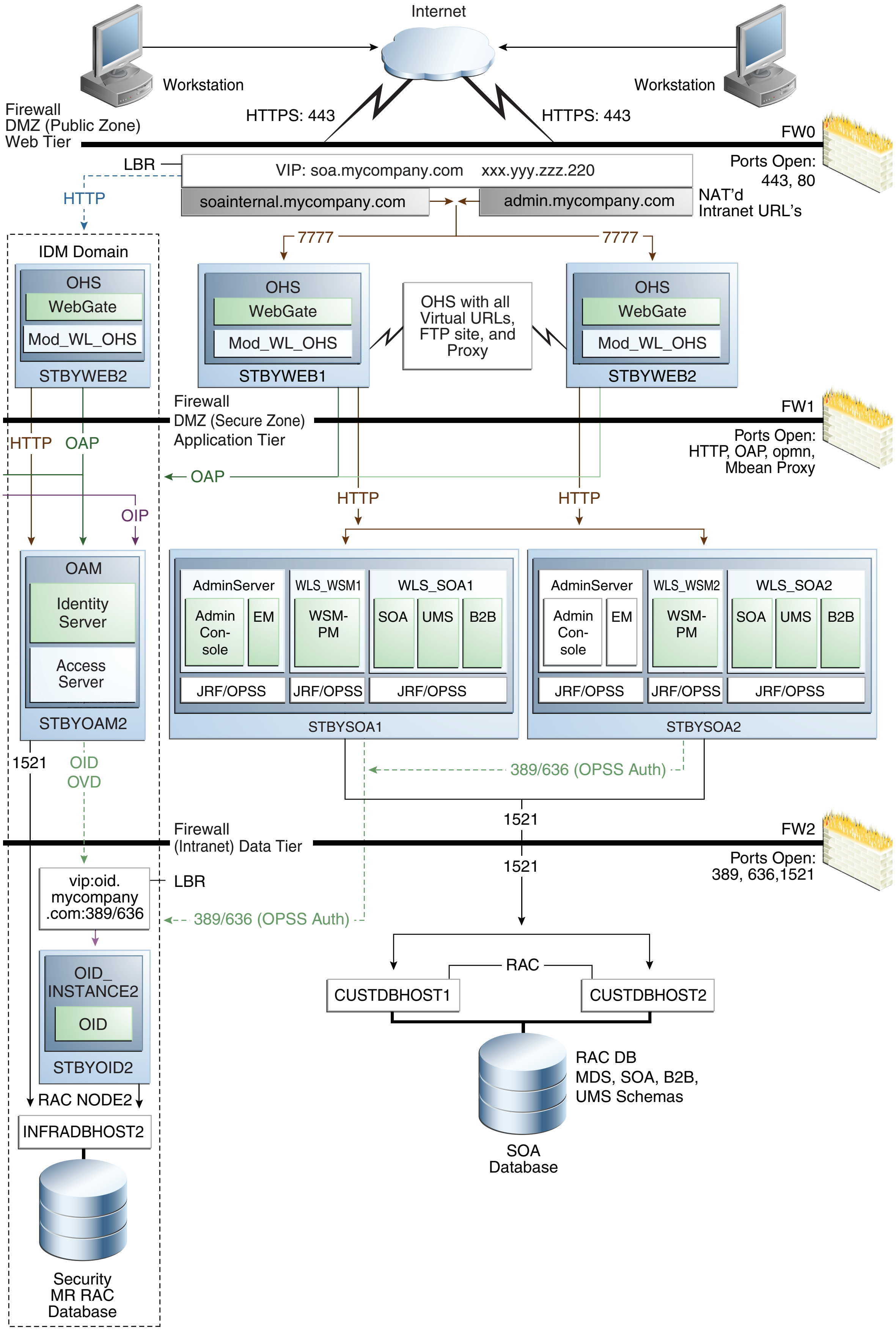
> **Note:** If you use separate DNS servers to resolve host names, then you can use the same physical host names for the production site hosts and standby site hosts, and you do not need to define the alias host names on the standby site hosts that are recommended in Table 3–2. See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" for more information about using separate DNS servers to resolve host names.

*Table 3–2 IP Addresses, Physical Host Names, and Alias Host Names for SOA Suite Standby Site Hosts*

| IP Address | Physical Host Name[1] | Alias Host Name |
|---|---|---|
| 123.2.2.111 | STBYWEB1 | WEBHOST1 |
| 123.2.2.112 | STBYWEB2 | WEBHOST2 |
| 123.2.2.113 | STBYSOA1 | SOAHOST1 |
| 123.2.2.114 | STBYSOA2 | SOAHOST2 |

[1] See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" and Section 3.1.1.4, "Resolving Host Names Using a Global DNS Server" for information on defining physical host names.

*Figure 3–2 Physical Host Names Used at Oracle SOA Suite Deployment Standby Site*


Internet
Workstation
Workstation
HTTPS: 443
HTTPS: 443
Firewall
DMZ (Public Zone)
Web Tier
FW0
Ports Open:
443, 80
LBR
VIP: soa.mycompany.com xxx.yyy.zzz.220
soainternal.mycompany.com
admin.mycompany.com
NAT'd
Intranet URL's
HTTP
7777
7777
IDM Domain
OHS
WebGate
Mod_WL_OHS
STBYWEB2
OHS
WebGate
Mod_WL_OHS
STBYWEB1
OHS with all Virtual URLs, FTP site, and Proxy
OHS
WebGate
Mod_WL_OHS
STBYWEB2
Firewall
DMZ (Secure Zone)
Application Tier
FW1
Ports Open:
HTTP, OAP, opmn,
Mbean Proxy
HTTP
OAP
OAP
OIP
HTTP
HTTP
OAM
Identity Server
Access Server
STBYOAM2
AdminServer
Admin Con- sole
EM
WLS_WSM1
WSM-PM
WLS_SOA1
SOA
UMS
B2B
JRF/OPSS
JRF/OPSS
JRF/OPSS
STBYSOA1
AdminServer
Admin Con- sole
EM
WLS_WSM2
WSM-PM
WLS_SOA2
SOA
UMS
B2B
JRF/OPSS
JRF/OPSS
JRF/OPSS
STBYSOA2
1521
OID
OVD
389/636 (OPSS Auth)
1521
Firewall
(Intranet) Data Tier
FW2
Ports Open:
389, 636,1521
1521
vip:oid.
mycompany
.com:389/636
LBR
389/636 (OPSS Auth)
OID_
INSTANCE2
OID
STBYOID2
RAC
CUSTDBHOST1
CUSTDBHOST2
RAC NODE2
INFRADBHOST2
RAC DB
MDS, SOA, B2B,
UMS Schemas
SOA
Database
Security
MR RAC
Database

### Host Names for the Oracle WebCenter Production Site and Standby Site Hosts

Table 3–3 shows the IP addresses and physical host names that will be used for the Oracle WebCenter EDG deployment production site hosts. Figure 4–3 shows the configuration for the Oracle WebCenter EDG deployment at the production site.

*Table 3–3 IP Addresses and Physical Host Names for WebCenter Production Site Hosts*

| IP Address | Physical Host Name[1] | Alias Host Name |
|---|---|---|
| 123.1.2.111 | WEBHOST1 | None |
| 123.1.2.112 | WEBHOST2 | None |
| 123.1.2.113 | SOAHOST1 | None |
| 123.1.2.114 | SOAHOST2 | None |
| 123.1.2.115 | WCHOST1 | None |
| 123.1.2.116 | WCHOST2 | None |

[1] See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" and Section 3.1.1.4, "Resolving Host Names Using a Global DNS Server" for information on defining physical host names.

Table 3–4 shows the IP addresses, physical host names, and alias host names that will be used for the Oracle WebCenter EDG deployment standby site hosts. Figure 4–3 shows the configuration for the Oracle WebCenter EDG deployment at the standby site.

> **Note:** If you use separate DNS servers to resolve host names, then you can use the same physical host names for the production site hosts and standby site hosts, and you do not need to define the alias host names on the standby site hosts that are recommended in Table 3–4. See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" for more information about using separate DNS servers to resolve host names.

*Table 3–4 IP Addresses, Physical Host Names, and Alias Host Names for WebCenter Standby Site Hosts*

| IP Address | Physical Host Name[1] | Alias Host Name |
|---|---|---|
| 123.2.2.111 | STBYWEB1 | WEBHOST1 |
| 123.2.2.112 | STBYWEB2 | WEBHOST2 |
| 123.2.2.113 | STBYSOA1 | SOAHOST1 |
| 123.2.2.114 | STBYSOA2 | SOAHOST2 |
| 123.2.2.115 | STBYWC1 | WCHOST1 |
| 123.2.2.116 | STBYWC2 | WCHOST2 |

[1] See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" and Section 3.1.1.4, "Resolving Host Names Using a Global DNS Server" for information on defining physical host names.

### Host Names for the Oracle Identity Management Production Site and Standby Site Hosts

Table 3–5 shows the IP addresses and physical host names that will be used for the Oracle Identity Management EDG deployment production site hosts. Figure 4–5 shows the configuration for the Oracle Identity Management EDG deployment at the production site.

***Table 3–5 IP Addresses and Physical Host Names for Identity Management Production Site Hosts***

| IP Address | Physical Host Name[1] | Alias Host Name |
|---|---|---|
| 123.1.2.111 | WEBHOST1 | None |
| 123.1.2.112 | WEBHOST2 | None |
| 123.1.2.117 | OAMADMINHOST | None |
| 123.1.2.118 | IDMHOST1 | None |
| 123.1.2.119 | IDMHOST2 | None |
| 123.1.2.120 | OAMHOST1 | None |
| 123.1.2.121 | OAMHOST2 | None |
| 123.1.2.122 | OIDHOST1 | None |
| 123.1.2.123 | OIDHOST2 | None |
| 123.1.2.124 | OVDHOST1 | None |
| 123.1.2.125 | OVDHOST2 | None |

[1] See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" and Section 3.1.1.4, "Resolving Host Names Using a Global DNS Server" for information on defining physical host names.

Table 3–6 shows the IP addresses, physical host names, and alias host names that will be used for the Oracle Identity Management EDG deployment standby site hosts. Figure 4–5 shows the configuration for the Oracle Identity Management EDG deployment at the standby site.

> **Note:** If you use separate DNS servers to resolve host names, then you can use the same physical host names for the production site hosts and standby site hosts, and you do not need to define the alias host names on the standby site hosts that are recommended in Table 3–6. See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" for more information about using separate DNS servers to resolve host names.

***Table 3–6 IP Addresses, Physical Host Names, and Alias Host Names for Identity Management Standby Site Hosts***

| IP Address | Physical Host Name[1] | Alias Host Name |
|---|---|---|
| 123.2.2.111 | STBYWEB1 | WEBHOST1 |
| 123.2.2.112 | STBYWEB2 | WEBHOST2 |
| 123.2.2.117 | STBYADM | OAMADMINHOST |
| 123.2.2.118 | STBYIDM1 | IDMHOST1 |
| 123.2.2.119 | STBYIDM2 | IDMHOST2 |
| 123.2.2.120 | STBYOAM1 | OAMHOST1 |
| 123.2.2.121 | STBYOAM2 | OAMHOST2 |
| 123.2.2.122 | STBYOID1 | OIDHOST1 |

*Table 3–6 (Cont.) IP Addresses, Physical Host Names, and Alias Host Names for Identity Management Standby Site Hosts*

| IP Address | Physical Host Name[1] | Alias Host Name |
|---|---|---|
| 123.2.2.123 | STBYOID2 | OIDHOST2 |
| 123.2.2.124 | STBYOVD1 | OVDHOST1 |
| 123.2.2.125 | STBYOVD2 | OVDHOST2 |

[1] See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" and Section 3.1.1.4, "Resolving Host Names Using a Global DNS Server" for information on defining physical host names.

### Host Names for the Oracle Portal, Forms, Reports, and Discoverer Production Site and Standby Site Hosts

Table 3–7 shows the IP addresses and physical host names that will be used for the Oracle Portal, Forms, Reports, and Discoverer enterprise deployment production site hosts. Figure 4–6 shows the configuration for the Oracle Portal enterprise deployment at the production site and Figure 4–7 shows the configuration for the Oracle Forms, Reports, and Discoverer enterprise deployment at the production site.

*Table 3–7 IP Addresses and Physical Host Names for Oracle Portal, Forms, Reports, and Discoverer Production Site Hosts*

| IP Address | Physical Host Names[1] | Alias Host Names |
|---|---|---|
| 123.1.2.111 | WEBHOST1 | None |
| 123.1.2.112 | WEBHOST2 | None |
| 123.1.2.126 | APPHOST1 | None |
| 123.1.2.127 | APPHOST2 | None |

[1] See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" and Section 3.1.1.4, "Resolving Host Names Using a Global DNS Server" for information on defining physical host names.

Table 3–8 shows the IP addresses, physical host names, and alias host names that will be used for the Oracle Portal, Forms, Reports, and Discoverer enterprise deployment standby site hosts. Figure 4–6 shows the configuration for the Oracle Portal enterprise deployment at the production site and Figure 4–7 shows the configuration for the Oracle Forms, Reports, and Discoverer enterprise deployment at the production site.

**Note:** If you use separate DNS servers to resolve host names, then you can use the same physical host names for the production site hosts and standby site hosts, and you do not need to define the alias host names on the standby site hosts that are recommended in Table 3–8. See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" for more information about using separate DNS servers to resolve host names.

*Table 3–8 IP Addresses, Physical Host Names, and Alias Host Names for Oracle Portal, Forms, Reports, and Discoverer Standby Site Hosts*

| IP Address | Physical Host Name[1] | Alias Host Name |
|---|---|---|
| 123.2.2.111 | STBYWEB1 | WEBHOST1 |

*Table 3–8 (Cont.) IP Addresses, Physical Host Names, and Alias Host Names for Oracle Portal, Forms, Reports, and Discoverer Standby Site Hosts*

| IP Address | Physical Host Name[1] | Alias Host Name |
|---|---|---|
| 123.2.2.112 | STBYWEB2 | WEBHOST1 |
| 123.2.2.126 | STBYAPP1 | APPHOST1 |
| 123.2.2.127 | STBYAPP2 | APPHOST2 |

[1] See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" and Section 3.1.1.4, "Resolving Host Names Using a Global DNS Server" for information on defining physical host names.

The alias host names in Table 3–2, Table 3–4, Table 3–6, and Table 3–7 are resolved locally at the standby site to the correct IP address. Section 3.1.1.1, "Host Name Resolution" describes two ways to configure host name resolution in an Oracle Fusion Middleware Disaster Recovery topology.

### 3.1.1.1 Host Name Resolution

Host name resolution is the process of resolving a host name to the proper IP address for communication. Host name resolution can be configured in one of the following ways:

- Resolving host names locally

  Local host name resolution uses the host name to IP address mapping that is specified by the `/etc/hosts` file on each host.

  See Section 3.1.1.2, "Resolving Host Names Locally" for more information about using the `/etc/hosts` file to implement local host name file resolution.

- Resolving host names using DNS

  A DNS Server is a dedicated server or a service that provides DNS name resolution in an IP network.

  See Section 3.1.1.3, "Resolving Host Names Using Separate DNS Servers" and Section 3.1.1.4, "Resolving Host Names Using a Global DNS Server" for more information about two methods of implementing DNS server host name resolution.

You must determine the method of host name resolution you will use for your Oracle Fusion Middleware Disaster Recovery topology when you are planning the deployment of the topology. Most site administrators use a combination of these resolution methods in a precedence order to manage host names.

The Oracle Fusion Middleware hosts and the shared storage system for each site must be able to communicate with each other.

#### Host Name Resolution Precedence

To determine the host name resolution method used by a particular host, search for the value of the `hosts` parameter in the `/etc/nsswitch.conf` file on the host.

As shown in Example 3–1, make the `files` entry the first entry for the `hosts` parameter if you want to resolve host  names locally on the host. When `files` is the first entry for the `hosts` parameter, entries in the host's `/etc/hosts` file will be used first to resolve host names:

***Example 3–1 Specifying the Use of Local Host Name Resolution***

```
hosts:   files   dns   nis
```

As shown in Example 3–2, make the `dns` entry the first entry for the `hosts` parameter if you want to resolve host names using DNS on the host. When `dns` is the first entry for the `hosts` parameter, DNS server entries will be used first to resolve host names:

***Example 3–2 Specifying the Use of DNS Host Name Resolution***

```
hosts:   dns    files   nis
```

For simplicity and consistency, it is recommended that all the hosts within a site (production site or standby site) use the same host name resolution method (resolving host names locally or resolving host names using separate DNS servers or a global DNS server).

The recommendations in the following sections are high-level recommendations that you can adapt to meet the host name resolution standards used by your enterprise.

#### 3.1.1.2 Resolving Host Names Locally

Local host name resolution uses the host name to IP mapping defined in the `/etc/hosts` file of a host. When you use this method to resolve host names for your Disaster Recovery topology, the following guidelines apply:

1. Ensure that the `hosts` parameter in the `/etc/nsswitch.conf` file on all the production site and standby site hosts looks like this:

   ```
   hosts:   files   dns   nis
   ```

2. The `/etc/hosts` file entries on the hosts of the production site should have their physical host names mapped to their IP addresses. For the sake of simplicity and ease of maintenance, it is recommended to have the same entries on all the hosts of the production site. Example 3–3 shows the `/etc/hosts` file for the production site of a SOA Enterprise Deployment topology:

***Example 3–3 Making /etc/hosts File Entries for a Production Site Host***

```
127.0.0.1      localhost.localdomain    localhost
123.1.2.111    WEBHOST1.MYCOMPANY.COM    WEBHOST1
123.1.2.112    WEBHOST2.MYCOMPANY.COM    WEBHOST2
123.1.2.113    SOAHOST1.MYCOMPANY.COM    SOAHOST1
123.1.2.114    SOAHOST2.MYCOMPANY.COM    SOAHOST2
```

3. The `/etc/hosts` file entries on the hosts of the standby site should have their physical host names mapped to their IP addresses along with the physical host names of their corresponding peer on the production site defined as the alias host names. For the sake of simplicity and ease of maintenance, it is recommended to have the same entries on all the hosts of the standby site. Example 3–4 shows the `/etc/hosts` file for the production site of a SOA Enterprise Deployment topology:

***Example 3–4 Making /etc/hosts File Entries for a Standby Site Host***

```
127.0.0.1      localhost.localdomain    localhost
123.2.2.111    STBYWEB1.MYCOMPANY.COM    WEBHOST1
123.2.2.112    STBYWEB2.MYCOMPANY.COM    WEBHOST2
123.2.2.113    STBYSOA1.MYCOMPANY.COM    SOAHOST1
123.2.2.114    STBYSOA2.MYCOMPANY.COM    SOAHOST2
```

4. After setting up host name resolution using `/etc/host` file entries, use the `ping` command to test host name resolution. For a system configured with static IP addressing and the `/etc/hosts` file entries shown in Example 3–3, a `ping webhost1` command on the production site would return the correct IP address (123.1.2.111) and also indicate that the host name is fully qualified.

5. Similarly, for a system configured with static IP addressing and the `/etc/hosts` file entries shown in Example 3–4, a `ping webhost1` command on the standby site will return the correct IP address (123.2.2.111) and it will also show that the name WEBHOST1 is also associated with that IP address.

#### 3.1.1.3 Resolving Host Names Using Separate DNS Servers

This manual uses the term "separate DNS servers" to refer to a Disaster Recovery topology where the production site and the standby site have their own DNS servers. When you use separate DNS servers to resolve host names for your Disaster Recovery topology, the following guidelines apply:

1. Ensure that the `hosts` parameter in the `/etc/nsswitch.conf` file on all the production site and standby site hosts looks like this:

   ```
   hosts:   dns   files   nis
   ```

2. The DNS servers on the production site and standby site must not be aware of each other and must contain entries for host names used within their own site.

3. The DNS server entries on the production site should have the physical host names mapped to their IP addresses. Example 3–5 shows the DNS server entries for the production site of a SOA Enterprise Deployment topology:

***Example 3–5 DNS Entries for a Production Site Host in a Separate DNS Servers Configuration***

```
WEBHOST1.MYCOMPANY.COM    IN    A    123.1.2.111
WEBHOST2.MYCOMPANY.COM    IN    A    123.1.2.112
SOAHOST1.MYCOMPANY.COM    IN    A    123.1.2.113
SOAHOST2.MYCOMPANY.COM    IN    A    123.1.2.114
```

4. The DNS server entries on the standby site should have the physical host names of the production site mapped to their IP addresses. Example 3–6 shows the DNS server entries for the standby site of a SOA Enterprise Deployment topology:

***Example 3–6 DNS Entries for a Standby Site Host in a Separate DNS Servers Configuration***

```
WEBHOST1.MYCOMPANY.COM    IN    A    123.2.2.111
WEBHOST2.MYCOMPANY.COM    IN    A    123.2.2.112
SOAHOST1.MYCOMPANY.COM    IN    A    123.2.2.113
SOAHOST2.MYCOMPANY.COM    IN    A    123.2.2.114
```

5. Make sure there are no entries in the `/etc/hosts` file for any host at the production site or standby site.

6. Test the host name resolution using the `ping` command. For a system configured with the production site DNS entries shown in Example 3–5, a `ping webhost1` command on the production site would return the correct IP address (123.1.2.111) and also indicate that the host name is fully qualified.

7. Similarly, for a system configured with the standby site DNS entries shown in Example 3–6, a `ping webhost1` command on the standby site will return the

correct IP address (123.2.2.111) and it will also indicate that the host name is fully qualified.

#### 3.1.1.4 Resolving Host Names Using a Global DNS Server

This manual uses the term "global DNS server" to refer to a Disaster Recovery topology where a single DNS server is used for both the production site and the standby site. When you use a global DNS server to resolve host names for your Disaster Recovery topology, the following guidelines apply:

1. When using a global DNS server, for the sake of simplicity, a combination of local host name resolution and DNS host name resolution is recommended.
2. In this example, it is assumed that the production site uses DNS host name resolution and the standby site uses local host name resolution.
3. The global DNS server should have the entries for both the production and standby site hosts. Example 3–7 shows the entries for a SOA Enterprise Deployment topology:

***Example 3–7 DNS Entries for Production Site and Standby Site Hosts When Using a Global DNS Server Configuration***

```
WEBHOST1.MYCOMPANY.COM    IN    A    123.1.2.111
WEBHOST2.MYCOMPANY.COM    IN    A    123.1.2.112
SOAHOST1.MYCOMPANY.COM    IN    A    123.1.2.113
SOAHOST2.MYCOMPANY.COM    IN    A    123.1.2.114
STBYWEB1.MYCOMPANY.COM    IN    A    123.2.2.111
STBYWEB2.MYCOMPANY.COM    IN    A    123.2.2.112
STBYSOA1.MYCOMPANY.COM    IN    A    123.2.2.113
STBYSOA2.MYCOMPANY.COM    IN    A    123.2.2.114
```

4. Ensure that the `hosts` parameter in the `/etc/nsswitch.conf` file on all the production site hosts looks like this:

   ```
   hosts:   dns   files   nis
   ```

5. Ensure that the `hosts` parameter in the `/etc/nsswitch.conf` file on all the standby site hosts looks like this:

   ```
   hosts:   files   dns   nis
   ```

6. The `/etc/hosts` file entries on the hosts of the standby site should have their physical host names mapped to their IP addresses along with the physical host names of their corresponding peer on the production site defined as the alias host names. For the sake of simplicity and ease of maintenance, it is recommended to have the same entries on all the hosts of the standby site. Example 3–8 shows the `/etc/hosts` file for the production site of a SOA Enterprise Deployment topology:

***Example 3–8 Standby Site /etc/hosts File Entries When Using a Global DNS Server Configuration***

```
127.0.0.1      localhost.localdomain    localhost
123.2.2.111    STBYWEB1.MYCOMPANY.COM    WEBHOST1
123.2.2.112    STBYWEB2.MYCOMPANY.COM    WEBHOST2
123.2.2.113    STBYSOA1.MYCOMPANY.COM    SOAHOST1
123.2.2.114    STBYSOA2.MYCOMPANY.COM    SOAHOST2
```

7. Test the host name resolution using the `ping` command. A `ping webhost1` command on the production site would return the correct IP address (123.1.2.111) and also indicate that the host name is fully qualified.
8. Similarly, a `ping webhost1` command on the standby site would return the correct IP address (123.2.2.111) and also indicate that the host name is fully qualified.

#### 3.1.1.5 Testing the Host Name Resolution

Validate that you have assigned host names properly by connecting to each host at the production site and using the `ping` command to ensure that the host can locate the other hosts at the production site.

Then, connect to each host at the standby site and use the `ping` command to ensure that the host can locate the other hosts at the standby site.

### 3.1.2 Load Balancers and Virtual IP Considerations

Oracle Fusion Middleware components require a hardware load balancer when deployed in high availability topologies. It is recommended that the hardware load balancer have the following features:

1. 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.
2. Port translation configuration.
3. Monitoring of ports (HTTP and HTTPS).
4. Virtual servers and port configuration: Ability to configure virtual server names and ports on your external load balancer, and the virtual server names and ports must meet 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 more than one port. For example, for Oracle Internet Directory clusters, the load balancer must be configured with a virtual server and ports for LDAP and LDAPS traffic.
   - The virtual server names must be associated with IP addresses and be part of your DNS. Clients must be able to access the load balancer through the virtual server names.
5. Ability to detect node failures and immediately stop routing traffic to the failed node.
6. Resource monitoring, port monitoring, and process failure detection: The load balancer must be able to detect service and node failures (through notification or some other means) and stop directing non-Oracle Net traffic to the failed node. If your load balancer can automatically detect failures, you should use this feature.
7. Fault-tolerant mode: It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
8. Other: 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 system.

9. Sticky routing capability: Ability to maintain sticky connections to components based on cookies or URL.
10. SSL acceleration: This feature is recommended, but not required.
11. For the Identity Management configuration with Oracle Access Manager, configure the load balancer in the directory tier with higher timeout numbers (such as 59 minutes).

    Oracle Access Manager uses persistent LDAP connections for better performance and does not support using load balancers between the servers and directory servers as they tend to disrupt these persistent LDAP connections.

The virtual servers and associated ports must be configured on the load balancer for different types of network traffic and monitoring. These should be configured to the appropriate real hosts and ports for the services running. Also, the load balancer should be configured to monitor the real host and ports for availability so that the traffic to these is stopped as soon as possible when a service is down. This will ensure that incoming traffic on a given virtual host is not directed to an unavailable service in the other tiers.

It is recommended to use two load balancers when dealing with external and internal traffic. In such a topology, one load balancer is set up for external HTTP traffic and the other load balancer is set up for internal LDAP traffic. A deployment may choose to have a single load balancer device due to a variety of reasons. While this is supported, the deployment should consider the security implications of doing this and if found appropriate, open up the relevant firewall ports to allow traffic across the various DMZs. It is worth noting that in either case, it is highly recommended to deploy a given load balancer device in fault tolerant mode. The virtual servers required for the various Oracle Fusion Middleware products are described in the following tables.

***Table 3–9 Virtual Servers for Oracle SOA Suite***

| Components | Access | Virtual Server Name |
|---|---|---|
| Oracle SOA | External | soa.mycompany.com |
| Oracle SOA | Internal | soainternal.mycompany.com |
| Administration Consoles | Internal | admin.mycompany.com |

***Table 3–10 Virtual Servers for Oracle WebCenter***

| Components | Access | Virtual Server Name |
|---|---|---|
| Oracle WebCenter | External | wc.mycompany.com |
| Oracle WebCenter | Internal | wcinternal.mycompany.com |
| Oracle SOA Internal | Internal | soainternal.mycompany.com[1] |
| Administration Consoles | Internal | admin.mycompany.com |

[1] Required when extending with SOA domain.

***Table 3–11 Virtual Servers for Oracle Identity Management***

| Components | Virtual Server Name |
|---|---|
| Oracle Internet Directory | oid.mycompany.com |
| Oracle Virtual Directory | ovd.mycompany.com |
| Oracle Identity Federation | oif.mycompany.com |

*Table 3–11 (Cont.) Virtual Servers for Oracle Identity Management*

| Components | Virtual Server Name |
|---|---|
| Single Sign-On | sso.mycompany.com |
| Administration Consoles | admin.mycompany.com |

*Table 3–12 Virtual Servers for Oracle Portal, Forms, Reports, and Discoverer*

| Components | Virtual Server Name |
|---|---|
| Oracle Portal | portal.mycompany.com |
| Oracle Forms and Oracle Reports | forms.mycompany.com |
| Discoverer | disco.mycompany.com |
| Administration Consoles | admin.mycompany.com |

## 3.1.3 Wide Area DNS Operations

When a site switchover or failover is performed, client requests must be redirected transparently to the new site that is playing the production role. To direct client requests to the entry point of a production site, use DNS resolution. To accomplish this redirection, the wide area DNS that resolves requests to the production site has to be switched over to the standby site. The DNS switchover can be accomplished by either using a global load balancer or manually changing DNS names.

> **Note:** A hardware load balancer is assumed to be front-ending each site. Check for supported load balancers at:
>
> `http://support.oracle.com`

The following topics are described in this section:

- Using a Global Load Balancer
- Manually Changing DNS Names

### 3.1.3.1 Using a Global Load Balancer

When a global load balancer is deployed in front of the production and standby sites, it provides fault detection services and performance-based routing redirection for the two sites. Additionally, the load balancer can provide authoritative DNS name server equivalent capabilities.

During normal operations, the global load balancer can be configured with the production site's load balancer name-to-IP mapping. When a DNS switchover is required, this mapping in the global load balancer is changed to map to the standby site's load balancer IP. This allows requests to be directed to the standby site, which now has the production role.

This method of DNS switchover works for both site switchover and failover. One advantage of using a global load balancer is that the time for a new name-to-IP mapping to take effect can be almost immediate. The downside is that an additional investment must be made for the global load balancer.

#### 3.1.3.2 Manually Changing DNS Names

This method of DNS switchover involves the manual change of the name-to-IP mapping that is originally mapped to the IP address of the production site's load balancer. The mapping is changed to map to the IP address of the standby site's load balancer. Follow these instructions to perform the switchover:

1. Make a note of the current Time to Live (TTL) value of the production site's load balancer mapping. This mapping is in the DNS cache and it will remain there until the TTL expires. As an example, let's assume that the TTL is 3600 seconds.
2. Modify the TTL value to a short interval (for example, 60 seconds).
3. Wait one interval of the original TTL. This is the original TTL of 3600 seconds from Step 1.
4. Ensure that the standby site is switched over to receive requests.
5. Modify the DNS mapping to resolve to the standby site's load balancer, giving it the appropriate TTL value for normal operation (for example, 3600 seconds).

This method of DNS switchover works for switchover or failover operations. The TTL value set in Step 2 should be a reasonable time period where client requests cannot be fulfilled. The modification of the TTL is effectively modifying the caching semantics of the address resolution from a long period of time to a short period. Due to the shortened caching period, an increase in DNS requests can be observed.

## 3.2 Storage Considerations

This section provides recommendations for designing storage for the Disaster Recovery solution for your enterprise deployment.

### 3.2.1 Oracle Fusion Middleware Artifacts

The Oracle Fusion Middleware components in a given environment are usually interdependent on each other, so it is important to have the components in the topology be in sync. This is an important consideration for designing volumes and consistency groups. Some of the artifacts are static while others are dynamic.

**Static Artifacts**

Static artifacts are files and directories are that do not change frequently. These include:

- MW_HOME: The Oracle Middleware home usually consists of an Oracle home and an Oracle WebLogic Server home.
- Oracle Inventory: The `oraInst.loc` and `oratab` files, which are located in the `/etc` directory.
- BEA Home List: On UNIX, this is located at *`user_home`*`/bea/beahomelist`.

**Dynamic or Run-Time Artifacts**

Dynamic or run-time artifacts are files that change frequently. Run-time artifacts include:

- Domain Home: Domain directories of the Administration Server and the Managed Servers.
- Oracle Instances: Oracle Instance home directories.
- Application artifacts, such as `.ear` or `.war` files.

- Database artifacts such as the MDS repository.
- Database metadata repositories used by Oracle Fusion Middleware.
- Persistent stores, such as JMS Providers and transaction logs.

### 3.2.2 Oracle Home and Oracle Inventory

Oracle Fusion Middleware allows creating multiple Managed Servers from one single binary installation. This allows the installation of binaries in a single location on a shared storage and the reuse of this installation by the servers in different nodes. However, for maximum availability, Oracle recommends using redundant binary installations.

When an ORACLE_HOME or a WL_HOME is shared by multiple servers in different nodes, it is recommended to 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 `user_home/bea/beahomelist` file. This would be required for any nodes installed additionally to the ones shown in this topology.

### 3.2.3 Storage Replication

This section provides guidelines on creating volumes on the shared storage. Depending on the capabilities of the storage replication technology available with your preferred storage device you may need to create mount points, directories and symbolic links on each of the nodes within a tier.

If your storage device's storage replication technology guarantees consistent replication across multiple volumes:

- Create one volume per server running on that tier. For example, on the application tier, you can create one volume for the WebLogic Administration Server and another volume for the Managed Servers.
- Create one consistency group for each tier with the volumes for that tier as its members.
- Note that if a volume is mounted by two systems simultaneously, a clustered file system may be required for this, depending on the storage subsystem. However, there is no known case of a single file or directory tree being concurrently accessed by Oracle processes on different systems. NFS is a clustered file system, so no additional clustered file system software is required if you are using NFS-attached storage.

If your storage device's storage replication technology does not guarantee consistent replication across multiple volumes:

- Create a volume for each tier. For example, you can create one volume for the application tier, one for the web tier, and so on.
- Create a separate directory for each node in that tier. For example, you can create a directory for SOAHOST1 under the application tier volume; create a directory for WEBHOST1 under the web tier volume, and so on.
- Create a mount point directory on each node to the directory on the volume.

- Create a symbolic link to the mount point directory. A symbolic link should be created so that the same directory structure can be used across the nodes in a tier.
- Note that if a volume is mounted by two systems simultaneously, a clustered file system may be required for this, depending on the storage subsystem. However, there is no known case of a single file or directory tree being concurrently accessed by Oracle processes on different systems. NFS is a clustered file system, so no additional clustered file system software is required if you are using NFS-attached storage.

> **Note:** Before you set up the shared storage for your Disaster Recovery sites, read the high availability chapter in the *Oracle Fusion Middleware Release Notes* to learn of any known shared storage-based deployment issues in high availability environments.
>
> The release notes for Oracle Fusion Middleware can be found at this URL:
>
> `http://www.oracle.com/technology/documentation/middleware.html`

### 3.2.4 File-Based Persistent Store

The WebLogic Server application servers are usually clustered for high-availability. For the local site high availability of the Oracle SOA Suite topology, a file-based persistent store is used for the Java Message Services (JMS) and Transaction Logs (TLogs). This file-based persistent store must reside on shared storage that is accessible by all members of the cluster.

A SAN storage system should use either a host based clustered or shared file system technology such as the Oracle Clustered File System (OCFS2). OCFS2 is a symmetric shared disk cluster file system which allows each node to read and write both metadata and data directly to the SAN.

Additional clustered file systems are not required when using NAS storage systems.

## 3.3 Database Considerations

This section provides the recommendations and considerations for setting up Oracle databases that will be used in the Oracle Fusion Middleware Disaster Recovery topology.

1. Oracle recommends creating Real Application Cluster databases on both the production site and standby site as required by your topology.
2. Oracle Data Guard is the recommended disaster protection technology for the databases running the metadata repositories.
3. The Oracle Data Guard configuration used should be decided based on the data loss requirements of the database as well as the network considerations such as the available bandwidth and latency when compared to the redo generation. Make sure that this is determined correctly before setting up the Oracle Data Guard configuration.

   Please refer to *Oracle Data Guard Concepts and Administration* as well as related Maximum Availability Architecture collateral at the following URL for more information:

http://www.oracle.com/technology/deploy/availability/htdocs/maa.htm

4. Ensure that your network is configured for low latency with sufficient bandwidth, since synchronous redo transmission can cause an impact on response time and throughput.
5. The `LOG_ARCHIVE_DEST_n` parameter on standby site databases should have the LGRW SYNC and AFFIRM archive attributes.
6. The standby site database should be in the Managed Recovery mode. This ensures that the standby site databases are in a constant state of media recovery. The managed recovery mode is enables for shorter failover times.
7. The `tnsnames.ora` file on the production site and the standby site must have entries for databases on both the production and standby sites.
8. It is strongly recommended to force Data Guard to perform manual database synchronization whenever middle tier synchronization is performed. This is especially true for components that store configuration data in the metadata repositories.
9. It is strongly recommended to set up aliases for the database host  names on both the production and standby sites. This enables seamless switchovers, switchbacks and failovers.

### 3.3.1 Making TNSNAMES.ORA Entries for Databases

Because Oracle Data Guard is used to synchronize production and standby databases, the production database and standby database must be able to reference each other.

Oracle Data Guard uses `tnsnames.ora` file entries to direct requests to the production and standby databases, so entries for production and standby databases must be made to the `tnsnames.ora` file. See *Oracle Data Guard Concepts and Administration* in the Oracle Database documentation set for more information about using tnsnames.ora files with Oracle Data Guard.

### 3.3.2 Manually Forcing Database Synchronization with Oracle Data Guard

For Oracle Fusion Middleware components that store middle tier configuration data in Oracle database repositories, use Oracle Data Guard to manually force a database synchronization whenever a middle tier synchronization is performed. Use the SQL `alter system archive log all` statement to switch the logs, which forces the synchronization of the production site and standby site databases.

Example 3–9 shows the SQL statement to use to force the synchronization of a production site database and standby site database.

***Example 3–9 Manually Forcing an Oracle Data Guard Database Synchronization***

```
ALTER SYSTEM ARCHIVE LOG ALL;
```

### 3.3.3 Setting Up Database Host Name Aliases

Optionally, you can set up database host name aliases for the databases at your production site and standby site. The alias must be defined in DNS or in the `/etc/hosts` file on each node running a database instance.

In a Disaster Recovery environment, the site that actively accepts connections is the production site. At the completion of a successful failover or switchover operation, the standby site becomes the new production site.

This section includes an example of defining an alias for database hosts named custdbhost1 and stbycustdbhost1. Table 3–13 shows the database host names and the connect strings for the databases before the alias is defined.

*Table 3–13 Database Host Names and Connect Strings*

| Site | Database Host Name | Database Connect String |
|---|---|---|
| Production | custdbhost1.us.oracle.com | custdbhost1.us.oracle.com:1521:orcl |
| Standby | stbycustdbhost1.us.oracle.com | stbycustdbhost1.us.oracle.com:1521:orcl |

In this example, all database connect strings on the production site take the form "custdbhost1.us.oracle.com:1521:orcl." After a failover or switchover operation, this connect string must be changed to "stbycustdbhost1.us.oracle.com:1521:orcl." However, by creating an alias of "proddb1" for the database host name as shown in Table 3–14, you can avoid manually changing the connect strings, which enables seamless failovers and switchovers:

*Table 3–14 Specifying an Alias for a Database Host*

| Site | Database Host Name | Alias | Database Connect String |
|---|---|---|---|
| Production | custdbhost1.us.oracle.com | proddb1.us.oracle.com | proddb1.us.oracle.com:1521:orcl |
| Standby | stbycustdbhost1.us.oracle.com | proddb1.us.oracle.com | proddb1.us.oracle.com:1521:orcl |

In this example, the production site database host name and the standby site database host name are aliased to "proddb1.us.oracle.com" and the connect strings on the production site and the standby site can take the form "proddb1.us.oracle.com:1521:orcl". On failover and switchover operations, the connect string does not need to change, thus enabling a seamless failover and switchover.

The format for specifying aliases in /etc/hosts file entries is:

```
<IP>    <ALIAS WITH DOMAIN> <ALIAS>    <HOST NAME WITH DOMAIN> <HOST NAME>
```

In this example, you create a database host name alias of proddb1 for host custdbhost1 at the production site and for host stbycustdbhost1 at the standby site. The hosts file entry should specify the fully qualified database host name alias with the `<ALIAS WITH DOMAIN>` parameter, the short database host name alias with the `<ALIAS>` parameter, the fully qualified host name with the `<HOST NAME WITH DOMAIN>` parameter, and the short host name with the `<HOST NAME>` parameter.

So, in the `/etc/hosts` files at the production site, make sure the entry for host custdbhost1 looks like this:

```
152.68.196.213 proddb1.us.oracle.com proddb1 custdbhost1.us.oracle.com custdbhost1
```

And, in the /etc/hosts files at the standby site, make sure the entry for host stbycustdbhost1 looks like this:

```
140.87.25.40   proddb1.us.oracle.com proddb1 stbycustdbhost1.us.oracle.com
stbycustdbhost1
```

# 3.4 Starting Points

Before setting up the standby site, the administrator must evaluate the starting point of the project. The starting point for designing an Oracle Fusion Middleware Disaster Recovery topology is usually one of the following:

- The production site is already created and the standby site is being planned and created.

  Section 3.4.1, "Starting with an Existing Site" describes how to design the Oracle Fusion Middleware Disaster Recovery standby site when you have an existing production site.

- There is no existing production site or standby site. Both need to be designed and created.

  Section 3.4.2, "Starting with New Sites" describes how to design a new Oracle Fusion Middleware Disaster Recovery production site and standby site when you do not have an existing production site or standby site.

- Some hosts or components may exist at a current production site, but new hosts or components need to be added at that site or at a standby site to set up a functioning Oracle Fusion Middleware Disaster Recovery topology.

  Use the pertinent information in this chapter to design and implement an Oracle Fusion Middleware Disaster Recovery topology.

## 3.4.1 Starting with an Existing Site

When the administrator's starting point is an existing production site, the configuration data and the Oracle binaries for the production site already exist on the file system. Also, the host names, ports, and user accounts are already defined. When a production site exists, the administrator can choose to:

- Design a symmetric standby site. See Section 3.5.1, "Design Considerations for a Symmetric Topology."
- Design an asymmetric standby site. See Section 3.5.2, "Design Considerations for an Asymmetric Topology."
- Migrate the production site to shared storage, if not already on shared storage, and then create either a symmetric standby site or asymmetric standby site. See Section 3.4.1.1, "Migrating an Existing Production Site to Shared Storage."

### 3.4.1.1 Migrating an Existing Production Site to Shared Storage

The Oracle Fusion Middleware Disaster Recovery solution relies on shared storage to implement storage replication for disaster protection of the Oracle Fusion Middleware middle tier configuration. When a production site has already been created, it is likely that the Oracle home directories for the Oracle Fusion Middleware instances that comprise the site are not located on the shared storage. If this is the case, then these homes have to be migrated completely to the shared storage to implement the Oracle Fusion Middleware Disaster Recovery solution.

Follow these guidelines for migrating the production site from the local disk to shared storage:

1. All backups performed must be offline backups. For more information, see "Types of Backups" and "Recommended Backup Strategy" in *Oracle Fusion Middleware Administrator's Guide*.

2. The backups must be performed as the root user and the permissions must be preserved. See the "Overview of the Backup Strategies" section in *Oracle Fusion Middleware Administrator's Guide*.
3. This is a one-time operation, so it is recommended to recover the entire domain.
4. The directory structure on the shared storage must be set up as described in Section 4.1.1, "Directory Structure and Volume Design."
5. For Oracle SOA Suite, see "Backup and Recovery Recommendations for Oracle SOA Suite" in *Oracle Fusion Middleware Administrator's Guide*.
6. For Oracle WebCenter, see "Backup and Recovery Recommendations for Oracle WebCenter" in *Oracle Fusion Middleware Administrator's Guide*.
7. For Oracle Identity Management, see "Backup and Recovery Recommendations for Oracle Identity Management" in *Oracle Fusion Middleware Administrator's Guide*.
8. For Oracle WebLogic Server, see "Backup and Recovery Recommendations for Oracle JRF Installations" in *Oracle Fusion Middleware Administrator's Guide*.
9. For the Web Tier, see "Backup and Recovery Recommendations for Web Tier Installations" in *Oracle Fusion Middleware Administrator's Guide*.
10. For Oracle Portal, Oracle Forms, Oracle Reports, and Discoverer backup and recovery recommendations, see "Backup and Recovery Recommendations for Oracle Portal, Oracle Forms Services, and Oracle Reports Installations" in *Oracle Fusion Middleware Administrator's Guide*.

### 3.4.2 Starting with New Sites

This section presents the logic to implementing a new production site for an Oracle Fusion Middleware Disaster Recovery topology. It describes the planning and setup of the production site by pre-planning host names, configuring the hosts to resolve the alias host names and physical host names, and ensuring that storage replication is set up to copy the configuration based on these names to the standby site. When you design the production site, you should also plan the standby site, which can be a symmetric standby site or an asymmetric standby site.

When you are designing a new production site (not using a pre-existing production site), you will use Oracle Universal Installer to install software on the production site, and parameters such as alias host names and software paths must be carefully designed to ensure that they are the same for both sites.

The flexibility you have when you create a new Oracle Fusion Middleware Disaster Recovery production site and standby site includes:

1. You can design your Oracle Fusion Middleware Disaster Recovery solution so that each host at the production site and at the standby site has the desired alias host name and physical host name. Host name planning was discussed in Section 3.1.1, "Planning Host Names."
2. When you design and create your production site from scratch, you can choose the Oracle home name and Oracle home directory for each Fusion Middleware installation.

   Designing and creating your site from scratch is easier than trying to modify an existing site to meet the design requirements described in this chapter.
3. You can assign ports for the Fusion Middleware installations for the production site hosts that will not conflict with the ports that will be used at the standby site hosts.

This is easier than having to check for and resolve port conflicts between an existing production site and standby site.

## 3.5 Topology Considerations

This section describes design considerations for:

- A symmetric topology
- An asymmetric topology

### 3.5.1 Design Considerations for a Symmetric Topology

A symmetric topology is an Oracle Fusion Middleware Disaster Recovery configuration that is completely identical across tiers on the production site and standby site. In a symmetric topology, the production site and standby site have the identical number of hosts, load balancers, instances, and applications. The same ports are used for both sites. The systems are configured identically and the applications access the same data. This manual describes how to set up a symmetric Oracle Fusion Middleware Disaster Recovery topology for an enterprise configuration.

### 3.5.2 Design Considerations for an Asymmetric Topology

An asymmetric topology is an Oracle Fusion Middleware Disaster Recovery configuration that is different across tiers on the production site and standby site. In an asymmetric topology, the standby site can use less hardware (for example, the production site could include four hosts with four Fusion Middleware instances while the standby site includes two hosts with four Fusion Middleware instances. Or, in a different asymmetric topology, the standby site can use fewer Fusion Middleware instances (for example, the production site could include four Fusion Middleware instances while the standby site includes two Fusion Middleware instances). Another asymmetric topology might include a different configuration for a database (for example, using a Real Application Clusters database at the production site and a single instance database at the standby site).

# 4

# Setting Up and Managing Disaster Recovery Sites

This chapter uses the Oracle SOA Suite enterprise deployment and the Oracle Identity Management enterprise deployment topologies as examples to illustrate the steps required to set up the production site and standby site.

It includes the following topics:

## 4.1 Setting Up the Site

This section provides the steps to create the production site. The Oracle SOA enterprise deployment topology and the Oracle Identity Management Enterprise deployment topology are used as examples.

Ensure that you have performed the following prerequisites before you start creating the production site:

- Set up the host name aliases for the middle tier hosts, which was described in Section 3.1.1, "Planning Host Names."
- Create the required volumes on the shared storage on the production site, which is described in Section 4.1.1, "Directory Structure and Volume Design."
- Create the mount points and the symbolic links (if required). Refer to Section 3.2.3, "Storage Replication" to determine whether you must create symbolic links for the production site.
- The Oracle Data Guard configuration used should be decided based on the data loss requirements of the database as well as the network considerations such as the available bandwidth and latency when compared to the redo generation. Ensure that this is determined correctly before setting up the Oracle Data Guard configuration.

  Please refer to *Oracle Data Guard Concepts and Administration* as well as related Maximum Availability Architecture collateral at the following URL for more information:

http://www.oracle.com/technology/deploy/availability/htdocs/maa.htm

### 4.1.1 Directory Structure and Volume Design

The following section details the directory structure recommended by Oracle. The end user is free to choose other directory layouts, but the model adopted here enables maximum availability, providing the best isolation of components and symmetry in the configuration, and facilitating backup and disaster recovery.

This list describes directories and directory environment variables:

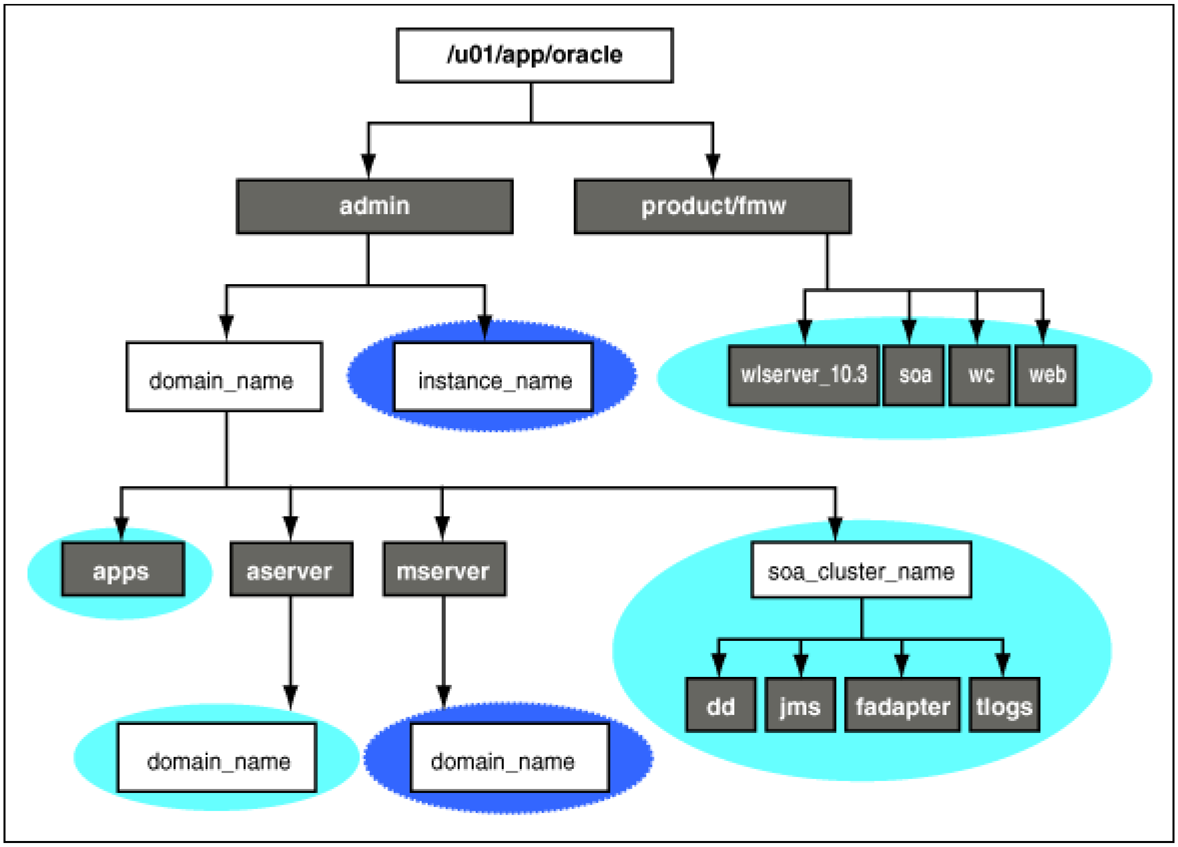
- ORACLE_BASE: This environment variable and related directory path refers to the base directory under which Oracle products are installed.
- MW_HOME: This environment variable and related directory path refers to the location where Oracle Fusion Middleware resides.
- WL_HOME: This environment variable and related directory path contains installed files necessary to host a WebLogic Server.
- ORACLE_HOME: This environment variable and related directory path refers to the location where a product suite (such as Oracle Fusion Middleware SOA Suite, Oracle WebCenter, or Oracle Identity Management) is installed.
- DOMAIN directory: This directory path refers to the location where the Oracle WebLogic Domain information (configuration artifacts) is stored. Different WebLogic Servers can use different domain directories even when in the same node as described below.
- ORACLE_INSTANCE: An Oracle instance contains one or more system components, such as Oracle Web Cache, Oracle HTTP Server, or Oracle Internet Directory. An Oracle instance directory contains updatable files, such as configuration files, log files, and temporary files.

#### 4.1.1.1 Directory Structure Recommendations for Oracle SOA Suite

Oracle Fusion Middleware 11*g* allows creating multiple SOA Managed Servers from one single binary installation. This allows the installation of binaries in a single location on a shared storage and the reuse of this installation by the servers in different nodes. However, for maximum availability, Oracle recommends using redundant binary installations. In this model, two MW HOMEs (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 for redundant binary location, thus isolating as much as possible the failures in each volume. For additional protection, Oracle recommends using storage replication for these volumes. 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.

Oracle also recommends separating the domain directory used by the Administration Server from the domain directory used by 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 node with the same configuration. It is also recommended to have the Managed Servers' domain directories on a shared storage, even though having them on the local file system is also supported. This is especially true when designing a production site with the disaster recovery site in mind. Figure 4–1 represents the directory structure layout for Oracle SOA Suite.

***Figure 4–1 Directory Structure for SOA***



Detailed information about setting up this directory structure is included in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite* and in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter*.

Table 4–1 explains what the color-coded elements in Figure 4–1 mean. The directory structure in Figure 4–1 does not show other required internal directories such as oracle_common and jrockit.

***Table 4–1 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 shared storage. |
| 🔵 | The Managed Server domain directories can be on a local disk or shared storage. Further, if you want to share the Managed Server domain directories on multiple nodes, then you must mount the same shared storage location across the nodes. The `instance_name` directory for the web tier can be on a local disk or shared storage. |
| ■ | Fixed name. |

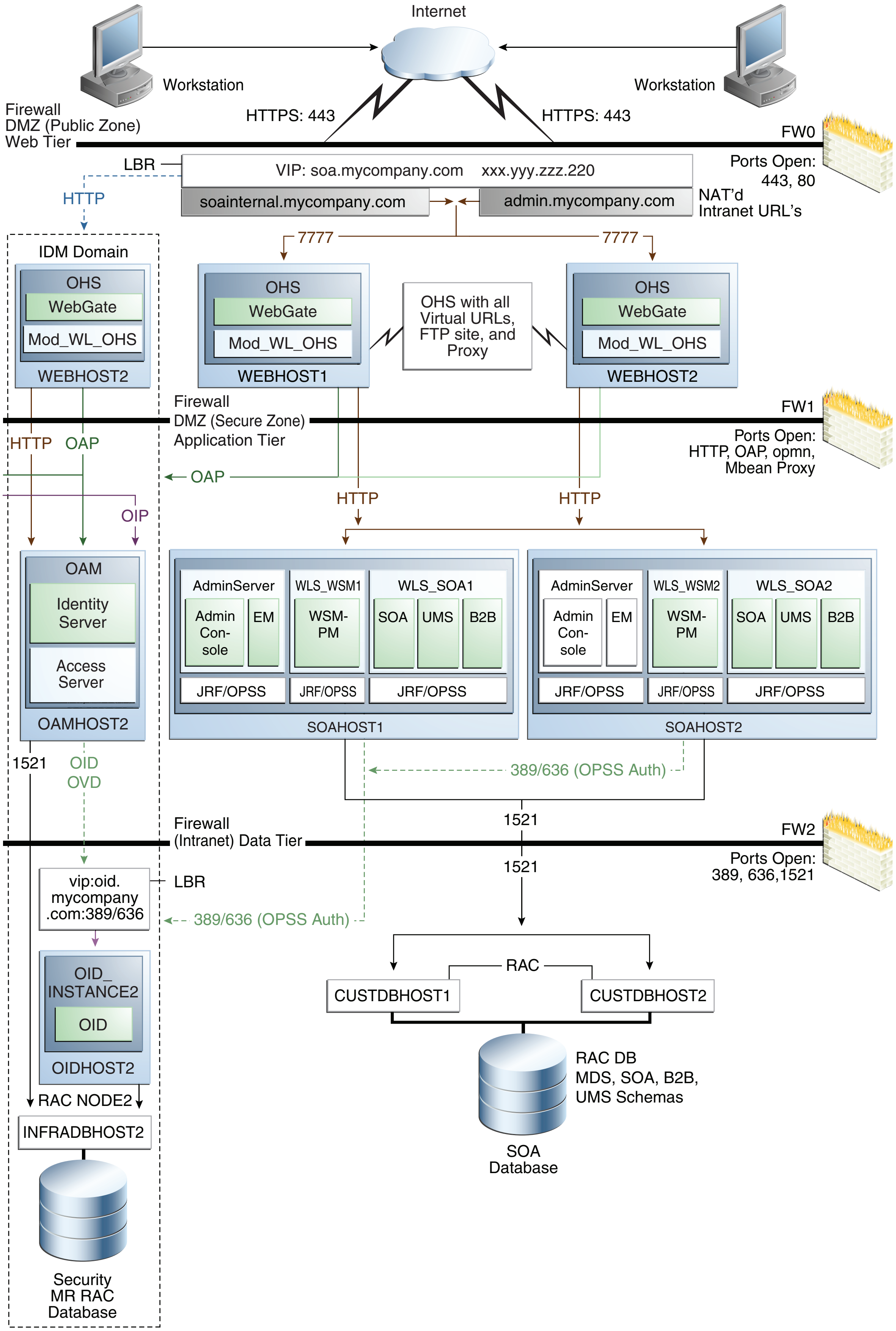
*Table 4–1 (Cont.) Directory Structure Elements*

| Element | Explanation |
|---|---|
| □ | Installation-dependent name. |

#### 4.1.1.1.1 Volume Design for Oracle SOA Suite

Figure 4–2 shows an Oracle SOA Suite topology diagram. The volume design described in this section is for this Oracle SOA Suite topology. Detailed instructions for installing and configuring this topology are provided in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*.

*Figure 4–2 MySOACompany Topology with Oracle Access Manager*


Internet
Workstation
Workstation
Firewall
DMZ (Public Zone)
Web Tier
HTTPS: 443
HTTPS: 443
FW0
Ports Open:
443, 80
LBR
VIP: soa.mycompany.com xxx.yyy.zzz.220
soainternal.mycompany.com
admin.mycompany.com
NAT'd
Intranet URL's
HTTP
IDM Domain
OHS
WebGate
Mod_WL_OHS
WEBHOST2
7777
7777
OHS
WebGate
Mod_WL_OHS
WEBHOST1
OHS with all
Virtual URLs,
FTP site, and
Proxy
OHS
WebGate
Mod_WL_OHS
WEBHOST2
Firewall
DMZ (Secure Zone)
Application Tier
FW1
Ports Open:
HTTP, OAP, opmn,
Mbean Proxy
HTTP
OAP
OAP
OIP
HTTP
HTTP
OAM
Identity
Server
Access
Server
OAMHOST2
AdminServer
Admin
Con-
sole
EM
WLS_WSM1
WSM-
PM
WLS_SOA1
SOA
UMS
B2B
JRF/OPSS
JRF/OPSS
JRF/OPSS
SOAHOST1
AdminServer
Admin
Con-
sole
EM
WLS_WSM2
WSM-
PM
WLS_SOA2
SOA
UMS
B2B
JRF/OPSS
JRF/OPSS
JRF/OPSS
SOAHOST2
1521
OID
OVD
389/636 (OPSS Auth)
1521
Firewall
(Intranet) Data Tier
FW2
Ports Open:
389, 636,1521
1521
vip:oid.
mycompany
.com:389/636
LBR
389/636 (OPSS Auth)
RAC
CUSTDBHOST1
CUSTDBHOST2
OID_
INSTANCE2
OID
OIDHOST2
RAC DB
MDS, SOA, B2B,
UMS Schemas
SOA
Database
RAC NODE2
INFRADBHOST2
Security
MR RAC
Database

For disaster recovery of this Oracle SOA Suite topology, Oracle recommends the following volume design:

- Provision two volumes for two Middleware Homes that contain redundant product binaries (VOLFMW1 and VOLFMW2 in Table 4–2)
- Provision one volume for the Administration Server domain directory (VOLADMIN in Table 4–2)
- Provision one volume on each node for the Managed Server domain directory (VOLSOA1 and VOLSOA2 in Table 4–2). This directory is shared between all the Managed Servers on that node.
- Provision one volume for the JMS file-store and JTA transaction logs (VOLDATA in Table 4–2). There will be one volume for the entire domain that is mounted on all the nodes in the domain.
- Provision one volume on each node for the Oracle HTTP Server Oracle home (VOLWEB1 and VOLWEB2 in Table 4–2).
- Provision one volume on each node for the Oracle HTTP Server Oracle instance (VOLWEBINST1 and VOLWEBINST2 in Table 4–2).

Table 4–2 provides a summary of Oracle recommendations for volume design for the Oracle SOA Suite topology shown in Figure 4–2:

***Table 4–2 Volume Design Recommendations for Oracle SOA Suite***

| Tier | Volume Name | Mounted on Host | Mount Point | Comments |
|---|---|---|---|---|
| Web | VOLWEB1 | WEBHOST1 | /u01/app/oracle/product/fmw/web | Volume for Oracle HTTP Server installation |
| Web | VOLWEB2 | WEBHOST2 | /u01/app/oracle/product/fmw/web | Volume for Oracle HTTP Server installation |
| Web | VOLWEBINST1 | WEBHOST1 | /u01/app/oracle/admin/ohs_instance | Volume for Oracle HTTP Server instance |
| Web | VOLWEBINST2 | WEBHOST2 | /u01/app/oracle/admin/ohs_instance | Volume for Oracle HTTP Server instance |
| Web | VOLSTATIC1[1] | WEBHOST1 | /u01/app/oracle/admin/ohs_instance/config/static | Volume for static HTML content |
| Web | VOLSTATIC2[2] | WEBHOST2 | /u01/app/oracle/admin/ohs_instance/config/static | Volume for static HTML content |
| Application | VOLFMW1 | SOAHOST1 | /u01/app/oracle/product/fmw | Volume for the WebLogic Server and Oracle SOA Suite binaries |
| Application | VOLFMW2 | SOAHOST2 | /u01/app/oracle/product/fmw | Volume for the WebLogic Server and Oracle SOA Suite binaries. |
| Application | VOLADMIN | SOAHOST1 | /u01/app/oracle/admin/soaDomain/admin | Volume for Administration Server domain directory |

*Table 4–2 (Cont.) Volume Design Recommendations for Oracle SOA Suite*

| Tier | Volume Name | Mounted on Host | Mount Point | Comments |
|---|---|---|---|---|
| Application | VOLSOA1 | SOAHOST1 | /u01/app/oracle/admin/soaDomain/mng1 | Volume for Managed Server domain directory |
| Application | VOLSOA2 | SOAHOST2 | /u01/app/oracle/admin/soaDomain/mng2 | Volume for Managed Server domain directory |
| Application | VOLDATA | SOAHOST1,<br>SOAHOST2 | /u01/app/oracle/admin/soaDomain/soaCluster/jms<br>/u01/app/oracle/admin/soaDomain/soaCluster/tlogs | Volume for transaction logs and JMS data |

[1] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

[2] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

**4.1.1.1.2 Consistency Group Recommendations for Oracle SOA Suite** Oracle recommends the following consistency groups for the Oracle SOA Suite topology:

- Create one consistency group with the volumes containing the domain directories for the Administration Server and Managed Servers as members (DOMAINGROUP in Table 4–3).
- Create one consistency group with the volume containing the JMS file store and transaction log data as members (DATAGROUP in Table 4–3).
- Create one consistency group with the volume containing the Middleware Homes as members (FMWHOMEGROUP in Table 4–3).
- Create one consistency group with the volumes containing the Oracle HTTP Server Oracle homes as members (WEBHOMEGROUP in Table 4–3).
- Create one consistency group with the volumes containing the Oracle HTTP Server Oracle instances as members (WEBINSTANCEGROUP in Table 4–3).

Table 4–3 provides a summary of Oracle recommendations for consistency groups for the Oracle SOA Suite topology shown in Figure 4–2.

*Table 4–3 Consistency Groups for Oracle SOA Suite*

| Tier | Group Name | Members | Comments |
|---|---|---|---|
| Application | DOMAINGROUP | VOLADMIN<br>VOLSOA1<br>VOLSOA2 | Consistency group for the Administration Server, Managed Server domain directory |
| Application | DATAGROUP | VOLDATA | Consistency group for the JMS file store and transaction log data |
| Application | FMWHOMEGROUP | VOLFMW1<br>VOLFMW2 | Consistency group for the Middleware homes |
| Web | WEBHOMEGROUP | VOLWEB1<br>VOLWEB2 | Consistency group for the Oracle HTTP Server Oracle homes |

*Table 4–3 (Cont.) Consistency Groups for Oracle SOA Suite*

| Tier | Group Name | Members | Comments |
|---|---|---|---|
| Web | WEBINSTANCEGROUP | VOLWEBINST1<br>VOLWEBINST2<br>VOLSTATIC1[1]<br>VOLSTATIC2[2] | Consistency group for the Oracle HTTP Server Oracle instances |

[1] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

[2] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

### 4.1.1.2 Directory Structure Recommendations for Oracle WebCenter

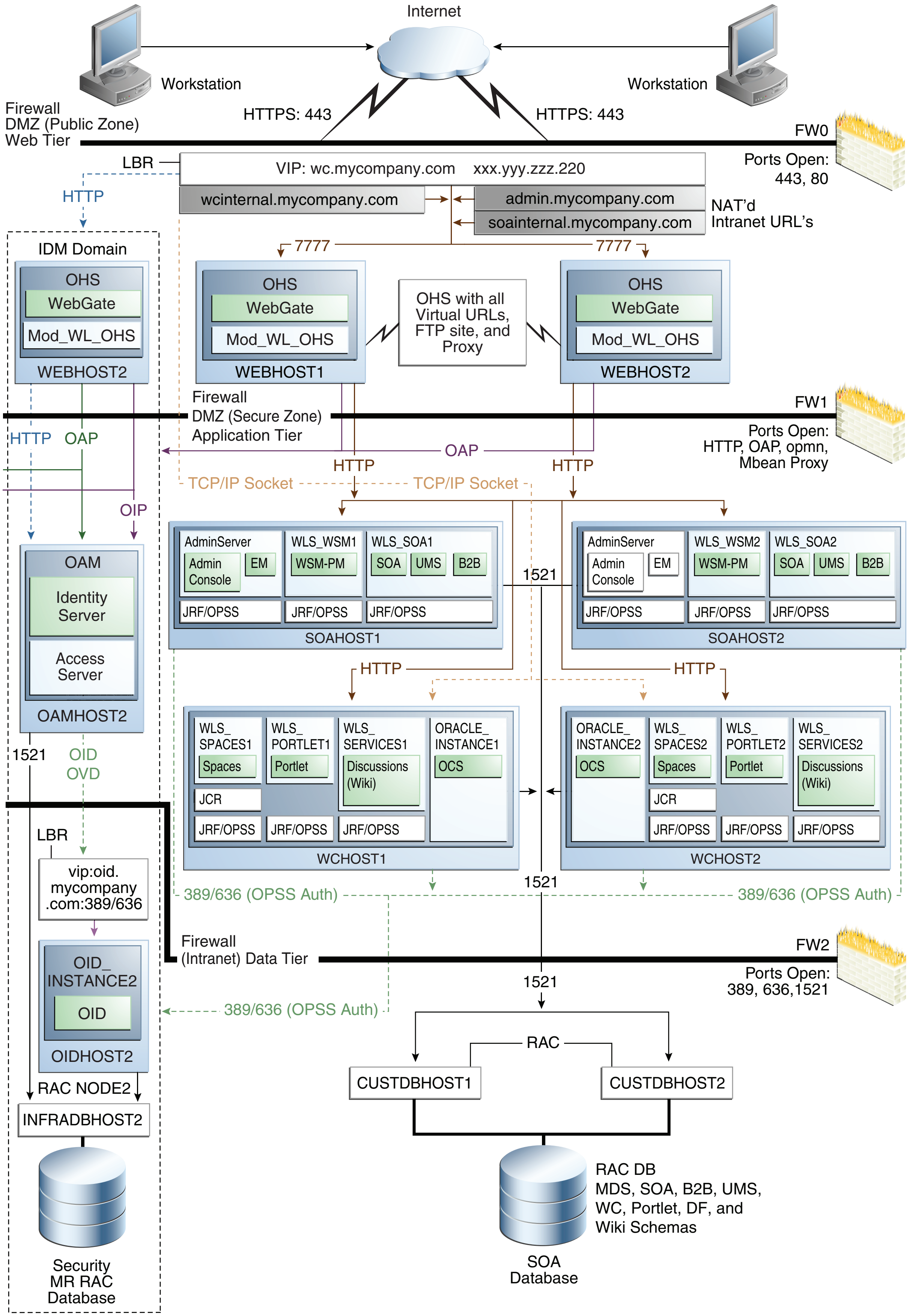
Oracle Fusion Middleware 11*g* allows creating multiple WebCenter Managed Servers from one single binary installation. This allows the installation of binaries in a single location on a shared storage and the reuse of this installation by the servers in different nodes. However, for maximum availability, Oracle recommends using redundant binary installations. In this model, two MW HOMEs (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 for redundant binary location, thus isolating as much as possible the failures in each volume. For additional protection, Oracle recommends using storage replication for these volumes. 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.

Oracle also recommends separating the domain directory used by the Administration Server from the domain directory used by 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 node with the same configuration. It is also recommended to have the Managed Servers' domain directories on a shared storage, even though having them on the local file system is also supported. This is especially true when designing a production site with the disaster recovery site in mind. Figure 4–1 shows the directory structure layout for Oracle WebCenter (the same directory structure layout is used for both Oracle SOA Suite and Oracle WebCenter).

#### 4.1.1.2.1 Volume Design for Oracle WebCenter

Figure 4–3 shows an Oracle WebCenter topology diagram. The volume design described in this section is for this Oracle WebCenter topology. Instructions for installing and configuring this topology are provided in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter*.

***Figure 4–3 MyWCCompany Topology with Oracle Access Manager***


Internet
Workstation
Workstation
HTTPS: 443
HTTPS: 443
Firewall
DMZ (Public Zone)
Web Tier
FW0
Ports Open:
443, 80
LBR
VIP: wc.mycompany.com xxx.yyy.zzz.220
wcinternal.mycompany.com
admin.mycompany.com
soainternal.mycompany.com
NAT'd
Intranet URL's
HTTP
IDM Domain
7777
7777
OHS
WebGate
Mod_WL_OHS
WEBHOST2
OHS
WebGate
Mod_WL_OHS
WEBHOST1
OHS with all
Virtual URLs,
FTP site, and
Proxy
OHS
WebGate
Mod_WL_OHS
WEBHOST2
Firewall
DMZ (Secure Zone)
Application Tier
FW1
Ports Open:
HTTP, OAP, opmn,
Mbean Proxy
HTTP
OAP
OAP
HTTP
HTTP
TCP/IP Socket
TCP/IP Socket
OIP
OAM
Identity
Server
Access
Server
OAMHOST2
AdminServer
Admin
Console
EM
WLS_WSM1
WSM-PM
WLS_SOA1
SOA
UMS
B2B
JRF/OPSS
JRF/OPSS
JRF/OPSS
SOAHOST1
1521
AdminServer
Admin
Console
EM
WLS_WSM2
WSM-PM
WLS_SOA2
SOA
UMS
B2B
JRF/OPSS
JRF/OPSS
JRF/OPSS
SOAHOST2
HTTP
HTTP
WLS_
SPACES1
Spaces
JCR
WLS_
PORTLET1
Portlet
WLS_
SERVICES1
Discussions
(Wiki)
ORACLE_
INSTANCE1
OCS
JRF/OPSS
JRF/OPSS
JRF/OPSS
WCHOST1
ORACLE_
INSTANCE2
OCS
WLS_
SPACES2
Spaces
JCR
WLS_
PORTLET2
Portlet
WLS_
SERVICES2
Discussions
(Wiki)
JRF/OPSS
JRF/OPSS
JRF/OPSS
WCHOST2
1521
OID
OVD
LBR
vip:oid.
mycompany
.com:389/636
389/636 (OPSS Auth)
1521
389/636 (OPSS Auth)
OID_
INSTANCE2
OID
OIDHOST2
Firewall
(Intranet) Data Tier
FW2
Ports Open:
389, 636,1521
1521
389/636 (OPSS Auth)
RAC NODE2
INFRADBHOST2
Security
MR RAC
Database
RAC
CUSTDBHOST1
CUSTDBHOST2
RAC DB
MDS, SOA, B2B, UMS,
WC, Portlet, DF, and
Wiki Schemas
SOA
Database

For disaster recovery of this Oracle WebCenter topology, Oracle recommends the following volume design:

- Provision two volumes for two Middleware Homes that contain redundant product binaries (VOLFMW1 and VOLFMW2 in Table 4–4)
- Provision one volume for the Administration Server domain directory (VOLADMIN in Table 4–4)
- Provision one volume on each node for the Managed Server domain directory for SOA (VOLSOA1 and VOLSOA2 in Table 4–4). This directory is shared between all the Managed Servers on that node.
- Provision one volume on each node for the Managed Server domain directory for WebCenter (VOLWC1 and VOLWC2 in Table 4–4). This directory is shared between all the Managed Servers on that node.
- Provision one volume for the JMS file-store and JTA transaction logs (VOLDATA in Table 4–4). There will be one volume for the entire domain that is mounted on all the nodes in the domain.
- Provision one volume on each node for the Oracle HTTP Server Oracle home (VOLWEB1 and VOLWEB2 in Table 4–4).
- Provision one volume on each node for the Oracle HTTP Server Oracle instance (VOLWEBINST1 and VOLWEBINST2 in Table 4–4).

Table 4–4 provides a summary of Oracle recommendations for volume design for the Oracle WebCenter topology shown in Figure 4–3:

***Table 4–4 Volume Design Recommendations for Oracle WebCenter***

| Tier | Volume Name | Mounted on Host | Mount Point | Comments |
|---|---|---|---|---|
| Web | VOLWEB1 | WEBHOST1 | /u01/app/oracle/product/fmw/web | Volume for Oracle HTTP Server installation |
| Web | VOLWEB2 | WEBHOST2 | /u01/app/oracle/product/fmw/web | Volume for Oracle HTTP Server installation |
| Web | VOLWEBINST1 | WEBHOST1 | /u01/app/oracle/admin/ohs_instance | Volume for Oracle HTTP Server instance |
| Web | VOLWEBINST2 | WEBHOST2 | /u01/app/oracle/admin/ohs_instance | Volume for Oracle HTTP Server instance |
| Web | VOLSTATIC1[1] | WEBHOST1 | /u01/app/oracle/admin/ohs_instance/config/static | Volume for static HTML content |
| Web | VOLSTATIC2[2] | WEBHOST2 | /u01/app/oracle/admin/ohs_instance/config/static | Volume for static HTML content |
| Application | VOLFMW1 | SOAHOST1 | /u01/app/oracle/product/fmw | Volume for the WebLogic Server and Oracle SOA Suite binaries |
| Application | VOLFMW2 | SOAHOST2 | /u01/app/oracle/product/fmw | Volume for the WebLogic Server and Oracle SOA Suite binaries. |
| Application | VOLADMIN | SOAHOST1 | /u01/app/oracle/admin/soaDomain/admin | Volume for Administration Server domain directory |

*Table 4–4 (Cont.) Volume Design Recommendations for Oracle WebCenter*

| Tier | Volume Name | Mounted on Host | Mount Point | Comments |
|---|---|---|---|---|
| Application | VOLSOA1 | SOAHOST1 | /u01/app/oracle/admin/soaDomain/mng1 | Volume for Managed Server domain directory for SOA |
| Application | VOLSOA2 | SOAHOST2 | /u01/app/oracle/admin/soaDomain/mng2 | Volume for Managed Server domain directory for SOA |
| Application | VOLWC1 | WCHOST1 | /u01/app/oracle/admin/wcDomain/mng1 | Volume for Managed Server domain directory for WebCenter. |
| Application | VOLWC2 | WCHOST2 | /u01/app/oracle/admin/wcDomain/mng2 | Volume for Managed Server domain directory for WebCenter. |
| Application | VOLDATA | SOAHOST1, SOAHOST2, WCHOST1, WCHOST2 | /u01/app/oracle/admin/soaDomain/soaCluster/jms<br>/u01/app/oracle/admin/soaDomain/soaCluster/tlogs | Volume for transaction logs and JMS data |

[1] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

[2] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

#### 4.1.1.2.2 Consistency Group Recommendations for Oracle WebCenter

Oracle recommends the following consistency groups for the Oracle WebCenter topology:

- Create one consistency group with the volumes containing the domain directories for the Administration Server and Managed Servers as members (DOMAINGROUP in Table 4–5).
- Create one consistency group with the volume containing the JMS file store and transaction log data as members (DATAGROUP in Table 4–5).
- Create one consistency group with the volume containing the Middleware Homes as members (FMWHOMEGROUP in Table 4–5).
- Create one consistency group with the volumes containing the Oracle HTTP Server Oracle homes as members (WEBHOMEGROUP in Table 4–5).
- Create one consistency group with the volumes containing the Oracle HTTP Server Oracle instances as members (WEBINSTANCEGROUP in Table 4–5).

Table 4–5 provides a summary of Oracle recommendations for consistency groups for the Oracle WebCenter topology shown in Figure 4–3.

*Table 4–5 Consistency Groups for Oracle WebCenter*

| Tier | Group Name | Members | Comments |
|---|---|---|---|
| Application | DOMAINGROUP | VOLADMIN<br>VOLSOA1<br>VOLSOA2 | Consistency group for the Administration Server, Managed Server domain directory |
| Application | DATAGROUP | VOLDATA | Consistency group for the JMS file store and transaction log data |

*Table 4–5 (Cont.) Consistency Groups for Oracle WebCenter*

| Tier | Group Name | Members | Comments |
|---|---|---|---|
| Application | FMWHOMEGROUP | VOLFMW1<br>VOLFMW2 | Consistency group for the Middleware homes |
| Web | WEBHOMEGROUP | VOLWEB1<br>VOLWEB2 | Consistency group for the Oracle HTTP Server Oracle homes |
| Web | WEBINSTANCEGROUP | VOLWEBINST1<br>VOLWEBINST2<br>VOLSTATIC1[1]<br>VOLSTATIC2[2] | Consistency group for the Oracle HTTP Server Oracle instances |

[1] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

[2] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

### 4.1.1.3 Directory Structure Recommendations for Oracle Identity Management

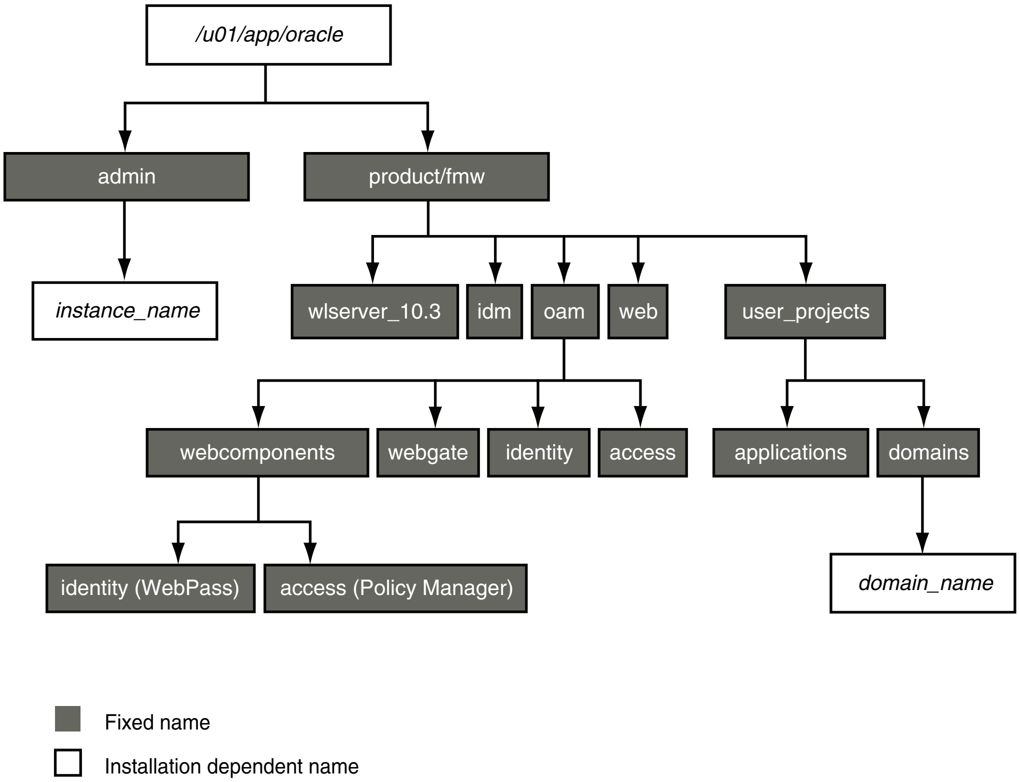
Oracle Fusion Middleware 11*g* allows the separation of the product binaries and the run-time artifacts for Oracle Identity Management components. The product binaries are under the ORACLE_HOME directory and the run-time time artifacts are located under the ORACLE_INSTANCE directory.

In this model, for the web tier and the data tier, it is recommended to have one ORACLE_HOME (for product binaries) per host and one ORACLE_INSTANCE for an instance, installed on the shared storage. The ORACLE_HOME is shared among all the instances running on the host, whereas each instance has its own ORACLE_INSTANCE location. Additional, servers (when scaling out or up) of the same type can use either one of the same location without requiring more installations.

For the application tier, it is recommended to have one Middleware Home (MW HOME) per host (each of which has a WLS HOME and an ORACLE_HOME for each product suite) installed on the shared storage. Additional servers (when scaling out or up) of the same type can use the same location without requiring more installations.

Separation of the domain directory and the MW_HOME is not supported. The domain directory is under the MW_HOME and is shared between all the Administration Servers and Managed Servers running on the host. Section 4–4, "Directory Structure for Oracle Identity Management" shows the directory structure layout for Oracle Identity Management:

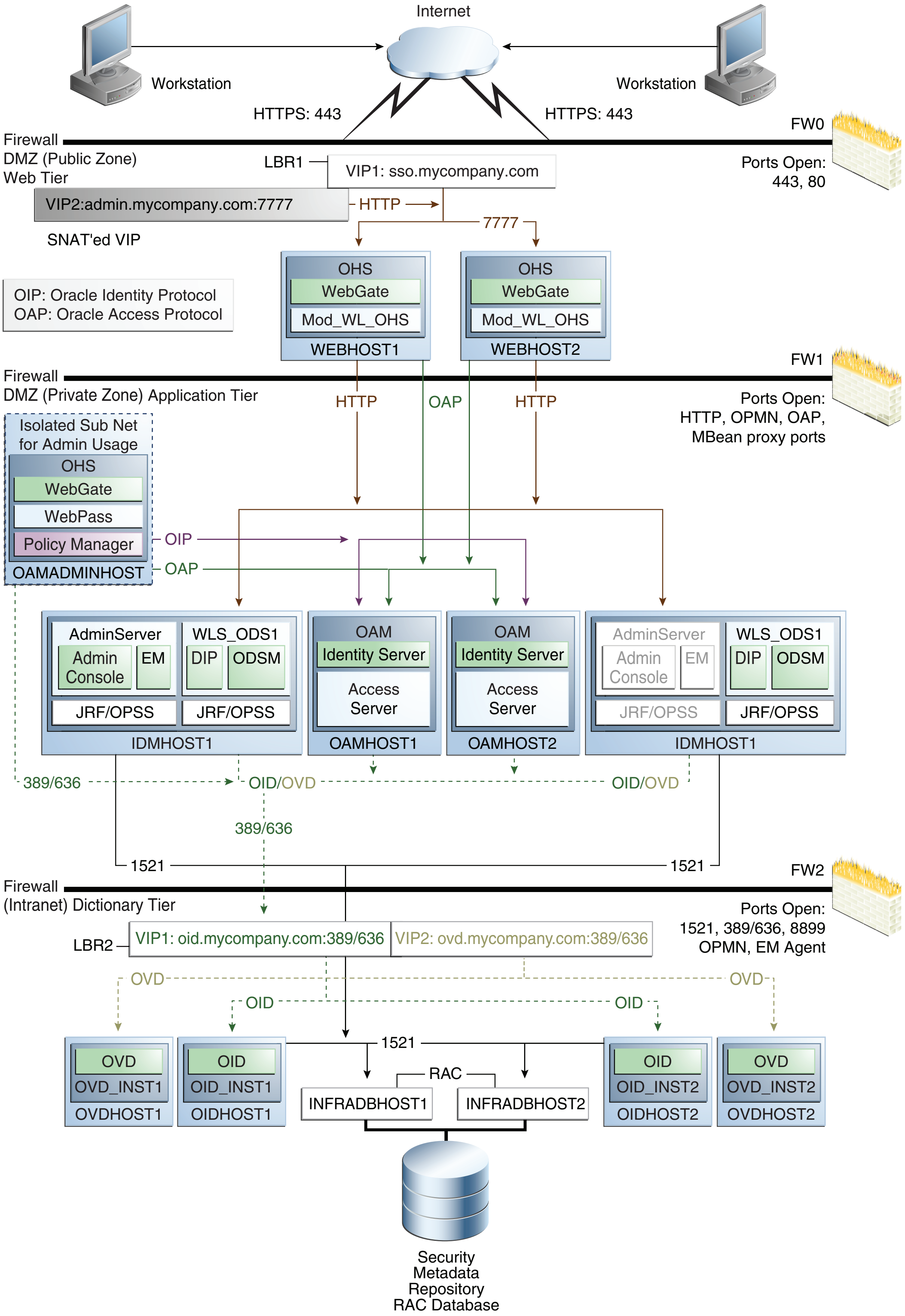
*Figure 4–4 Directory Structure for Oracle Identity Management*



The *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* manual describes how to set up the Oracle Identity Management enterprise deployment shown in Figure 4–4. The directory structure in Figure 4–4 does not show other required internal directories such as oracle_common and jrockit

**4.1.1.3.1 Volume Design for Oracle Identity Management** Figure 4–5 shows an Oracle Identity Management topology diagram. The volume design described in this section is for this Oracle Identity Management topology. Instructions for installing and configuring this topology are provided in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

*Figure 4–5 MyIMCompany Topology with Oracle Access Manager*


Internet
Workstation
Workstation
HTTPS: 443
HTTPS: 443
FW0
Firewall
DMZ (Public Zone)
Web Tier
LBR1
VIP1: sso.mycompany.com
Ports Open:
443, 80
VIP2:admin.mycompany.com:7777
HTTP
7777
SNAT'ed VIP
OIP: Oracle Identity Protocol
OAP: Oracle Access Protocol
OHS
WebGate
Mod_WL_OHS
WEBHOST1
OHS
WebGate
Mod_WL_OHS
WEBHOST2
FW1
Firewall
DMZ (Private Zone) Application Tier
HTTP
OAP
HTTP
Ports Open:
HTTP, OPMN, OAP,
MBean proxy ports
Isolated Sub Net
for Admin Usage
OHS
WebGate
WebPass
Policy Manager
OAMADMINHOST
OIP
OAP
AdminServer
Admin Console
EM
WLS_ODS1
DIP
ODSM
JRF/OPSS
JRF/OPSS
IDMHOST1
OAM
Identity Server
Access Server
OAMHOST1
OAM
Identity Server
Access Server
OAMHOST2
AdminServer
Admin Console
EM
WLS_ODS1
DIP
ODSM
JRF/OPSS
JRF/OPSS
IDMHOST1
389/636
OID/OVD
OID/OVD
389/636
1521
1521
FW2
Firewall
(Intranet) Dictionary Tier
Ports Open:
1521, 389/636, 8899
OPMN, EM Agent
LBR2
VIP1: oid.mycompany.com:389/636
VIP2: ovd.mycompany.com:389/636
OVD
OVD
OID
OID
1521
RAC
OVD
OVD_INST1
OVDHOST1
OID
OID_INST1
OIDHOST1
INFRADBHOST1
INFRADBHOST2
OID
OID_INST2
OIDHOST2
OVD
OVD_INST2
OVDHOST2
Security
Metadata
Repository
RAC Database

The *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* manual describes how to set up the Oracle Identity Management enterprise deployment shown in Figure 4–5.

Oracle recommends the following volume design for Oracle Identity Management:

- Provision one volume on each of the Identity Management nodes for the Middleware Homes. This volume will also contain the WebLogic Server Home, Identity Management Oracle home, domain directory for the Administration Server and Managed Server running on that host. These are VOLIDM1 and VOLIDM2 in Table 4–6.
- Provision one volume on each node for the Oracle homes in the directory tier and web tier. These are VOLWEB1, VOLWEB2, VOLOID1, VOLOID2, VOLOVD1, and VOLOVD2 in Table 4–6.
- Provision one volume on each node for the Oracle instance home in the directory tier and web tier. These are VOLWEBINST1, VOLWEBINST2, VOLOIDINST1, VOLOIDINST2, VOLOVDINST1, and VOLIOVDINST2 in Table 4–6.
- Provision one volume on each node for the Identity Management Oracle instances in the application tier. This volume is shared by the Administration Server and Managed Server instances. These are VOLIDMINST1 and VOLIDMINST2 in Table 4–6.
- Provision one volume on each Oracle Access Manager node for the Oracle Access Manager homes. This volume contains the Identity Server and Access Server homes. These are VOLOAM1 and VOLOAM2 in Table 4–6.
- Provision one volume on the OAMADMINHOST for the Oracle HTTP Server Oracle home, Oracle HTTP Server Oracle instance, WebGate, WebPass and Policy Manager homes. This is VOLOAMADMIN in Table 4–6.

Table 4–6 provides a summary of Oracle recommendations for volume design for the Oracle Identity Management topology shown in Figure 4–5:

***Table 4–6 Volume Recommendations for Oracle identity Management***

| Tier | Volume Names | Mounted on Nodes | Mount Point | Comments |
|---|---|---|---|---|
| Web | VOLWEB1 | WEBHOST1 | /u01/app/oracle/product/fmw/web | Volume for Oracle HTTP Server installations |
| Web | VOLWEB2 | WEBHOST2 | /u01/app/oracle/product/fmw/web | Volume for Oracle HTTP Server installations |
| Web | VOLWEBINST1 | WEBHOST1 | /u01/app/oracle/admin/ohs_instance | Volume for Oracle HTTP Server instances |
| Web | VOLWEBINST2 | WEBHOST2 | /u01/app/oracle/admin/ohs_instance | Volume for Oracle HTTP Server instances |
| Web | VOLSTATIC1[1] | WEBHOST1 | /u01/app/oracle/admin/ohs_instance/config/static | Volume for static HTML content |
| Web | VOLSTATIC2[2] | WEBHOST2 | /u01/app/oracle/admin/ohs_instance/config/static | Volume for static HTML content |
| Application | VOLIDM1 | IDMHOST1 | /u01/app/oracle/product/fmw | Volume for Identity Management Middleware homes |

*Table 4–6 (Cont.) Volume Recommendations for Oracle identity Management*

| Tier | Volume Names | Mounted on Nodes | Mount Point | Comments |
|---|---|---|---|---|
| Application | VOLIDM2 | IDMHOST2 | /u01/app/oracle/product/fmw | Volume for Identity Management Middleware homes |
| Application | VOLIDMINST1 | IDMHOST1 | /u01/app/oracle/admin | Volume for Oracle instances |
| Application | VOLIDMINST2 | IDMHOST2 | /u01/app/oracle/admin | Volume for Oracle instances |
| Application | VOLOAM1 | OAMHOST1 | /u01/app/oracle/product/fmw/oam | Volume for Oracle Access Manager Identity Server and Access Server homes |
| Application | VOLOAM2 | OAMHOST2 | /u01/app/oracle/product/fmw/oam | Volume for Oracle Access Manager Identity Server and Access Server homes |
| Application | VOLOAMADMIN | OAMADMINHOST | /u01/app/oracle | Volume for Oracle Access Manager administration components |
| Directory | VOLOID1 | OIDHOST1 | /u01/app/oracle/product/fmw/idm | Volume for Oracle Internet Directory Oracle homes |
| Directory | VOLOID2 | OIDHOST2 | /u01/app/oracle/product/fmw/idm | Volume for Oracle Internet Directory Oracle homes |
| Directory | VOLOIDINST1 | OIDHOST1 | /u01/app/oracle/admin | Volume for Oracle Internet Directory Oracle instances |
| Directory | VOLOIDINST2 | OIDHOST2 | /u01/app/oracle/admin | Volume for Oracle Internet Directory Oracle instances |
| Directory | VOLOVD1 | OVDHOST1 | /u01/app/oracle/product/fmw/idm | Volume for Oracle Virtual Directory Oracle homes |
| Directory | VOLOVD2 | OVDHOST2 | /u01/app/oracle/product/fmw/idm | Volume for Oracle Virtual Directory Oracle homes |
| Directory | VOLOVDINST1 | OVDHOST1 | /u01/app/oracle/admin | Volume for Oracle Virtual Directory Oracle instances |
| Directory | VOLOVDINST2 | OVDHOST2 | /u01/app/oracle/admin | Volume for Oracle Virtual Directory Oracle instances |

[1] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

[2] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

**4.1.1.3.2 Consistency Group Recommendations for Oracle Identity Management** Oracle recommends the following consistency groups for the Oracle Identity Management topology:

- Create one consistency group with the volumes containing the application tier Middleware home directories as members. This is the IDMMWGROUP group in Table 4–7.
- Create one consistency group with the volumes containing the application tier Oracle instances directories as members. This is the IDMINSTGROUP group in Table 4–7.
- Create one consistency group with the volumes containing the Oracle Internet Directory Oracle homes as members. This is the OIDHOMEGROUP group in Table 4–7.
- Create one consistency group with the volumes containing the Oracle Internet Directory Oracle instances as members. This is the OIDINSTGROUP group in Table 4–7.
- Create one consistency group with the volumes containing the Oracle Virtual Directory Oracle homes as members. This is the OVDHOMEGROUP group in Table 4–7.
- Create one consistency group with the volumes containing the Oracle Virtual Directory Oracle instances as members. This is the OVDINSTGROUP group in Table 4–7.
- Create one consistency group with the volume containing the Oracle Access Manager Oracle homes for Oracle Access Manager administration components as members. This is the OAMADMINGROUP group in Table 4–7.
- Create one consistency group with the volume containing the Oracle Access Manager Oracle homes for Oracle Access Manager Identity and Access Server components as members. This is the OAMGROUP group in Table 4–7.
- Create one consistency group with the volumes containing the Oracle HTTP Server Oracle homes as members. This is the WEBHOMEGROUP in Table 4–7.
- Create one consistency group with the volumes containing the Oracle HTTP Server Oracle instances as members. This is the WEBINSTGROUP group in Table 4–7.

Table 4–7 provides a summary of Oracle recommendations for consistency groups for the Oracle Identity Management topology shown in Figure 4–5:

***Table 4–7 Consistency Groups for Oracle Identity Management***

| Tier | Group Name | Members | Comments |
|---|---|---|---|
| Directory | OIDHOMEGROUP | VOLOID1<br>VOLOID2 | Consistency group for Oracle Internet Directory Oracle homes |
| Directory | OIDINSTGROUP | VOLOIDINST1<br>VOLOIDINST2 | Consistency group for Oracle Internet Directory Oracle instances |
| Directory | OVDHOMEGROUP | VOLOVD1<br>VOLOVD2 | Consistency group for Oracle Virtual Directory Oracle homes |
| Directory | OVDINSTGROUP | VOLOVDINST1<br>VOLOVDINST2 | Consistency group for Oracle Virtual Directory Oracle instances |
| Application | IDMMWGROUP | VOLIDM1<br>VOLIDM2 | Consistency group for the Middleware homes |

*Table 4–7 (Cont.) Consistency Groups for Oracle Identity Management*

| Tier | Group Name | Members | Comments |
|---|---|---|---|
| Application | IDMINSTGROUP | VOLIDMINST1<br>VOLIDMINST2 | Consistency group for the Identity Management instances |
| Application | OAMGROUP | VOLOAM1<br>VOLOAM2 | Consistency group for the Oracle Access Manager Identity Server and Access Server homes |
| Application | OAMADMINGROUP | VOLOAMADMIN | Consistency group for the Oracle Access Manager administration host components |
| Web | WEBHOMEGROUP | VOLWEB1<br>VOLWEB2 | Consistency group for the Oracle HTTP Server Oracle homes |
| Web | WEBINSTGROUP | VOLWEBINST1<br>VOLWEBINST2<br>VOLSTATIC1[1]<br>VOLSTATIC2[2] | Consistency group for the Oracle HTTP Server Oracle instances |

[1] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

[2] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

#### 4.1.1.4 Directory Structure Recommendations for Oracle Portal, Forms, Reports, and Discoverer

Figure 4–6 shows the Oracle Portal enterprise deployment topology diagram. The volume design and consistency groups described in Section 4.1.1.4.1, "Volume Design for Oracle Portal, Forms, Reports, and Discover" and Section 4.1.1.4.2, "Consistency Group Recommendations for Oracle Portal, Forms, Reports, and Discoverer" can be used for a Disaster Recovery site that includes this Oracle Portal topology.

Detailed information about the Oracle Portal enterprise topology in Figure 4–6 is available in the 11.1.1.2 *Oracle Portal Enterprise Deployment Guide*. See Article ID 952068.1 "Oracle Fusion Middleware 11g (11.1.1.2) Enterprise Deployment Guides for Portal, Forms, Reports, and Discover" at My Oracle Support (formerly Oracle *MetaLink*) for information on obtaining the manual. The URL for My Oracle Support is:

```
http://support.oracle.com
```

***Figure 4–6 Oracle Portal Topology Diagram***

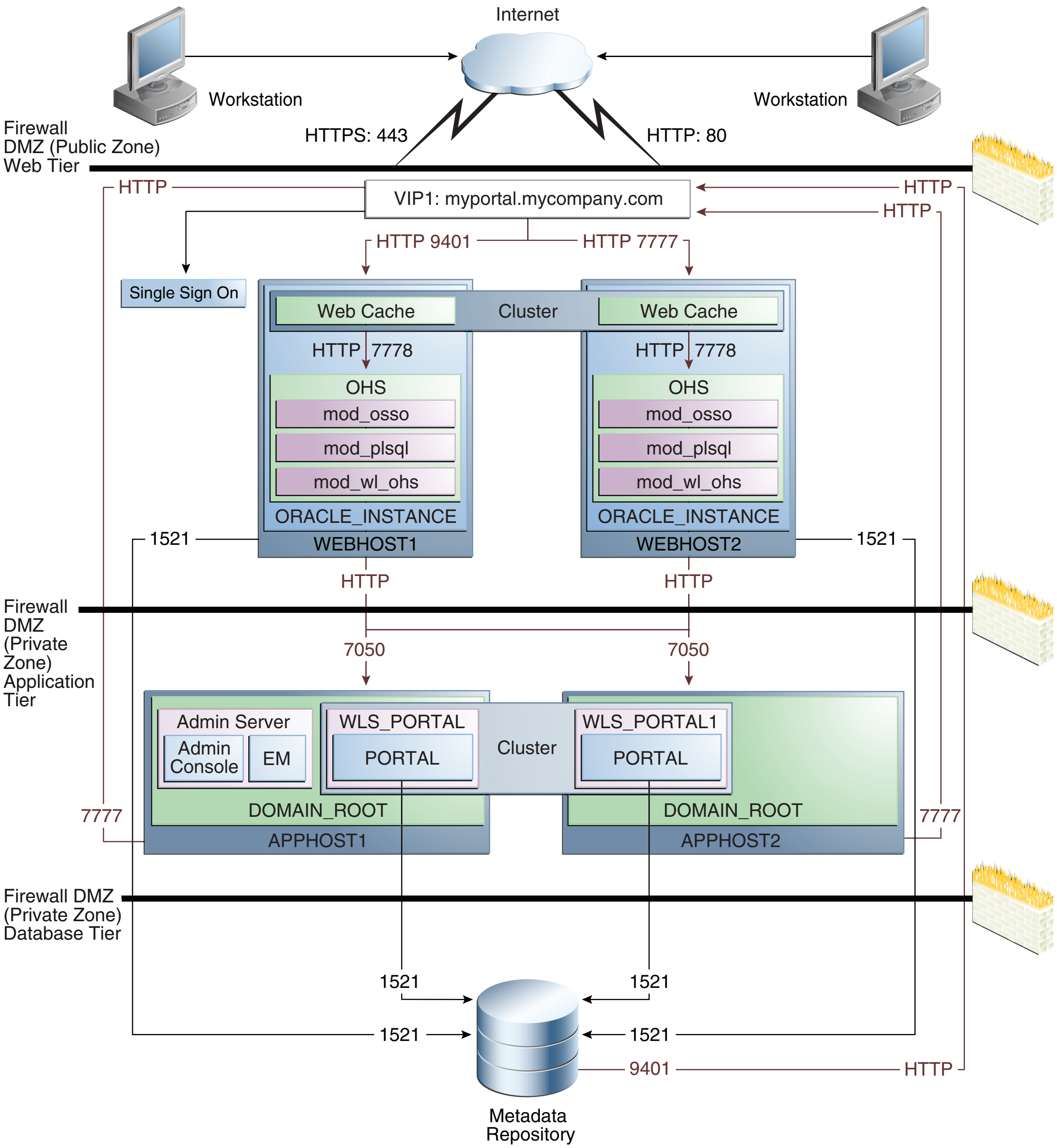
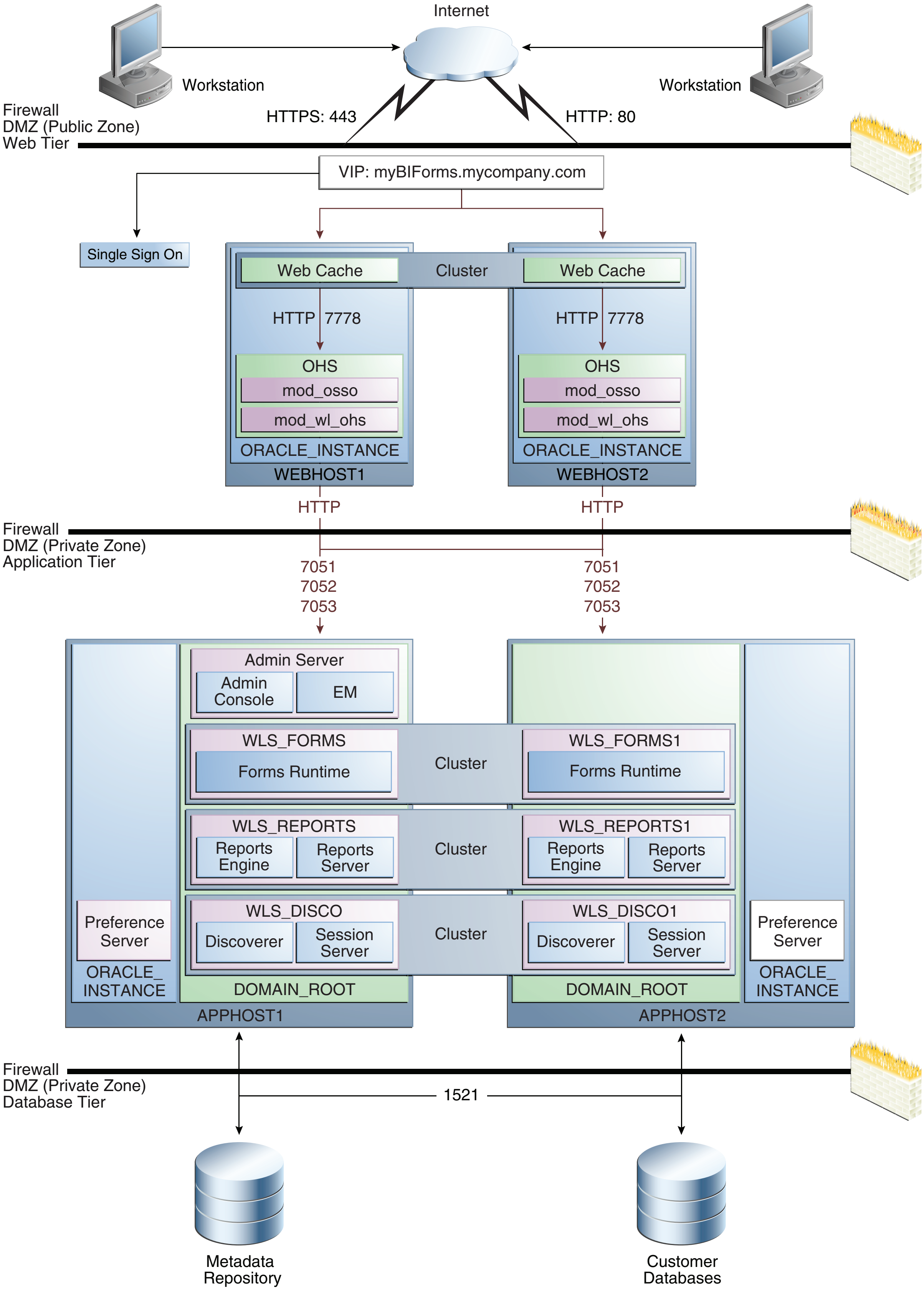


Figure 4–7 shows the Oracle Forms, Reports, and Discoverer enterprise topology diagram. The volume design and consistency groups described in Section 4.1.1.4.1, "Volume Design for Oracle Portal, Forms, Reports, and Discover" and Section 4.1.1.4.2, "Consistency Group Recommendations for Oracle Portal, Forms, Reports, and Discoverer" can be used for a Disaster Recovery site that includes this topology.

Detailed information about the Oracle Forms, Reports, and Discoverer enterprise topology in Figure 4–7 is available in the 11.1.1.2 *Oracle Forms, Reports, and Discoverer Enterprise Deployment Guide*. See Article ID 952068.1 "Oracle Fusion Middleware 11g (11.1.1.2) Enterprise Deployment Guides for Portal, Forms, Reports, and Discover" at My Oracle Support (formerly Oracle *MetaLink*) for information on obtaining the manual. The URL for My Oracle Support is:

http://support.oracle.com

***Figure 4–7 Oracle Forms, Reports, and Discoverer Topology***


Internet
Workstation
Workstation
Firewall
DMZ (Public Zone)
Web Tier
HTTPS: 443
HTTP: 80
VIP: myBIForms.mycompany.com
Single Sign On
Web Cache
Cluster
Web Cache
HTTP
7778
HTTP
7778
OHS
mod_osso
mod_wl_ohs
ORACLE_INSTANCE
WEBHOST1
OHS
mod_osso
mod_wl_ohs
ORACLE_INSTANCE
WEBHOST2
HTTP
HTTP
Firewall
DMZ (Private Zone)
Application Tier
7051
7052
7053
7051
7052
7053
Admin Server
Admin Console
EM
WLS_FORMS
Forms Runtime
Cluster
WLS_FORMS1
Forms Runtime
WLS_REPORTS
Reports Engine
Reports Server
Cluster
WLS_REPORTS1
Reports Engine
Reports Server
WLS_DISCO
Discoverer
Session Server
Cluster
WLS_DISCO1
Discoverer
Session Server
Preference Server
ORACLE_ INSTANCE
DOMAIN_ROOT
APPHOST1
DOMAIN_ROOT
Preference Server
ORACLE_ INSTANCE
APPHOST2
Firewall
DMZ (Private Zone)
Database Tier
1521
Metadata Repository
Customer Databases

**4.1.1.4.1 Volume Design for Oracle Portal, Forms, Reports, and Discover** Oracle recommends the following volume design for a Disaster Recovery site that includes both the Oracle Portal topology shown in Figure 4–6 and the Oracle Forms, Reports, and Discoverer topology shown in Figure 4–7:

- Provision one volume on each of the application tier hosts for the Middleware Homes. This volume will also contain the WebLogic Server Home, Oracle home for the Oracle Portal, Reports, Forms, and Discoverer components, and the domain directory for the Administration Server and Managed Server running on that host. These are VOLPFRD1 and VOLPFRD2 in Table 4–8.
- Provision one volume on each node for the Oracle homes in the web tier. These are VOLWEB1 and VOLWEB2 in Table 4–8.
- Provision one volume on each node for the Oracle instance homes in the directory web tier. These are VOLWEBINST1 and VOLWEBINST2 in Table 4–8.
- Provision one volume on each node for the Oracle Instance homes in the application tier. This volume is shared by the Administration Server and Managed Server instances. These are VOLPFRDINST1 and VOLPFRDINST2 in Table 4–8.
- Provision one volume for the Oracle Reports output directory in the application tier. This volume is mounted on all the nodes running the Oracle Reports server. This is VOLREPOUT in Table 4–6.

Table 4–8 provides a summary of Oracle recommendations for volume design for a Disaster Recovery site that includes both the Oracle Portal topology shown in Figure 4–6 and the Oracle Forms, Reports, and Discoverer topology shown in Figure 4–7:

*Table 4–8 Volume Design Recommendations for Oracle Portal, Reports, Forms, and Discoverer*

| Tier | Volume Name | Mounted on Host | Mount Point | Comments |
|---|---|---|---|---|
| Web | VOLWEB1 | WEBHOST1 | /u01/app/oracle/product/fmw/web | Volume for Oracle HTTP Server installation |
| Web | VOLWEB2 | WEBHOST2 | /u01/app/oracle/product/fmw/web | Volume for Oracle HTTP Server installation |
| Web | VOLWEBINST1 | WEBHOST1 | /u01/app/oracle/admin/ohs_instance | Volume for Oracle HTTP Server instance |
| Web | VOLWEBINST2 | WEBHOST2 | /u01/app/oracle/admin/ohs_instance | Volume for Oracle HTTP Server instance |
| Web | VOLSTATIC1[1] | WEBHOST1 | /u01/app/oracle/admin/ohs_instance/config/static | Volume for static HTML content |
| Web | VOLSTATIC2[2] | WEBHOST2 | /u01/app/oracle/admin/ohs_instance/config/static | Volume for static HTML content |
| Application | VOLPFRD1 | APPHOST1 | /u01/app/oracle/product/fmw | Volume for the WebLogic Server and Oracle Portal, Forms, Reports, and Discoverer binaries. |
| Application | VOLPFRD2 | APPHOST2 | /u01/app/oracle/product/fmw | Volume for the WebLogic Server and Oracle Portal, Forms, Reports, and Discoverer binaries. |

*Table 4–8 (Cont.) Volume Design Recommendations for Oracle Portal, Reports, Forms, and Discoverer*

| Tier | Volume Name | Mounted on Host | Mount Point | Comments |
|---|---|---|---|---|
| Application | VOLPFRDINST 1 | APPHOST1 | /u01/app/oracle/admin | Volume for Oracle instances |
| Application | VOLPFRDINST 2 | APPHOST2 | /u01/app/oracle/admin | Volume for Oracle instances |
| Application | VOLREPOUT | APPHOST1, APPHOST2 | /u01/app/oracle/admin | Volume for report output |

[1] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

[2] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it

**4.1.1.4.2 Consistency Group Recommendations for Oracle Portal, Forms, Reports, and Discoverer** Oracle recommends the following consistency groups for a Disaster Recovery site that includes both the Oracle Portal topology shown in Figure 4–6 and the Oracle Forms, Reports, and Discoverer topology shown in Figure 4–7:

- Create one consistency group with the volumes containing the web tier Oracle homes as members. This is WEBHOMEGROUP in Table 4–9.
- Create one consistency group with the volumes containing the web tier Oracle Instances as members. This is WEBINSTGROUP in Table 4–9.
- Create one consistency group with the volumes containing the application tier Middleware homes. This is PFRDMWGROUP in Table 4–9.
- Create one consistency group with the volumes containing the application tier Oracle instance homes. This is PFRDINSTGROUP in Table 4–9.
- Create one consistency group with the volume containing the Oracle Reports output directory as a member. This is REPOUTGROUP in Table 4–9.

Table 4–9 summarizes the consistency group recommendations for a Disaster Recovery site that includes both the Oracle Portal topology shown in Figure 4–6 and the Oracle Forms, Reports, and Discoverer topology shown in Figure 4–7.

*Table 4–9 Consistency Groups for Oracle Portal, Forms, Reports, and Discoverer*

| Tier | Volume Name | Members | Comments |
|---|---|---|---|
| Application | PFRDMWGROUP | VOLPFRD2<br>VOLPFRD2 | Consistency group for Middleware homes |
| Application | PFRDINSTGROUP | VOLPFRDINST1<br>VOLPFRDINST2 | Consistency group for the instance homes |
| Application | REPOUTGROUP | VOLREPOUT | Consistency group for the Reports output directory |
| Web | WEBHOMEGROUP | VOLWEB1<br>VOLWEB2 | Consistency group for the Oracle HTTP Server Oracle homes |
| Web | WEBINSTGROUP | VOLWEBINST1<br>VOLWEBINST2<br>VOLSTATIC1[1]<br>VOLSTATIC2[2] | Consistency group for the Oracle HTTP Server Oracle instance |

[1] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

[2] This volume for static HTML data is optional. Oracle Fusion Middleware will operate normally without it.

### 4.1.2 Storage Replication

Follow these steps to set up storage replication for the Oracle Fusion Middleware Disaster Recovery topology:

1. On the standby site, ensure that aliases host names are created that are the same as the physical host names used for the peer hosts at the production site.
2. On the shared storage at the standby site, create the same volumes as were created on the shared storage at the production site.
3. On the standby site, create the same mount points and symbolic links that you created at the production site (note that symbolic links only need to be set up on the standby site if you set up symbolic links at the production site). Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links.
4. It is not necessary to install the same Oracle Fusion Middleware instances at the standby site as were installed at the production site. When the production site storage is replicated to the standby site storage, the Oracle software installed on the production site volumes will be replicated at the standby site volumes.
5. Perform any other necessary configuration required by the shared storage vendor to enable storage replication between the production site shared storage and the standby site shared storage.
6. Create the baseline snapshot copy of the production site shared storage that sets up the replication between the production site and standby site shared storage. Create the initial baseline copy and subsequent snapshot copies using asynchronous replication mode. After the baseline snapshot copy is performed, validate that all the directories inside the standby site volumes have the same contents as the directories inside the production site volumes.
7. Set up the frequency of subsequent copies of the production site shared storage, which will be replicated at the standby site. When asynchronous replication mode is used, then at the requested frequency the changed data blocks at the production site shared storage (based on comparison to the previous snapshot copy) become the new snapshot copy, and the snapshot copy is transferred to the standby site shared storage.
8. Ensure that disaster protection for any database that is included in the Oracle Fusion Middleware Disaster Recovery production site is provided by Oracle Data Guard. Do not use storage replication technology to provide disaster protection for Oracle databases.
9. The standby site shared storage receives snapshots transferred on a periodic basis from the production site shared storage. After the snapshots are applied, the standby site shared storage will include all the data up to and including the data contained in the last snapshot transferred from the production site before the failover or switchover.
10. It is strongly recommended to manually force a synchronization operation whenever a change is made to the middle tier at the production site (for example, when a new application is deployed at the production site). Follow the vendor-specific instructions for forcing a synchronization using storage replication technology.

## 4.1.3 Database

See Section 3.3, "Database Considerations" for recommendations and considerations for setting up Oracle databases that will be used in the Oracle Fusion Middleware Disaster Recovery topology.

### 4.1.3.1 Setting Up Oracle Data Guard

Oracle Data Guard should be set up between the Oracle Fusion Middleware Repository databases on the primary site and standby site. The databases on the standby site should be set up as Physical Standby Databases. This section describes the setup and configuration of the data tier on the standby site.

For more information regarding Oracle Data Guard, refer to *Oracle Data Guard Concepts and Administration* in the Oracle Database documentation set.

**4.1.3.1.1 Prerequisites and Assumptions** The Oracle Data Guard setup and configuration steps below assume that the following conditions are met:

- The RAC cluster and ASM instances on the standby site have been created.
- The RAC databases on the standby site and the production site are using a Flash Recovery Area.
- The database hosts on the standby site already have Oracle software installed.
- The physical path for the DB_HOME on the standby site matches that of the production site.

**4.1.3.1.2 Oracle Data Guard Environment Description** The Oracle Data Guard steps use the environment variables shown inTable 4–10 for the SOA database at the production site.

*Table 4–10 Environment Variables Used for SOA Databases at the Production Site*

| Variable | Value |
|---|---|
| SOA Database Host Names | soadbhost1.mycompany.com<br>soadbhost2.mycompany.com |
| ORACLE_HOME | /u01/app/oracle/product/db_1 |
| SOA_DBNAME | PSOA |
| SOA_DB_UNIQUE_NAME | PSOA |
| SOA_DB_INSTANCE_NAMES | PSOA1, PSOA2 |

The Oracle Data Guard steps use the environment variables shown in Table 4–11 for the SOA database at the standby site.

*Table 4–11 Environment Variables Used for SOA Databases at the Standby Site*

| Variable | Value |
|---|---|
| SOA Database Host Names | soadbhost1.mycompany.com<br>soadbhost2.mycompany.com |
| ORACLE_HOME | /u01/app/oracle/product/db_1 |
| SOA_DBNAME | SSOA |
| SOA_DB_UNIQUE_NAME | SSOA |
| SOA_DB_INSTANCE_NAMES | SSOA1, SSOA2 |

These high level steps for setting up Oracle Data Guard are described in detail in the following sections:

- Gather Files and Perform Backup
- Configure Oracle Net Services on the Standby Site
- Create Instances and Database on the Standby Site
- Test Database Switchover and Switchback

**4.1.3.1.3 Gather Files and Perform Backup** Follow these steps to gather files and perform the database backup:

1. On the SOADBHOST1 of the primary site, create a directory for staging purposes. For example:

   ```
   $ mkdir -p /u01/app/stage/psoa
   ```

2. Create the exact path on SOADBHOST1 of the standby site. Follow the example shown in step 1.
3. On the SOADBHOST1 of the primary site, connect to the database instance psoa1 and create a pfile from the spfile. For example:

   ```
   SQL > create pfile='/u01/app/stage/psoa/initpsoa.ora' from spfile;
   ```

4. On the SOADBHOST1 of the primary site, connect to RMAN, perform a backup of the database, and place the backup files in the stage directory. For example:

   ```
   $ $ORACLE_HOME/bin/rman target /

   RMAN> backup device type disk format '/u01/app/stage/psoa/%U' database plus
   archivelog;

   RMAN> backup device type disk format '/u01/app/stage/psoa/%U' current
   controlfile for standby;
   ```

5. Follow the steps below to validate that the backups created by RMAN are valid.
6. Connect to RMAN on SOADBHOST1 of the primary site and then list the backup summary.
7. Validate the backup sets created by RMAN in step 4:

   ```
   RMAN> list backup summary;
   using target database control file instead of recovery catalog
   List of Backups
   ===============
   Key     TY LV S Device Type Completion Time #Pieces #Copies Compressed Tag
   ------- -- -- - ----------- --------------- ------- ------- ---------- ---
   93      B  A  A DISK        14-MAY-07       1       1       NO
   TAG20070514T122312
   94      B  F  A DISK        14-MAY-07       1       1       NO
   TAG20070514T122315
   95      B  F  A DISK        14-MAY-07       1       1       NO
   TAG20070514T122315
   96      B  A  A DISK        14-MAY-07       1       1       NO
   TAG20070514T122629
   97      B  F  A DISK        14-MAY-07       1       1       NO
   TAG20070514T123220

   RMAN> validate backupset 93;
   allocated channel: ORA_DISK_1
   ```

```
channel ORA_DISK_1: sid=451 instance=psoa1 devtype=DISK
channel ORA_DISK_1: starting validation of archive log backupset
channel ORA_DISK_1: reading from backup piece /u01/app/stage/psoa/34ihmtdg_1_1
channel ORA_DISK_1: restored backup piece 1
piece handle=/u01/app/stage/psoa/34ihmtdg_1_1 tag=TAG20070514T122312
channel ORA_DISK_1: validation complete, elapsed time: 00:00:02
```

8. On SOADBHOST1 of the primary site, copy the `listener.ora`, `sqlnet.ora`, and `tnsnames.ora` files from the *$ORACLE_HOME*`/network/admin` directory to the staging directory.
9. Using operating system utilities, copy the contents of staging directory on SOADBHOST1of the primary site to the staging directory on SOADBHOST1 of the standby site.

**4.1.3.1.4 Configure Oracle Net Services on the Standby Site** Follow these steps to configure Oracle Net Services on the standby site:

1. Copy the `listener.ora`, `sqlnet.ora`, and `tnsnames.ora` files from the staging directory on SOADBHOST1 on the primary site to the *$ORACLE_HOME*`/network/admin` directory on all the nodes of the standby site.
2. Modify the `listener.ora` file on each of the standby host to contain the virtual IP of that host.
3. Modify the `tnsnames.ora` file on each node, including the primary RAC nodes and standby RAC nodes, to contain all primary and standby net service names.
4. Modify the Oracle Net aliases that are used for the local_listener and remote_listener parameters to point to the listener on each standby host. The example below shows excerpts from the `tnsnames.ora` file:

```
#local_listener
PSOA =
(DESCRIPTION =
(ADDRESS =
(PROTOCOL = TCP)
(HOST = soadbhost1-vip)
(HOST = soadbhost2-vip)
(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = psoa)
)
)
#remote_listener
SSOA =
(DESCRIPTION =
(ADDRESS =
(PROTOCOL = TCP)
(HOST = soadbhost1-vip)
(HOST = soadbhost2-vip)
(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = ssoa)
)
)
```

5. Start the listeners on the standby database hosts.

#### 4.1.3.1.5 Create Instances and Database on the Standby Site

Follow these steps to create instances and the database on the standby site:

1. To enable secure transmission of redo data, make sure the databases on the primary and standby sites use a password file, and make sure the password for the SYS user is identical on every system. Create a password file on both the nodes of the standby databases. For example:

   On SOADBHOST1 of the standby site

   ```
   $ cd $ORACLE_HOME/dbs
   $ orapwd file=orapwpsoa1 password=welcome1
   ```

   On SOADBHOST2 of the standby site

   ```
   $ cd $ORACLE_HOME/dbs
   $ orapwd file=orapwpsoa2 password=welcome1
   ```

2. Copy and rename the pfile from the staging area to the `$ORACLE_HOME/dbs` directory on SOADBHOST1 of the standby site. For example:

   ```
   $ cp /u01/app/stage/psoa/initpsoa.ora $ORACLE_HOME/dbs/initpsoa1.ora
   ```

3. Modify the standby initialization parameter file copied from the primary node to include the parameters shown Table 4–12:

*Table 4–12 Parameters to Specify in the Standby Initialization Parameter File*

| Parameter | Value |
|---|---|
| RAC Parameters | *.cluster_database=true |
| | PSOA1.instance_name=PSOA1 |
| | PSOA2.instance_name=PSOA2 |
| | PSOA1.instance_number=1 |
| | PSOA2.instance_number=2 |
| | PSOA1.thread=1 |
| | PSOA1.thread=2 |
| | PSOA1.undo_tablespace=UNDOTBS1 |
| | PSOA2.undo_tablespace=UNDOTBS2 |
| | *.remote_listener=LISTENERS_PSOA |
| Data Guard Parameters | *.db_unique_name=SSOA |
| | *.log_archive_config='dg_config=(SSOA,PSOA)' |
| | *.log_archive_dest_2='service=PSOA valid_for=(online_logfiles,primary_role) db_unique_name=PSOA' |
| | *.db_file_name_convert='+DATA/PSOA/','+DATA/SSOA/','+RECO/PSOA','+RECO/SSOA' |
| | *.log_file_name_convert='+DATA/PSOA/','+DATA/SSOA/','+RECO/PSOA','+RECO/SSOA' |
| | *.standby_file_management=auto |
| | *.fal_server='PSOA' |
| | *.fal_client='SSOA' |

*Table 4–12 (Cont.) Parameters to Specify in the Standby Initialization Parameter File*

| Parameter | Value |
|---|---|
| Miscellaneous Parameters | *.background_dump_dest=/u01/app/admin/PSOA/bdump<br>*.core_dump_dest=/u01/app/admin/PSOA/cdump<br>*.user_dump_dest=/u01/app/admin/PSOA/udump<br>*.audit_file_dest=/u01/app/admin/PSOA/adump<br>*.db_recovery_dest='+RECO'<br>*.log_archive_dest_3='LOCATION=USE_DB_RECOVERY_FILE_DEST'<br>*.dispatchers=PSOAXDB |

4. Connect to the ASM instance on SOADBHOST1 of the standby site, and create a directory within the DATA disk group that has the same name as the DB_UNIQUE_NAME of the standby database. For example:

```
SQL> alter diskgroup data add directory '+DATA/SSOA';
```

5. Connect to the standby database on SOADBHOST1 of the standby site, with the standby database in the IDLE state, and create an SPFILE in the standby DATA disk group. For example:

```
SQL> CREATE SPFILE='+DATA/SSOA/spfilepsoa.ora' FROM
PFILE='?/dbs/initpsoa1.ora';
```

6. In the *$ORACLE_HOME*/dbs directory on SOADBHOST1 and SOADBHOST2 of the standby site, create a PFILE that contains a pointer to the SPFILE. The PFILE should follow the naming convention init<OracleSID>.ora. For example:

   On SOADBHOST1:

```
$ cd $ORACLE_HOME/dbs
$ echo "SPFILE='+DATA/SSOA/spfilepsoa.ora'" > initpsoa1.ora
```

   On SOADBHOST2:

```
$ cd $ORACLE_HOME/dbs
$ echo "SPFILE='+DATA/SSOA/spfilepsoa.ora'" > initpsoa2.ora
```

7. Create the dump directories on all standby hosts as referenced in the standby initialization parameter file. For example:

```
$ mkdir -p $ORACLE_BASE/admin/psoa/bdump
$ mkdir -p $ORACLE_BASE/admin/psoa/cdump
$ mkdir -p $ORACLE_BASE/admin/psoa/udump
$ mkdir -p $ORACLE_BASE/admin/psoa/adump
```

8. On SOADBHOST1 of the standby site, set the ORACLE_HOME, PATH, ORACLE_SID and startup the standby database without mounting the control file. This host should have the staging directory. For example:

```
SQL > startup nomount
```

9. From SOADBHOST1 of the primary site where the standby instance was just started, duplicate the primary database as a standby into the ASM disk group by using RMAN. For example:

```
$ rman target sys/oracle@psoa auxiliary /
RMAN> duplicate target database for standby;
```

10. Use SQL*Plus to log in to the newly created database to validate that it was created correctly. For example:

    ```
    $ sqlplus '/as sysdba'
    ```

11. Connect to the standby database on SOADBHOST1 of the standby site, and create the standby redo logs to support the standby role. For example:

    ```
    SQL> ALTER DATABASE ADD STANDBY LOGFILE THREAD 1
    GROUP 5 SIZE 300M,
    GROUP 6 SIZE 300M,
    GROUP 7 SIZE 300M;

    SQL> ALTER DATABASE ADD STANDBY LOGFILE THREAD 2
    GROUP 8 SIZE 300M,
    GROUP 9 SIZE 300M,
    GROUP 10 SIZE 300M;
    ```

12. On SOADBHOST1 of the standby site, start managed recovery and real-time apply on the standby database. For example:

    ```
    SQL> ALTER DATABASE recover managed standby database using current logfile
    disconnect;
    ```

13. On SOADBHOST1 and SOADBHOST2 of the standby site, register the standby database and the database instances with the Oracle Cluster Registry (OCR) using the Server Control (SRVCTL) utility. For example:

    ```
    $ srvctl add database -d psoa -o /u01/app/oracle/product/10.2.0/db_1
    $ srvctl add instance -d psoa -i psoa1 -n soadbhost1
    $ srvctl add instance -d psoa -i psoa2 -n soadbhost2
    ```

14. Establish a dependency between the database and the ASM instance. For example:

    ```
    $ srvctl modify instance -d psoa -i psoa1 -s +ASM1
    $ srvctl modify instance -d psoa -i psoa2 -s +ASM2
    $ srvctl enable asm -n stbdd03 -i +ASM1
    $ srvctl enable asm -n stbdd04 -i +ASM2
    ```

15. Configure the primary database for Oracle Data Guard by modifying/adding the Data Guard parameters in the primary initialization file to the values shown below:

    ```
    *.log_archive_config='dg_config=(SSOA,PSOA)'

    *.log_archive_dest_2='service=SSOA valid_for=(online_logfiles,primary_role) db_
    unique_name=SSOA'

    *.db_file_name_convert='+DATA/SSOA/','+DATA/PSOA/','+RECO/SSOA','+RECO/PSOA'

    *.log_file_name_convert='+DATA/SSOA/','+DATA/PSOA/','+RECO/SSOA','+RECO/PSOA'

    *.standby_file_management=auto

    *.fal_server='PSOA'

    *.fal_client='PSOA'
    ```

16. Restart the primary database after modifying the parameters.

17. Create the standby redo logs on the primary database to support the standby role. For example:

    ```
    SQL> ALTER DATABASE ADD STANDBY LOGFILE THREAD 1
    GROUP 5 SIZE 300M,
    GROUP 6 SIZE 300M,
    GROUP 7 SIZE 300M;

    SQL> ALTER DATABASE ADD STANDBY LOGFILE THREAD 2
    GROUP 8 SIZE 300M,
    GROUP 9 SIZE 300M,
    GROUP 10 SIZE 300M;
    ```

18. Verify the Oracle Data Guard configuration by querying the V$ARCHIVED_LOG view to identify existing files in the archived redo log. For example:

    ```
    SQL> select sequence#, first_time, next_time from v$archived_log order by
    sequence#;
    ```

19. On the primary database, issue the following SQL statement to force a log switch and archive the current online redo log file group:

    ```
    SQL> alter system archive log current;
    ```

20. On the standby database, query the V$ARCHIVED_LOG view to verify that the redo data was received and archived on the standby database:

    ```
    SQL> select sequence#, first_time, next_time from v$archived_log order by
    sequence#;
    ```

**4.1.3.1.6 Test Database Switchover and Switchback** Follow these steps to test that the database switchover and switchback operation works correctly between the newly-created physical standby database and the primary RAC databases:

1. Shutdown all but one instance of the RAC databases (PSOA) on the primary site. For example, run the command below on SOADBHOST1 of the production site:

    ```
    $ srvctl stop instance -d psoa -i psoa2
    ```

2. Initiate the role transition to the physical standby on the current primary database. For example, run the command below on SOADBHOST1 of the production site:

    ```
    SQL > ALTER DATABASE COMMIT TO SWITCHOVER TO PHYSICAL STANDBY WITH SESSION
    SHUTDOWN;
    ```

3. Shut down the primary instance and mount the primary instance. For example, run the command below on SOADBHOST1 of the production site:

    ```
    SQL > shutdown immediate
    SQL > startup mount
    ```

4. At this point, both the databases are in Physical Standby mode. To verify that both the databases are in Physical Standby mode, run this SQL query on both the databases:

    ```
    SQL> select database_role from v$database;
    DATABASE_ROLE
    ----------------
    PHYSICAL_STANDBY
    ```

5. Switch the physical standby database role to the primary role. For example, run the command below on SOADBHOST1 of the standby site:

   ```
   SQL> ALTER DATABASE COMMIT TO SWITCHOVER TO PRIMARY WITH SESSION SHUTDOWN;
   ```

6. Now the physical standby database is the new primary.
7. Shut down the new primary database and start up both the RAC nodes using srvctl. For example, run the following command on the SOADBHOST1 of the standby site:

   ```
   srvctl start database -d psoa
   ```

8. On the new physical standby database (the old primary) start the managed recovery of the database. For example, run the command below on SOADBHOST1 of the primary site:

   ```
   SQL> ALTER DATABASE RECOVER MANAGED STANDBY DATABASE DISCONNECT FROM SESSION;
   ```

9. Start sending the redo data to the new physical standby database. For example, run the command below on SOADBHOST1 of the standby site:

   ```
   SQL> ALTER SYSTEM SWITCH LOGFILE;
   ```

10. Check the new physical standby database to see if it is receiving the archive log files by querying the V$ARCHIVED_LOG view.

### 4.1.4 Node Manager

The Node Manager communicates with the Administration Server over SSL. For this communication to work correctly on the standby site, you must create SSL certificates using the physical host names. This section includes these topics:

- Generate Self Signed Certificates
- Create an Identity KeyStore
- Create Trust KeyStore
- Configure Node Manager for Custom KeyStores

The examples in these sections show how to perform these tasks for the Oracle SOA Suite enterprise topology shown in Figure 4–2.

> **Note:** Remember that when you are setting up the Oracle SOA Suite enterprise topology shown in Figure 4–2 as the production site for a Disaster Recovery topology, you must use the physical host names shown in Table 3–1 for the production site hosts instead of the host names shown in Figure 4–2.
>
> The steps in this section must performed on the application tier hosts on which WebLogic Server is installed.

#### 4.1.4.1 Generate Self Signed Certificates

Follow these steps to generate self signed certificates:

1. Set your environment using the `setWLSenv` script located under the *$WL_HOME*`/server/bin` directory.

2. Create a user-defined directory for the certificates. For example, create the certs directory under the *$MW_HOME*/user_projects/domains/SOADomain directory.

3. Run the utils.CertGen tool from the user-defined directory to create the certificates for the application tier hosts on which WebLogic Server is installed. The syntax is:

   ```
   Syntax: java utils.CertGen <key_passphrase> <cert_file_name> <key_file_name>
   [export|domestic] [hostname]
   ```

   For example, enter these commands:

   ```
   java utils.CertGen welcome1 soahost1_cert soahost1_key domestic soahost1
   java utils.CertGen welcome1 soahost2_cert soahost2_key domestic soahost2
   ```

#### 4.1.4.2 Create an Identity KeyStore

Follow these steps to create an identity keystore using the utils.ImportPrivateKey utility:

1. Create a new identity keystore called appIdentityKeyStore using the utils.ImportPrivateKey utility.

2. Create this keystore under the same directory as the certificates, for example:

   ```
   $MW_HOME/user_projects/domains/j2eeDomain/certs
   ```

3. 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.

4. Import the certificate and private key for the application tier hosts on which WebLogic Server is installed into the Identity Store; also make sure to use a different alias for each of the certificate/key pair imported. The syntax is:

   ```
   Syntax: java utils.ImportPrivateKey <keystore_file> <keystore_password>
   <certificate_alias_to_use> <private_key_passphrase> <certificate_file>
   <private_key_file> [<keystore_type>]
   ```

   For example, enter these commands:

   ```
   java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1 appIdentity1
   welcome1 $MW_HOME/user_projects/domains/SOADomain/certs/soahost1_cert.pem
   $MW_HOME/user_projects/domains/SOADomain/certs/soahost1_key.pem

   java utils.ImportPrivateKey appIdentityKeyStore.jks welcome1 appIdentity2
   welcome1 $MW_HOME/user_projects/domains/SOADomain/certs/soahost2_cert.pem
   $MW_HOME/user_projects/domains/SOADomain/certs/soahost2_key.pem
   ```

#### 4.1.4.3 Create Trust KeyStore

Follow these steps to create a trust keystore:

1. Create a new trust keystore called appTrustKeyStore using the keytool utility.

2. Use the standard java keystore to create the new trust keystore since it already contains most of the root CA certificates needed. It is recommended not to modify the standard Java trust key store directly.

3. Copy the standard Java keystore `cacerts` located under the *$WL_HOME*`/server/lib` directory to the same directory as the certificates. For example:

   ```
   cp $WL_HOME/server/lib/cacerts
   $MW_HOME/user_projects/domains/SOADomain/certs/appTrustKeyStore.jks
   ```

4. The default password for the standard Java keystore is `changeit` and it is always recommended to change the default password. Use the keytool utility to do this. The syntax is:

   ```
   keytool -storepasswd -new <NewPassword> -keystore <TrustKeyStore> -storepass
   <Original Password>
   ```

   For example, enter this command:

   ```
   keytool -storepasswd -new welcome1 -keystore appTrustKeyStore.jks -storepass
   changeit
   ```

5. The CA certificate `CertGenCA.der` is used to sign all certificates generated by `utils.CertGen` tool and is located at *$WL_HOME*`/server/lib` directory. This CA certificate must be imported into the appTrustKeyStore using the `keytool` utility. The syntax is:

   ```
   keytool -import -v -noprompt -trustcacerts -alias <AliasName> -file
   <CAFileLocation> -keystore <KeyStoreLocation> -storepass <KeyStore Password>
   ```

   For example, enter this command:

   ```
   keytool -import -v -noprompt -trustcacerts -alias clientCACert -file
   $WL_HOME/server/lib/CertGenCA.der -keystore appTrust.jks -storepass welcome1
   ```

### 4.1.4.4 Configure Node Manager for Custom KeyStores

Configure Node Manager on each of the nodes to use the newly-created custom keystores by editing the following lines at the end of the `nodemanager.properties` file located under the *$WL_HOME*`/common/nodemanager` directory. These lines and their meanings are shown below:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=<Identity KeyStore>
CustomIdentityKeyStorePassPhrase=<Identity KeyStore Password>
CustomIdentityAlias=<Identity Key Store Alias>
CustomIdentityPrivateKeyPassPhrase=<Private Key used when creating Certificate>
CustomTrustKeyStoreFileName=<Trust KeyStore>
CustomTrustKeyStorePassPhrase=<Trust KeyStore Password>
```

For example, make these edits in the `nodemanager.properties` file on SOAHOST1:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=$MW_HOME/user_projects/domains/SOADomain/certs
/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=welcome1
CustomIdentityAlias=appIdentity1
CustomIdentityPrivateKeyPassPhrase=welcome1
CustomTrustKeyStoreFileName=$MW_HOME/user_projects/domains/SOADomain/certs
/appTrust.jks
CustomTrustKeyStorePassPhrase=welcome1
```

For example, make these edits in the `nodemanager.properties` file on SOAHOST2:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=$MW_HOME/user_projects/domains/SOADomain/certs
/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=welcome1
CustomIdentityAlias=appIdentity2
CustomIdentityPrivateKeyPassPhrase=welcome1
CustomTrustKeyStoreFileName=$MW_HOME/user_projects/domains/SOADomain/certs
/appTrust.jks
CustomTrustKeyStorePassPhrase=welcome1
```

## 4.2 Creating a Production Site

This section provides the steps to create the production site. The Oracle SOA enterprise deployment topology and the Oracle Identity Management Enterprise deployment topology are used as examples.

Ensure that you have performed the following prerequisites before you start creating the production site:

- Set up the host name aliases for the middle tier hosts, which was described in Section 3.1.1, "Planning Host Names."
- Create the required volumes on the shared storage on the production site, which was described in Section 4.1.1, "Directory Structure and Volume Design."
- Create the mount points and the symbolic links (if required). Refer to Section 3.2.3, "Storage Replication" to determine whether you must create symbolic links for the production site.

### 4.2.1 Creating the Production Site for the Oracle SOA Suite Topology

The production site should be installed and configured as described in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite* with the following variations. The steps to install and configure the production site are listed below and should be followed in the sequence listed.

1. Create volumes and consistency groups on the shared storage device, as described in Section 4.1.1.1.1, "Volume Design for Oracle SOA Suite."
2. Set up physical host names on the production site and physical host names and alias host names for the standby site. See Section 3.1.1, "Planning Host Names" for information on planning host names for the production and standby sites.
3. Install and configure Oracle SOA Suite as described in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite* with the following modifications:
    a. Install the Oracle SOA Suite components into the volumes created on the shared storage device.
    b. Use the physical host names when installing and configuring WebLogic domain.
    c. Create a separate volume on each site for the JMS stores and transaction logs.
    d. After the installation and configuration of the production site, turn off host name verification. See the "Disabling Host Name Verification for the Oracle WebLogic Administration Server and the WLS_WSM1 Managed Server" section in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite* for detailed instructions about turning off host name verification for an Administration Server and Managed Server.

e. If you do not plan on turning host name verification off, follow the steps in Section 4.1.4, "Node Manager" to configure Node Manager communication.

f. Create SSL certificates using the host name aliases on all of the Oracle Fusion Middleware hosts for proper Node Manager communication.

### 4.2.2 Creating the Production Site for the Oracle Identity Management Topology

The production site should be installed and configured as described in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* with the following variations. The steps to install and configure the production site are listed below and should be followed in the sequence listed.

1. Create volumes and consistency groups on the shared storage device, as described in Section 4.1.1.3.1, "Volume Design for Oracle Identity Management."
2. Set up physical host names on the production site and physical host names and alias host names for the standby site. See Section 3.1.1, "Planning Host Names" for information on planning host names for the production and standby sites.
3. Install and configure Oracle Identity Management as described in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* with the following modifications:

   a. Install the Oracle Identity Management components into the volumes created on the shared storage device.

   b. Use the physical host names when installing and configuring the WebLogic domain.

   c. Create a separate volume on each site for the JMS stores and transaction logs.

   d. After the installation and configuration of the production site, turn off host name verification. See the "Disabling Host Name Verification for the Oracle WebLogic Administration Server and the WLS_WSM1 Managed Server" section in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite* for detailed instructions about turning off host name verification for an Administration Server and Managed Server.

   e. If you do not plan on turning host name verification off, follow the steps in Section 4.1.4, "Node Manager" to configure Node Manager communication.

   f. Create SSL certificates using the host name aliases on all of the Oracle Fusion Middleware hosts for proper Node Manager communication.

### 4.2.3 Creating the Production Site for the Oracle WebCenter Topology

The production site should be installed and configured as described in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter* with the following variations. The steps to install and configure the production site are listed below and should be followed in the sequence listed.

1. Create volumes and consistency groups on the shared storage device, as described in Section 4.1.1.2.1, "Volume Design for Oracle WebCenter."
2. Set up physical host names on the production site and physical host names and alias host names for the standby site. See Section 3.1.1, "Planning Host Names" for information on planning host names for the production and standby sites.
3. Install and configure Oracle WebCenter as described in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter* with the following modifications:

a. Install the Oracle WebCenter components into the volumes created on the shared storage device.

b. Use the physical host names when installing and configuring WebLogic domain.

c. After the installation and configuration of the production site, turn off host name verification. See the "Disabling Host Name Verification for the Oracle WebLogic Administration Server and the WLS_WSM1 Managed Server" section in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter* for detailed instructions about turning off host name verification for an Administration Server and Managed Server.

d. If you do not plan on turning host name verification off, follow the steps in Section 4.1.4, "Node Manager" to configure Node Manager communication.

e. Create SSL certificates using the host name aliases on all of the Oracle Fusion Middleware hosts for proper Node Manager communication.

### 4.2.4 Creating the Production Site for the Oracle Portal, Forms, Reports, and Discoverer Topology

The production site should be installed and configured as described in the enterprise deployment manuals for the following products:

- Oracle Portal:

  Detailed instructions for setting up and configuring a production site that uses the Oracle Portal enterprise topology shown in Figure 4–6 are provided in the 11.1.1.2 *Oracle Portal Enterprise Deployment Guide*. See Article ID 952068.1 "Oracle Fusion Middleware 11g (11.1.1.2) Enterprise Deployment Guides for Portal, Forms, Reports, and Discover" at My Oracle Support (formerly Oracle *MetaLink*) for information on obtaining the manual. The URL for My Oracle Support is:

  `http://support.oracle.com`

- Oracle Forms, Reports, and Discoverer

  Detailed instructions for setting up and configuring a production site that uses the Oracle Forms, Reports, and Discoverer enterprise topology shown in Figure 4–7 are provided in the 11.1.1.2 *Oracle Forms, Reports, and Discoverer Enterprise Deployment Guide*. See Article ID 952068.1 "Oracle Fusion Middleware 11g (11.1.1.2) Enterprise Deployment Guides for Portal, Forms, Reports, and Discover" at My Oracle Support (formerly Oracle *MetaLink*) for information on obtaining the manual. The URL for My Oracle Support is:

  `http://support.oracle.com`

Follow the installation and configuration instructions in the manuals above, except for the following variations. The following steps should be performed in the sequence listed:

1. Create volumes and consistency groups on the shared storage device, as described in Section 4.1.1.4.1, "Volume Design for Oracle Portal, Forms, Reports, and Discover."

2. Set up physical host names on the production site and physical host names and alias host names for the standby site. See Section 3.1.1, "Planning Host Names" for information on planning host names for the production and standby sites.

3. Install and configure Oracle Portal, Forms, Reports, and Discoverer as described in the white papers linked to above, with the following modifications:

a. Install the Oracle Portal, Forms, Reports, and Discoverer components into the volumes created on the shared storage device.

b. Use the physical host names when installing and configuring WebLogic domain.

c. After the installation and configuration of the production site, turn off host name verification. See the "Disabling Host Name Verification for the Oracle WebLogic Administration Server and the WLS_WSM1 Managed Server" section in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter* for detailed instructions about turning off host name verification for an Administration Server and Managed Server.

d. If you do not plan on turning host name verification off, follow the steps in Section 4.1.4, "Node Manager" to configure Node Manager communication.

e. Create SSL certificates using the host name aliases on all of the Oracle Fusion Middleware hosts for proper Node Manager communication.

### 4.2.5 Validating the Production Site Setup

To validate the production site setup for the Oracle SOA Suite enterprise topology, follow the validation steps in these sections of the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*:

- In the "Installing Oracle HTTP Server" chapter, follow the validation steps in this section:
  - "Validating Oracle HTTP Server Through the Load Balancer"
- In the "Creating a Domain" chapter, follow the validation steps in these sections:
  - "Validating the Administration Server"
  - "Starting and Validating the WLS_WSM1 Managed Server"
  - "Starting and Validating the WLS_WSM2 Managed Server"
  - "Validating Access Through Oracle HTTP Server"
  - "Validating Access to SOAHOST2 Through Oracle HTTP Server"
- In the "Extending the Domain for SOA Components" chapter, follow the validation steps in these sections:
  - "Validating the WLS_SOA1 and WLS_WSM1 Managed Servers"
  - "Starting and Validating the WLS_SOA2 Managed Server"
  - "Validating Access Through Oracle HTTP Server"
- In the "Extending the Domain to Include BAM" chapter, follow the validation steps in this section:
  - "Validating Access Through Oracle HTTP Server"

## 4.3 Creating a Standby Site

This section provides the steps to create the standby site. The Oracle SOA enterprise deployment topology and the Oracle Identity Management Enterprise deployment topology are used as examples.

## 4.3.1 Creating the Standby Site

Ensure that you have performed the following prerequisites before you start creating the standby site:

- On the standby site, ensure that you set up the correct alias host names and physical host names by following the instructions in Section 3.1.1, "Planning Host Names."

  Ensure that each standby site host has an alias host name that is the same as the physical host  name of its peer host at the production site.

- On the shared storage on the standby site, create the same volumes that were created on the shared storage at the production site.
- On the standby site, create the same mount points and symbolic links (if required) that you created at the production site. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links.

### 4.3.1.1 Database Setup

Oracle Data Guard should be set up between the Oracle Fusion Middleware Repository databases on the primary site and standby site. The databases on the standby site should be set up as physical standby databases. Refer to Section 4.1.3.1, "Setting Up Oracle Data Guard" for instructions on setting up Oracle Data Guard between databases running the metadata repositories on the primary and standby sites.

Also, ensure that the databases running the metadata repositories on the standby site are in the Managed Recovery mode. To enable the standby database to be in the managed recovery mode run the following SQL command (the disconnect option ends the SQL session after the command is completed successfully):

```
SQL> ALTER DATABASE RECOVERY MANAGED STANDBY DATABASE DISCONNECT FROM SESSION;
```

### 4.3.1.2 Middle Tier Setup

The middle tier hosts on the standby site do not require the installation or configuration of the of any Oracle Fusion Middleware or WebLogic Server software. When the production site storage is replicated to the standby site storage, the software installed on the production site volumes will be replicated at the standby site volumes.

Follow the steps below to set up the middle tier hosts on the standby site:

1. Create a baseline snapshot copy of shared storage on the production site, which sets up the replication between the storage devices. Create the initial baseline copy and subsequent snapshot copies using asynchronous replication mode.
2. Synchronize the shared storage at the production site with the shared storage at the standby site. This will transfer the initial baseline snapshot from the production site to the standby site.
3. Set up the frequency of subsequent copies of the production site shared storage, which will be replicated at the standby site. When asynchronous replication mode is used, then at the requested frequency the changed data blocks at the production site shared storage (based on comparison to the previous snapshot copy) become the new snapshot copy, and the snapshot copy is transferred to the standby site shared storage.

4. After the baseline snapshot copy is performed, validate that all the directories inside the standby site volumes have the same contents as the directories inside the production site volumes.

### 4.3.2 Validating the Standby Site Setup

Validate the standby site by following the steps below:

1. Shut down any processes still running on the production site. This includes the database instances in the data tier, Oracle Fusion Middleware instances and any other processes in the application tier and web tier.
2. Stop the replication between the production site shared storage and the standby site shared storage.
3. Use Oracle Data Guard to fail over the databases.
4. On the standby site hots, manually start all the processes. This includes the database instances in the data tier, Oracle Fusion Middleware instances and any other processes in the application tier and web tier.
5. Use a browser client to perform post-failover testing to confirm that requests are being resolved and redirected to the standby site.

## 4.4 Creating an Asymmetric Standby Site

The steps in this section describe how to set up an asymmetric Oracle Fusion Middleware Disaster Recovery topology.

An asymmetric topology is a disaster recovery configuration that is different across tiers at the production site and standby site. In most asymmetric Oracle Fusion Middleware Disaster Recovery topologies, the standby site has fewer resources than the production site.

Before you read this section, be sure to read and understand the concepts and information on setting up a symmetric topology presented earlier in this manual. Many of the concepts for setting up a symmetric topology are also valid for setting up an asymmetric topology.

Section 4.4.1, "Creating the Asymmetric Standby Site" describes the basic steps for creating an asymmetric topology. It does not describe in detail applicable concepts for setting up an asymmetric topology that were previously described for symmetric topologies earlier in this chapter.

### 4.4.1 Creating the Asymmetric Standby Site

This section describes the high level steps for creating any type of asymmetric Oracle Fusion Middleware Disaster Recovery topology. The production site is the Oracle SOA Suite enterprise deployment shown in Figure 4–2. The standby site will be different from the production site.

To create an asymmetric topology:

1. Design the production site and the standby site. Determine the resources that will be necessary at the standby site to ensure acceptable performance when the standby site assumes the production role.

**Note:** The ports for the standby site instances must use the same port numbers as the peer instances at the production site. Therefore, ensure that all the port numbers that will be required at the standby site are available (not in use at the standby site).

2. Create the Oracle Fusion Middleware Disaster Recovery production site by performing these operations:

   a. Create volumes on the production site's shared storage system for the Oracle Fusion Middleware instances that will be installed for the production site. For more information, see Section 4.1.1, "Directory Structure and Volume Design."

   b. Create mount points and symbolic links on the production site hosts to the Oracle home directories for the Oracle Fusion Middleware instances on the production site's shared storage system volumes. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links. For more information about volume design, see Section 4.1.1.1.1, "Volume Design for Oracle SOA Suite."

   c. Create mount points and symbolic links on the production site hosts to the Oracle Central Inventory directories for the Oracle Fusion Middleware instances on the production site's shared storage system volumes. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links. For more information about the Oracle Central Inventory directories, see Section 3.2.2, "Oracle Home and Oracle Inventory."

   d. Create mount points and symbolic links on the production site hosts to the static HTML pages directories for the Oracle HTTP Server instances on the production site's shared storage system volumes, if applicable. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links.

   e. Install the Oracle Fusion Middleware instances for the production site on the volumes in the production site's shared storage system. For more information, see Section 4.2.1, "Creating the Production Site for the Oracle SOA Suite Topology."

3. Create the same volumes with the same file and directory privileges on the standby site's shared storage system as you created for the Oracle Fusion Middleware instances on the production site's shared storage system. This step is critical because it enables you to use storage replication later to create the peer Oracle Fusion Middleware instance installations for the standby site instead of installing them using Oracle Universal Installer.

**Note:** When you configure storage replication, ensure that all the volumes you set up on the production site's shared storage system are replicated to the same volumes on the standby site's shared storage system.

Even though some of the instances and hosts at the production site may not exist at the standby site, you must configure storage replication for all the volumes set up for the production site's Oracle Fusion Middleware instances.

4. Perform any other necessary configuration required by the shared storage vendor to enable storage replication between the production site's shared storage system and the standby site's shared storage system. Configure storage replication to asynchronously copy the volumes in the production site's shared storage system to the standby site's shared storage system.
5. Create the initial baseline snapshot copy of the production site shared storage system to set up the replication between the production site and standby site shared storage systems. Create the initial baseline snapshot and subsequent snapshot copies using asynchronous replication mode. After the baseline snapshot copy is performed, validate that all the directories for the standby site volumes have the same contents as the directories for the production site volumes. Refer to the documentation for your shared storage vendor for information on creating the initial snapshot and enabled storage replication between the production site and standby site shared storage systems.
6. After the baseline snapshot has been taken, perform these steps for the Oracle Fusion Middleware instances for the standby site hosts:

   a. Set up a mount point directory on the standby site host to the Oracle home directory for the Oracle Fusion Middleware instance on the standby site's shared storage system. The mount point directory you set up for the peer instance on the standby site host must be the same as the mount point directory you set up for the instance on the production site host.

   b. Set up a symbolic link on the standby site host to the Oracle home directory for the Oracle Fusion Middleware instance on the standby site's shared storage system. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links. The symbolic link you set up for the peer instance on the standby site host must be the same as the symbolic link you set up for the instance on the production site host.

   c. Set up a mount point directory on the standby site host to the Oracle Central Inventory directory for the Oracle Fusion Middleware instance on the standby site's shared storage system. The mount point directory you set up for the peer instance on the standby site host must be the same as the mount point directory you set up for the instance on the production site host.

   d. Set up a symbolic link on the standby site host to the Oracle Central Inventory directory for the Oracle Fusion Middleware instance on the standby site's shared storage system. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links. The symbolic link you set up for the peer instance on the standby site host must be the same as the symbolic link you set up for the instance on the production site host.

e. Set up a mount point directory on the standby site host to the Oracle HTTP Server static HTML pages directory for the Oracle HTTP Server instance on the standby site's shared storage system. The mount point directory you set up for the peer instance on the standby site host must be the same as the mount point directory you set up for the instance on the production site host.

f. Set up a symbolic link on the standby site host to the Oracle HTTP Server static HTML pages directory for the Oracle HTTP Server instance on the standby site's shared storage system. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links. The symbolic link you set up for the peer instance on the standby site host must be the same as the symbolic link you set up for the instance on the production site host.

After completing these steps, the Oracle Fusion Middleware instance installations for the production site have been replicated to the standby site. At the standby site, all of the following are true:

- The Oracle Fusion Middleware instances are installed into the same Oracle home directories on the same volumes as at the production site, and the hosts use the same mount point directories and symbolic links for the Oracle home directories as at the production site. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links.
- The Oracle Central Inventory directories are located in same directories on the same volumes as at the production site, and the hosts use the same mount point directories and symbolic links for the Oracle Central Inventory directories as at the production site. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links.
- The Oracle HTTP Server static HTML pages directories are located in same directories on the same volumes as at the production site, and the hosts use the same mount point directories and symbolic links for the Oracle HTTP Server static HTML pages directories as at the production site. Note that symbolic links are required only in cases where the storage system does not guarantee consistent replication across multiple volumes; see Section 3.2.3, "Storage Replication" for more details about symbolic links.
- The same ports are used for the standby site Oracle Fusion Middleware instances as were used for the same instances at the production site.

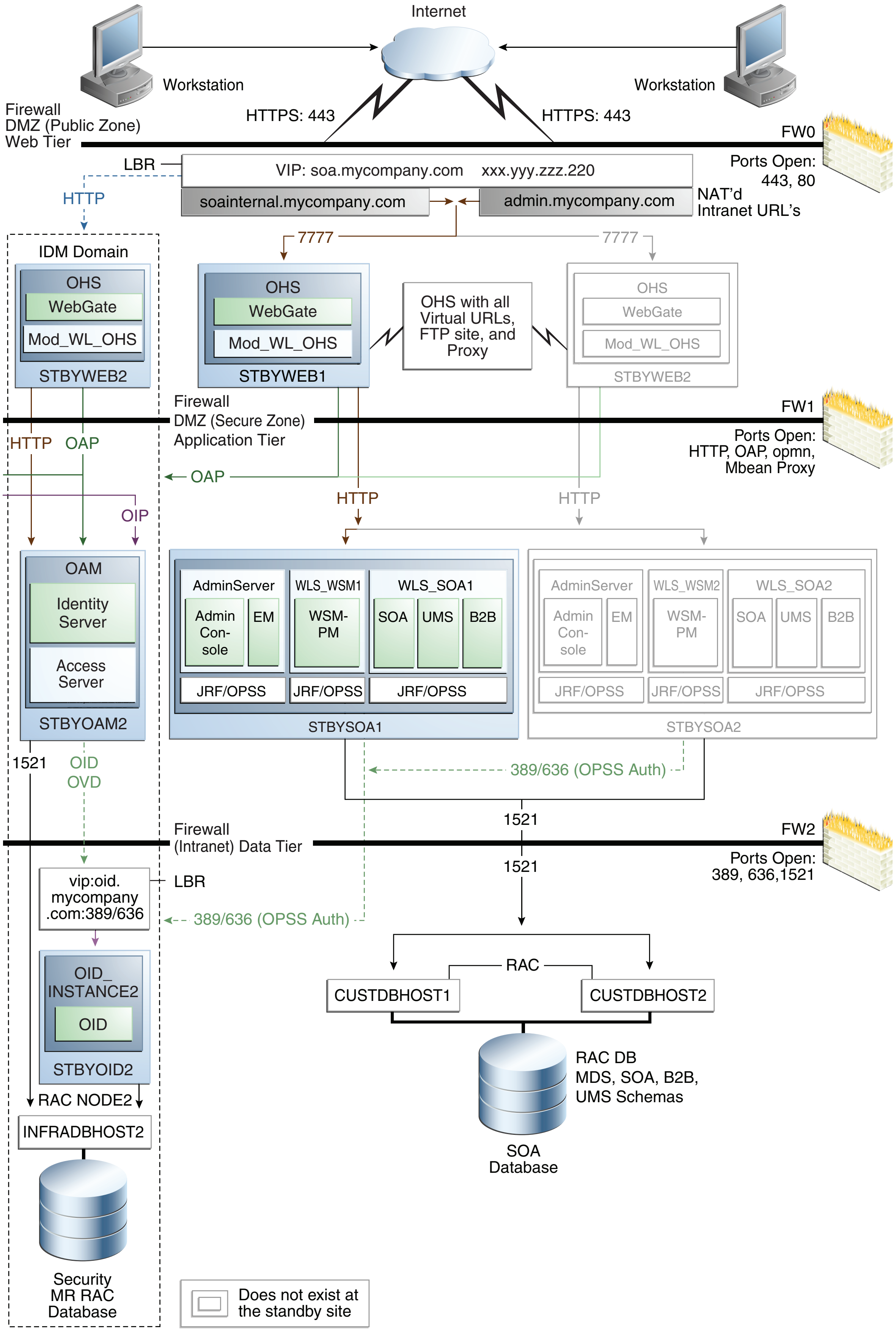
#### 4.4.1.1 Creating an Asymmetric Standby Site with Fewer Hosts and Instances

This section describes how to create an asymmetric standby site that has fewer hosts and Oracle Fusion Middleware instances than the production site.

The production site for this Oracle Fusion Middleware Disaster Recovery topology is the Oracle SOA Suite enterprise deployment shown in Figure 4–2. Section 4.1, "Setting Up the Site" through Section 4.1.1, "Directory Structure and Volume Design" describe how to set up this production site and the volumes for its shared storage system, and how to create the necessary mount points.

Figure 4–8 shows the asymmetric standby site for the production site shown in Figure 4–2.

*Figure 4–8 An Asymmetric Standby Site with Fewer Hosts and Instances*


Internet
Workstation
Workstation
HTTPS: 443
HTTPS: 443
Firewall
DMZ (Public Zone)
Web Tier
FW0
Ports Open:
443, 80
LBR
VIP: soa.mycompany.com xxx.yyy.zzz.220
soainternal.mycompany.com
admin.mycompany.com
NAT'd
Intranet URL's
HTTP
7777
7777
IDM Domain
OHS
WebGate
Mod_WL_OHS
STBYWEB2
OHS
WebGate
Mod_WL_OHS
STBYWEB1
OHS with all
Virtual URLs,
FTP site, and
Proxy
OHS
WebGate
Mod_WL_OHS
STBYWEB2
Firewall
DMZ (Secure Zone)
Application Tier
FW1
Ports Open:
HTTP, OAP, opmn,
Mbean Proxy
HTTP
OAP
OAP
OIP
HTTP
HTTP
OAM
Identity
Server
Access
Server
STBYOAM2
AdminServer
Admin
Con-
sole
EM
WLS_WSM1
WSM-
PM
WLS_SOA1
SOA
UMS
B2B
JRF/OPSS
JRF/OPSS
JRF/OPSS
STBYSOA1
AdminServer
Admin
Con-
sole
EM
WLS_WSM2
WSM-
PM
WLS_SOA2
SOA
UMS
B2B
JRF/OPSS
JRF/OPSS
JRF/OPSS
STBYSOA2
1521
OID
OVD
389/636 (OPSS Auth)
1521
Firewall
(Intranet) Data Tier
FW2
Ports Open:
389, 636,1521
1521
vip:oid.
mycompany
.com:389/636
LBR
389/636 (OPSS Auth)
OID_
INSTANCE2
OID
STBYOID2
RAC
CUSTDBHOST1
CUSTDBHOST2
RAC NODE2
INFRADBHOST2
RAC DB
MDS, SOA, B2B,
UMS Schemas
SOA
Database
Security
MR RAC
Database
Does not exist at
the standby site

The Oracle SOA Suite asymmetric standby site shown in Figure 4–8 has fewer hosts and instances than the Oracle SOA Suite production site shown in Figure 4–2.

The hosts WEBHOST2 and SOAHOST2 and the instances on those hosts exist at the production site in Figure 4–2, but these hosts and their instances do not exist at the asymmetric standby site in Figure 4–8. The standby site therefore has fewer hosts and fewer instances than the production site.

It is important to ensure that this asymmetric standby site will have sufficient resources to provide adequate performance when it assumes the production role.

When you follow the steps in Section 4.4.1, "Creating the Asymmetric Standby Site" to set up this asymmetric standby site, the standby site should be properly configured to assume the production role.

To set up the asymmetric standby site correctly, create the same volumes and consistency groups on the standby site shared storage as you did on the production site shared storage. For example, for the Oracle SOA Suite deployment, the volume design recommendations in Table 4-4 and the consistency group recommendations in Table 4-5) were used to set up the production site shared storage. You will use these same volume design recommendations and consistency group recommendations that you used for the production site shared storage to set up the asymmetric standby site's shared storage.

Note that at an asymmetric standby site, some hosts that exist at the production site do not exist at the standby site. For example, in the case of the asymmetric standby site for Oracle SOA Suite shown in Figure 4–8, WEBHOST2 and SOAHOST2 do not exist at the standby site, therefore it is not possible or necessary for you to create mount points on these hosts to the standby site shared storage volumes.

### 4.4.2 Validating the Asymmetric Standby Site Setup

Validate the standby site by following the steps below:

1. Shut down any processes still running on the production site. This includes the database instances in the data tier, Oracle Fusion Middleware instances and any other processes in the application tier and web tier.
2. Stop the replication between the production site shared storage and the standby site shared storage.
3. Use Oracle Data Guard to fail over the databases.
4. On the standby site hots, manually start all the processes. This includes the database instances in the data tier, Oracle Fusion Middleware instances and any other processes in the application tier and web tier.
5. Use a browser client to perform post-failover testing to confirm that requests are being resolved and redirected to the standby site.

## 4.5 Performing Site Operations and Administration

This section describes operations and administration to perform on your Oracle Fusion Middleware Disaster Recovery topology.

### 4.5.1 Synchronizing the Sites

The standby site shared storage receives snapshots transferred on a periodic basis from the production site shared storage. After the snapshots are applied, the standby site shared storage will include all the data up to and including the data contained in the last snapshot transferred from the production site before the failover or switchover.

You should manually force a synchronization operation whenever a change is made to the middle tier at the production site (for example, when a new application is deployed at the production site). Follow the vendor-specific instructions for forcing a synchronization using storage replication technology.

The synchronization of the databases in the Oracle Fusion Middleware Disaster Recovery topology is managed by Oracle Data Guard.

### 4.5.2 Performing a Switchover

When you plan to take down the production site (for example, to perform maintenance) and make the current standby site the new production site, you must perform a switchover operation so that the standby site takes over the production role.

Follow these steps to perform a switchover operation:

1. Shut down any processes still running on the production site. This includes the database instances in the data tier, Oracle Fusion Middleware instances and any other processes in the application tier and web tier.
2. Stop the replication between the production site shared storage and the standby site shared storage.
3. Use Oracle Data Guard to switch over the databases.
4. On the standby site hots, manually start all the processes. This includes the database instances in the data tier, Oracle Fusion Middleware instances and any other processes in the application tier and web tier.
5. Ensure that all user requests are routed to the standby site by performing a global DNS push or something similar, such as updating the global load balancer.
6. Use a browser client to perform post-switchover testing to confirm that requests are being resolved and redirected to the standby site.

   At this point, the former standby site is the new production site and the former production site is the new standby site.
7. Reestablish the replication between the two sites, but configure the replication so that the snapshot copies go in the opposite direction (from the current production site to the current standby site). Refer to the documentation for your shared storage to learn how to configure the replication so that snapshot copies are transferred in the opposite direction.

After these steps have been performed, the former standby site is the new production site. At this point, you can perform maintenance at the original production site. After performing the planned tasks on the original production site, you can use it again at some point in the future as either the production site or standby site.

To use the original production site as the new production site, perform the switchback steps described in Section 4.5.3, "Performing a Switchback."

### 4.5.3 Performing a Switchback

After a switchover operation has been performed, a switchback operation can be performed to revert the current production site and the current standby site to the roles they had prior to the switchover operation.

Follow these steps to perform a switchback operation:

1. Shut down any processes running on the current production site. This includes the database instances in the data tier, Oracle Fusion Middleware instances and any other processes in the application tier and web tier.
2. Stop the replication between the current production site shared storage and standby site shared storage.
3. Use Oracle Data Guard to switch back the databases.
4. On the new production site hosts, manually start all the processes. This includes the database instances in the data tier, Oracle Fusion Middleware instances and any other processes in the application tier and web tier.
5. Ensure that all user requests are routed to the new production site by performing a global DNS push or something similar, such as updating the global load balancer.
6. Use a browser client to perform post-switchback testing to confirm that requests are being resolved and redirected to the new production site.

   At this point, the former standby site is the new production site and the former production site is the new standby site.
7. Reestablish the replication between the two sites, but configure the replication so that the snapshot copies go in the opposite direction (from the new production site to the new standby site). Refer to the documentation for your shared storage to learn how to configure the replication so that snapshot copies are transferred in the opposite direction.

### 4.5.4 Performing a Failover

When the production site becomes unavailable unexpectedly, you must perform a failover operation so that the standby site takes over the production role.

Follow these steps to perform a failover operation:

1. Stop the replication between the production site shared storage and the standby site shared storage.
2. From the standby site, use Oracle Data Guard to fail over the databases.
3. On the standby site hosts, manually start all the processes. This includes the database instances in the data tier, Oracle Fusion Middleware instances and any other processes in the application tier and web tier.
4. Ensure that all user requests are routed to the standby site by performing a global DNS push or something similar, such as updating the global load balancer.
5. Use a browser client to perform post-failover testing to confirm that requests are being resolved and redirected to the production site.

   At this point, the standby site is the new production site. You can examine the issues that caused the former production site to become unavailable.
6. To use the original production site as the current standby site, you must reestablish the replication between the two sites, but configure the replication so that the snapshot copies go in the opposite direction (from the current production site to the current standby site). Refer to the documentation for your shared storage system to learn how to configure the replication so that snapshot copies are transferred in the opposite direction.

To use the original production site as the new production site, perform the switchback steps in Section 4.5.3, "Performing a Switchback."

### 4.5.5 Performing Periodic Testing of the Standby Site.

This manual describes how to set up Disaster Recovery for an Oracle Fusion Middleware production site and standby site. In a normal Oracle Fusion Middleware Disaster Recovery configuration, the following are true:

- Storage replication is used to copy Oracle Fusion Middleware middle tier file systems and data from the production site shared storage to the standby site shared storage. During normal operation, the production site is active and the standby site is passive. When the production site is active, the standby site is passive and the standby site shared storage is in read-only mode; the only write operations made to the standby site shared storage are the storage replication operations from the production site shared storage to the standby site shared storage.
- Oracle Data Guard is used to copy database data for the production site Oracle databases to the standby databases at standby site. By default, the production site databases are active and the standby databases at the standby site are passive. The standby databases at the standby site are in managed recovery mode while the standby site is in the standby role (is passive). When the production site is active, the only write operations made to the standby databases are the database synchronization operations performed by Oracle Data Guard.
- When the production site becomes unavailable, the standby site is enabled to take over the production role. If the current production site becomes unavailable unexpectedly, then a failover operation (described in Section 4.5.4, "Performing a Failover") is performed to enable the standby site to assume the production role. Or, if the current production site is taken down intentionally (for example, for planned maintenance), then a switchover operation (described in Section 4.5.2, "Performing a Switchover") is performed to enable the standby site to assume the production role.

The usual method of testing a standby site is to shut down the current production site and perform a switchover operation to enable the standby site to assume the production role. However, some enterprises may want to perform periodic testing of their Disaster Recovery standby site without shutting down the current production site and performing a switchover operation.

An alternate method of testing the standby site without shutting down the current production site is to create a clone of the read-only standby site shared storage and then use the cloned standby site shared storage in testing. To use this alternate testing method, perform these steps:

1. Use the cloning technology provided by the shared storage vendor to create a clone of the standby site's read-only volumes on the shared storage at the standby site. Ensure that the cloned standby site volumes are writable. If you want to test the standby site just once, then this can be a one-time clone operation, but if you want to test the standby site regularly, you can set up periodic cloning of the standby site read-only volumes to the standby site's cloned read/write volumes.
2. Perform a backup of the standby site databases, then modify the Oracle Data Guard replication between the production site and standby site databases.
   - For 10.1 databases, break the replication by following the instructions in the 10.1 Oracle Data Guard documentation.
   - For 10.2 and later databases, follow these steps to establish a snapshot standby database:
     a. If you do not have a Flash Recovery Area, set one up.

   b. Cancel Redo Apply:

      ```
      SQL> ALTER DATABASE RECOVER MANAGED STANDBY
           DATABASE CANCEL;
      ```

   c. Create a guaranteed restore point:

      ```
      SQL> CREATE RESTORE POINT standbytest
           GUARANTEE FLASHBACK DATABASE;
      ```

   d. Archive the current logs at the primary (production) site:

      ```
      SQL> ALTER SYSTEM ARCHIVE LOG CURRENT;
      ```

   e. Defer the standby site destination that you will activate:

      ```
      SQL> ALTER SYSTEM SET
           LOG_ARCHIVE_DEST_STATE_2=DEFER;
      ```

   f. Activate the target standby database:

      ```
      SQL> ALTER DATABASE ACTIVATE STANDBY DATABASE;
      ```

   g. Mount the database with the Force option if the database was opened read-only:

      ```
      SQL> STARTUP MOUNT FORCE;
      ```

   h. Lower the protection mode and open the database:

      ```
      SQL> ALTER DATABASE SET STANDBY DATABASE TO
           MAXIMIZE PERFORMANCE;
      SQL> ALTER DATABASE OPEN;
      ```

- For 11*g* databases, use the procedure to establish a snapshot standby database in the "Managing a Snapshot Standby Database" section in *Oracle Data Guard Concepts and Administration*.

3. Use Oracle Data Guard database recovery procedures to bring the standby databases online.
4. On the standby site computers, modify the mount commands to point to the volumes on the standby site's cloned read/write shared storage by following these steps:
   a. Unmount the read-only shared storage volumes.
   b. Mount the cloned read/write volumes at the same mount point.
5. Before doing the standby site testing, modify the host  name resolution method for the computers that will be used to perform the testing to ensure that the host names point to the standby site computers and not the production site computers. For example, on a Linux computer, change the `/etc/hosts` file to point to the virtual IP of the load balancer for the standby site.
6. Perform the standby site testing.

After you complete the standby site testing, follow these steps to begin using the original production site as the production site again:

1. Modify the mount commands on the standby site computers to point to the volumes on the standby site's read-only shared storage: In other words, reset the mount commands back to what they were before the testing was performed.
   a. Unmount the cloned read/write shared storage volume.

   b. Mount the read-only shared storage volumes.

   At this point, the mount commands are reset to what they were before the standby site testing was performed.

2. Configure Oracle Data Guard to perform replication between the production site databases and standby databases at the standby site. Performing this configuration puts the standby database into managed recovery mode again:

   - For 10.1 databases, reinstantiate the databases by following the instructions in the 10.1 Oracle Data Guard documentation.
   - For 10.2 and later databases, follow these steps:

     a. Revert the activated database back to a physical standby database:

     ```
     SQL> STARTUP MOUNT FORCE;
     SQL> FLASHBACK DATABASE TO POINT standbytest;
     SQL> ALTER DATABASE CONVERT TO PHYSICAL STANDBY;
     SQL> STARTUP MOUNT FORCE;
     ```

     b. Restart managed recovery:

     ```
     SQL> ALTER DATABASE RECOVER MANAGED STANDBY
          DATABASE USING CURRENT LOGFILE DISCONNECT;
     ```

     c. Reenable the standby destination and switch logs:

     ```
     SQL> ALTER SYSTEM SET
          LOG ARCHIVE DEST STATE 2=ENABLE;
     ```

   - For 11*g* databases, set up the replication again by following the steps in the "Managing a Snapshot Standby Database" section in *Oracle Data Guard Concepts and Administration*.

3. Before using the original production site again, modify the host  name resolution method for the computers that will be used to access the production site to ensure that the host names point to the production site computers and not the standby site computers. For example, on a Linux computer, change the `/etc/hosts` file to point to the virtual IP of the load balancer for the production site.

### 4.5.6 Using Peer to Peer File Copy for Testing

As an alternative to using storage replication technology for disaster protection and disaster recovery of Oracle Fusion Middleware middle tier components, you can use peer to peer file copy mechanisms in test environments to replicate middle tier file system data from a production site host to a standby site peer host in an Oracle Fusion Middleware Disaster Recovery topology. An example of a peer to peer file copy mechanism is rsync (an open source utility for UNIX systems).

This section describes how to use rsync instead of storage replication in your Oracle Fusion Middleware Disaster Recovery topology. This section discusses rsync in the context of symmetric topologies. For more information about symmetric topologies, refer to Section 4.4, "Creating an Asymmetric Standby Site." The information provided for rsync in this section also applies to other peer to peer file copy mechanisms.

Before you read this section, read the rest of this manual to ensure that you are familiar with how to use storage replication and Oracle Data Guard in an Oracle Fusion Middleware Disaster Recovery topology. There are many similarities between using storage replication and rsync for disaster protection and disaster recovery of your Oracle Fusion Middleware components.

**Note:** You can use rsync instead of storage replication technology to replicate middle tier file system data from the production site to the standby site. However, be aware that the following beneficial storage replication features are not available when you use rsync:

- With storage replication, you can roll changes back to the point in time when any previous snapshot was taken at the production site.

  With rsync, replicated production site data overwrites the standby site data, and you cannot roll back a replication.

- With storage replication, the volume you set up for each host cluster in the shared storage systems ensures data consistency for that host cluster across the production site's shared storage system and the standby site's shared storage system.

  With rsync, data consistency is not guaranteed.

Because of these deficiencies in comparison to storage replication, rsync is not supported for disaster recovery use in actual production environments.

#### 4.5.6.1 Using rsync and Oracle Data Guard for Oracle Fusion Middleware Disaster Recovery Topologies

These two basic principles apply when you use rsync and Oracle Data Guard to provide disaster protection and disaster recovery for your Oracle Fusion Middleware Disaster Recovery topology:

1. Use rsync for disaster protection of your Oracle Fusion Middleware middle tier components.
2. Use Oracle Data Guard for disaster protection of Oracle databases that are used in your Oracle Fusion Middleware topology. Section 3.3, "Database Considerations" describes how to set up Oracle Data Guard to provide disaster recovery for Oracle database.

**4.5.6.1.1 Using rsync for Oracle Fusion Middleware Middle Tier Components** Follow these steps to use rsync to provide disaster protection and disaster recovery for your Oracle Fusion Middleware middle tier components:

1. Set up rsync to enable replication of files from a production site host to its standby site peer host. See the rsync man page for instructions on installing and setting up rsync, and for syntax and usage information. Information about rsync is also available at http://rsync.samba.org.
2. For each production site host on which one or more Oracle Fusion Middleware components has been installed, set up rsync to copy the following directories and files to the same directories and files on the standby site peer host:
   - The Oracle Fusion Middleware home directory and subdirectories, and all the files in them.
   - The Oracle Central Inventory directory and files for the host, which includes the Oracle Universal Installer entries for the Oracle Fusion Middleware installations.
   - If applicable, the Oracle Fusion Middleware static HTML pages directory for the Oracle HTTP Server installations on the host.

- If applicable, the .fmb and .fmx deployment artifact files created by Oracle Forms on the host, and the .rdf deployment artifact files created by Oracle Reports on the host.

> **Note:** Run rsync as root. If you want rsync to work without prompting users for a password, set up SSH keys between the production site host and standby site host, so that SSH does not prompt for a password.

3. Set up scheduled jobs, for example, cron jobs, for the production site hosts for which you set up rsync in the previous step. These scheduled jobs enable rsync to automatically perform replication of these files from the production site hosts to the standby site hosts on a regular interval. An interval of once a day is recommended for a production site where the Oracle Fusion Middleware configuration does not change very often.
4. Whenever a change is made to the configuration of an Oracle Fusion Middleware middle tier configuration on a production site host (for example, when a new application is deployed), you should perform a manual synchronization of that host with its standby site peer host using rsync.
5. Whenever you perform a manual rsync synchronization of an Oracle Fusion Middleware middle tier instance on a production site host to the peer standby site host, you should also manually force a synchronization of any associated database repository for the production site's Oracle Fusion Middleware instance to the standby site using Oracle Data Guard. See Section 3.3.2, "Manually Forcing Database Synchronization with Oracle Data Guard" for more information on manually forcing a synchronization of an Oracle database using Oracle Data Guard.

**4.5.6.1.2 Performing Failover and Switchover Operations** Follow these steps to perform a failover or switchover from the production site to the standby site when you are using rsync:

1. Shut down any processes still running on the production site (if applicable).
2. Stop the rsync jobs between the production site hosts and their standby site peer hosts.
3. Use Oracle Data Guard to fail over the production site databases to the standby site.
4. On the standby site, manually start the processes for the Oracle Fusion Middleware Server instances.
5. Route all user requests to the standby site by performing a global DNS push or something similar, such as updating the global load balancer.
6. Use a browser client to perform post-failover or post-switchover testing to confirm that requests are being resolved at the standby site (current production site).

   At this point, the standby site is the new production site and the production site is the new standby site.
7. Reestablish the rsync replications between the two sites, but configure the replications so that they go in the opposite direction (from the current production site to the current standby site).

To use the original production site as the new production site, you perform the steps above again, but configure the rsync replications to go in the original direction (from the original production site to the original standby site).

## 4.6 Patching an Oracle Fusion Middleware Disaster Recovery Site

This section describes how to apply an 11*g* Oracle Fusion Middleware patch set to upgrade the Oracle homes that participate in an Oracle Fusion Middleware Disaster Recovery site.

The list in this section describes the steps for applying a patch set to upgrade the 11*g* Oracle Fusion Middleware homes in an Oracle Fusion Middleware Disaster Recovery production site.

The following steps assume that the Oracle Central Inventory for any Oracle Fusion Middleware instance that you are patching is located on the production site shared storage, so that the Oracle Central Inventory for the patched instance can b e replicated to the standby site.

Use the following procedure to upgrade 11*g* Oracle Fusion Middleware patch versions:

1. Perform a backup of the production site to ensure that the starting state is secured.
2. Apply the patch set to upgrade the production site instances.
3. After applying the patch set, manually force a synchronization of the production site shared storage and standby site shared storage. This replicates the production site's patched instance and Oracle Central Inventory in the standby site's shared storage.
4. After applying the patch set, use Oracle Data Guard to manually force a synchronization of the Oracle databases at the production site and standby sites. Some Oracle Fusion Middleware patch sets may make updates to repositories, so this step ensures that any changes made to production site databases are synchronized to the standby site databases.
5. The upgrade is now complete. Your Disaster Recovery topology is ready to resume processing.

**Note:** Patches must be applied only at the production site for an 11*g* Oracle Fusion Middleware Disaster Recovery topology. If a patch is for an Oracle Fusion Middleware instance or for the Oracle Central Inventory, the patch will be copied when the production site shared storage is replicated to the standby site shared storage. A synchronization operation should be performed when a patch is installed at the production site.

Similarly, if a patch is installed for a production site database, Oracle Data Guard will copy the patch to the standby database at the standby site when a synchronization is performed.

# 5
# Troubleshooting Disaster Recovery

This chapter describes common situations that you might encounter when deploying and managing Oracle Fusion Middleware in Disaster Recovery topologies, and explains the steps for addressing them. It contains the following topics:

- Troubleshooting Oracle Fusion Middleware Disaster Recovery Topologies
- Need More Help?

## 5.1 Troubleshooting Oracle Fusion Middleware Disaster Recovery Topologies

This section describes common situations and steps to perform in Oracle Fusion Middleware configurations. It contains the following topics:

- Verify Host Name Resolution at the Production and Standby Sites
- Resolving Issues with Components in a Disaster Recovery Topology
- Resolving Issues with Components Deployed on Shared Storage

### 5.1.1 Verify Host Name Resolution at the Production and Standby Sites

Many issues that may arise with your Disaster Recovery topology are caused by host name resolution not having been set up properly for the production site and standby site.

Make sure that host name resolution is set up properly by performing the host name validation steps in Section 3.1.1.5, "Testing the Host Name Resolution."

### 5.1.2 Resolving Issues with Components in a Disaster Recovery Topology

Some issues that may arise with a component in a Disaster Recovery topology are not Disaster Recovery issues, but rather are issues with the component itself.

If you encounter problems with an Oracle Fusion Middleware component used in a Disaster Recovery topology, check the Troubleshooting section in the *Oracle Fusion Middleware High Availability Guide* for that component to see if the problem is described there.

Similarly, if your Disaster Recovery topology is based on one or more of the enterprise deployments described in the following manuals and you encounter a problem, check the Troubleshooting section of that manual to see if the problem is described there:

- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter*

- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

### 5.1.3 Resolving Issues with Components Deployed on Shared Storage

Some problems that may arise with a component in your Disaster Recovery topology are not Disaster Recovery issues, but are issues associated with deploying the component on shared storage.

If you do not find any shared storage problems described in the manuals mentioned in Section 5.1.2, "Resolving Issues with Components in a Disaster Recovery Topology," then look for notes that describe shared storage problems in the *Oracle Fusion Middleware Release Notes*, available on the Oracle Technology Network at:

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

## 5.2 Need More Help?

In case the information in the previous section is not sufficient, you can find more solutions on My Oracle Support (formerly Oracle *MetaLink*) at:

`http://support.oracle.com`

If you do not find a solution for your problem, log a service request.

You can also read the *Oracle Fusion Middleware Release Notes*, available on the Oracle Technology Network at:

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

# A

# Managing Oracle Inventory

This appendix describes how to manage your Oracle Inventory on the production and standby sites for an Oracle Fusion Middleware Disaster Recovery topology.

It includes this topic:

- Updating Oracle Inventory

## A.1 Updating Oracle Inventory

When you update the Oracle inventory (for example, by installing new Oracle software, or by applying an Oracle patch set or patch to existing Oracle software) on a production site host, you must make sure that the same software updates are made on the standby site peer host.

To do this, you must update the Oracle inventory on the standby site peer host by executing the following script:

```
ORACLE_HOME/oui/bin/attachHome.sh
```

In addition, you must update the `beahomelist` file to edit the location of a Middleware home. Edit the following file to update the Middleware home information:

```
user_home/bea/beahomelist
```

# Index