

# **Oracle® Fusion Middleware**

Disaster Recovery Guide

12c (12.2.1.2)

**E77916-03**

May 2017

This document describes the Disaster Recovery solutions for Oracle Fusion Middleware products.

Oracle Fusion Middleware Disaster Recovery Guide, 12c (12.2.1.2)

E77916-03

Copyright © 2015, 2017, Oracle and/or its affiliates. All rights reserved.

Primary Author: Carlos Subi

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

---

---

# Contents

<b>Preface</b> .....	xiii
Audience .....	xiii
Documentation Accessibility .....	xiii
Related Documents.....	xiii
Conventions.....	xiv
<b>1 Introduction to Oracle Fusion Middleware Disaster Recovery</b>	
1.1 Overview of Oracle Fusion Middleware Disaster Recovery .....	1-1
1.1.1 Problem Description and Common Solutions .....	1-1
1.1.2 Terminology .....	1-2
1.2 Setting Up Disaster Recovery for Oracle Fusion Middleware Components .....	1-5
1.2.1 Oracle Fusion Middleware Disaster Recovery Architecture Overview .....	1-5
1.2.2 Components Described in This Document.....	1-9
<b>2 Recommendations for Oracle Fusion Middleware Components</b>	
2.1 Recommendations for Oracle WebLogic Server .....	2-2
2.1.1 Recommendations for Oracle WebLogic Server Java Message Service (JMS) and Transaction Logs (T-Logs).....	2-3
2.1.2 Recommendations for Oracle Platform Security Services.....	2-5
2.2 Recommendations for Oracle SOA Suite .....	2-5
2.2.1 Recommendations for Oracle SOA Service Infrastructure.....	2-8
2.2.2 Recommendations for Oracle BPEL Process Manager .....	2-9
2.2.3 Recommendations for Oracle Mediator .....	2-9
2.2.4 Recommendations for Oracle Human Workflow .....	2-10
2.2.5 Recommendations for Oracle B2B .....	2-11
2.2.6 Recommendations for Oracle Web Services Manager .....	2-12
2.2.7 Recommendations for Oracle User Messaging Service .....	2-13
2.2.8 Recommendations for Oracle Java EE Connector Architecture (JCA) Adapters.....	2-14
2.2.9 Recommendations for Oracle Business Activity Monitoring .....	2-15
2.2.10 Recommendations for Oracle Business Process Management .....	2-16
2.3 Recommendations for Oracle Business Intelligence Suite.....	2-16

2.3.1	Common Recommendations for All Oracle Business Intelligence Suite Components .....	2-17
2.3.2	Recommendations for Oracle Business Intelligence Enterprise Edition (EE) .....	2-18
2.3.3	Recommendations for Oracle Business Intelligence Publisher .....	2-19
2.4	Recommendations for Oracle WebCenter Portal .....	2-20
2.4.1	Common Recommendations for All Oracle WebCenter Portal Components .....	2-21
2.4.2	Recommendations for Oracle WebCenter Portal Server .....	2-22
2.4.3	Recommendations for Oracle WebCenter Analytics .....	2-22
2.4.4	Recommendations for Oracle WebCenter Discussion Server .....	2-23
2.4.5	Recommendations for Oracle WebCenter Portlet and Pagelet Services .....	2-23
2.5	Recommendations for Oracle WebCenter Content .....	2-24
2.5.1	Common Recommendations for All Oracle WebCenter Content Components .....	2-25
2.5.2	Recommendations for Oracle WebCenter Content .....	2-26
2.5.3	Recommendations for Oracle WebCenter Content Inbound Refinery .....	2-27
2.5.4	Recommendations for Oracle WebCenter Content Enterprise Capture .....	2-27
2.5.5	Recommendations for Oracle WebCenter Content: Content User Interface .....	2-28

### 3 Design Considerations

3.1	Network Considerations .....	3-3
3.1.1	Planning Host Names .....	3-4
3.1.2	Virtual IP and Virtual Host Name Considerations .....	3-11
3.1.3	Load Balancer Considerations .....	3-12
3.1.4	Virtual Server Considerations .....	3-13
3.1.5	External Clients Considerations .....	3-14
3.1.6	Wide Area DNS Operations .....	3-15
3.2	Storage Considerations .....	3-16
3.2.1	Oracle Fusion Middleware Artifacts .....	3-17
3.2.2	Oracle Home and Oracle Inventory .....	3-17
3.2.3	Storage Replication .....	3-17
3.2.4	File-Based Persistent Store .....	3-19
3.3	Database Considerations .....	3-19
3.3.1	Making TNSNAMES.ORA Entries for Databases .....	3-20
3.3.2	Synchronizing Databases Manually .....	3-21
3.3.3	Setting Up Database Host Name Aliases .....	3-21
3.4	Starting Points .....	3-22
3.4.1	Starting with an Existing Site .....	3-23
3.4.2	Starting with a New Site .....	3-24
3.5	Topology Considerations .....	3-24
3.5.1	Design Considerations for a Symmetric Topology .....	3-24
3.5.2	Design Considerations for an Asymmetric Topology .....	3-25

### 4 Setting Up and Managing Disaster Recovery Sites

4.1	Setting Up a Site .....	4-1
-----	-------------------------	-----

4.1.1	Designing Directory Structure and Volumes .....	4-2
4.1.2	Setting Up Storage Replication.....	4-9
4.1.3	Installing and Configuring Databases.....	4-10
4.2	Creating a Production Site.....	4-24
4.2.1	Creating a Production Site for the Oracle SOA Suite Topology.....	4-24
4.2.2	Configuring Data Sources for Oracle Fusion Middleware Active-Passive Deployment .....	4-25
4.3	Creating a Standby Site.....	4-27
4.3.1	Preparing the Standby Site.....	4-27
4.3.2	Updating Self-Signed Certificates and Keys on the Standby Site .....	4-28
4.3.3	Validating the Standby Site Setup .....	4-31
4.4	Creating an Asymmetric Standby Site.....	4-31
4.4.1	Creating an Asymmetric Standby Site .....	4-32
4.4.2	Validating the Asymmetric Standby Site Setup.....	4-37
4.5	Performing Site Operations and Administration.....	4-37
4.5.1	Synchronizing the Production and Standby Sites .....	4-38
4.5.2	Performing a Switchover.....	4-38
4.5.3	Performing a Switchback .....	4-41
4.5.4	Performing a Failover .....	4-41
4.5.5	Testing the Standby Site .....	4-44
4.5.6	Using Peer-To-Peer File Copy for Testing .....	4-46
4.6	Using Oracle Site Guard for Disaster Recovery .....	4-49
4.7	Patching an Oracle Fusion Middleware Disaster Recovery Site.....	4-49
<b>5</b>	<b>Troubleshooting Oracle Fusion Middleware Disaster Recovery</b>	
5.1	Troubleshooting Oracle Fusion Middleware Disaster Recovery Topologies.....	5-1
5.1.1	Verifying Host Name Resolution at the Production and Standby Sites.....	5-1
5.1.2	Resolving Issues with Components in a Disaster Recovery Topology .....	5-1
5.1.3	Resolving Issues with Components Deployed on Shared Storage .....	5-2
5.2	Need More Help?.....	5-2
<b>A</b>	<b>Managing Oracle Inventory</b>	
A.1	Updating Oracle Inventory .....	A-1
A.2	Updating the Windows Registry.....	A-1



## List of Examples

3-1	Specifying the Use of Local Host Name Resolution.....	3-8
3-2	Specifying the Use of DNS Host Name Resolution.....	3-8
3-3	Making /etc/hosts File Entries for a Production Site Host.....	3-9
3-4	Making /etc/hosts File Entries for a Standby Site Host.....	3-9
3-5	DNS Entries for a Production Site Host in a Separate DNS Servers Configuration.....	3-10
3-6	DNS Entries for a Standby Site Host in a Separate DNS Servers Configuration.....	3-10
3-7	DNS Entries for Production Site and Standby Site Hosts When Using a Global DNS Server Configuration.....	3-11
3-8	Standby Site /etc/hosts File Entries When Using a Global DNS Server Configuration	3-11
4-1	Script for Creating and Starting a Listener with Static SID.....	4-16
4-2	Script for Creating and Starting a Listener with Static SID.....	4-16
4-3	Script for Creating an Oracle Net Alias.....	4-16
4-4	Sample tnsnames.ora File on Primary Node 1 (SOADC1.DBHOST1).....	4-17
4-5	Sample tnsnames.ora File on Standby Node 1 (SOADC2.DBHOST1).....	4-17
4-6	Duplicating Data Between Two Systems with Different Disk-Group Names.....	4-18
4-7	Duplicating Data Between Two Systems with Same Disk-Group Name +DATA.....	4-18
4-8	Sample Redo Log.....	4-18
4-9	Accessing dgmgrl to Create the Data Guard Broker Configuration on Primary Host...	4-20
4-10	Verifying the Data Guard Broker Configuration.....	4-21



## List of Figures

1-1	Production and Standby Sites for Oracle Fusion Middleware Disaster Recovery Topology.....	1-7
3-1	Deployment Used at Production and Standby Sites for Oracle Fusion Middleware Disaster Recovery.....	3-2
3-2	Physical Host Names Used at Oracle SOA Suite Deployment Standby Site.....	3-6
4-1	Directory Structure for Oracle SOA Suite.....	4-4
4-2	Oracle SOA Suite and Oracle Business Activity Monitoring Enterprise Topology Diagram.....	4-5
4-3	Oracle SOA Suite and Oracle Service Bus Enterprise Deployment Reference Topology Diagram.....	4-6
4-4	An Asymmetric Standby Site with Fewer Hosts and Instances.....	4-36



## List of Tables

2-1	JMS Queues Used by Oracle B2B.....	2-11
2-2	JMS Resources Used by Oracle User Messaging Service.....	2-13
3-1	IP Addresses and Physical Host Names for SOA Suite Production Site Hosts.....	3-5
3-2	Floating IP Addresses.....	3-7
3-3	Virtual IP Addresses and Virtual Host Names for the SOA Suite Production Site Hosts .....	3-12
3-4	Virtual IP Addresses, Virtual Host Names, and Alias Host Names for SOA Suite Standby Site Hosts.....	3-12
3-5	Virtual Servers for Oracle SOA Suite Production Site.....	3-14
3-6	Virtual Servers for Oracle SOA Suite Standby Site.....	3-14
3-7	Database Host Names and Connect Strings.....	3-21
3-8	Specifying an Alias for a Database Host.....	3-21
4-1	Volume Design Recommendations for Oracle SOA Suite.....	4-7
4-2	Consistency Groups for Oracle SOA Suite.....	4-9
4-3	Variables Used by Primary and Standby Databases.....	4-11



---

# Preface

This preface contains the following 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

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

### Access to Oracle Support

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

## Related Documents

For 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 Portal*
- *Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*
- *Understanding an Enterprise Deployment*

## Conventions

The following text conventions are used in this document:

<b>Convention</b>	<b>Meaning</b>
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.

---

# Introduction to Oracle Fusion Middleware Disaster Recovery

Oracle Fusion Middleware Disaster Recovery is a disaster recovery solution that provides protection to Oracle Fusion Middleware components in different Oracle product suites.

This chapter includes the following sections:

## [Overview of Oracle Fusion Middleware Disaster Recovery](#)

Learn what problems Oracle Fusion Middleware Disaster Recovery solves and get familiar with the terminology.

## [Setting Up Disaster Recovery for Oracle Fusion Middleware Components](#)

Learn how to set up your Disaster Recovery for an Oracle Fusion Middleware enterprise deployment.

## 1.1 Overview of Oracle Fusion Middleware Disaster Recovery

Learn what problems Oracle Fusion Middleware Disaster Recovery solves and get familiar with the terminology.

This overview includes the following sections:

### [Problem Description and Common Solutions](#)

Learn how to deploy an Oracle Fusion Middleware Disaster Recovery solution for enterprise deployments on Linux and UNIX operating systems, making use of storage replication and Oracle Data Guard technologies.

### [Terminology](#)

Learn about Disaster Recovery terminology.

### 1.1.1 Problem Description and Common Solutions

Learn how to deploy an Oracle Fusion Middleware Disaster Recovery solution for enterprise deployments on Linux and UNIX operating systems, making use of storage replication and Oracle Data Guard technologies.

Providing Oracle 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, cluster integration, GridLink, load balancing, failover, backup and recovery, rolling upgrades, and rolling configuration changes, which protect an enterprise deployment from unplanned downtime 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 periodically to the standby site. 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 usually 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 inter-operates with other technologies and business applications. For instance, Oracle Fusion Middleware products 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.

## 1.1.2 Terminology

Learn about Disaster Recovery terminology.

Disaster Recovery uses the following terms:

- **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. [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.

- **Virtual Host Name**

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

---

---

**Note:**

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

---

---

- **Virtual IP**

Generally, a virtual IP can be assigned to a hardware cluster or load balancer. To present a single system view of a cluster to network clients, a virtual IP serves as an entry point IP address to the group of servers which are members of the cluster. A virtual IP can be assigned to a server load balancer or a hardware cluster.

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

nodes. The node with current ownership of a cluster IP address is active for that address.

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

- **Production Site Setup**

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 binary files 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 [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 [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 guide 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.

- **Target**

Targets are core Enterprise Manager entities which represent the infrastructure and business components in an enterprise. These components need to be monitored and managed for efficient functioning of the business. For example, Oracle Fusion Middleware farm or Oracle Database.

- **System**

A System is the set of targets (hosts, databases, application servers, and so on) that work together to host your applications. To monitor an application in Enterprise Manager, you would first create a System, that consists of the database, listener, application server, and hosts targets on which the application runs.

- **Site**

Site is a set of different targets in a datacenter needed to run a group of applications. For example, a site could consist of Oracle Fusion Middleware instances, databases, storage, and so on. A datacenter may have more than one site defined by Oracle Site Guard and each of them managed independently for operations like switchover and failover.

## 1.2 Setting Up Disaster Recovery for Oracle Fusion Middleware Components

Learn how to set up your Disaster Recovery for an Oracle Fusion Middleware enterprise deployment.

The following section describe the setup details:

- [Oracle Fusion Middleware Disaster Recovery Architecture Overview](#)

Learn about the deployment architecture for Oracle Fusion Middleware components and the methods it supports to protect Oracle Fusion Middleware data and database content.

- [Components Described in This Document](#)

Learn about the Oracle product suites that Oracle Fusion Middleware Disaster Recovery supports.

### 1.2.1 Oracle Fusion Middleware Disaster Recovery Architecture Overview

Learn about the deployment architecture for Oracle Fusion Middleware components and the methods it supports to protect Oracle Fusion Middleware data and database content.

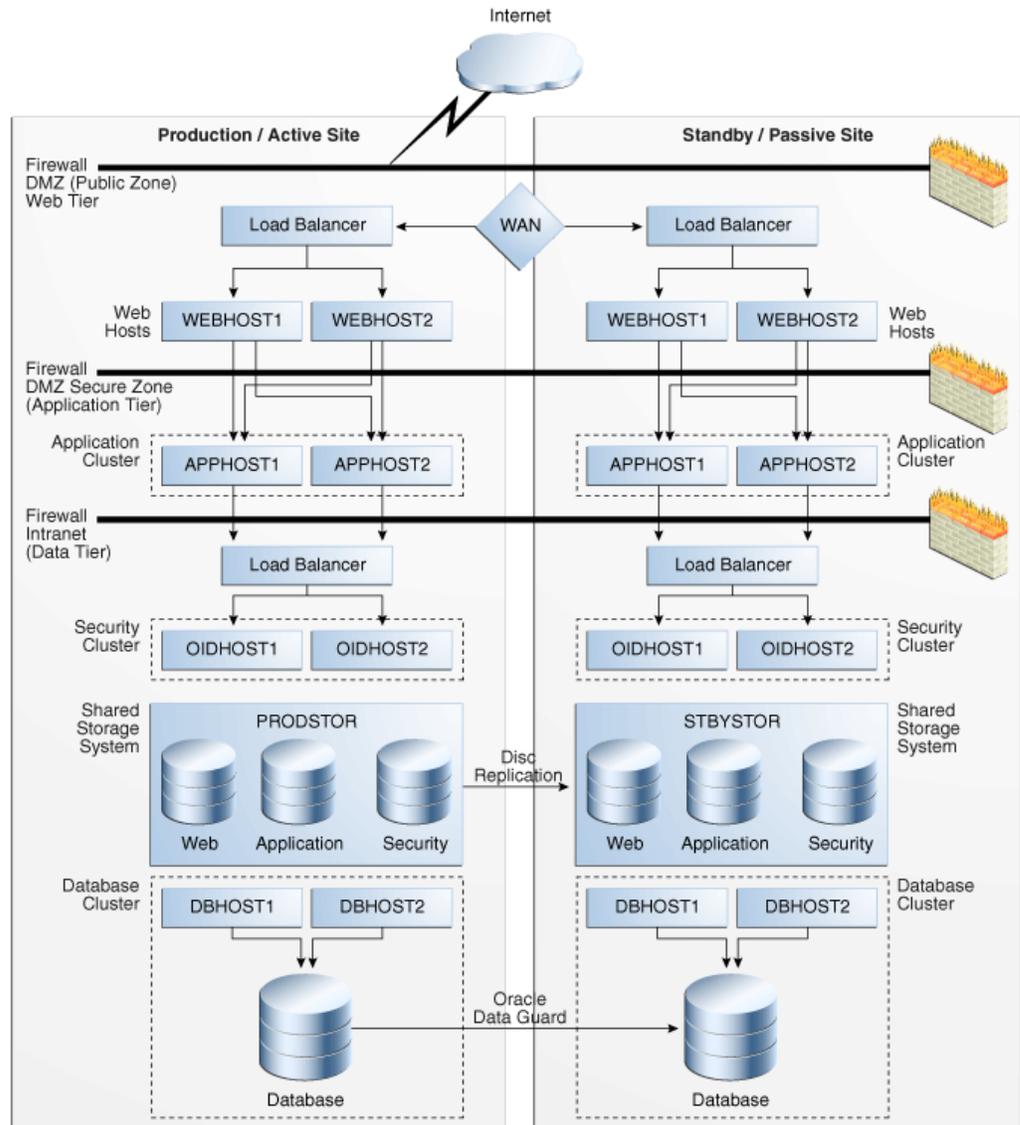
The product binary files and configuration for Oracle Fusion Middleware components and applications get deployed in Oracle home directories on the middle tier. Additionally, most of the products also have metadata or runtime data stored in a database repository. Therefore, the Oracle Fusion Middleware 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.

To protect Oracle Fusion Middleware data and database content, Oracle Fusion Middleware Disaster Recovery supports the following methods:

- Oracle Fusion Middleware product binary files, configuration files, 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 Sites 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 binary files 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 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 [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 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 [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. See [Recommendations for Oracle 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 [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, 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 reroute 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

Learn about the Oracle product suites that Oracle Fusion Middleware Disaster Recovery supports.

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

- Oracle WebLogic Server

See [Recommendations for Oracle WebLogic Server](#) for Disaster Recovery recommendations for Oracle WebLogic Server 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
  - Oracle Business Process Management

See [Recommendations for Oracle SOA Suite](#) for Disaster Recovery recommendations for Oracle SOA Suite components.
- Oracle BI Suite components
  - Oracle Business Intelligence Enterprise Edition (EE)
  - Oracle Business Intelligence Publisher

See [Recommendations for Oracle Business Intelligence Suite](#) for Disaster Recovery recommendations for Oracle BI Suite components.



---

## Recommendations for Oracle Fusion Middleware Components

Learn about the disaster protection requirements for Oracle Fusion Middleware components in different Oracle product suites and recommendations for synchronizing those components.

Oracle Fusion Middleware Disaster Recovery uses storage replication to synchronize the middle tier content, and use Oracle Data Guard to synchronize data in Oracle databases and custom application databases included in your topology.

---

**Note:**

Certain artifacts like Oracle Inventory, the `beahomelist`, the `oratab` and the `oraInst.loc` files are common across all Oracle product deployments. These artifacts change very rarely and need not be part of the regular storage replication and synchronization activity. Oracle recommends placing Oracle Inventory, the `beahomelist`, the `oratab`, and the `oraInst.loc` files on the local disk of your 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. For information about managing Oracle Inventory, see [Managing Oracle Inventory](#).

---

For related information, see the following documents:

- *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 Portal*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence*
- *Oracle Fusion Middleware Administering Oracle Fusion Middleware*

This chapter includes the following sections:

### [Recommendations for Oracle WebLogic Server](#)

Oracle WebLogic Server is a scalable, enterprise-ready Java Platform, Enterprise Edition (Java EE) application server.

### [Recommendations for Oracle SOA Suite](#)

Oracle SOA Suite is an Oracle Fusion Middleware component that provides a complete set of service infrastructure components for designing, deploying, and managing SOA composite applications.

### [Recommendations for Oracle Business Intelligence Suite](#)

Oracle Business Intelligence Suite (Oracle BI) is a portfolio of technology and applications that provides the industry's first integrated, end-to-end Enterprise Performance Management System, including Oracle Business Intelligence foundation and tools as well as financial performance management applications, operational Oracle Business Intelligence applications, and data warehousing.

### [Recommendations for Oracle WebCenter Portal](#)

Oracle WebCenter Portal is an Oracle Fusion Middleware component that provides a personalized, secure, and efficient way of presenting and consuming information, collaborating with others, and interacting with applications in the context of business processes.

### [Recommendations for Oracle WebCenter Content](#)

Oracle WebCenter Content is an integrated suite of products designed to manage enterprise content.

## 2.1 Recommendations for Oracle WebLogic Server

Oracle WebLogic Server is a scalable, enterprise-ready Java Platform, Enterprise Edition (Java EE) application server.

The Oracle WebLogic Server infrastructure supports the deployment of many types of distributed applications, and is an ideal foundation for building applications based on the Oracle Fusion Middleware product suite.

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

- **Artifacts on the File System**

Oracle home: The Oracle home consists of a WebLogic home that has the WebLogic Server binary files.

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

- **Network Artifacts**

Oracle recommends using a virtual alias (instead of physical host names) as the listen address for both Oracle WebLogic Administration server and the Managed Servers. As long as this alias can be resolved on both the production and standby sites, there is no need to update this value after a Disaster Recovery operation.

If your environment requires whole server migration to be configured, then 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, ensure 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 Java Message Service \(JMS\) and Transaction Logs \(T-Logs\)](#)

Learn about the Oracle WebLogic Server JMS and T-Log artifacts and what Oracle recommends for disaster recovery.

### Recommendations for Oracle Platform Security Services

Learn about the Oracle Platform Security Services artifacts and what Oracle recommends for disaster recovery.

## 2.1.1 Recommendations for Oracle WebLogic Server Java Message Service (JMS) and Transaction Logs (T-Logs)

Learn about the Oracle WebLogic Server JMS and T-Log artifacts and what Oracle recommends for disaster recovery.

- **Artifacts on the File System:**

File-based persistent stores: The file store location for the JMS and 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.

When automatic whole server migration is configured, the required leasing table is in the database.

- **Special Considerations:**

- Messages are lost if they were enqueued 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 the reverse. This may delete unprocessed messages in addition to duplicate messages.
- If the store is not dedicated to JMS use, then 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 WebLogic Scripting Tools (WLST).
- When applications use both queues and topics, ensure that you manipulate both the queue and topic subscriptions.

- **Synchronization Recommendations:**

- If JMS data is critical, then synchronize transaction log data and JMS data in real time using synchronous replication. Using synchronous replication may have performance implications.
- If data consistency between tiers is important, then 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 create a consistent backup. This ensures that the persistence store is not being written to while the copy operation is being performed. In a clustered environment, shut down one server at a time, back it up, and restart it. You also can create a script to perform these operations using WLST.
- **Recovery Recommendations:**  
Recover the database schemas containing the persistent stores for the Administration Server and the Managed Servers in the WLS domain to the most recent point in time.

Also, use the following recovery recommendations to avoid duplicate messages.

### Avoiding Duplicate Messages

Perform the following procedure before recovery to filter messages in the JMS queue after persistent-store recovery, to avoid processing duplicate messages:

---



---

**Note:**

Do not drain and discard messages without 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 in to the Oracle WebLogic Server Administration Console.
2. Before recovery, configure JMS server to pause Production, Insertion, and Consumption operations at Startup. This ensures 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 that 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, and then select a destination.
- c. Select **Monitoring**, and then click **Show Messages**.
- d. Click **Delete All**.

Resume operations by following the instructions listed in step 2.

## 2.1.2 Recommendations for Oracle Platform Security Services

Learn about the Oracle Platform Security Services artifacts and what Oracle recommends for disaster recovery.

- **Artifacts in the Database:**

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

- **Synchronization Recommendations:**

You must manually synchronize the application tier with the standby site after making configuration changes and applying patches.

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database. See [Synchronizing Databases Manually](#) and [Applying Redo Data to Physical Standby Databases](#).

- **Recovery Recommendations:**

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

## 2.2 Recommendations for Oracle SOA Suite

Oracle SOA Suite is an Oracle Fusion Middleware component that 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 that combine multiple technology components.

A SOA composite application consists of:

- **Service components:** Service components are the basic building blocks of SOA composite applications. Service components implement 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 older Oracle SOA Suite releases, like 11g, the soa-infra and service-engine configuration files were stored in local or shared storage files as part of the domain configuration. Starting with Oracle SOA Suite 12c R1, those files reside in the metadata repository database. 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 12c R2 (12.2.1) release.

---

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 binary files and domain-related configuration files are stored on a local or shared file system.

**Common Artifacts and Considerations for All Oracle SOA Suite Components**

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

**Artifacts on the File System**

Oracle home: The Oracle home consists of a WebLogic home that has the WebLogic Server binary files and an Oracle home containing the Oracle SOA Suite binary files.

Oracle Common Home: This is 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 sites, 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 for updating an IP address to a virtual host name.

The load balancer virtual hosts required for accessing the Oracle 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 changes in the domain-related configuration, deploying composites, and applying patches.

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database. See [Synchronizing Databases Manually](#) and [Applying Redo Data to Physical Standby Databases](#).

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

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

The following sections describe Disaster Recovery recommendations for Oracle SOA Suite components:

### [Recommendations for Oracle SOA Service Infrastructure](#)

Oracle SOA Service Infrastructure is a Java EE application that provides the foundation services for running Oracle SOA Suite.

### [Recommendations for Oracle BPEL Process Manager](#)

The Oracle BPEL Process engine is the service engine running in an Oracle SOA Service Infrastructure that allows the execution of BPEL processes.

### [Recommendations for Oracle Mediator](#)

Oracle Mediator is a service engine within the Oracle SOA Service Infrastructure that provides the framework to mediate between providers and consumers of services and events.

### [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 and the human interaction support such as approvals, rejects, and reassign actions.

### [Recommendations for Oracle B2B](#)

Oracle B2B connects SOA composite applications to external services, applications, and technologies, and offers a multi-protocol gateway that supports industry-recognized business-to-business (B2B) standards.

#### [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. Oracle Web Services Manager consists of the Policy Manager and the Agent.

#### [Recommendations for Oracle User Messaging Service](#)

Oracle User Messaging Service enables two-way communication between users and deployed applications and it supports a variety of channels, such as e-mail, IM, SMS, and text-to-voice messages.

#### [Recommendations for Oracle Java EE Connector Architecture \(JCA\) Adapters](#)

Oracle JCA Adapters are JCA binding components that allow the Service Infrastructure to communicate using different protocols.

#### [Recommendations for Oracle Business Activity Monitoring](#)

Oracle Business Activity Monitoring (Oracle BAM) provides the tools for monitoring business services and processes in the enterprise and allows quickly correlation of market indicators to the actual and changing business processes.

#### [Recommendations for Oracle Business Process Management](#)

The Oracle Business Process Management ( Oracle BPM) Suite provides an integrated environment for developing, administering, and using business applications centered around business processes.

## 2.2.1 Recommendations for Oracle SOA Service Infrastructure

Oracle SOA Service Infrastructure is a Java EE application that provides the foundation services for running Oracle SOA Suite.

This Java EE application is a runtime engine that is automatically deployed when Oracle 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 lifecycle and run-time operations of the composite.

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 Oracle SOA Service Infrastructure database.

### **Synchronization Recommendations**

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

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in

Managed Recovery mode, then you should manually synchronize the standby database.

### **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.

## **2.2.2 Recommendations for Oracle BPEL Process Manager**

The Oracle BPEL Process engine is the service engine running in an Oracle 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.

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

### **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, because no cleanup is required after performing a Disaster Recovery operation. If non-idempotent 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.

## **2.2.3 Recommendations for Oracle Mediator**

Oracle Mediator is a service engine within the Oracle SOA Service Infrastructure that provides the framework to mediate between providers and consumers of services and events.

Oracle Mediator 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. 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.

---

---

**Note:**

Sequential routing rules do not persist their messages into the database as part of the execution.

---

---

### **Synchronization Recommendations**

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

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

### **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 application.

## **2.2.4 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 and the human interaction support such as approvals, rejects, and reassign actions.

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 changes in the domain configuration and applying patches.

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

### Recovery Recommendations

The database must be recovered to the most recent point in time, along with the Managed Server running the SOA application. The Oracle Human Workflow engine uses Oracle User Messaging Service to send and receive notifications. See [Recommendations for Oracle User Messaging Service](#) for details about Oracle User Messaging Service.

## 2.2.5 Recommendations for Oracle B2B

Oracle B2B connects SOA composite applications to external services, applications, and technologies, and offers a multi-protocol gateway that supports industry-recognized business-to-business (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 that Oracle B2B uses internally.

**Table 2-1 JMS Queues 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 e-mail 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, see [Recommendations for Oracle WebLogic Server Java Message Service \(JMS\) and Transaction Logs \(T-Logs\)](#).

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

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

#### **Recovery Recommendations**

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

## **2.2.6 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. Oracle Web Services Manager consists of the Policy Manager and the Agent.

Oracle WSM provides capabilities to build, enforce, execute and monitor web services policies including security, Web Services Reliable Messaging, Message Transmission Optimization Mechanism and addressing policies.

The Policy Manager reads and writes security and management policies, including predefined and custom policies from the MDS repository. The 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, gathering of runtime statistics. The agent is available on all Oracle Fusion Middleware Managed Servers and is configured on the same server as the application 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 changes in the domain-related configuration and applying patches.

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then manually synchronize the standby database.

#### **Recovery Recommendations**

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

## 2.2.7 Recommendations for Oracle User Messaging Service

Oracle User Messaging Service enables two-way communication between users and deployed applications and it supports a variety of channels, such as e-mail, IM, SMS, and text-to-voice messages.

Oracle User Messaging Service is integrated with Oracle Fusion Middleware components such as Oracle BPEL Process Manager, Oracle Human Workflow, Oracle Business Activity Monitoring (BAM) and Oracle WebCenter Portal. It is typically deployed with Oracle User, 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 that Oracle User Messaging Service uses.

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

JMS Artifact Name	Type	JNDI Name
OraSDPMAAppDefRcvQ1_auto	Distributed queue	OraSDPM/Queues/ OraSDPMAAppDefRcvQ1
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 the 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 changes in the configuration, deploying additional Oracle User Messaging Service drivers, and applying patches.

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

### **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 the 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, see Synchronization Recommendations in [Recommendations for Oracle WebLogic Server Java Message Service \(JMS\) and Transaction Logs \(T-Logs\)](#).

## **2.2.8 Recommendations for Oracle Java EE Connector Architecture (JCA) Adapters**

Oracle JCA Adapters are JCA binding components that allow the Service Infrastructure to communicate using different protocols.

Oracle JCA Adapters are deployed as a JCA resource (RAR) and are not part of the Oracle SOA Service Infrastructure.

The Oracle JCA Adapters include:

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

See the *Oracle Fusion Middleware Understanding 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 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 location of each `weblogic-ra.xml`

file 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 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 changes in the domain-related configuration (that is, adapter configuration changes) and applying patches.

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then manually synchronize the standby database.

#### **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.

## **2.2.9 Recommendations for Oracle Business Activity Monitoring**

Oracle Business Activity Monitoring (Oracle BAM) provides the tools for monitoring business services and processes in the enterprise and allows quickly correlation of market indicators to the actual and changing business processes.

Oracle BAM provides the necessary tools and runtime 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 Oracle BAM schemas and the metadata repository.

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

#### **Recovery Recommendations**

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

## 2.2.10 Recommendations for Oracle Business Process Management

The Oracle Business Process Management ( Oracle BPM) Suite provides an integrated environment for developing, administering, and using business applications centered around business processes.

Oracle BPM Suite provides a seamless integration of all stages of the application development life cycle from design-time and implementation to runtime and application management.

The Oracle BPM Suite is layered on the Oracle SOA Suite and shares many of the same product components, including:

- Oracle Business Rules
- Oracle Human Workflow
- Oracle adapter framework for integration
- SOA Composite Architecture

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

### Artifacts on the File System

BPM JMS Persistent Store (BPMJMSFileStore\_auto): The file-based JMS persistent store. The persistence store must be synchronized with the standby site to resume processing after failover.

### Artifacts in the Database

Process definition, deployed applications, and configuration files are stored in the Oracle Metadata Services (MDS) repository. Oracle BPM also uses a separate MDS partition to share projects and project templates between process analysts and process developers.

### Synchronization Recommendations

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

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

When the application tier synchronization is initiated on the storage, the standby database is also updated to the same point in time. This is recommended if a snapshot Standby database is used.

### Recovery Recommendations

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

## 2.3 Recommendations for Oracle Business Intelligence Suite

Oracle Business Intelligence Suite (Oracle BI) is a portfolio of technology and applications that provides the industry's first integrated, end-to-end Enterprise Performance Management System, including Oracle Business Intelligence foundation

and tools as well as financial performance management applications, operational Oracle Business Intelligence applications, and data warehousing.

Oracle BI has the following components:

- **Administration Server:** runs in a dedicated Java virtual machine and is used for administering the system. When using two or more servers for HA, the Administration Server exists on both hosts but is only active on one host.
- **Managed Server:** runs in a dedicated Java virtual machine and provides the runtime environment for the Java-based services and applications.
- **Node Manager:** provides management services for the Administration Server, Managed Servers and the System Components.
- **System Components:** server processes that provide the core services to Oracle BI. Oracle BI components are as follows:
  - BI Server
  - BI Scheduler
  - BI Java Host
  - BI Preservation Server
  - Cluster Controller

Other domain contents includes the configuration file, WebLogic Server Tool commands, security, and connection information required to run Oracle BI.

Oracle BI 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 binary files and domain-related configuration files are stored on a local or shared file system.

For more information about Oracle BI Architecture, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence*.

This section contains the following recommendations:

#### [Common Recommendations for All Oracle Business Intelligence Suite Components](#)

Learn about what Oracle recommends for all Oracle Business Intelligence Suite (Oracle BI) components.

#### [Recommendations for Oracle Business Intelligence Enterprise Edition \(EE\)](#)

Oracle Business Intelligence Enterprise Edition (Oracle BI EE) brings business visibility and insight to a wide variety of users in an enterprise.

#### [Recommendations for Oracle Business Intelligence Publisher](#)

Oracle Business Intelligence Publisher (BI Publisher, formerly XML Publisher) allows you to create highly formatted reports that are suitable for printing Business Intelligent reports.

### **2.3.1 Common Recommendations for All Oracle Business Intelligence Suite Components**

Learn about what Oracle recommends for all Oracle Business Intelligence Suite (Oracle BI) components.

The following artifacts and considerations apply to all Oracle BI components, in addition to the component specific considerations.

#### **Artifacts on the File System**

Oracle home — The Oracle home consists of a WebLogic home that has the WebLogic Server binary files and an Oracle home containing the Oracle BI Suite binary files.

Domain home — The domain home contains the WebLogic Administration Server and WebLogic Managed Server configuration data, logs, and Oracle BI applications for the domain.

SDD (Singleton Data Directory) — A directory that contains the metadata and other cross-cluster files. There is exactly one SDD for each domain. The SDD path (by default `DOMAIN_HOME/bidata`) is defined in the file `bi-environment.xml`, located at `DOMAIN_HOME/config/fmwconfig/bienv/core/bi-environment.xml`.

#### **Network Artifacts**

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

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

#### **Artifacts in the Database**

The Oracle Business Intelligence schemas are located in the Oracle Business Intelligence database.

Schema-based metadata – This is nondesign-time metadata that is stored in database schemas (including schemas for the Scheduler, usage statistics, event polling, repository files, and the Oracle BI Presentation Catalog).

#### **Synchronization Recommendations**

The directory tier must be manually synchronized with the standby site after changing the domain configuration, after deploying composites, or after applying patches.

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

Oracle recommends synchronizing the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database. See *Applying Redo Data to Physical Standby Databases in Oracle Data Guard Concepts and Administration*.

#### **Recovery Recommendations**

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

## **2.3.2 Recommendations for Oracle Business Intelligence Enterprise Edition (EE)**

Oracle Business Intelligence Enterprise Edition (Oracle BI EE) brings business visibility and insight to a wide variety of users in an enterprise.

Oracle BI EE is a comprehensive set of enterprise business intelligence tools and infrastructure, including a scalable and efficient query and analysis server, an ad-hoc query and analysis tool, interactive dashboards, proactive intelligence and alerts, real-time predictive intelligence, and an enterprise reporting engine.

The following are recommendations specific to Oracle BI EE.

#### **Artifacts in the Database**

BIPLATFORM schema is part of the Oracle BI EE database.

#### **Special Considerations**

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

#### **Synchronization Recommendations**

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

Oracle recommends synchronizing the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

#### **Recovery Recommendations**

Recover the Middleware home, the domain, and the Oracle instance containing the Oracle BI EE components. On Windows, import Oracle BI EE Registry entries. Recover the database to the most recent point in time, if needed.

### **2.3.3 Recommendations for Oracle Business Intelligence Publisher**

Oracle Business Intelligence Publisher (BI Publisher, formerly XML Publisher) allows you to create highly formatted reports that are suitable for printing Business Intelligent reports.

BI Publisher reports are built on top of BI Publisher data models. BI Publisher data model can consist of data sets from a wide range of sources, such as subject areas from the Oracle Business Intelligence Server or analyses, SQL queries against relational data bases, MDX queries against Subbase, LDAP, web services, Microsoft Excel, HTTP feeds, or XML files. BI Publisher supports a wide range of layout types, so you can create the full range of documents that your organization might need. Within Oracle Business Intelligence Enterprise Edition you can view, create, edit, and schedule BI Publisher reports and then include them in dashboard pages.

The following are recommendations specific to BI Publisher.

#### **Artifacts in the Database**

BIPLATFORM schema is a part of the Oracle Business Intelligence Publisher database.

#### **Special Considerations**

Load balancer virtual hosts for Oracle Business Intelligence Publisher 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 changes in the configuration and applying patches.

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

### **Recovery Recommendations**

Recover the WebLogic Managed Server containing the BI Publisher component.

## **2.4 Recommendations for Oracle WebCenter Portal**

Oracle WebCenter Portal is an Oracle Fusion Middleware component that provides a personalized, secure, and efficient way of presenting and consuming information, collaborating with others, and interacting with applications in the context of business processes.

Oracle WebCenter Portal optimizes the connections between people, information, and applications; provides a context for users to navigate, discover, and access content relevant to your business needs.

Oracle WebCenter Portal includes the following servers, applications, and services:

- Portal Managed Servers:
  - Portal application and services
  - Analytics Collector service
- Collaboration Managed Servers:
  - Discussions application and services
- Portlet Managed Servers:
  - Portlet Producer services
  - Pagelet Producer service

This section contains the following recommendations:

### [Common Recommendations for All Oracle WebCenter Portal Components](#)

Learn about what Oracle recommends for all Oracle WebCenter Portal components.

### [Recommendations for Oracle WebCenter Portal Server](#)

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

### [Recommendations for Oracle WebCenter Analytics](#)

Oracle WebCenter Portal allows for a single active analytics collector registration. The Analytics Collector receives usage metrics from the Portal application. All connections to the Analytics Collector are stateless.

### [Recommendations for Oracle WebCenter Discussion Server](#)

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

### Recommendations for Oracle WebCenter Portlet and Pagelet Services

Oracle WebCenter Portal supports deployment and execution of both standards-based portlets (WSRP 2.0), and traditional Oracle (Portlet Developer Kit) PDK-Java based portlets. Oracle WebCenter Portal provides several ready-to-use producers.

## 2.4.1 Common Recommendations for All Oracle WebCenter Portal Components

Learn about what Oracle recommends for all Oracle WebCenter Portal components.

The following artifacts and considerations apply to all Oracle WebCenter Portal components.

### Artifacts on the File System

**Oracle home** — The Oracle home consists of a WebLogic home that has the Oracle WebLogic Server binary files.

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

There are no shared files system persistence store requirements for any Oracle WebCenter Portal runtime components.

### Network Artifacts

Oracle recommends using a virtual alias (instead of physical host names) as the listen address for both Oracle WebLogic Administration server and the Oracle Managed Servers. As long as this alias can be resolved on both the production and standby sites, there is no need to update this value after a Disaster Recovery operation.

Oracle WebCenter Portal does not require whole server migration or service migration to be configured. No special considerations are needed in this regard.

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

### Artifacts in the Database

Oracle WebCenter Portal stores all data and metadata in database schemas created with the Repository Creation Utility. Application runtime configuration metadata is store via the Metadata Services Repository (MDS).

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making changes in the domain-related configuration, deploying applications or shared libraries, or applying patches.

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization can occur automatically when Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database. See *Applying Redo Data to Physical Standby Databases in Oracle Data Guard Concepts and Administration*, and [Synchronizing Databases Manually](#).

### Recovery Recommendations

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

## 2.4.2 Recommendations for Oracle WebCenter Portal Server

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

The following are recommendations specific to Oracle WebCenter Portal Server.

### Artifacts in the Database

Portal application data is stored in the `WEBCENTER` database schema. Portal customized metadata is stored in the `MDS` database schema

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after changing the configuration, deploying applications, or applying patches.

Oracle Data Guard should be configured for the Oracle database containing the `WEBCENTER` schema, and metadata repository.

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization can occur automatically when Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database. See *Applying Redo Data to Physical Standby Databases in Oracle Data Guard Concepts and Administration*, and [Synchronizing Databases Manually](#).

### 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 Portal domain.

## 2.4.3 Recommendations for Oracle WebCenter Analytics

Oracle WebCenter Portal allows for a single active analytics collector registration. The Analytics Collector receives usage metrics from the Portal application. All connections to the Analytics Collector are stateless.

Following an Enterprise Deployment Guide topology deployment, each portal server has one active local analytics collector service responsible for collecting metrics for all portal traffic on that portal server. The recommended configuration is to set the portal's common connection registration to `localhost`, and the default port of `31314`. Each portal server connects locally. Load-balancer configurations are not required and no configuration changes are needed for failover to the secondary site for analytics functionality.

The following are recommendations specific to Oracle WebCenter Analytics.

### Artifacts in the Database

Analytics Collector data is stored in the Oracle WebCenter Portal's `ACTIVITIES` schema.

### Synchronization Recommendations

The application tier must be manually synchronized with the standby site after making any changes in the configuration to the Analytics Collector MBeans, the Portal's Analytics service registration, or applying patches.

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization can occur automatically when Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database. See *Applying Redo Data to Physical Standby Databases in Oracle Data Guard Concepts and Administration*, and [Synchronizing Databases Manually](#).

#### **Recovery Recommendations**

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

### **2.4.4 Recommendations for Oracle WebCenter Discussion Server**

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

The following are recommendations specific to Oracle WebCenter Discussion. Server.

#### **Artifacts in the Database**

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

#### **Synchronization Recommendations**

The application tier must be manually synchronized with the standby site after changing the configuration, deploying applications, or applying patches.

Oracle Data Guard should be configured for the Oracle database containing the Oracle Discussion Server schema, and metadata repository.

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization can occur automatically when Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database. See *Applying Redo Data to Physical Standby Databases in Oracle Data Guard Concepts and Administration*, and [Synchronizing Databases Manually](#).

#### **Recovery Recommendations**

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

### **2.4.5 Recommendations for Oracle WebCenter Portlet and Pagelet Services**

Oracle WebCenter Portal supports deployment and execution of both standards-based portlets (WSRP 2.0), and traditional Oracle (Portlet Developer Kit) PDK-Java based portlets. Oracle WebCenter Portal provides several ready-to-use producers.

The following are recommendations specific to Oracle WebCenter Portlet and Pagelet.

#### **Artifacts in the Database**

The PORTLET schema stores user customized data and is part of the Oracle WebCenter Portal schemas. The MDS repository stores portlet metadata and configuration information.

### **Synchronization Recommendations**

The application tier must be manually synchronized with the standby site after changing the configuration, deploying applications, or applying patches.

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization can occur automatically when Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database. See *Applying Redo Data to Physical Standby Databases in Oracle Data Guard Concepts and Administration*, and [Synchronizing Databases Manually](#).

### **Recovery Recommendations**

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

## **2.5 Recommendations for Oracle WebCenter Content**

Oracle WebCenter Content is an integrated suite of products designed to manage enterprise content.

Oracle WebCenter Content enables you to leverage industry-leading document management, Web content management, digital asset management, and records management functionality to build your business applications. The ability to manage the enterprise content helps you reduce costs, share content across the enterprise, minimize risk, automate manual processes, and consolidate multiple Web sites onto a single platform.

Oracle Enterprise Content Management includes the following components:

- Oracle WebCenter Content
- Oracle WebCenter Content: Inbound Refinery
- Oracle WebCenter Content: Enterprise Capture
- Oracle WebCenter Content: Content User Interface

This section contains the following recommendations:

#### [Common Recommendations for All Oracle WebCenter Content Components](#)

Learn about what Oracle recommends for all Oracle WebCenter Content components.

#### [Recommendations for Oracle WebCenter Content](#)

Oracle WebCenter Content provides a unified application for several different kinds of content management.

#### [Recommendations for Oracle WebCenter Content Inbound Refinery](#)

Oracle WebCenter Content Inbound Refinery is a conversion server that manages file conversions for electronic assets such as documents, digital images, and motion video.

### [Recommendations for Oracle WebCenter Content Enterprise Capture](#)

Oracle WebCenter Enterprise Capture (Enterprise Capture) provides organizations with a single system to capture both paper and electronic documents.

### [Recommendations for Oracle WebCenter Content: Content User Interface](#)

WebCenter Content User Interface is a user-friendly and a feature-rich user interface for managing Oracle WebCenter Content based on Oracle Application Development Framework.

## 2.5.1 Common Recommendations for All Oracle WebCenter Content Components

Learn about what Oracle recommends for all Oracle WebCenter Content components.

The following artifacts and considerations apply to all Oracle WebCenter Content components.

### **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 Content 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.

**Domain Home:** The domain home contains the Administration Server and Managed Server configuration data and Oracle WebCenter Content applications for the domain.

**Oracle Instance:** The Oracle instance contains the configuration data for non-J2EE Oracle WebCenter Content applications like OPMN configuration and Enterprise Manager Agent configuration data.

**WebCenter Content Shared Directories files:** In a clustered implementation of WebCenter Content as per Enterprise Deployment guidelines shared directories are required for domain configuration as well as WebCenter Content shared directory files such as data, audit, and vault directories.

### **Network Artifacts**

Oracle recommends using a virtual alias (instead of physical host names) as the listen address for both Oracle WebLogic Administration server and the Oracle Managed Servers. As long as this alias can be resolved on both the production and standby sites, there is no need to update this value after a Disaster Recovery operation.

The load balancer virtual hosts used for accessing Oracle WebCenter Content Management components must be configured on both the production and standby sites.

### **Artifacts in the Database**

The Oracle WebCenter Content schemas are located in the Oracle WebCenter Content database.

### **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 the Oracle database metadata repository.

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization can occur automatically when Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

### **Recovery Recommendations**

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

## **2.5.2 Recommendations for Oracle WebCenter Content**

Oracle WebCenter Content provides a unified application for several different kinds of content management.

Through user-friendly interfaces, roles-based authentication and security models, Oracle WebCenter Content empowers users throughout the enterprise to view, collaborate on or retire content, ensuring that all accessible distributed or published information is secure, accurate and up-to-date.

The following are recommendations specific to Oracle WebCenter Content.

### **Artifacts in the Database**

The OCS (Oracle Content Schema) schema is part of the Oracle WebCenter Content database.

### **Artifacts in the File System**

WebCenter Content shared directories along with any Oracle Secure Files or the setup of file-based persistent stores need to be replicated across to the standby site for having them disaster protected.

### **Special Considerations**

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

### **Synchronization Recommendations**

The directory tier must be manually synchronized with the standby site after changing the configuration, deploying applications, or applying patches.

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

Oracle recommends that you synchronize the standby database when the application tier synchronization is initiated on the storage. This synchronization can occur automatically when Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

For file-based persistent stores, you must synchronize the file-based persistent stores on the standby site.

### **Recovery Recommendations**

Oracle WebCenter Content must be recovered with the OCS and MDS schemas to the most recent point in time..

### 2.5.3 Recommendations for Oracle WebCenter Content Inbound Refinery

Oracle WebCenter Content Inbound Refinery is a conversion server that manages file conversions for electronic assets such as documents, digital images, and motion video.

Oracle WebCenter Content Inbound Refinery provides thumbnail functionality for documents and images, storyboarding for video, and the ability to extract and use EXIF data from digital images and XMP data from electronic files generated from programs such as Adobe Photoshop and Adobe Illustrator. You can use Oracle WebCenter Content Inbound Refinery to convert content items stored in Oracle Content Server.

The following are recommendations specific to Oracle WebCenter Content Inbound Refinery.

#### **Artifacts in the Database**

Oracle WebCenter Content Inbound Refinery does not have any database dependencies.

#### **Special Considerations**

The load balancer virtual hosts required for Oracle WebCenter Content Inbound Refinery should be configured on both the production and the standby sites.

#### **Synchronization Recommendations**

The directory tier must be manually synchronized with the standby site after changing the configuration or applying patches.

#### **Recovery Recommendations**

Recover the Oracle WebCenter Content Inbound Refinery instance.

### 2.5.4 Recommendations for Oracle WebCenter Content Enterprise Capture

Oracle WebCenter Enterprise Capture (Enterprise Capture) provides organizations with a single system to capture both paper and electronic documents.

Enterprise Capture supports both centralized and distributed image capture from a user-friendly web interface capable of using high-volume, production-level scanners. Support for the industry-standard TWAIN scanning interface enables Enterprise Capture to use a wide variety of industry-leading document imaging. Enterprise Capture provides organizations with a single system to capture both paper and electronic documents scanners to digitize paper content. Existing electronic document files can be easily captured by users or automatically captured through an importing process that can monitor an email server or network folder. Once captured, documents are organized and indexed by applying metadata through manual or automated processes that use bar code recognition technology. After documents are completed, they are committed into a content management system. Enterprise Capture is fully integrated with Oracle WebCenter Content to provide organizations with one system to capture, store, manage and retrieve their mission critical business content.

The following are recommendations specific to Oracle WebCenter Content Enterprise Capture.

#### **Artifacts in the Database**

Resides in Oracle WebCenter Enterprise Capture schema.

#### **Artifacts in the File System**

There are no file system artifacts for Enterprise Capture unless its JMS servers are stored in file-based persistent stores. The recommendation is to configure JMS servers with database-based persistent stores so that Oracle Data Guard is leveraged to replicate the database schema across sites.

#### **Special Considerations**

The load balancer virtual hosts required for Oracle WebCenter Content Inbound Refinery should be configured on both the production and the standby sites.

#### **Synchronization Recommendations**

The directory tier must be manually synchronized with the standby site after changing the configuration or applying patches.

#### **Recovery Recommendations**

Enterprise Capture must be recovered with the Enterprise Capture schema to the most recent point in time, along with the Managed Server running the Oracle WebCenter Content Capture application, and the associated instances.

## **2.5.5 Recommendations for Oracle WebCenter Content: Content User Interface**

WebCenter Content User Interface is a user-friendly and a feature-rich user interface for managing Oracle WebCenter Content based on Oracle Application Development Framework.

The following are recommendations specific to Oracle WebCenter Content User Interface.

#### **Artifacts in the Database**

The Metadata Services schemas (MDS) are part of the Oracle WebCenter Content User Interface.

#### **Special Considerations**

Load balancer virtual hosts for Oracle WebCenter Content User Interface must be configured on both the production and standby sites.

#### **Synchronization Recommendations**

The directory tier must be manually synchronized with the standby site after changing the configuration or applying patches.

Oracle recommends that the standby database be synchronized when the application tier synchronization is initiated on the storage. This synchronization occurs automatically because Oracle Data Guard is configured in Managed Recovery mode (the recommended configuration) for the database. If the standby database is not in Managed Recovery mode, then you should manually synchronize the standby database.

#### **Recovery Recommendations**

Recover the Managed Servers running the Oracle WebCenter Content User Interface application, along with the Administration Server.

---

## Design Considerations

Learn about the design considerations to keep in mind when adapting an Oracle Fusion Middleware Disaster Recovery solution for your enterprise deployment

This chapter provides instructions about how to set up an Oracle Fusion Middleware Disaster Recovery production and standby sites for the Linux and UNIX operating systems. The procedures use the Oracle SOA Suite enterprise deployment (see [Figure 3-1](#)) in the examples to illustrate how to set up the Oracle Fusion Middleware Disaster Recovery solution for that enterprise deployment. After you understand how to set up Disaster Recovery for the Oracle SOA Suite enterprise topology, use that information to set up a Disaster Recovery for your other enterprise deployments as well.

---

**Note:**

- You can automate disaster recovery operations like switchover and failover, using Oracle Site Guard. For information about the product, see *Oracle Site Guard Administrator's Guide*.
- For information about installing and configuring Oracle SOA Suite components in an enterprise deployment, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*.
- See *Oracle Fusion Middleware Release Notes for Oracle Fusion Middleware Infrastructure* for updates about errors.

---

**Note:**

The Oracle Fusion Middleware 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 Oracle Fusion Middleware Disaster Recovery production and standby sites.

---

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

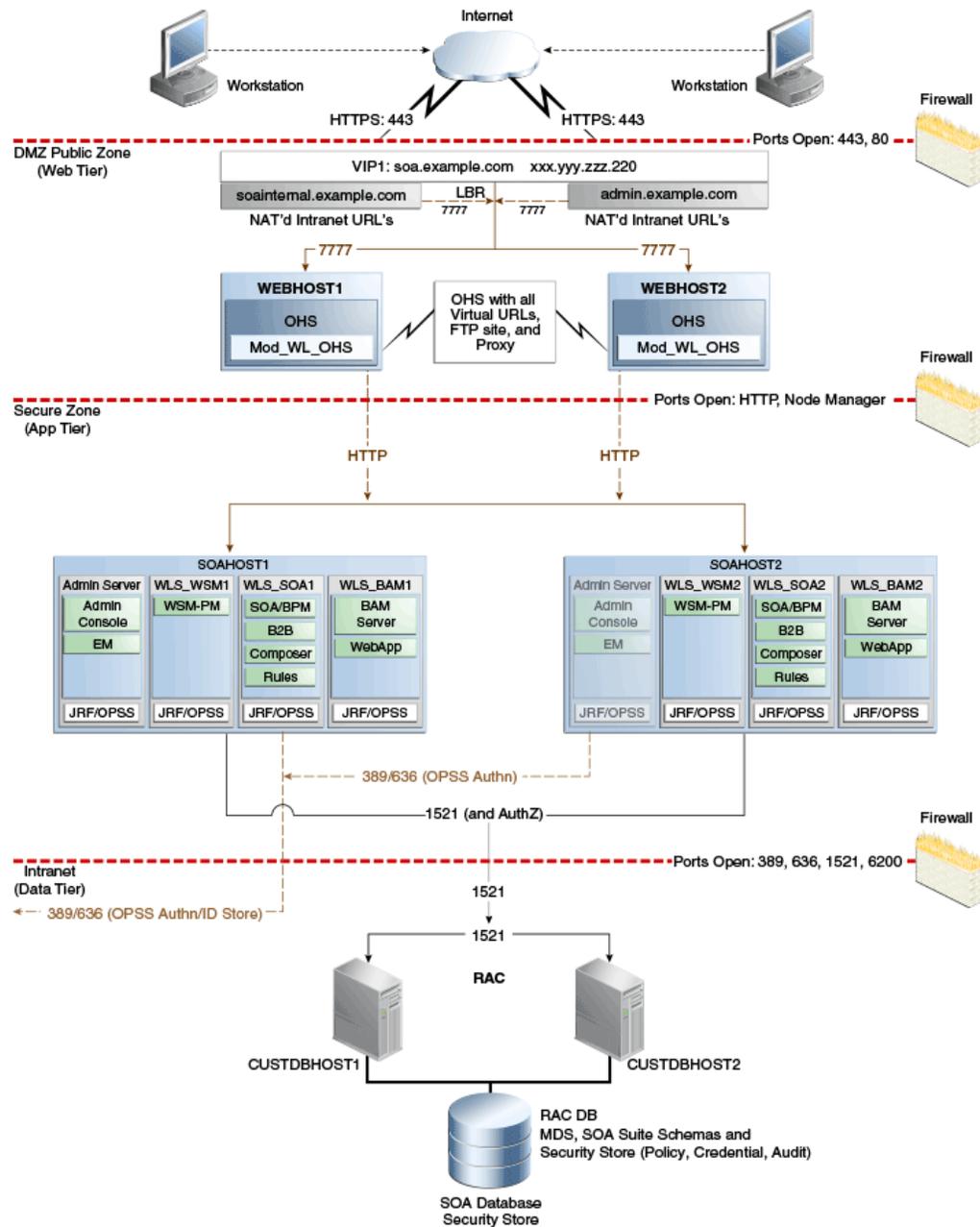


Figure 3-1 shows a diagram of the Oracle SOA, Business Process Management (BPM), and Oracle Service Bus enterprise deployment topology. See the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite* for detailed information about installing and configuring an Oracle SOA Suite enterprise deployment.

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

[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, then 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.

This chapter includes the following topics:

[Network Considerations](#)

When planning your Disaster Recovery solution, consider host names, load balance, and external clients.

[Storage Considerations](#)

When designing storage for your Disaster Recovery solution, consider Fusion Middleware artifacts, storage replication, and file-based persistent stores.

[Database Considerations](#)

When planning your Disaster Recovery solution, consider the synchronizing the databases in your system with Oracle Data Guard.

[Starting Points](#)

When planning your Disaster Recovery solution, consider starting with an existing site or creating a new site.

[Topology Considerations](#)

When planning your for your Disaster Recovery solution, consider designing a symmetric or an asymmetric topology.

## 3.1 Network Considerations

When planning your Disaster Recovery solution, consider host names, load balance, and external clients.

This section includes the following topics:

#### 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.

#### Virtual IP and Virtual Host Name Considerations

Virtual IP addresses and host names are required to enable the Oracle WebLogic Administration Server to continue servicing requests when the machine hosting the Oracle WebLogic Administration Server fails.

#### Load Balancer Considerations

Oracle Fusion Middleware components require a hardware load balancer when deployed in high availability topologies.

#### Virtual Server Considerations

Virtual servers and associated ports must be configured on the load balancer for different types of network traffic and monitoring.

#### External Clients Considerations

Systems directly accessing the servers in the topology need to be aware of the listen address used by different Oracle WebLogic Server instances.

#### Wide Area DNS Operations

When a site switchover or failover is carried out, client requests must be redirected transparently to the new site that is playing the production role.

### 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.

It is important to plan the host names for the production site and standby site. After failover from a primary site to a standby site, the alias host name for the middle tier host on the standby site becomes active. You do not need to reconfigure the host name for the host on the standby site if you set up an alias for the standby site.

Creating aliases for physical host names is required only when using a single global DNS server to resolve host names.

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 host-name-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 172.16.10.255), then use the host name `SOAHOST1.EXAMPLE.COM`, which resolves to 172.16.10.255.

The following section shows how to set up host names at the Disaster Recovery production and standby sites:

**Note:**

In the examples listed, IP addresses for hosts at the initial production site have the format 172.16.x.x and IP addresses for hosts at the initial standby site have the format 172.26.x.x.

### [Host Names for the Oracle SOA Suite Production and Standby Site Hosts](#)

Learn about the Oracle SOA Suite production and standby sites.

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

Learn about the Oracle SOA Suite production and standby sites.

[Table 3-1](#) shows the IP addresses and physical host names that will be used for the Oracle SOA Suite Enterprise Deployment Guide (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**

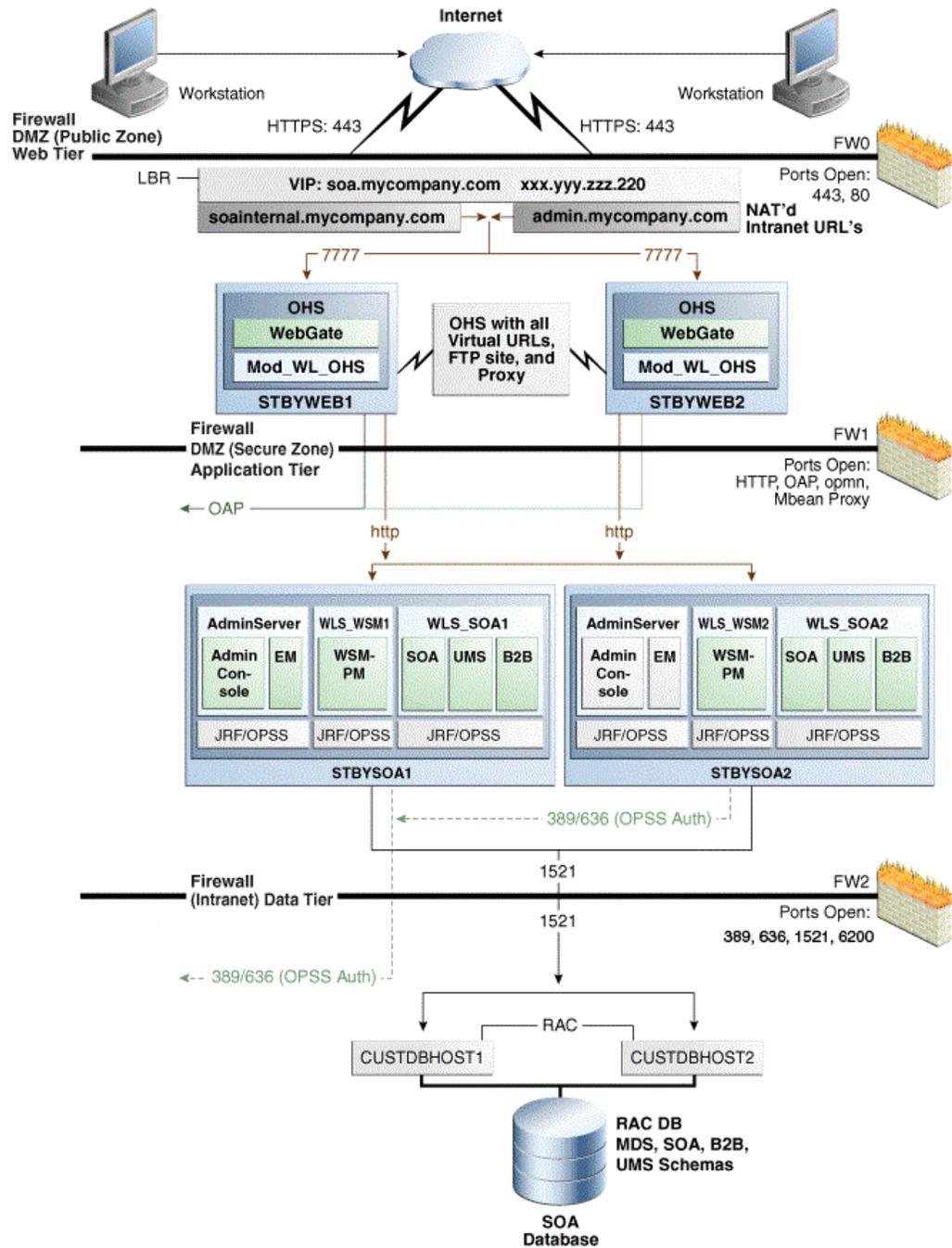
IP Address	Physical Host Name	Host Name Alias
172.16.2.111	WEBHOST1	None
172.16.2.112	WEBHOST2	None
172.16.2.113	SOAHOST1	None
172.16.2.114	SOAHOST2	None

[Figure 3-2](#) shows the physical host names used for the Oracle SOA Suite 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. For more information about using separate DNS servers to resolve host names, see [Resolving Host Names Using Separate DNS Servers](#).

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



The Administration Server, the Managed Servers, and the SOA Managed Servers require a floating IP address to be provisioned on each site (Table 3-2). Ensure that you provision the floating IP addresses with the same virtual host names on the production site and the standby site.

**Table 3-2 Floating IP Addresses**

Physical Host Name	Virtual Host Name	Floating IP
AdminServer	ADMINVHN	172.16.2.134
WEBHOST1	WEBVHN1	172.16.2.135
WEBHOST2	WEBVHN2	172.16.2.136
SOAHOST1	SOAVHN1	172.16.2.137
SOAHOST2	SOAVHN2	172.16.2.138

The following topics describe the host name resolution and testing:

#### Host Name Resolution

Host name resolution means mapping a host name to the proper IP address for communication.

#### Resolving Host Names Locally

Local host name resolution uses the host name to IP mapping defined in the `/etc/hosts` file of a host.

#### Resolving Host Names Using Separate DNS Servers

Use separate DNS servers to resolve host names for your Disaster Recovery topology.

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

Use a global DNS server to resolve host names for your Disaster Recovery topology.

#### Testing the Host Name Resolution

Validate host name assignment 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.

#### 3.1.1.1.1 Host Name Resolution

Host name resolution means mapping 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.

For more information about using the `/etc/hosts` file to implement local host name file resolution, see [Resolving Host Names Locally](#).

- Resolving host names using DNS

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

For more information about two methods of implementing DNS server host name resolution, see [Resolving Host Names Using Separate DNS Servers](#) and [Resolving Host Names Using a Global DNS Server](#).

You must determine the method of host name resolution that 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 `/etc/hosts` file are used first to resolve host names.

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 are used first to resolve host names.

For simplicity and consistency, Oracle recommends that all the hosts within a site (production site or standby site) should 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.

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

```
hosts:  files  dns  nis
```

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

```
hosts:  dns  files  nis
```

#### **3.1.1.1.2 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 resolve host names for your Disaster Recovery topology in this way, consider the following points:

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 simplicity and ease of maintenance, Oracle recommends that you provide 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.
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 simplicity and ease of maintenance, Oracle recommends that you have the same entries on all the hosts of the standby site. [Example 3-4](#) shows the `/etc/hosts` file for the standby site of a SOA enterprise deployment topology.

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 returns the correct IP address (172.16.2.111) and indicates 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 returns the correct IP address (172.26.2.111) and it shows that the name `WEBHOST1` is associated with that IP address.

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

```
174.0.0.1      localhost.localdomain  localhost
172.16.2.111  WEBHOST1.EXAMPLE.COM  WEBHOST1
172.16.2.112  WEBHOST2.EXAMPLE.COM  WEBHOST2
172.16.2.113  SOAHOST1.EXAMPLE.COM  SOAHOST1
172.16.2.114  SOAHOST2.EXAMPLE.COM  SOAHOST2
```

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

```
176.0.0.1      localhost.localdomain  localhost
172.26.2.111  STBYWEB1.EXAMPLE.COM  STBYWEB1 WEBHOST1.EXAMPLE.COM WEBHOST1
172.26.2.112  STBYWEB2.EXAMPLE.COM  STBYWEB2 WEBHOST2.EXAMPLE.COM WEBHOST2
172.26.2.113  STBYSOA1.EXAMPLE.COM  STBYSOA1 SOAHOST1.EXAMPLE.COM SOAHOST1
172.26.2.114  STBYSOA2.EXAMPLE.COM  STBYSOA2 SOAHOST2.EXAMPLE.COM SOAHOST2
```

---

**Note:** The subnets in the production site and standby site are different.

---

### 3.1.1.1.3 Resolving Host Names Using Separate DNS Servers

Use separate DNS servers to resolve host names for your Disaster Recovery topology.

The term "separate DNS servers" refers to a Disaster Recovery topology where the production site and the standby site have separate and distinct DNS servers. When you use separate DNS servers to resolve host names for your Disaster Recovery topology, consider the following points:

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.
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.
5. Ensure that 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 returns the correct IP address (172.16.2.111) and indicates 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 returns the correct IP address (172.26.2.111) and indicates that the host name is fully qualified.

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

```
WEBHOST1.EXAMPLE.COM    IN    A    172.16.2.111
WEBHOST2.EXAMPLE.COM    IN    A    172.16.2.112
SOAHOST1.EXAMPLE.COM    IN    A    172.16.2.113
SOAHOST2.EXAMPLE.COM    IN    A    172.16.2.114
```

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

```
WEBHOST1.EXAMPLE.COM    IN    A    172.26.2.111
WEBHOST2.EXAMPLE.COM    IN    A    172.26.2.112
SOAHOST1.EXAMPLE.COM    IN    A    172.26.2.113
SOAHOST2.EXAMPLE.COM    IN    A    172.26.2.114
```

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

Use a global DNS server to resolve host names for your Disaster Recovery topology.

The term "global DNS server" refers 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, consider the following guidelines points:

1. When using a global DNS server, for the sake of simplicity, use a combination of local host name resolution and DNS host name resolution.
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.
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 simplicity and ease of maintenance, Oracle recommends having 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:

7. Test the host name resolution using the `ping` command. A `ping webhost1` command on the production site returns the correct IP address (172.16.2.111) and indicates that the host name is fully qualified.
8. Similarly, a `ping webhost1` command on the standby site returns the correct IP address (172.26.2.111) and indicates that the host name is fully qualified.

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

```

WEBHOST1.EXAMPLE.COM    IN    A    172.16.2.111
WEBHOST2.EXAMPLE.COM    IN    A    172.16.2.112
SOAHOST1.EXAMPLE.COM    IN    A    172.16.2.113
SOAHOST2.EXAMPLE.COM    IN    A    172.16.2.114
STBYWEB1.EXAMPLE.COM    IN    A    172.26.2.111
STBYWEB2.EXAMPLE.COM    IN    A    172.26.2.112
STBYSOA1.EXAMPLE.COM    IN    A    172.26.2.113
STBYSOA2.EXAMPLE.COM    IN    A    172.26.2.114

```

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

```

176.0.0.1      localhost.localdomain  localhost
172.26.2.111   STBYWEB1.EXAMPLE.COM   WEBHOST1
172.26.2.112   STBYWEB2.EXAMPLE.COM   WEBHOST2
172.26.2.113   STBYSOA1.EXAMPLE.COM   SOAHOST1
172.26.2.114   STBYSOA2.EXAMPLE.COM   SOAHOST2

```

### 3.1.1.1.5 Testing the Host Name Resolution

Validate host name assignment 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.

In addition, 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 Virtual IP and Virtual Host Name Considerations

Virtual IP addresses and host names are required to enable the Oracle WebLogic Administration Server to continue servicing requests when the machine hosting the Oracle WebLogic Administration Server fails.

Virtual IP addresses enable Managed Servers in your domain to participate in server migration. Virtual servers should be provisioned in the application tier so that they can be bound to a network interface on any host in the application tier.

In a Disaster Recovery topology, the production site virtual IP 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 the standby site. After failover from a primary site to a standby site, the alias host name for the middle tier host on the standby site becomes active. You do not need to reconfigure a host name for the host on the standby site if you set up aliases for the standby site.

This section describes how to plan virtual IP host names and alias host names for the middle tier hosts that use the Oracle Fusion Middleware instances at the production site and the standby site. This is required when you have a single corporate DNS.

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 the 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.

The following subsections show how to set up virtual IP addresses and host names at the Disaster Recovery production site and standby site for the following enterprise deployments:

Virtual IP Addresses and Virtual Host Names for the Oracle SOA Suite Production Site and Standby Site Hosts

[Table 3-3](#) shows the virtual IP addresses and virtual 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 3-3 Virtual IP Addresses and Virtual Host Names for the SOA Suite Production Site Hosts**

Virtual IP Address	Virtual Host Name	Alias Host Name
172.16.2.115	ADMINVHN	None
172.16.2.116	SOAVHN1	None
172.16.2.117	SOAVHN2	None

[Table 3-4](#) shows the virtual IP addresses, virtual 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 3-4](#) 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 virtual IP addresses and virtual host names for the production site hosts and standby site hosts, and you do not need to define the alias host names.

For more information about using separate DNS servers to resolve host names, see [Resolving Host Names Using Separate DNS Servers](#).

---



---

**Table 3-4 Virtual IP Addresses, Virtual Host Names, and Alias Host Names for SOA Suite Standby Site Hosts**

Virtual IP Address	Virtual Host Name	Host Name Alias
172.26.2.115	STBYADMINVHN	ADMINVHN
172.26.2.116	STBYSOAVHN1	SOAVHN1
172.26.2.117	STBYSOAVHN2	SOAVHN2

### 3.1.3 Load Balancer Considerations

Oracle Fusion Middleware components require a hardware load balancer when deployed in high availability topologies.

Oracle recommends that your hardware load balancer support the following features:

- Ability to load balance traffic to a pool of real servers through a virtual host name: Clients access services using the virtual host name (instead of using actual host names). The load balancer can then load balance requests to the servers in the pool.
- Port translation configuration.
- Monitoring of ports (HTTP and HTTPS).
- Virtual servers and port configuration: Ability to configure virtual server names and ports on your external load balancer. 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.
- Ability to detect node failures and immediately stop routing traffic to the failed node.
- 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.
- Fault-tolerant mode: It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
- 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.
- Sticky routing capability: Ability to maintain sticky connections to components based on cookies or URLs.
- SSL acceleration: This feature is recommended, but not required.
- For the Identity Management configuration with Oracle Access Manager, configure the virtual servers in the load balancer for the directory tier with a high value for the connection timeout for TCP connections. This value should be more than the maximum expected time over which no traffic is expected between the Oracle Access Manager and the directory tier.
- Ability to preserve the client IP addresses: The load balancer must have the capability to insert the original client IP address of a request in an X-Forwarded-For HTTP header to preserve the client IP address.

### 3.1.4 Virtual Server Considerations

Virtual servers and associated ports must be configured on the load balancer for different types of network traffic and monitoring.

Configure them 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 ensures that incoming traffic on a given virtual host is not directed to an unavailable service in the other tiers.

Oracle recommends that you 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. Although this is supported, the deployment should consider the security implications of doing this and if 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.

Some of the virtual servers defined in the load balancer are used for inter-component communication. These virtual servers are used for internal traffic and are defined in the internal DNS of a company. Oracle highly recommends that you create aliases for these virtual servers when you use a single global DNS server to resolve host names.

Creating aliases is not required when using separate DNS servers to resolve host names.

The virtual servers required for the various Oracle Fusion Middleware products are described in [Table 3-5](#) and [Table 3-6](#).

**Table 3-5 Virtual Servers for Oracle SOA Suite Production Site**

Components	Access	Virtual Server Name	Alias Name
Oracle SOA	External	soa.example.com	None
Oracle SOA	Internal	soainternal.example.com	None
Administration Consoles	Internal	admin.example.com	None

**Table 3-6 Virtual Servers for Oracle SOA Suite Standby Site**

Components	Access	Virtual Server Name	Alias Virtual Server Name
Oracle SOA	External	soa.example.com	None
Oracle SOA	Internal	stbysoainternal.example.com	soainternal.example.com
Administration Consoles	Internal	admin.example.com	None

### 3.1.5 External Clients Considerations

Systems directly accessing the servers in the topology need to be aware of the listen address used by different Oracle WebLogic Server instances.

An appropriate host name resolution needs to be provided to the clients so that the host name alias used by the servers as listen address is correctly resolved. This is also applicable to the Oracle JDeveloper deployments. The client hosting Oracle JDeveloper needs to map the SOAHOSTx and SOAVHNx aliases to correct the IP addresses for deployments to succeed.

### 3.1.6 Wide Area DNS Operations

When a site switchover or failover is carried out, 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 serve as a front end for each site. Check for supported load balancers at:

<http://support.oracle.com>

---

---

This section includes the following topics:

#### [Using a Global Load Balancer](#)

A global load balancer deployed in front of the production and standby sites provides fault detection services and performance-based routing redirection for the two sites.

#### [Manually Changing DNS Names](#)

The DNS switch-over involves to manually change the name-to-IP mapping of the production site's load balancer.

#### 3.1.6.1 Using a Global Load Balancer

A global load balancer deployed in front of the production and standby sites 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.

#### 3.1.6.2 Manually Changing DNS Names

The DNS switch-over involves to manually change the name-to-IP mapping 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. Note 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, 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.

If the clients that point to SOA are running on Java, another TTL property can be taken in account. Java has a DNS cache that can be configured for caching the successful DNS resolutions, so in that case, the change in DNS server is not refreshed until Java is restarted. This can be modified by setting the property `networkaddress.cache.ttl` to a low value:

- You can do it globally, for all the applications running the JVM, by modifying the property in `JAVA_HOME/jre/lib/security/java.security` file:  
`networkaddress.cache.ttl=60`
- You can define it for a specific application only, by setting that property in the application's initialization code:  

```
java.security.Security.setProperty("networkaddress.cache.ttl"  
    " , "60")
```

## 3.2 Storage Considerations

When designing storage for your Disaster Recovery solution, consider Fusion Middleware artifacts, storage replication, and file-based persistent stores.

This section includes the following topics:

### [Oracle Fusion Middleware Artifacts](#)

Oracle Fusion Middleware components in a given environment are usually interdependent on one another, so it is important that the components in the topology be synchronized.

### [Oracle Home and Oracle Inventory](#)

Oracle Fusion Middleware allows you to create multiple Oracle WebLogic Server Managed Servers from one single binary file installation.

### [Storage Replication](#)

Learn about the guidelines to create volumes on a shared storage.

### [File-Based Persistent Store](#)

The Java Message Service (JMS) and transaction logs (TLogs) use a file-based persistent store in the local site high availability of the Oracle SOA Suite topology.

### 3.2.1 Oracle Fusion Middleware Artifacts

Oracle Fusion Middleware components in a given environment are usually interdependent on one another, so it is important that the components in the topology be synchronized.

This synchronization is important when designing volumes and consistency groups. Some artifacts are static whereas others are dynamic.

#### Static Artifacts

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

- **home:** The Oracle home usually consists of an Oracle home and an Oracle WebLogic Server home.
- **Oracle Inventory:** This includes `oraInst.loc` and `oratab` files, which are located in the `/etc` directory.

#### Dynamic or Runtime Artifacts

Dynamic or runtime artifacts are files that change frequently. Runtime 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
- **Deployment plans:** Used for updating technology adapters such as file and JMS adapters. They need to be saved in a location that is accessible to all nodes in the cluster that the artifacts are being deployed to.

### 3.2.2 Oracle Home and Oracle Inventory

Oracle Fusion Middleware allows you to create multiple Oracle WebLogic Server Managed Servers from one single binary file installation.

You can install binary files in a single location on a shared storage and reuse this installation by servers in different nodes. Note that, for maximum availability, Oracle recommends using redundant binary installations.

When an Oracle home or a WebLogic home is shared by multiple servers in different nodes, Oracle recommends that you keep the Oracle Inventory and Oracle home list in those nodes updated for consistency in the installations and application of patches.

To update the inventory files in a node and attach an installation in a shared storage to it, use `ORACLE_HOME/oui/bin/attachHome.sh`.

### 3.2.3 Storage Replication

Learn about the guidelines to create volumes on a 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, then:

- 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, then:

- 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. This enables the same directory structure to 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 Java Message Service (JMS) and transaction logs (TLogs) use a file-based persistent store in the local site high availability of the Oracle SOA Suite topology.

Oracle WebLogic Servers are usually clustered for high availability, and this file-based persistent store must reside on a shared storage that is accessible to all members of the cluster.

A Storage Area Network (SAN) storage system should use either a host-based clustered or a shared file system technology such as the Oracle Clustered File System (OCFS2). OCFS2 is a symmetric shared disk cluster file system that 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

When planning your Disaster Recovery solution, consider the synchronizing the databases in your system with Oracle Data Guard.

This section provides the recommendations and considerations to set up Oracle databases used in an Oracle Fusion Middleware Disaster Recovery topology.

- Oracle recommends creating Oracle Real Application Cluster (Oracle RAC) databases on both the production site and standby site as required by your topology.
- Oracle Data Guard is the recommended disaster protection technology for the databases running the metadata repositories. You can also use Oracle Active Data Guard or Oracle GoldenGate.

---

---

**Note:**

You can use Oracle GoldenGate only in an active-passive configuration.

---

---

For more information about Oracle Active Data Guard and Oracle GoldenGate, see <http://www.oracle.com/in/products/database/options/active-data-guard/index.html> <http://www.oracle.com/technetwork/middleware/goldengate/overview/index.html>

- 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.

For more information about Oracle Maximum Availability Architecture, see <http://www.oracle.com/technology/deploy/availability/htdocs/maa.htm>

- Ensure that your network is configured for low latency with sufficient bandwidth, because synchronous redo transmission can affect the response time and throughput.

- The `LOG_ARCHIVE_DEST_n` parameter on standby site databases should have the `SYNC` or `ASYN` attributes. `ASYN` is the default attribute if no attributes are specified.
- The standby site database should be in Managed Recovery mode. This ensures that the standby site databases are in a constant state of media recovery. Managed Recovery mode is enabled for shorter failover times.
- The `tnsnames.ora` file on the production site and the standby site must have entries for databases on both the production and standby sites.
- Oracle strongly recommends that you force Oracle Data Guard to perform manual database synchronization whenever middle tier synchronization is performed. This is especially important for components that store configuration data in the metadata repositories.
- Oracle strongly recommends that you set up aliases for the database host names on both the production and standby sites. This enables seamless switchovers, switchbacks, and failovers.
- When one of the databases at either site is an Oracle RAC database, it is required that the single instance database at the peer site must have the same value for `instance_name`.

---

---

**Note:**

- The values for `ORACLE_HOME`, `home`, `ORACLE_INSTANCE`, `DOMAIN_HOME` in the middle tier must be identical.
  - The values for `DB_NAME`, `INSTANCE_NAME`, `Listen Port`, and `ORACLE_SID` in the database tier must be identical.
  - To avoid manipulation of the WLS data sources, the `SERVICE_NAME` specified in the Application Data Source must be identical. However, each database can have additional services defined.
- 
- 

The following sections explain database points:

#### [Making TNSNAMES.ORA Entries for Databases](#)

Oracle Data Guard is used to synchronize production and standby databases, so the production and standby databases can reference each other.

#### [Synchronizing Databases Manually](#)

Use SQL to synchronize production and standby databases.

#### [Setting Up Database Host Name Aliases](#)

Set up database host name aliases for the databases at your production site and standby site.

### 3.3.1 Making TNSNAMES.ORA Entries for Databases

Oracle Data Guard is used to synchronize production and standby databases, so the production and standby databases can reference each other.

Oracle Data Guard uses the `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 Synchronizing Databases Manually

Use SQL to synchronize production and standby databases.

The SQL `alter system archive log all statement` switches logs and thus forces a synchronization of the production and standby site databases.

To manually synchronize production and standby site databases, use the following SQL statement:

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

### 3.3.3 Setting Up Database Host Name Aliases

Set up database host name aliases for the databases at your production site and standby site.

The aliases 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 3-7](#) shows the database host names and the connect strings for the databases before the alias is defined.

**Table 3-7 Database Host Names and Connect Strings**

Site	Database Host Name	Database Connect String
Production	<code>custdbhost1.example.com</code>	<code>custdbhost1.example.com:1521:orcl</code>
Standby	<code>stbycustdbhost1.example.com</code>	<code>stbycustdbhost1.example.com:1521:orcl</code>

In this example, all database connect strings on the production site take the form `custdbhost1.example.com:1521:orcl`. After a failover or switchover operation, this connect string must be changed to `stbycustdbhost1.example.com:1521:orcl`. However, by creating an alias of `proddb1` for the database host name as shown in [Table 3-8](#), you can avoid manually changing the connect strings, which enables seamless failovers and switchovers.

**Table 3-8 Specifying an Alias for a Database Host**

Site	Database Host Name	Alias	Database Connect String
Production	<code>custdbhost1.example.com</code>	<code>proddb1.example.com</code>	<code>proddb1.example.com:1521:orcl</code>
Standby	<code>stbycustdbhost1.example.com</code>	<code>proddb1.example.com</code>	<code>proddb1.example.com:1521:orcl</code>

In this example, the production site database host name and the standby site database host name are aliased to `proddb1.example.com` and the connect strings on the production site and the standby site can take the form `proddb1.example.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.

In the `/etc/hosts` file at the production site, ensure that the entry for host `custdbhost1` looks like this:

```
152.68.196.213 proddb1.example.com proddb1 custdbhost1.example.com custdbhost1
```

In the `/etc/hosts` file at the standby site, ensure that the entry for host `stbycustdbhost1` looks like this:

```
140.87.25.40 proddb1.example.com proddb1 stbycustdbhost1.example.com stbycustdbhost1
```

## 3.4 Starting Points

When planning your Disaster Recovery solution, consider starting with an existing site or creating a new site.

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.

[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.

[Starting with a New Site](#) 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 must 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.

This section includes the following topics:

### Starting with an Existing Site

When starting with an existing production site, the configuration data and the Oracle binary files for the production site are already on the file system.

### Starting with a New Site

When starting with a new production site for an Oracle Fusion Middleware Disaster Recovery topology, consider host names and ensure that storage replication is set up to copy the configuration (based on these names) to the standby site.

## 3.4.1 Starting with an Existing Site

When starting with an existing production site, the configuration data and the Oracle binary files for the production site are already on the file system.

In addition, the host names, ports, and user accounts are already defined. When starting with an existing production site, choose either of the following designs:

- Design a symmetric standby site. See [Design Considerations for a Symmetric Topology](#).
- Design an asymmetric standby site. See [Design Considerations for an Asymmetric Topology](#).
- First migrate the production site to shared storage (if not already in a shared storage), and then create either a symmetric standby or an asymmetric standby site using the migrated data.

To migrate a production site, see the following section:

### [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 must 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:

- All backups performed must be offline backups. See *Types of Backups and Recommended Backup Strategy* in *Oracle Fusion Middleware Administering Oracle Fusion Middleware*.
- The backups must be performed as the root user and the permissions must be preserved. See the *Overview of the Backup Strategies* in *Oracle Fusion Middleware Administering Oracle Fusion Middleware*.
- Because this is a one-time operation, you should recover the entire domain.
- The directory structure on the shared storage must be set up as described in [Designing Directory Structure and Volumes](#).

- For Oracle SOA Suite, see *Introducing Backup and Recovery in Oracle Fusion Middleware Administering Oracle Fusion Middleware*.
- For Web Tier, see *Introducing Backup and Recovery in Oracle Fusion Middleware Administering Oracle Fusion Middleware*.

### 3.4.2 Starting with a New Site

When starting with a new production site for an Oracle Fusion Middleware Disaster Recovery topology, consider host names and ensure that storage replication is set up to copy the configuration (based on these names) to the standby site.

When designing a new production site, plan also the standby site, and use Oracle Universal Installer to install software on the production site. Parameters such as alias host names and software paths must be carefully designed to ensure that they are the same on both sites.

When creating a new Oracle Fusion Middleware Disaster Recovery production and standby sites, consider the following choices:

- 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. For more information about host name planning, see [Planning Host Names](#).
- Choose the Oracle home name and Oracle home directory for each Fusion Middleware installation.

Designing and creating your own site is easier than modifying an existing site to meet the design requirements described in this chapter.

- Assign ports for the Oracle Fusion Middleware installations for the production site hosts that will not conflict with the ports used by the standby site hosts.

This setup is easier than checking for and resolving port conflicts between an existing production and standby sites.

## 3.5 Topology Considerations

When planning your for your Disaster Recovery solution, consider designing a symmetric or an asymmetric topology.

This section includes the following topics:

### [Design Considerations for a Symmetric Topology](#)

A symmetric topology is an Oracle Fusion Middleware Disaster Recovery configuration that is identical across tiers on the production and standby sites.

### [Design Considerations for an Asymmetric Topology](#)

An asymmetric topology is an Oracle Fusion Middleware Disaster Recovery configuration that differs across some tiers on the production and standby sites.

### 3.5.1 Design Considerations for a Symmetric Topology

A symmetric topology is an Oracle Fusion Middleware Disaster Recovery configuration that is identical across tiers on the production and standby sites.

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 differs across some tiers on the production and standby sites.

In an asymmetric topology, the standby site can use less hardware (for example, the production site could include four hosts with four Oracle Fusion Middleware instances while the standby site includes two hosts with four Oracle Fusion Middleware instances).

For example, consider an asymmetric topology where the standby site uses fewer Oracle Fusion Middleware instances (for example, the production site could include four Oracle Fusion Middleware instances while the standby site includes just two Oracle Fusion Middleware instances).

Another asymmetric topology includes a different configuration for a database (for example, using an Oracle Real Application Clusters (Oracle RAC) database at the production site and a single instance database at the standby site).



---

# Setting Up and Managing Disaster Recovery Sites

Learn about the Oracle SOA Suite enterprise deployment topology that illustrates how to set up production and standby sites.

---

**Note:**

You can automate disaster recovery operations like switchover and failover using Oracle Site Guard. See *Oracle Site Guard Administrator's Guide*.

---

This chapter includes the following sections:

[Setting Up a Site](#)

Learn how to set up an Oracle Disaster Recovery site.

[Creating a Production Site](#)

Learn how to create a production site on an Oracle SOA enterprise deployment topology.

[Creating a Standby Site](#)

Learn how create a standby site.

[Creating an Asymmetric Standby Site](#)

Learn how to create an asymmetric Oracle Fusion Middleware Disaster Recovery topology.

[Performing Site Operations and Administration](#)

Learn how to operate and administer your Oracle Fusion Middleware Disaster Recovery topology.

[Using Oracle Site Guard for Disaster Recovery](#)

Oracle Site Guard orchestrates switchover and failover between two disaster recovery sites.

[Patching an Oracle Fusion Middleware Disaster Recovery Site](#)

Apply an Oracle Fusion Middleware patch set to upgrade the Oracle homes that participate in an Oracle Fusion Middleware Disaster Recovery site.

## 4.1 Setting Up a Site

Learn how to set up an Oracle Disaster Recovery site.

Before you start creating the production site, ensure that you:

- Set up the host name aliases for the middle tier hosts, as described in [Planning Host Names](#).

- Create the required volumes on the shared storage on the production site as described in [Designing Directory Structure and Volumes](#)
- Determine the Oracle Data Guard configuration to use based on the data loss requirements of the database and network considerations such as the available bandwidth and latency when compared to the redo generation.

This section includes the following topics:

#### [Designing Directory Structure and Volumes](#)

Learn about the recommended directory structure in your disaster recovery topology.

#### [Setting Up Storage Replication](#)

Learn how to set up storage replication for the Oracle Fusion Middleware Disaster Recovery topology.

#### [Installing and Configuring Databases](#)

Learn how to install and configure Oracle Database 11.2 or Oracle Database 12.1 MAA databases in an Oracle SOA Suite enterprise deployment.

### 4.1.1 Designing Directory Structure and Volumes

Learn about the recommended directory structure in your disaster recovery topology.

You can choose a directory layout different from the one recommended in this document, but the model adopted enables maximum availability, provides the best isolation of components and symmetry in the configuration, and facilitates backup and disaster recovery.

The following list describes directories and directory environment variables:

- `ORACLE_BASE`: This environment variable and related directory path refers to the base directory below which Oracle products are installed.
- `ORACLE_HOME`: This related directory path refers to the location where Oracle Fusion Middleware resides.
- `WL_HOME`: This environment variable and related directory path contains installed files necessary to host an Oracle WebLogic Server.
- `PROD_DIR`: This environment variable and related directory path refers to the location where a product suite (such as Oracle SOA Suite, Oracle WebCenter Portal, 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.
- `ORACLE_INSTANCE`: An Oracle instance contains one or more system components. An Oracle instance directory contains updatable files, such as configuration files, log files, and temporary files.

See [Recommended Directory Structure for Oracle SOA Suite](#).

This section includes the following topic:

### [Recommended Directory Structure for Oracle SOA Suite](#)

Learn about the recommended directory structures for Oracle SOA Suite.

### [Recommended Volume Design for Oracle SOA Suite](#)

Learn about the recommended volume design for Oracle SOA Suite.

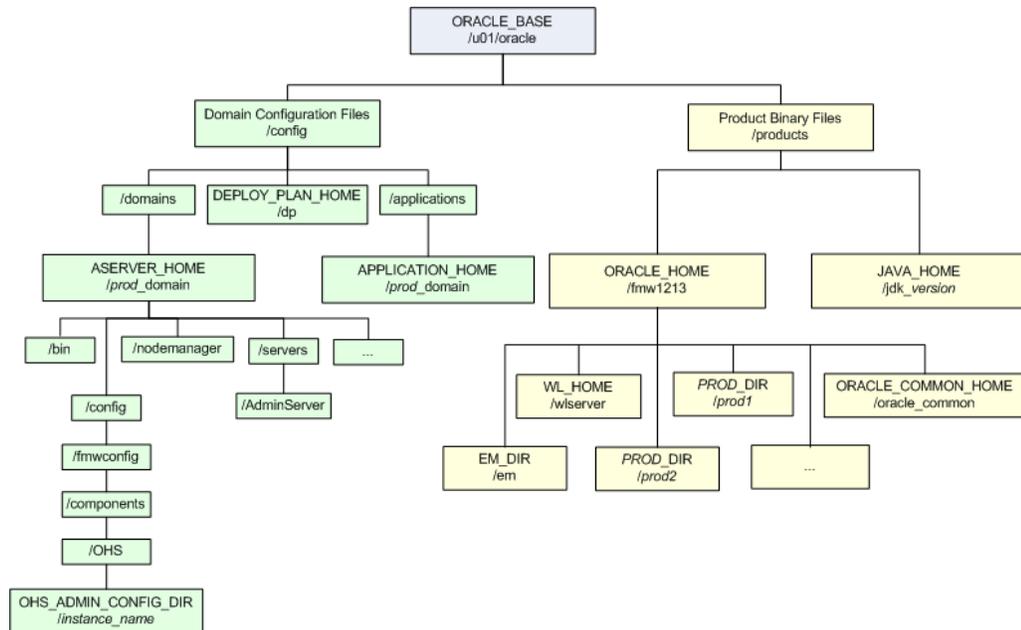
#### **4.1.1.1 Recommended Directory Structure for Oracle SOA Suite**

Learn about the recommended directory structures for Oracle SOA Suite.

Oracle Fusion Middleware allows you to create multiple SOA Managed Servers from a single binary installation. This allows the installation of binary files 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 Oracle 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, this isolating the failures as much as possible 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. In addition, Oracle recommends placing the Managed Servers' domain directories on a shared storage, although having them on the local file system is also supported. This is especially important 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 Oracle SOA Suite**



For information about setting up this directory structure, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*.

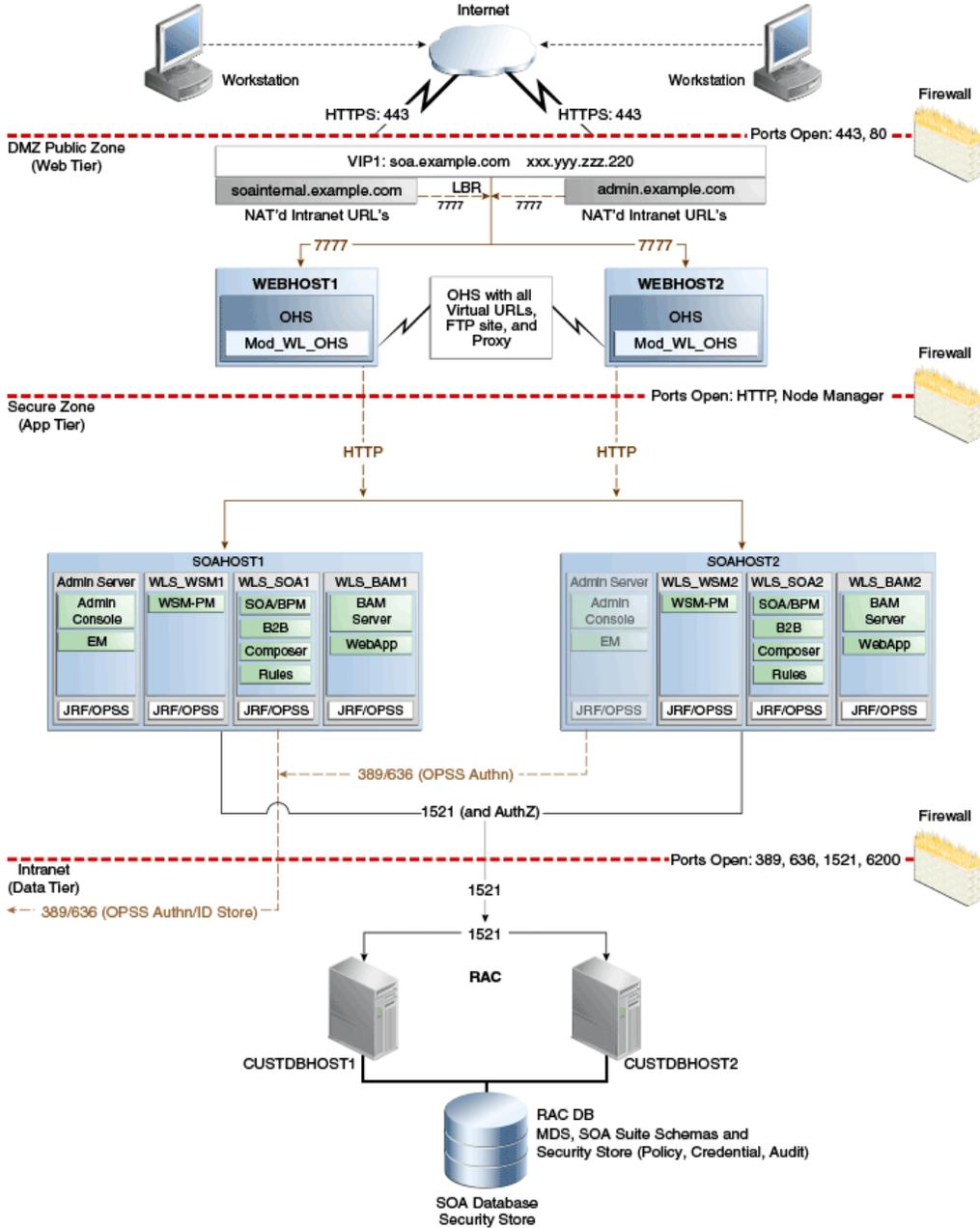
For volume design, see the following section:

#### 4.1.1.2 Recommended Volume Design for Oracle SOA Suite

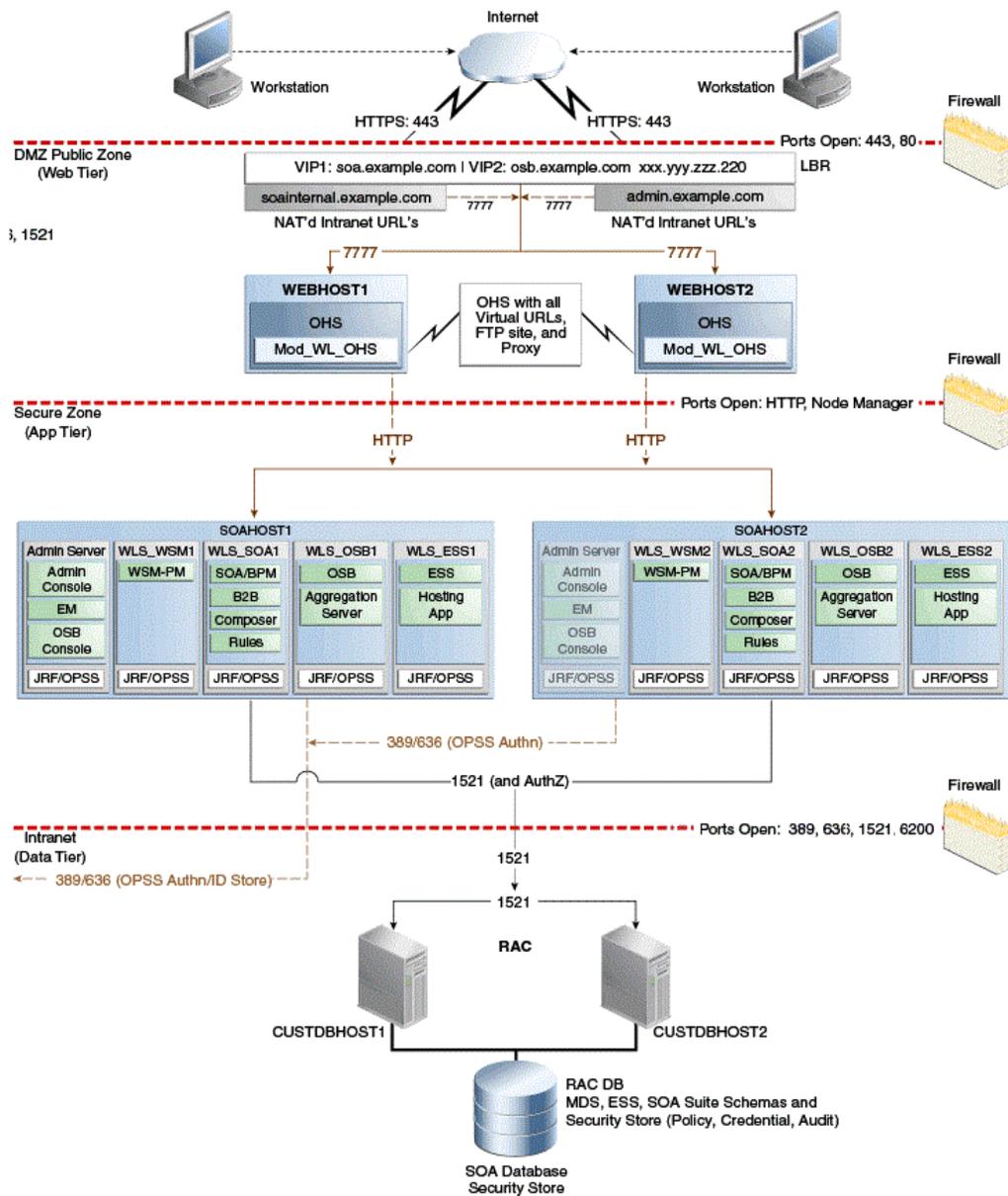
Learn about the recommended volume design for Oracle SOA Suite.

[Figure 4-2](#) and [Figure 4-3](#) 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 the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*.

Figure 4-2 Oracle SOA Suite and Oracle Business Activity Monitoring Enterprise Topology Diagram



**Figure 4-3 Oracle SOA Suite and Oracle Service Bus Enterprise Deployment Reference Topology Diagram**



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

- Provision two volumes for two Oracle homes that contain redundant product binary files (VOLFMW1 and VOLFMW2 in Table 4-1).
- Provision one volume for the Administration Server domain directory (VOLADMIN in Table 4-1).
- Provision one volume on each node for the Managed Server domain directory (VOLSOA1 and VOLSOA2 in Table 4-1). This directory is shared among all the Managed Servers on that node.

- Provision one volume for the JMS file store and JTA transaction logs (VOLDATA in [Table 4-1](#)). One volume for the entire domain 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 4-1](#)).
- Provision one volume on each node for the Oracle HTTP Server Domain Directory (VOLOHS1 and VOLOHS2 in [Table 4-1](#)).

---

**Note:** For WebTier hosts, local storage is usually recommended. You can replicate this configuration on a regular basis to one of the other app tier volumes to sync to standby or directly from production webhost to standby webhost.

---

[Table 4-1](#) provides a summary of Oracle recommendations for volume design for the Oracle SOA Suite topology shown in [Figure 4-2](#) and [Figure 4-3](#).

**Table 4-1 Volume Design Recommendations for Oracle SOA Suite**

Tier	Volume Name	Mounted on Host	Mount Point	Comments
Web	VOLWEB1	WEBHOST1	/u02/oracle/products/fmw	Volume for Oracle HTTP Server installation
Web	VOLWEB2	WEBHOST2	/u02/oracle/products/fmw	Volume for Oracle HTTP Server installation
Web	VOLOHS1	WEBHOST1	/u02/oracle/config/domains/ohs_domain	Volume for Oracle HTTP Server domain directory
Web	VOLOHS2	WEBHOST2	/u02/oracle/config/domains/ohs_domain	Volume for Oracle HTTP Server domain directory
Web	VOLSTATIC1	WEBHOST1	/u02/oracle/config/static	(Optional) Volume for static HTML content
Web	VOLSTATIC2	WEBHOST2	/u02/oracle/config/static	(Optional) Volume for static HTML content
Application	VOLFMW1	SOAHOST1	/u01/oracle/products/fmw	Volume for the WebLogic Server and Oracle SOA Suite binary files
Application	VOLFMW2	SOAHOST2	/u01/oracle/products/fmw	Volume for the WebLogic Server and Oracle SOA Suite binary files

**Table 4-1 (Cont.) Volume Design Recommendations for Oracle SOA Suite**

Tier	Volume Name	Mounted on Host	Mount Point	Comments
Application	VOLADMIN	SOAHOST1, SOAHOST2	/u01/oracle/ config	Volume for Administration Server domain directory and other shared config like Deployment Plans, applications, keystores
Application	VOLSOA1	SOAHOST1	/u02/oracle/ config	Volume for Managed Server domain directory
Application	VOLSOA2	SOAHOST2	/u02/oracle/ config	Volume for Managed Server domain directory
Application	VOLRUNTIME	SOAHOST1, SOAHOST2	/u01/oracle/ runtime	Volume for transaction logs and JMS data

For consistency group recommendations, see:

[Recommended Consistency Groups for Oracle SOA Suite](#)

Learn about the recommended consistency groups for Oracle SOA Suite.

**4.1.1.2.1 Recommended Consistency Groups for Oracle SOA Suite**

Learn about the recommended consistency groups 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 4-2](#)).
- Create one consistency group with the volume containing the JMS file store and transaction log data as members (RUNTIMEGROUP in [Table 4-2](#)).
- Create one consistency group with the volume containing the Oracle homes as members (FMWHOMEGROUP in [Table 4-2](#)).

[Table 4-2](#) provides a summary of Oracle recommendations for consistency groups for the Oracle SOA Suite topology shown in [Figure 4-2](#).

**Table 4-2 Consistency Groups for Oracle SOA Suite**

Tier	Group Name	Members	Comments
Application	DOMAINGROUP	VOLADMIN VOLSOA1 VOLSOA2	Consistency group for the Administration Server, Managed Server domain directory
Application	RUNTIMEGROUP	VOLRUNTIME	Consistency group for the JMS file store and transaction log data
Application	FMWHOMEGROUP	VOLFMW1 VOLFMW2	Consistency group for the Oracle homes

## 4.1.2 Setting Up Storage Replication

Learn how to set up storage replication for the Oracle Fusion Middleware Disaster Recovery topology.

To set up storage replication for the Oracle Fusion Middleware Disaster Recovery topology:

- On the standby site, ensure that alias host names that are created are the same as the physical host names used for the peer hosts at the production site.
- On the shared storage at the standby site, create the same volumes as were created on the shared storage at the production site.
- 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. For more information about symbolic links, see [Storage Replication](#).
- 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.
- 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.
- 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.

- 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.
- The standby site shared storage receives snapshots transferred on periodically from the production site shared storage. After the snapshots are applied, the standby site shared storage includes all the data up to and including the data contained in the last snapshot transferred from the production site before the failover or switchover.
- Oracle strongly recommends that you 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 Installing and Configuring Databases

Learn how to install and configure Oracle Database 11.2 or Oracle Database 12.1 MAA databases in an Oracle SOA Suite enterprise deployment.

For recommendations and considerations for setting up Oracle databases that are used in an Oracle Fusion Middleware Disaster Recovery topology, see [Database Considerations](#).

#### [Installing and Configuring Oracle Database 11.2 or 12.1 MAA Environments](#)

##### 4.1.3.1 Installing and Configuring Oracle Database 11.2 or 12.1 MAA Environments

Oracle Maximum Availability Architecture (MAA) is Oracle's comprehensive architecture for reducing downtime for scheduled outages, and preventing, detecting and recovering from unscheduled outages.

Real Application Clusters (RAC) and Data Guard provide the basis of the database MAA solution, where the primary site contains the RAC database, and the secondary site contains the RAC physical standby database.

This section contains the following topics:

- [Prerequisites and Assumptions](#)
- [Oracle Data Guard Environment Description](#)
- [Procedure for Duplicating the Primary Database](#)
- [Procedure for Completing RAC Configuration for Standby Database](#)
- [Creating a Data Guard Broker Configuration](#)
- [Verifying the Data Guard Broker Configuration](#)
- [Testing Database Switchover and Switchback](#)

**Tip:**

Alternatively, you can perform many of the tasks in this section using Oracle Enterprise Manager Cloud Control (Cloud Control).

Setting up and managing databases using Cloud Control helps in controlling downtime and simplifies disaster recovery operations.

For information about installing Enterprise Manager Cloud Control 12c, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

For more information about setting up Oracle Data Guard using Cloud Control, see *Set Up and Manage Oracle Data Guard using Oracle Enterprise Manager Cloud Control 12c*.

### [Prerequisites and Assumptions](#)

#### [Oracle Data Guard Environment Description](#)

#### [Procedure for Duplicating the Primary Database](#)

#### [Procedure for Completing RAC Configuration for Standby Database](#)

#### [Creating a Data Guard Broker Configuration](#)

#### 4.1.3.1.1 Prerequisites and Assumptions

Ensure that the following prerequisites are met:

- The Oracle RAC cluster and Automatic Storage Management (ASM) instances on the standby site have been created.
- The Oracle RAC databases on the standby site and the production site are using a flash recovery area.
- The Oracle RAC databases are running in `archivelog` mode.
- The database hosts on the standby site already have Oracle software installed.
- In a shared `ORACLE_HOME` configuration, the `TNS_ADMIN` directory must be a local, non-shared directory.

#### 4.1.3.1.2 Oracle Data Guard Environment Description

The examples given in this section contain environment variables as described in [Table 4-3](#).

**Table 4-3 Variables Used by Primary and Standby Databases**

Variable	Primary Database	Standby Database
Database names	soa	soa
SOA Database Host Names	soadc1.dbhost1, soadc1.dbhost2	soadc2.dbhost1, soadc2.dbhost2
Database unique names	psoa	ssoa
Instance names	soa1, soa2	soa1, soa2
Service names	psoa, ssoa	psoa, ssoa

#### 4.1.3.1.3 Procedure for Duplicating the Primary Database

Follow these steps to prepare the primary database for setting up Oracle Data Guard:

---



---

**Note:**

For information about prerequisites for setting up Oracle Data Guard, see Prerequisites in *Oracle Data Guard Broker*.

---



---

1. Enable force logging on the primary database:

```
SQL> alter database force logging;
SQL> select name, log_mode, force_logging from v$database;
NAME LOG_MODE FOR
-----
PSOA ARCHIVELOG YES
```

2. Create standby redo logs that are the same size as the online redo logs, on the primary database. The DUPLICATE command will automatically create the standby redo log on the standby database.

Oracle recommends having the same number plus one additional redo logs for each thread as shown in [#unique\\_103/unique\\_103\\_Connect\\_42\\_CJAHBBEC](#).

3. In the standby node 1, create and start a listener (for example, LISTENER\_DUPLICATE) that offers a static SID entry for the standby database, and has the same value of ORACLE\_SID as the primary (soa1), as shown in [Example 4-1](#).

Provide the following path to the listener.ora file:

```
GRID_HOME/network/admin/listener.ora
```

4. Run the following command to start and verify the listeners using lsnrctl from GRID\_HOME/bin::

```
lsnrctl start listener_duplicate
lsnrctl status listener_duplicate
```

5. In the standby node 2, create and start a listener (for example, LISTENER\_DUPLICATE) that offers a static SID entry for the standby database, and has the same value of ORACLE\_SID as the primary (soa2), as shown in [Example 4-2](#).

Provide the following path to the listener.ora file:

```
GRID_HOME/network/admin/listener.ora
```

**Note:**

Listeners are configured at the cluster level, and all nodes inherit the port and environment settings of the listener. Therefore, the `TNS_ADMIN` directory path have the same values on all nodes.

In a shared `ORACLE_HOME` configuration, the `TNS_ADMIN` directory must be a local, non-shared directory. These network files are included as `IFILES`.

Complete the following steps to set up `TNS_ADMIN` for a shared `ORACLE_HOME` in a two-node cluster, `SOADC1.DBHOST1` and `SOADC1.DBHOST2`, with respective instances `SOA1` and `SOA2`:

- a. Create a local network directory on each node. For example, /  
`local_network_dir/network_admin`.
- b. Create a local `listener.ora` file in the location: /  
`local_network_dir/network_admin` on each node.
- c. In the local `listener.ora` file, add the values for the  
`LISTENER_duplicate` parameter.
- d. In the common `listener.ora` file, in `GRID_HOME/network/admin`,  
add the `IFILE` parameter values, as follows:

```
IFILE=/local_network_dir/network_admin/listener.ora
```

6. Run the following command to start and verify the listeners:

```
lsnrctl start listener_duplicate
lsnrctl status listener_duplicate
```

7. In the database home of the primary node, create an Oracle Net alias to connect to the listener that you created in step 3. See [Example 4-3](#).

For example: `GRID_HOME/bin/tnsping dup`.

8. Configure Oracle password file authentication for redo transport. Make sure it meets the following requirements:

- Set `remote_login_passwordfile` to `EXCLUSIVE`.

```
SQL> show parameter
remote_login_passwordfile
NAME TYPE VALUE
-----
remote_login_passwordfile string EXCLUSIVE
```

- Copy the primary password file to the auxiliary instance location.

9. In the `ORACLE_HOME/dbs` directory of the standby host, create a `pfile`, `initsoa1.ora`, with the following parameters:

```
db_name=soa
db_unique_name=ssoa
sga_target=5g
```

10. Create the audit directory for the `soa` database on all standby hosts:

```
mkdir -p /u01/app/oracle/admin/soa/adump
```

11. Create an Oracle Net alias on all primary hosts to reach the `ssoa` database on the standby hosts.

Ensure that all hosts have Oracle Net alias for `psoa` and `ssoa`. All the aliases that you create need to reference the scan listener and not the node VIP. Also, if the `local_listener` variable is set to an alias on the primary host, then enter the details of the variable on the standby site, that point to the local listener on the primary host. See [Example 4-4](#) and [Example 4-5](#).

---

---

**Note:**

- For primary node 2 (`SOADC1.DBHOST2`), update the `HOST` value in `psoa_local_listener` to point to the VIP of primary node 2, as follows:

```
psoa_local_listener =
  (ADDRESS_LIST =
    (ADDRESS=(PROTOCOL = TCP)
      (HOST=prmy2-vip)(PORT = 1521))
    )
  )
```

- If you are using a shared Oracle home, add the VIPs of the two nodes to the `local_listener` parameter.

For example:

```
psoa_local_listener =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS=(PROTOCOL = TCP)
        (HOST=prmy1-vip)(PORT = 1521))
      (ADDRESS=(PROTOCOL = TCP)
        (HOST=prmy2-vip)(PORT = 1521))
    )
  )
```

---

---

**Note:**

- For standby node 2 (SOADC2.DBHOST2), update the `HOST` value in `ssoa_local_listener` to point to the VIP of standby node 2, as follows:

```
ssoa_local_listener = (ADDRESS_LIST =
  (ADDRESS=(PROTOCOL = TCP)
  (HOST=stby2-vip)(PORT = 1521))
  )
)
```

- If you are using a shared Oracle home, add the VIPs of the two nodes to the `local_listener` parameter.

For example:

```
ssoa_local_listener =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS=(PROTOCOL = TCP)
      (HOST=stby1-vip)(PORT = 1521))
      (ADDRESS=(PROTOCOL = TCP)
      (HOST=stby2-vip)(PORT = 1521))
    )
  )
```

12. On the standby host, set the `ORACLE_SID` to the same value as that of the primary database (`ORACLE_SID=soa1`), and run the `startup nomount` command on the standby database with standby `PFIL` as created in step 9.
13. To obtain the values use this query:

```
SQL> select p.inst_id,instance_name, name,value from gv$parameter p, gv$instance
i where p.inst_id=i.inst_id and p.name='cluster_interconnects';
```

INST_ID	INSTANCE_NAME	NAME	VALUE
1	dbm1	cluster_inte rconnects	192.168.44.225
2	dbm2	cluster_inte rconnects	192.168.44.226

14. Disable the parameter `cluster_interconnects` on the primary host if it is set:
 

```
SQL> alter system reset cluster_interconnects scope=spfile sid='soa1';
SQL> alter system reset cluster_interconnects scope=spfile sid='soa2';
```
15. On the primary host, run the Recovery Manager (RMAN) script to duplicate the primary database using the command `duplicate target database for standby from active database`.

**Note:**

This command varies depending on your environment. For information about how to use the command, see *Duplicating a Database in Oracle Database Backup and Recovery User's Guide*.

See [Example 4-6](#) to understand how to duplicate between two systems with different disk-group names.

See [Example 4-7](#) to understand how to duplicate between two systems that have the same disk-group name +DATA.

16. If you have disabled the parameter `cluster_interconnects` on the primary host as described in step 14, then you must set it back to the original values in the spfile.
17. (Optional) Stop and remove the listener that you created in step 3.

**Example 4-1 Script for Creating and Starting a Listener with Static SID**

```

LISTENER_duplicate =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)
        (HOST = soadc2.dbhost1)
        (PORT = 1521)(IP = FIRST))))

SID_LIST_LISTENER_duplicate =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = soa1)
      (ORACLE_HOME = /u01/app/oracle/product/11.2.0/db_1)))

```

**Example 4-2 Script for Creating and Starting a Listener with Static SID**

```

LISTENER_duplicate =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)
        (HOST = soadc2.dbhost2)
        (PORT = 1521)(IP = FIRST))))

SID_LIST_LISTENER_duplicate =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = soa2)
      (ORACLE_HOME = /u01/app/oracle/product/11.2.0/db_1)))

```

**Example 4-3 Script for Creating an Oracle Net Alias**

```

dup =
  (DESCRIPTION =
    (ADDRESS =
      (PROTOCOL = TCP)
      (HOST = soadc2.dbhost1)
      (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SID = soa1)))

```

**Example 4-4 Sample tnsnames.ora File on Primary Node 1 (SOADC1.DBHOST1)**

```

psoa =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS=(PROTOCOL= TCP)
(HOST=prmy-scan)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = psoa)
    )
  )

ssoa =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS=(PROTOCOL = TCP)
(HOST=stby-scan)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = ssoa)
    )
  )

psoa_local_listener =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS=(PROTOCOL = TCP)
(HOST=prmy1-vip)(PORT = 1521))
    )
  )

```

**Example 4-5 Sample tnsnames.ora File on Standby Node 1 (SOADC2.DBHOST1)**

```

psoa =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS=(PROTOCOL= TCP)(HOST=prmy-scan)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = psoa)
    )
  )

ssoa =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS=(PROTOCOL = TCP)
(HOST=stby-scan)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = ssoa)
    )
  )

ssoa_local_listener =
  (DESCRIPTION =
    (ADDRESS_LIST =

```

```

        (ADDRESS=(PROTOCOL = TCP)
(HOST=stby1-vip)(PORT = 1521))
    )
)

```

#### **Example 4-6 Duplicating Data Between Two Systems with Different Disk-Group Names**

```

rman <<EOF
connect target sys/password;
connect auxiliary sys/password@dup;
run {
allocate channel prmy1 type disk;
allocate channel prmy2 type disk;
allocate channel prmy3 type disk;
allocate channel prmy4 type disk;
allocate auxiliary channel stby type disk;
duplicate target database for standby from active database
spfile
parameter_value_convert '+DATA_prmy','+DATA_stby','+RECO_prmy','+RECO_stby'
set db_file_name_convert '+DATA_prmy','+DATA_stby'
set db_unique_name='ssoa'
set db_create_online_log_dest_1='+DATA_stby'
set db_create_file_dest='+DATA_stby'
set db_recovery_file_dest='+RECO_stby'
set log_file_name_convert '+DATA_prmy','+DATA_stby','+RECO_prmy','+RECO_stby'
set control_files='+DATA_stby/ssoa/standby.ctl'
set local_listener='ssoa_local_listener'
set remote_listener='stby-scan:1521';
} EOF

```

#### **Example 4-7 Duplicating Data Between Two Systems with Same Disk-Group Name +DATA**

```

rman <<EOF
connect target sys/password;
connect auxiliary sys/password@dup;
run {
allocate channel prmy1 type disk;
allocate channel prmy2 type disk;
allocate channel prmy3 type disk;
allocate channel prmy4 type disk;
allocate auxiliary channel stby type disk;

duplicate target database for standby from active database
spfile
set db_unique_name='ssoa'
set control_files='+DATA/ssoa/standby.ctl'
set local_listener='ssoa_local_listener'
set remote_listener='stby-scan:1521';
}
EOF

```

#### **Example 4-8 Sample Redo Log**

```

SQL> alter database add standby logfile thread 1
group 9 size 500M,
group 10 size 500M,
group 11 size 500M;

```

```

SQL> alter database add standby logfile thread 2
group 12 size 500M,

```































































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 Oracle Fusion Middleware 12c 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.

---

---



If you encounter problems with an Oracle Fusion Middleware component used in a Disaster Recovery topology, see Troubleshooting 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 documents and you encounter a problem, see Troubleshooting in the respective document:

- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle SOA Suite*
- *Oracle Fusion Middleware Enterprise Deployment Guide for OBI*

### 5.1.3 Resolving Issues with Components Deployed on Shared Storage

Troubleshoot issues with components deployed on share storage.

Some problems that arise with a component in a 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 documents mentioned in [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?

Find solutions on My Oracle Support.

You can find more solutions on My Oracle Support at

<http://support.oracle.com>

If you do not find a solution for your problem, then 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>



```
regedit /I C:\oracleregistry.reg
```

Alternatively, you can use the Registry Editor to import the key. See Registry Editor Help.